Software Version 5.3
August 2014
702P03158

Embedded for Xerox EPA-EIP
Setup Guide

Document Version: 1.0 (August 2014)

Table of Contents

1 Introduction

Topics

This Setup and Administration Guide provides instructions for installing and configuring the Xerox Secure Access application within an Xerox Secure Access environment.

This chapter includes:

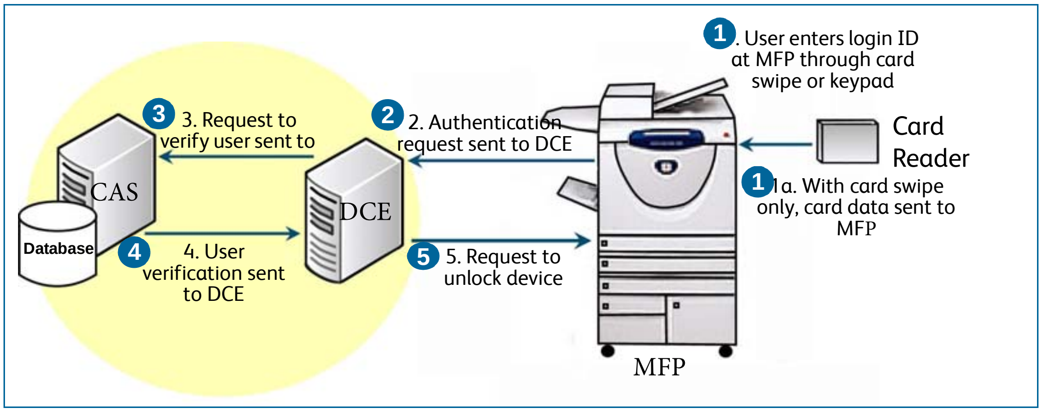
- An overview of the Xerox Secure Access user authentication process
- An overview of the secure document release process
- A list of supported Xerox MFP devices and card readers
- Installation and configuration prerequisites
- A list of unique terms and related documents

About User Authentication

Xerox Secure Access controls access to the print, copy and fax functions of Xerox multi-function product (MFP) devices by requiring users to enter login credentials, either by using a card or manually entering data on the MFP front panel. This login action initiates an access request.

The Device Control Engine (DCE) handles all communication with the MFP devices. Using the Authentication Agent API, the MFP forwards the login request to the DCE, which then contacts the Core Accounting Server (CAS) to verify the user account data associated with the login ID.

The MFP can be configured to lock all or individual services requiring authentication before use. If the CAS 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.

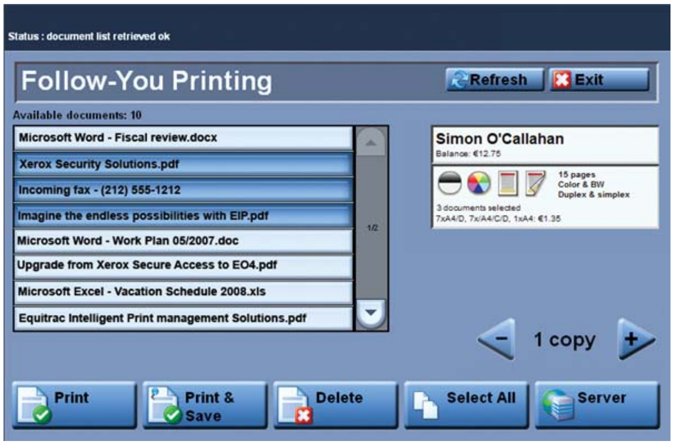

1. User enters login ID at MFP through card swipe or keypad
Card Reader
1a. With card swipe only, card data sent to MFP
2. Authentication request sent to DCE
3. Request to verify user sent to
CAS
Database
DCE
4. User verification sent to DCE
5. Request to unlock device
MFP

Note

Legacy model Xerox MFPs may require an authentication device to make use of serial cards. In this case, the appropriate authentication device is an additional hardware component that attaches to the card reader and forwards authorization requests to the DCE.

About Secure Document Release

If you configure the Core Accounting Server (CAS) to support secure document release, the MFP screen panel can include a Follow-You Printing screen. This screen displays queued print jobs for the current user, who can then select one or more jobs, and release or delete them directly from the MFP.



Status : document list retrieved ok

Follow-You Printing

Available documents: 10

- Microsoft Word - Fiscal review.docx
- Xerox Security Solutions.pdf
- Incoming fax - (212) 555-1212
- Imagine the endless possibilities with EIP.pdf
- Microsoft Word - Work Plan 05/2007.doc
- Upgrade from Xerox Secure Access to EO4.pdf
- Microsoft Excel - Vacation Schedule 2008.xls
- Equitrac Intelligent Print management Solutions.pdf

Simon O'Callahan
Balance: €12.75

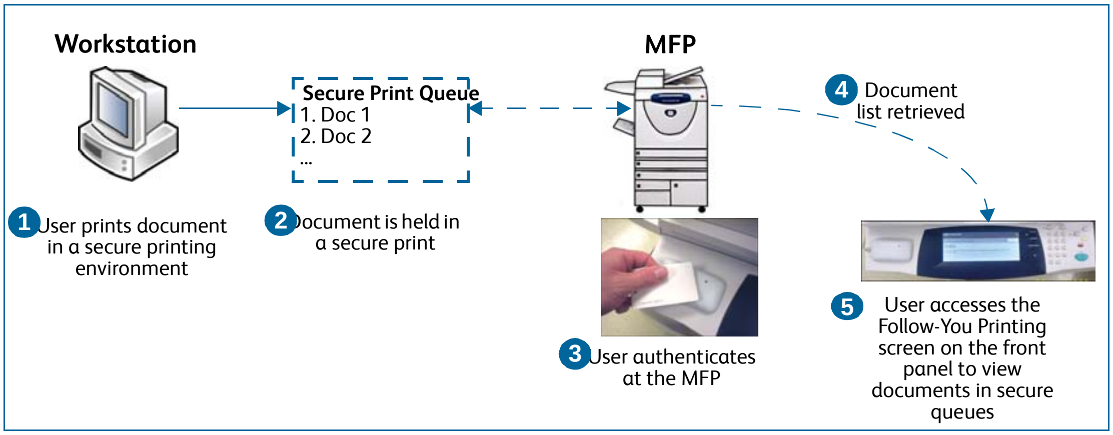
15 pages
Color & BW
Duplex & simplex

3 documents selected
7xA4/D, 7x/A4/C/D, 1xA4: €1.35

1 copy

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® , see the Advanced Printing Configuration chapter in the *Xerox Secure Access Administration Guide*.

The illustration below shows the process flow that occurs after a user submits a print job to a controlled queue. After sending the print job, the user can access the Follow-You Printing screen on the device panel and use the Embedded secure document release functions.



Workstation
MFP
Secure Print Queue
1. Doc 1
2. Doc 2
...
1 User prints document in a secure printing environment
2 Document is held in a secure print
3 User authenticates at the MFP
4 Document list retrieved
5 User accesses the Follow-You Printing screen on the front panel to view documents in secure queues

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. Immediately after the user authenticates, all jobs are released from the local or home server.

Supported MFPs

For a list of Xerox Secure Access supported MFP models, visit
http://www.nuance.com/for-business/by-product/equitrac/supported-devices/xerox/index.htm.

Supported MFP models must be EIP-enabled prior to installing the Xerox Secure Access solution. Please contact your local Xerox Sales Representative for more information.

Supported Card Readers

For a list of Xerox Secure Access supported card readers, visit
http://www.equitrac.com/card_readers.html.

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

To setup the card reader on the MFP, see Configuring Follow-You Printing® on page 14.

Magstripe Device Reader

Xerox Secure Access 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

Xerox Secure Access 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.

System Requirements

To review the system requirements for the machine or machines hosting the Core Accounting Server and Device Control Engine server components, see the *Xerox Secure Access Unified ID System® Installation Guide*.

Installation and Configuration Requirements

If you have already set up and configured your Xerox Secure Access server, you do not need to install the basic Xerox Secure Access application; you only need to follow configuration procedures.

For instructions on installing and configuring Xerox Secure Access, see the *Xerox Secure Access Unified ID System® Installation Guide* and the *Xerox Secure Access Administration Guide.*

Before configuring Xerox Secure Access, 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 System Manager. For details, see "Configuring Administrative Access" in the *Xerox Secure Access Administration Guide*.

Licensing, Server, and MFP Requirements

To enable the Embedded application, you must have the following:

1. **Xerox Secure Access Software**

Xerox Secure Access requires configuration of the Core Accounting Server and the MFPs, as described in this guide.

2. **One embedded license per MFP**

Each MFP requires an embedded license that is applied in System Manager. For example, if you plan to control 20 Xerox MFPs, you need to obtain 20 corresponding embedded licenses (enabled for Xerox). See Licensing Embedded Devices on page 2 for instructions to add licenses to CAS.

3. **Supported Xerox MFPs**

For a list of supported MFP models, see Supported MFPs on page 4.

List of Terms

The following unique terms are used within this guide.

Term	Description
Alternate Primary PIN	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.
Authentication	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.
Core Accounting Server (CAS)	The Core Accounting Server is a core component of Xerox Secure Access. This service controls the accounting database that stores all printer, user, transaction and balance information. The CAS also verifies users, calculates printing charges and assigns charges to an appropriate user.
Device Control Engine (DCE)	A core component of Xerox Secure Access, the DCE communicates with terminals that control access to MFPs.
Device Routing Engine (DRE)	A core component of Xerox Secure Access, 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.
Follow-You printing	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.
Follow-You Printing screen	An additional screens that appears as a custom service on the the MFP when the Follow-You Printing extension is configured. Users can select one or more jobs from different print servers.
Multi-server Follow-You Printing	A secure printing feature that extends the Follow-You functionality to allow users to view and release secure print jobs from different print servers.
Network Accounting	A feature of the Xerox MFP which automatically tracks print, server fax and copy usage for each user. Network accounting is run over a network and the accounting transactions are performed remotely by Xerox Secure Access server software.
Print Tracking	The ability to track the attributes of a released network print job. For example, number of pages, page size, color, etc. You can configure Xerox Secure Access to track printing through the embedded device or through an Equitrac Port.
Primary PIN	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.
Secondary PIN	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.

Term	Description
Secure Document Release (SDR)	An Xerox Secure Access 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.

Additional Documentation

It may be necessary to refer to one of the following documents when performing some server-side configuration tasks. These documents are located on the Xerox Secure Access product CD's, and are installed automatically with any server-side component in the Program Files\Xerox Secure Access\Xerox Secure Access\Documentation folder.

Guide	When to refer to this guide
Xerox Secure Access Installation Guide	Use this guide to perform an initial installation or upgrade.
Xerox Secure Access Administration Guide	After installing Xerox Secure Access, use this guide to configure advanced options for use on your campus or in your organization.

2

MFP and Server-Side Configuration

Topics

To enable Xerox Secure Access, you must configure the MFPs and the Core Accounting Server (CAS). This chapter includes instructions for configuring your MFP devices and the Xerox Secure Access server for Xerox Secure Access.

Licensing Embedded Devices

The Xerox Secure Access system utilizes a 6 tier licensing structure which allows licenses to be assigned on a per device basis. The license tiers are as follows:

Authentication – Any time the user approaches a device and authenticates themselves, they are using an Authentication license. This could be for a PageCounter, ID Controller, Web Release or Embedded device. Desktop Printing is not considered authentication.

- Licenses are assigned per device where authentication is required.
- Does not require a prerequisite.

Follow-You Printing® – Allows the user the ability to release a job from a device with this license assigned to it. Includes Web Release, PageCounter, Embedded and ID Controller.

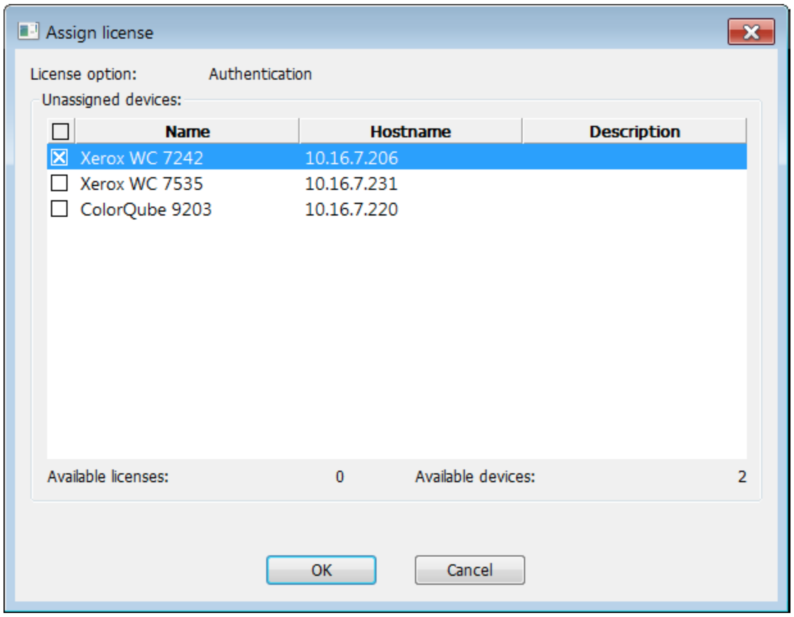
- License are assigned per device where Follow-You Printing is required.
- Requires an Authentication license as a prerequisite.

Assigning Licenses to Devices

Licenses must be assigned to each printer that will use that particular feature.

To assign a license, do the following:

1. Open **System Manager**, and select **Licensing** in the left pane.
2. Select the **Assignment View tab to open the** list of all assigned licenses.
3. Expand or right-click the desired license option, and select **Add** to open the **Assign license** dialog box.



License option: Authentication

Unassigned devices:

☐	Name	Hostname	Description
☒	Xerox WC 7242	10.16.7.206	
☐	Xerox WC 7535	10.16.7.231	
☐	ColorQube 9203	10.16.7.220	

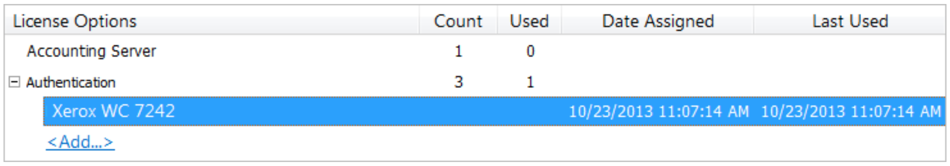
Available licenses: 0 Available devices: 2

4. On the **Assign license** dialog box, select the checkbox for the device(s) to assign the license to.

   At the bottom of the dialog box is a counter displaying the number of available licenses and available devices. These numbers decrease with every license assigned.

5. Click **OK** after the licenses have been assigned to the desired devices.

The devices assigned to the license now display under the selected license option.



License Options	Count	Used	Date Assigned	Last Used
Accounting Server	1	0		
⊟ Authentication	3	1		
Xerox WC 7242			10/23/2013 11:07:14 AM	10/23/2013 11:07:14 AM
<Add...>				

To remove an assigned license from a device, right-click the device and select **Remove assignment**. The number of used licenses will be adjusted accordingly.

Configuring Printer Ports

Controlled Xerox MFPs must use an Equitrac® Port (rather than standard TCP/IP ports) to enable secure printing. If you are configuring a secure print environment, ensure that your devices comply with this requirement.

You can create Equitrac printer ports directly for new devices, or convert existing devices from standard TCP/IP ports into Equitrac ports. For new devices, see Add a Printer on an Equitrac Printer Port (below). Alternatively, new devices can be created using standard TCP/IP ports and then converted it to an Equitrac ports. For existing devices, see Convert an Existing TCP/IP Port to Equitrac Port on page 6. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports to determine if reported errors within the print environment are due to the Xerox Secure Access server or the normal print environment.

Add a Printer on an Equitrac Printer Port

To create Equitrac printer ports for new devices, do the following:

1. Using the standard Windows interface, open the **Add Printer** wizard.
2. Follow the prompts to **add a local printer** and create a new port.
3. Select **Equitrac Port** as the type of port you want to create and click **Next**.
4. The Add Equitrac Printer Port wizard displays and you are prompted to ensure that the printer device is turned on, connected to the network, and properly configured. Click **Next** to continue.
5. Click **Next** and select **Physical printer** as your **Device Type** from the drop-down list.
6. Specify a **Printer name** or **IP Address**. The wizard supplies a Port name prefaced with ″**EQ_** ″based on the printer name or IP address. If another naming convention is preferred, rename the port accordingly.
7. Click **Next** to continue with the port configuration options. The Port Configuration screen displays. The **Detected device information** displays automatically if the wizard is able to collect this data from the printer.
8. Select the **Use custom settings** option:
   - If you select **Raw port** communication, identify the TCP **Port** number, and specify if the port monitor should hold the connection open.
   - If you select **LPR**, specify the name of the print **Queue** on the physical device (e.g. PORT1).
   - If you select **Specific device**, select the appropriate **Manufacturer** and **Model** from the drop-down lists. The device uses the relevant default communications parameters based on these selections.
9. Click **Next** and specify the **Physical device name**. This is the name of the device that is displayed within System Manager.
10. Review the details for this new port and device registration, and click **Finish** to close the Add Equitrac Printer Port wizard, or **Back** to change any of the settings.
11. Specify the Manufacture and model to install the printer driver, and click **Next**.

    Note

    If the device is part of a pull group, it must use the same drivers as all other devices in the pull group. You must select the model of the pull group driver, not the model of the device. If the DRE is a 64-bit server you must also load the 32-bit driver to the server.

12. Specify the version of the print driver to use, and click **Next**.
13. Enter the **Printer name**, and click **Next**. This is the name of the device that is displayed in System Manager.

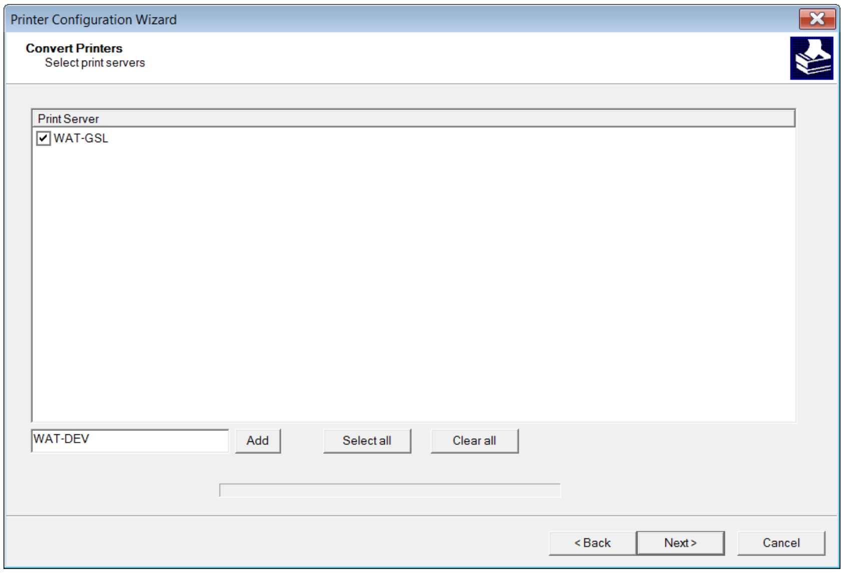
14. Select to share or not to share the printer with others, and click **Next**. If sharing the printer, enter a Share name, and optionally provide a printer location and any comments.
15. Click the **Print a test page** button, and click **Finish** to close the Add Printer wizard.
16. Confirm that the test page printed successfully.
17. Verify that the physical device and its printer port and print queue appear in **System Manager > Devices**.

Convert an Existing TCP/IP Port to Equitrac Port

Use the Printer Configuration Wizard to convert from a TCP/IP port to Equitrac ports. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports if desired.

To convert from TCP/IP printer ports to Equitrac ports, do the following:

1. Select **Start > All Programs > Xerox Secure Access > Printer Configuration Wizard**.
2. Click **Next** on the Welcome screen to continue with the conversion.
3. Select **Convert printers to use Equitrac Ports**, and click **Next**. Optional – Uncheck **Auto-discover model** if the printers are off-line or have SNMP disabled. If selected, the wizard sends an SNMP request to each device, and then times-out on each failed connection attempt, greatly increasing the time to run the conversion.
4. Select the desired print server(s) from the list, and click **Next**. Optionally, enter the name of other print servers in the Add field, and click the **Add** button to place them in the **PrintServer** list. Print servers can only be added one at a time.



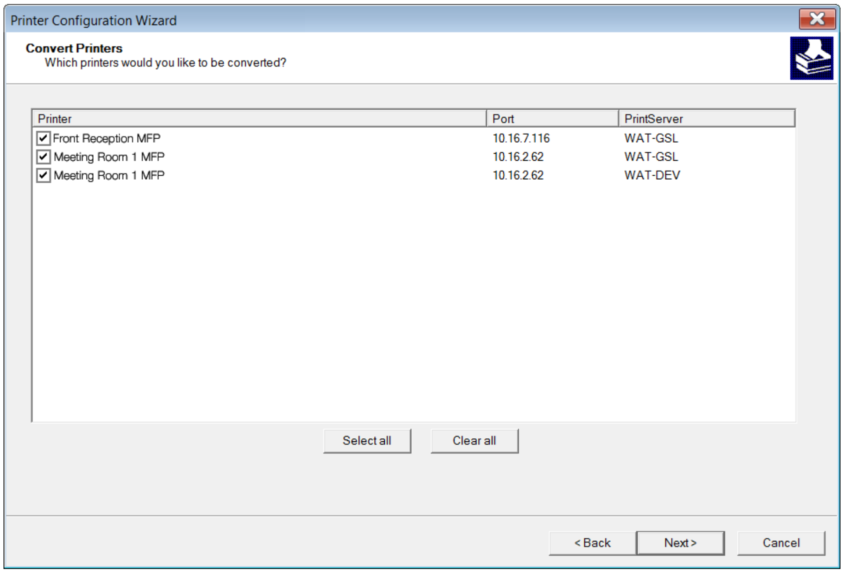
Printer Configuration Wizard

Convert Printers
Select print servers

Print Server
☑ WAT-GSL

WAT-DEV

5. Select the printer(s) to be converted, and click **Next**. If a printer exists on more than one print server, it displays multiple times in the **Printer** list along with the name of its associated server in the **PrintServer** list.



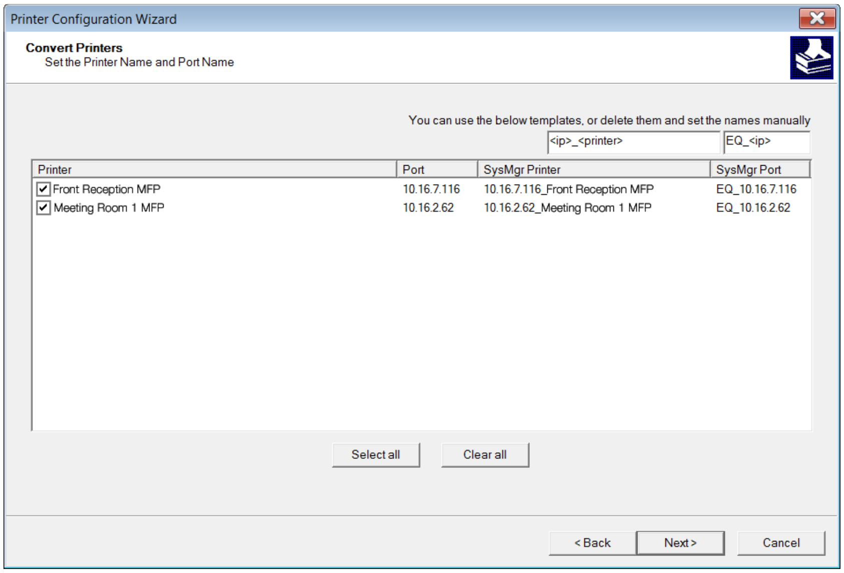
Printer Configuration Wizard

Convert Printers

Which printers would you like to be converted?

Printer	Port	PrintServer
☑ Front Reception MFP	10.16.7.116	WAT-GSL
☑ Meeting Room 1 MFP	10.16.2.62	WAT-GSL
☑ Meeting Room 1 MFP	10.16.2.62	WAT-DEV

6. Set the **Printer Name** and **Port Name** as they will display in the System Manager Devices view. You can use the default naming templates for the printer "**<ip>_<printer>** "and port '**EQ_<ip>"**, or change the names as desired. For example, you can change the printer default from "**<ip>_<printer>** "to '**2nd floor <printer>"** to associate the selected printer(s) with the 2nd floor in your environment, or you can remove "**<printer>**" from the name to only display the printer's IP address in System Manager.



Printer Configuration Wizard

Convert Printers

Set the Printer Name and Port Name

You can use the below templates, or delete them and set the names manually

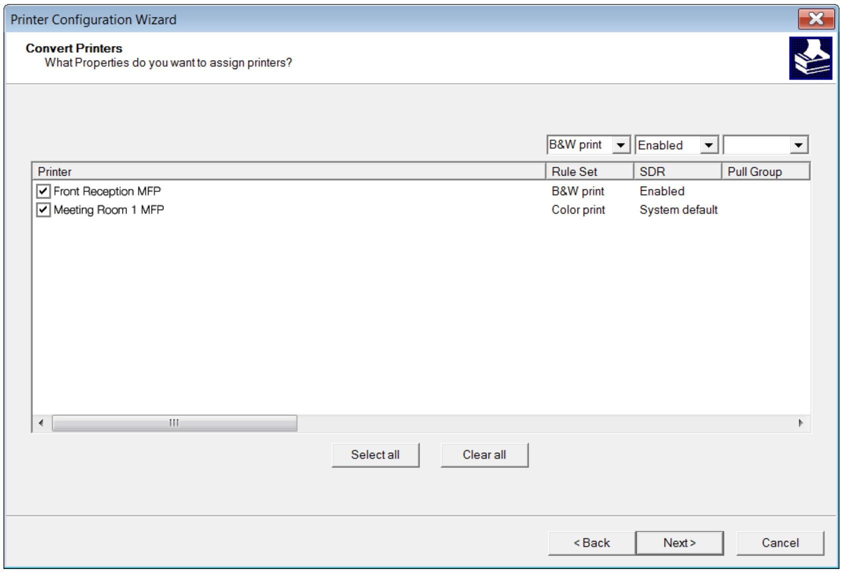
<ip>_<printer> EQ_<ip>

Printer	Port	SysMgr Printer	SysMgr Port
☑ Front Reception MFP	10.16.7.116	10.16.7.116_Front Reception MFP	EQ_10.16.7.116
☑ Meeting Room 1 MFP	10.16.2.62	10.16.2.62_Meeting Room 1 MFP	EQ_10.16.2.62

Note

The printer and port names can be changed individually or as a group. If multiple printers are selected, the naming convention affects the entire selection.

7. On the **Properties** page, select the properties you want to assign to the printers from the Rule Set, SDR and Pull Group drop-down lists. The properties can be applied to single or grouped printers.

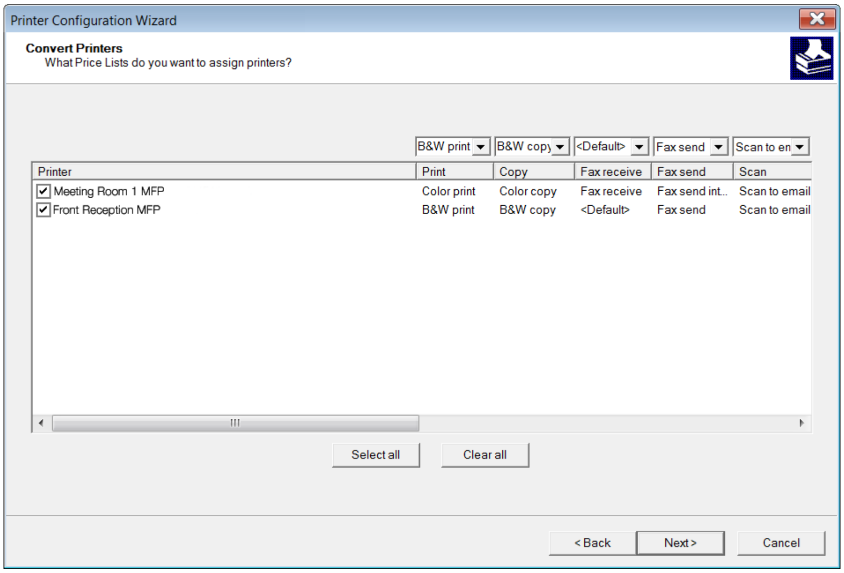


Convert Printers
What Properties do you want to assign printers?

B&W print ▾ | Enabled ▾ | ▾

Printer	Rule Set	SDR	Pull Group
☑ Front Reception MFP	B&W print	Enabled	
☑ Meeting Room 1 MFP	Color print	System default	

8. On the **Price Lists** page, select the price list. you want to assign from the Print, Copy, Fax receive, and Fax send drop-down lists. The price lists can be applied to single or grouped printers.



Convert Printers
What Price Lists do you want to assign printers?

B&W print ▾ | B&W copy ▾ | <Default> ▾ | Fax send ▾ | Scan to en ▾

Printer	Print	Copy	Fax receive	Fax send	Scan
☑ Meeting Room 1 MFP	Color print	Color copy	Fax receive	Fax send int...	Scan to email
☑ Front Reception MFP	B&W print	B&W copy	<Default>	Fax send	Scan to email

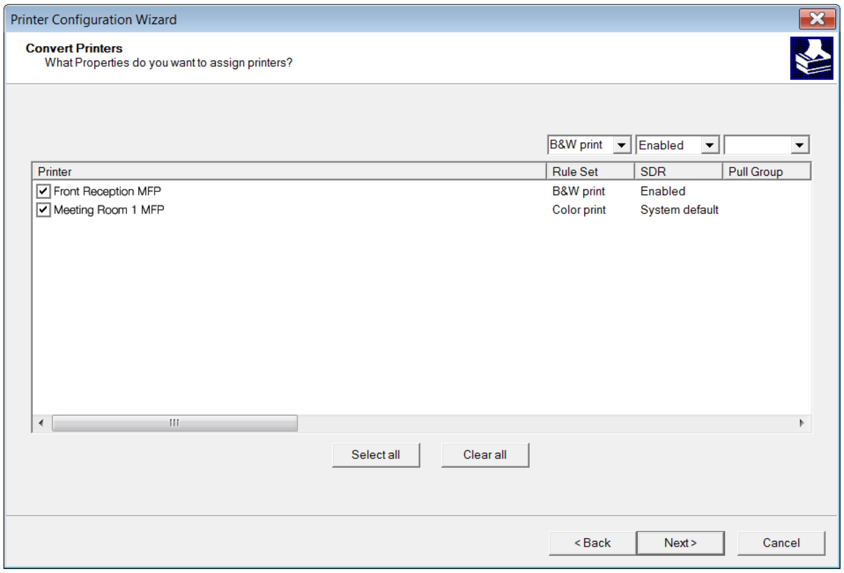
9. Click **Finish** to complete the conversion process. Alternatively, you can select the **Return to Start** checkbox and click **Next** to return to the Wizard's main page without completing the conversion.
10. Open the Printers and Faxes window, and print a test page for EACH converted printer.
11. Confirm that the test page printed successfully.
12. Verify that the physical device and its printer port and print queue display in **System Manager > Devices**.

Configuring Physical Devices with the Configuration Wizard

Use the Printer Configuration Wizard to reconfigure existing Xerox Secure Access printers. The wizard allows for properties such as price lists, rule sets, pull groups and SDR to be set across multiple devices simultaneously.

To configure existing Xerox Secure Access printers, do the following:

1. Select **Start > All Programs > Xerox Secure Access > Printer Configuration Wizard**.
2. Click **Next** on the Welcome screen to continue with the conversion.
3. Select **Configure Xerox Secure Access Printers**, and click **Next**. Optional – Uncheck **Auto-discover model** if the printers are off-line or have SNMP disabled. If selected, the wizard sends an SNMP request to each device, and then times-out on each failed connection attempt, greatly increasing the time to run the configuration.
4. On the **Properties** page, select the properties you want to assign to the printers from the Rule Set, SDR and Pull Group drop-down lists. The properties can be applied to single or grouped printers.



Printer Configuration Wizard

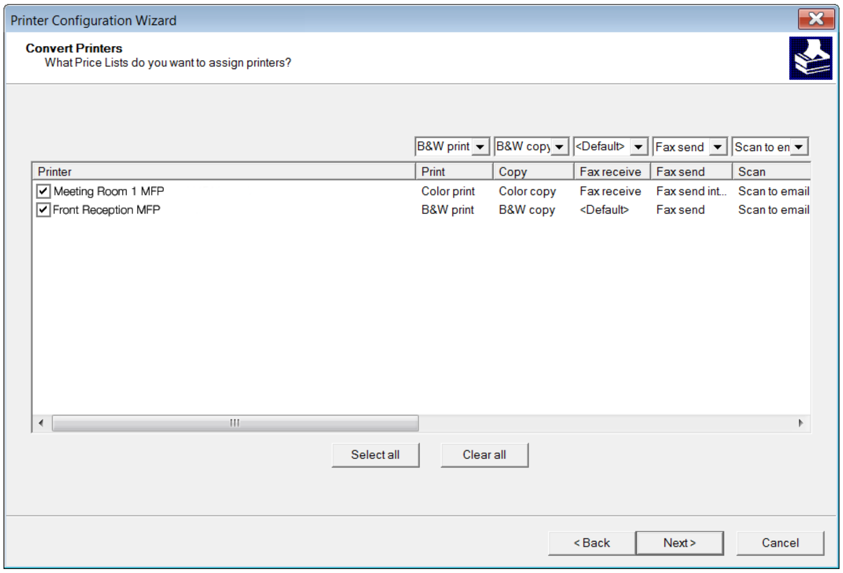
Convert Printers

What Properties do you want to assign printers?

Rule Set: B&W print · SDR: Enabled · Pull Group: (blank)

Printer	Rule Set	SDR	Pull Group
☑ Front Reception MFP	B&W print	Enabled	
☑ Meeting Room 1 MFP	Color print	System default	

5. On the **Price Lists** page, select the price list. you want to assign from the Print, Copy, Fax receive, and Fax send drop-down lists. The price lists can be applied to single or grouped printers.



Printer Configuration Wizard

Convert Printers

What Price Lists do you want to assign printers?

B&W print ▾ B&W copy ▾ <Default> ▾ Fax send ▾ Scan to en ▾

Printer	Print	Copy	Fax receive	Fax send	Scan
☑ Meeting Room 1 MFP	Color print	Color copy	Fax receive	Fax send int...	Scan to email
☑ Front Reception MFP	B&W print	B&W copy	<Default>	Fax send	Scan to email

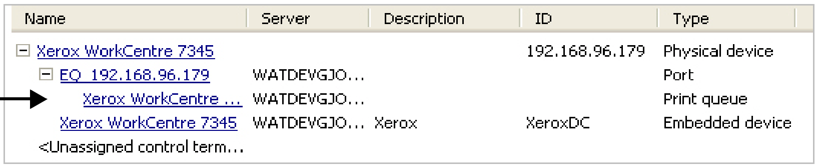
6. Click Finish to complete the configuration process.

Enabling Secure Printing on the Queue

If you are configuring a secure print environment, the queue must be configured to hold print jobs.

1. Open **System Manager** and select **Devices from the left pane.**
2. Click on the Print queue you want to configure. You may need to expand the Physical device to see the print queue.

Right-click on the print queue name to enable secure printing

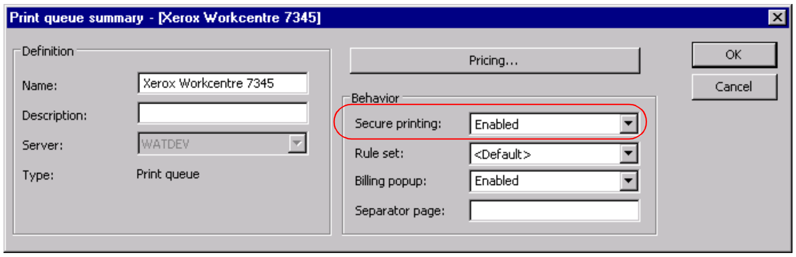


Name	Server	Description	ID	Type
⊟ Xerox WorkCentre 7345			192.168.96.179	Physical device
⊟ EQ 192.168.96.179	WATDEVGJO...			Port
Xerox WorkCentre ...	WATDEVGJO...			Print queue
Xerox WorkCentre 7345	WATDEVGJO...	Xerox	XeroxDC	Embedded device
<Unassigned control term...				

Note

The print queue is created automatically the first time a user prints to the controlled device, including when you print a test page upon configuration. If a print queue does not appear beneath the Physical Device, send a print job to the MFP, then wait 30 seconds and refresh System Manager.

3. In the Print Queue Summary dialog, set the Secure printing option to **Enabled** from the Behavior section, and click **OK**.



Print queue summary - [Xerox Workcentre 7345]

Definition

Name: Xerox Workcentre 7345

Description:

Server: WATDEV

Type: Print queue

Behavior

Secure printing: Enabled

Rule set: <Default>

Billing popup: Enabled

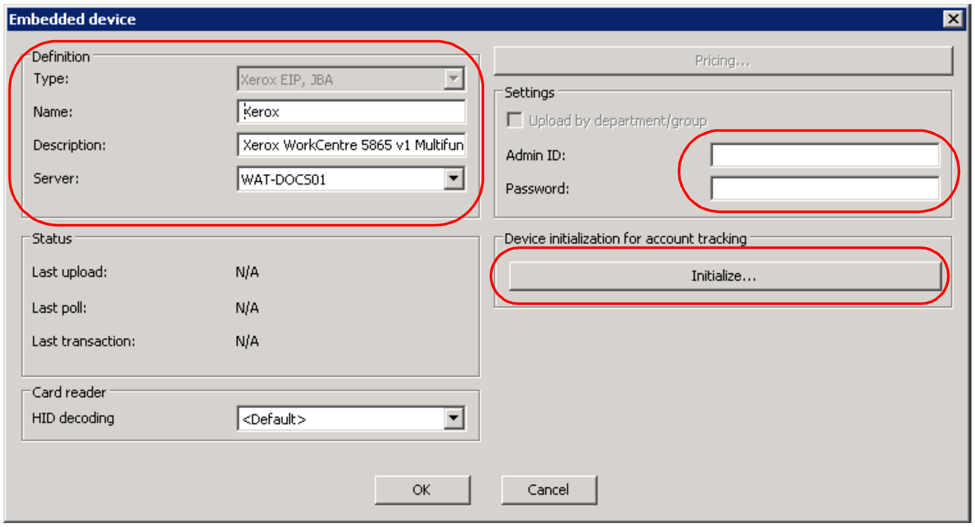
Separator page:

Creating Embedded Devices

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

Use System Manager to create an embedded interface for each Xerox MFP that is controlled by Xerox Secure Access.

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



Embedded device

Definition
Type: Xerox EIP, JBA
Name: Xerox
Description: Xerox WorkCentre 5865 v1 Multifun
Server: WAT-DOCS01

Status
Last upload: N/A
Last poll: N/A
Last transaction: N/A

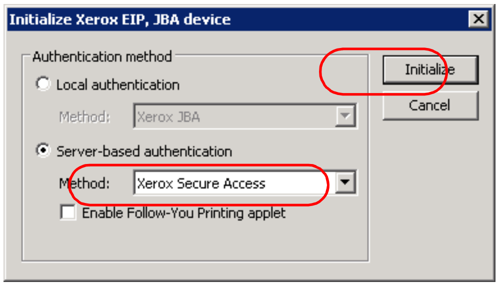
Card reader
HID decoding <Default>

Settings
□ Upload by department/group
Admin ID:
Password:

Device initialization for account tracking

3. Enter a **Name** and **Description** for the embedded device.
4. Specify the **Server** hosting the DCE associated with this physical and embedded 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 *Xerox Secure Access Administration Guide*.
7. **Pricing** is unavailable.
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.



Initialize Xerox EIP, JBA device

Authentication method
○ Local authentication
Method: Xerox JBA
● Server-based authentication
Method: Xerox Secure Access
□ Enable Follow-You Printing applet

10. Select the authentication method:
    - Select the **Local authentication** radio button, then select **Xerox JBA** or **Xerox Native SmartCard** from the drop-down menu to suit your installation.

      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.

    - In the Initialize dialog box, select the **Server-based authentication** option, and choose a method from the drop-down list.

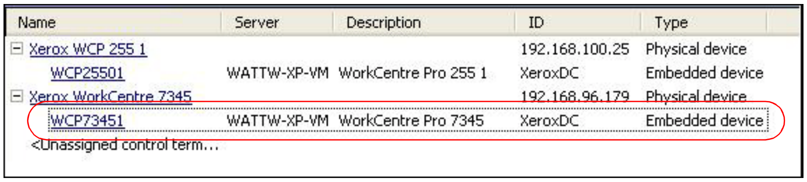
      Xerox Secure Access – to track printing through Xerox Network Accounting.

      Xerox off-box JBA – to validate prior to processing print activity.
11. Select the **Enable Follow-You Printing applet** checkbox to enable Follow-You Printing on the device.
12. Click the **Initialize** button to apply the communication settings between the device and server.

    Note

    Pressing Initialize changes the configuration on the device itself and requires the MFP to reboot itself. Ensure that the MFP is not in use before you press Initialize.

13. Click **OK** in the Embedded device dialog to save the settings. The new embedded device appears in the Devices list beneath the physical device name it is associated with.



Name	Server	Description	ID	Type
⊟ Xerox WCP 255 1			192.168.100.25	Physical device
WCP25501	WATTW-XP-VM	WorkCentre Pro 255 1	XeroxDC	Embedded device
⊟ Xerox WorkCentre 7345			192.168.96.179	Physical device
WCP73451	WATTW-XP-VM	WorkCentre Pro 7345	XeroxDC	Embedded device
<Unassigned control term...				

14. Repeat these steps to create an embedded device for 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 Printer Ports on page 4 and confirm that the MFP is properly configured.

After Initialization, log into an MFP configuration page as the Administrator to verify that the Admin ID and Password entered in System Manager are configured properly. See Configuring the MFP Through a Web Interface on page 19 for login details.

When login is successful, a web page opens displaying the Xerox MFP model name and its settings.

Configuring Follow-You Printing®

Follow-You Printing extends the basic functionality of secure printing by allowing a user to release a print job to other compatible devices in the organization. Even if you deployed multiple DRE print servers—each of which manages a separate set of devices—you can configure Xerox Secure Access to allow printing across multiple print servers.

For example, a user who works in two different buildings can submit a print job from their computer in Building A, and while on the way to a meeting in Building B, they can walk up to any MFP (with the embedded application installed on it) and pull the job to a compatible printer nearest them.

If you want to deploy the Embedded application in a single-server or a multi-server Follow-You Printing environment, do the following:

1. Enable secure printing on each MFP.

   Secure printing sets up a virtual print queue that holds jobs until they are released at the embedded device by a valid user.

2. Create and manage Pull groups.

   To allow users to release print jobs through the Embedded application, you must create Pull groups, then add each physical device hosting the embedded application to a Pull group.

3. Configure the Follow-You print settings.

   Determine the site where you want Follow-You Printing to be accessible from, and choose whether the print job is priced based on its properties before or after it is released.

4. Enable multi-server Follow-You to allow users to direct jobs across multiple servers. (optional)

   This option enables users to retrieve Follow-You print jobs on a device connected to a different CAS and DCE/DRE server.

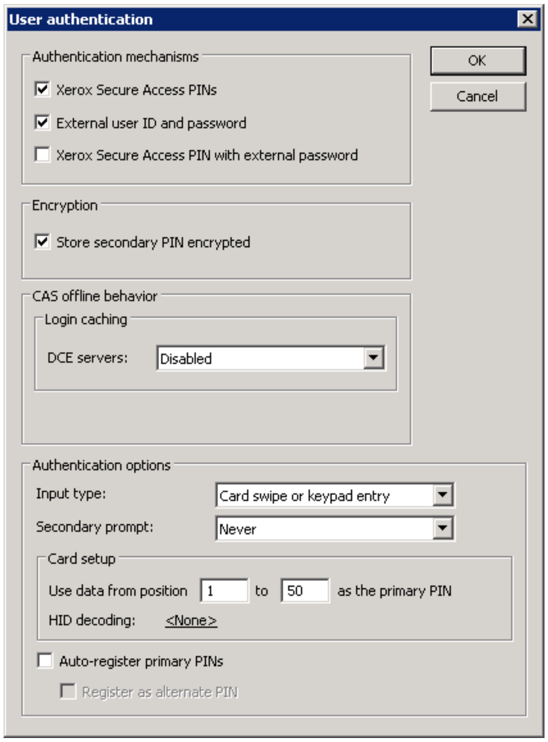
   Note

   See the Advanced Printing Configuration chapter in the *Xerox Secure Access Administration Guide* for details on configuring secure printing, Follow-You Printing, and device pull groups.

Configuring Authentication Prompts

The user authentication prompts that appear on the MFP login screen are configured in System Manager.

1. Open **System Manager** and navigate to **Configuration > User authentication**.



User authentication

Authentication mechanisms

☑ Xerox Secure Access PINs

☑ External user ID and password

□ Xerox Secure Access PIN with external password

Encryption

☑ Store secondary PIN encrypted

CAS offline behavior

Login caching

DCE servers: Disabled

Authentication options

Input type: Card swipe or keypad entry

Secondary prompt: Never

Card setup

Use data from position 1 to 50 as the primary PIN

HID decoding: <None>

□ Auto-register primary PINs

□ Register as alternate PIN

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 **Prompt from secondary PIN** 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 Prompt for secondary PIN option, then you must re-initialize the device in order to enable the new selection.
4. In the **Card setup** section, enter the data start and stop position in the **Use data from position** fields.

5. Select the **Auto-register primary PINs** checkbox if you want users to self-register their swipe cards. Optionally, you can select **Register as alternate PIN** to record the PIN as the Alternate PIN instead of the Primary PIN. See Configuring Card Self-Registration on page 16 for details.
6. Click **OK** to save the changes.

For more details on configuring user authentication options refer to Accounts System Configuration in the *Xerox Secure Access Administration Guide*.

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**:
   - **Xerox MPS PINs** – Select to connect an **Xerox Secure Access print** account with login information.
   - **External user ID and password** – Select to verify all user information outside of **Xerox Secure Access.**
   - **Xerox MPS PIN with external password** – Select if users swipe their cards for identification, and must also enter their domain user account password. **Xerox Secure Access** cross-checks the database for the corresponding Xerox Secure Access 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 > External authentication and** select an **External authority** – Windows or LDAP.

   Refer to External User Authentication in the *Xerox Secure Access 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.

Note

Self-registration must be enabled through both System Manager and Xerox Authentication Configuration.

After auto-registration has been configured in System Manager, proceed to Configuring Smart Card Through Xerox Authentication on page 24 to enable the user to self-register a card at the MFP.

Configuring the MFP for Card Reader Support

Warning

You must complete the instructions in Configuring Printer Ports on page 4 before you configure the MFP for card readers. If you configure the card readers first, accessory error 121-333 appears on the device panel and it is not be possible to bring the device into a state where the error can be acknowledged.

To enable a card reader to work properly on your Xerox device:

1. Use the device's System Administration access to set the NVM Read/Write setting **850-007** to a value of **10**.
2. Connect the card reader to the device.
3. Restart the device.

The device automatically sets the NVM Read/Write setting **850-001** to a value of **1**.

To disable a card reader:

1. Set the NVM Read/Write settings **850-007** and **850-001** to a value of **0**.
2. Remove the card reader.
3. Restart the device.

Warning

If the card reader is removed without resetting the NVM Read/Write values, Fault Code (Error 121-333) appears on the device panel. To correct the error, do one of the following:

- Install the card reader again and restart the device.
- Disable the card reader by resetting NVM Read/Write 850-007 and 850-001 to "0." Then restart the device.

Caution

After a restart you may be required to acknowledge the previous error before the machine boots completely.

Note

When an EPA card reader is attached to the MFP, the copy functionality is not available until authentication has been performed. This occurs even if you have configured the copy service as unlocked.

Registering the EIP Applet

You must run this applet for each Xerox MFP on which you wish to register the EIP. This applet enables the DCE service to communicate with the MFP and installs the Release My Documents screen on the MFP.

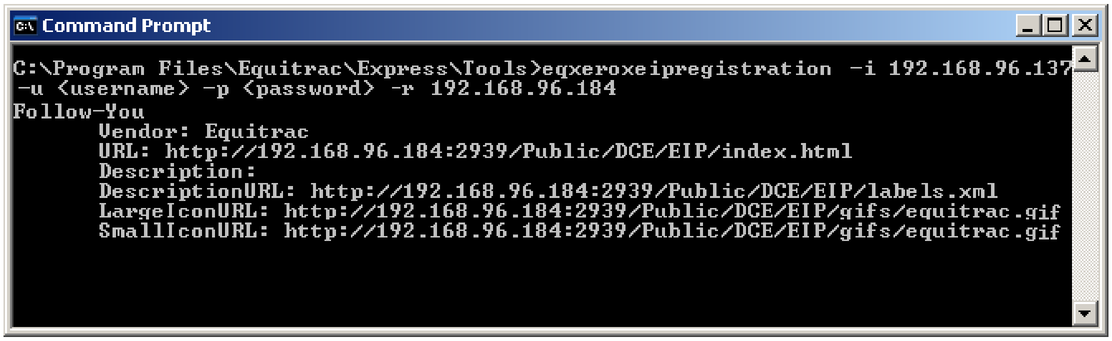
1. Open a command prompt, then change the directory to c:\Program files\Xerox\Xerox Secure Access\Tools.
2. Run the file **eqxeroxeipregistration.exe** with the following parameters

Parameter	Description
-i	IP address of the Xerox device
-u	Xerox device Admin ID
-p	Xerox device Admin password
-r	IP address of the DCE server
-v	Registration view

Note

You must add a space between the parameter and the text. For example,
-i 192.168.111.96

You can verify the registration file by typing "-v" at the end of the DCE IP address parameter to view the registration information. For example:



```
C:\Program Files\Equitrac\Express\Tools>eqxeroxeipregistration -i 192.168.96.137
 -u <username> -p <password> -r 192.168.96.184
Follow-You
        Vendor: Equitrac
        URL: http://192.168.96.184:2939/Public/DCE/EIP/index.html
        Description:
        DescriptionURL: http://192.168.96.184:2939/Public/DCE/EIP/labels.xml
        LargeIconURL: http://192.168.96.184:2939/Public/DCE/EIP/gifs/equitrac.gif
        SmallIconURL: http://192.168.96.184:2939/Public/DCE/EIP/gifs/equitrac.gif
```

3. Close the command prompt.

Note

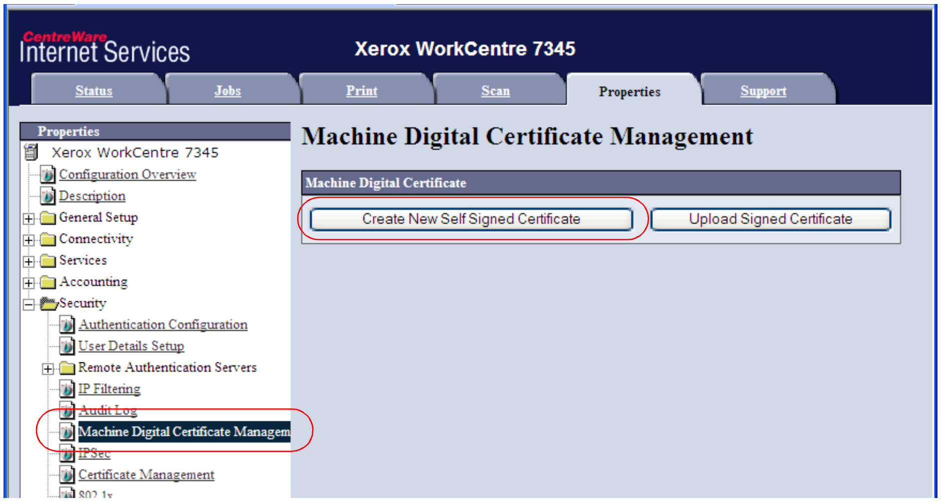
The Admin ID and password must correspond to the ID and password already configured on the MFP.

Configuring the MFP Through a Web Interface

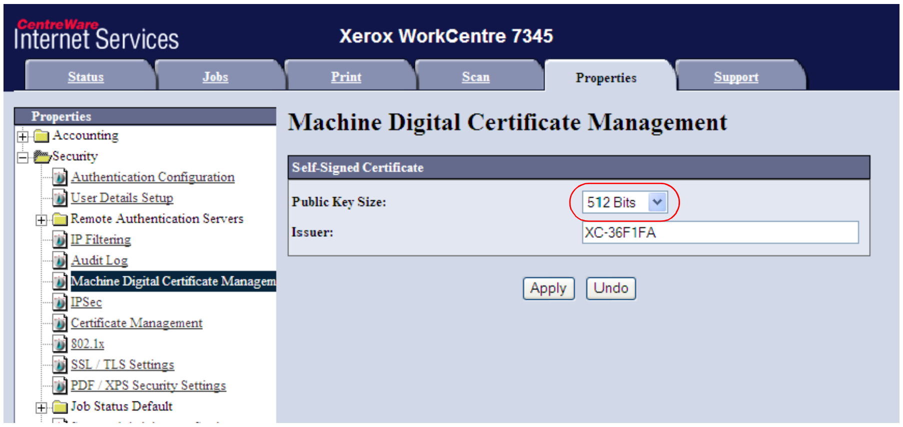
You must configure the MFP to use the Authentication Agent and communicate with the DCE Server. Xerox offers a web-based interface for configuring advanced Administrative options.

1. Open a web browser, and enter the IP address of the Xerox device in the **Address** field.
2. When prompted, enter your Administration User Name and Password.

   The Xerox web configuration page opens (CentreWare Internet Services).
3. Click the **Properties** tab, expand **the Security folder in the left pane, then select Machine Digital Certificate Management.**


CentreWare Internet Services
Xerox WorkCentre 7345
Status
Jobs
Print
Scan
Properties
Support
Properties
Xerox WorkCentre 7345
Configuration Overview
Description
General Setup
Connectivity
Services
Accounting
Security
Authentication Configuration
User Details Setup
Remote Authentication Servers
IP Filtering
Audit Log
Machine Digital Certificate Managem
IPSec
Certificate Management
802.1x
Machine Digital Certificate Management
Machine Digital Certificate
Create New Self Signed Certificate
Upload Signed Certificate

4. Click the **Create New Self Signed Certificate** button.



Public Key Size: 512 Bits

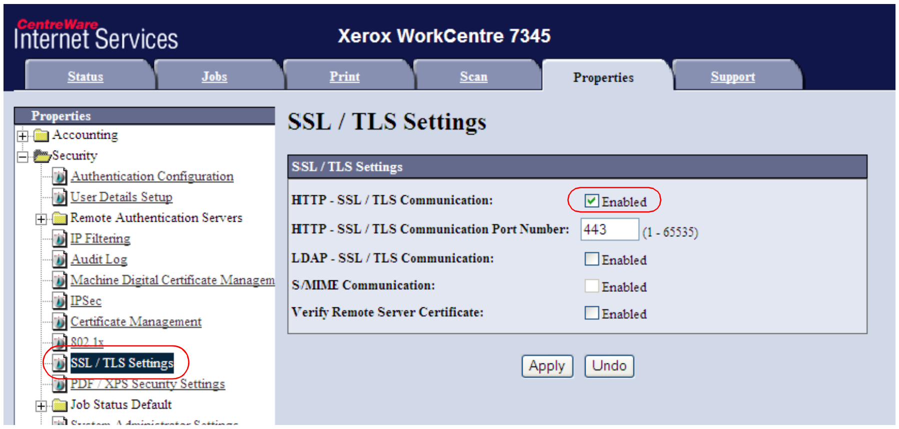
Issuer: XC-36F1FA

5. Select **Public Key Size** to 512 Bits/1024 Bits from the drop-down list, and click **Apply**.

   This step is required when you need to enable SSL in HTTP-SSL/TLS Communication.

   The page now displays the message **Settings have been changed**.

6. Expand **the Security folder in the left pane, then select SSL/TLS Settings.**



SSL / TLS Settings

SSL / TLS Settings

HTTP - SSL / TLS Communication: ☑ Enabled

HTTP - SSL / TLS Communication Port Number: 443 (1 - 65535)

LDAP - SSL / TLS Communication: □ Enabled

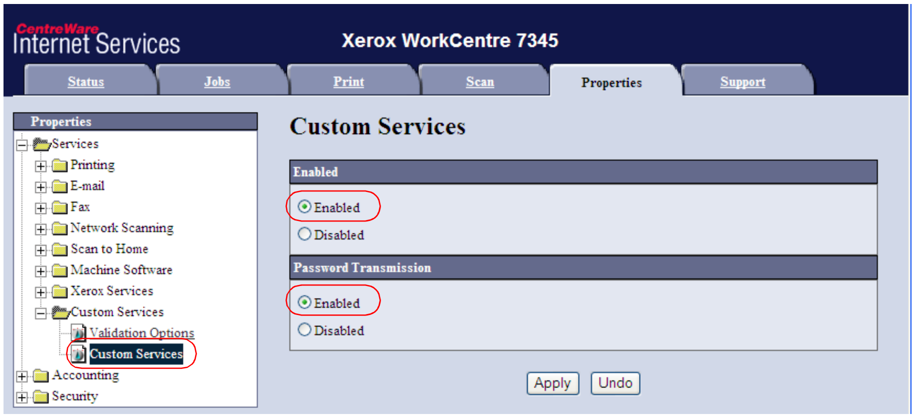
S/MIME Communication: □ Enabled

Verify Remote Server Certificate: □ Enabled

7. Enable **HTTP SSL/TLS Communication**, and click **Apply**.

Enable Custom Services

1. In the left pane, click on the **Services** folder, then click on the **Custom Services** subfolder.
2. Select the **Custom services** option to update the right pane.
3. Ensure both **Custom Services** and **Password Transmission** are set to **Enabled**, and then click **Apply**.



Custom Services

Enabled

● Enabled

○ Disabled

Password Transmission

● Enabled

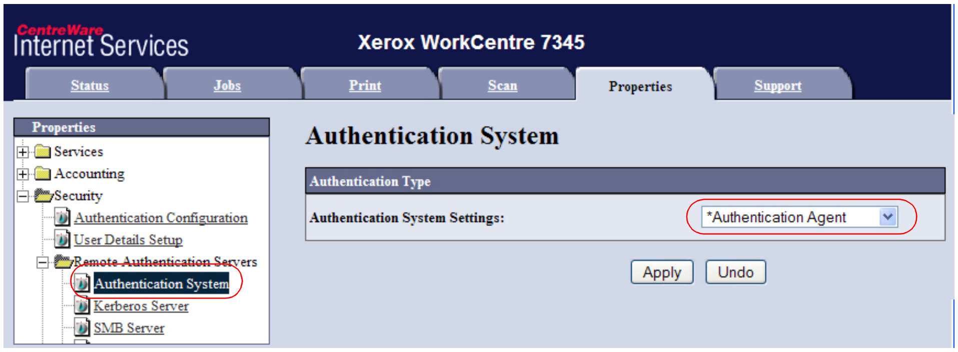
○ Disabled

The page now displays the message **Settings have been changed**. You may also be asked to reboot the machine at this time.

The Custom Services button appears on the MFP user interface when All Services is selected.

Set the Authentication System

1. In the left pane, click the **Security** folder, then select the **Remote Authentication Servers** subfolder.
2. Click **Authentication System** to view the Authentication Type options in the right pane.
3. Set the **Authentication System Settings** option to **Authentication Agent**, and then click **Apply**.



Authentication System

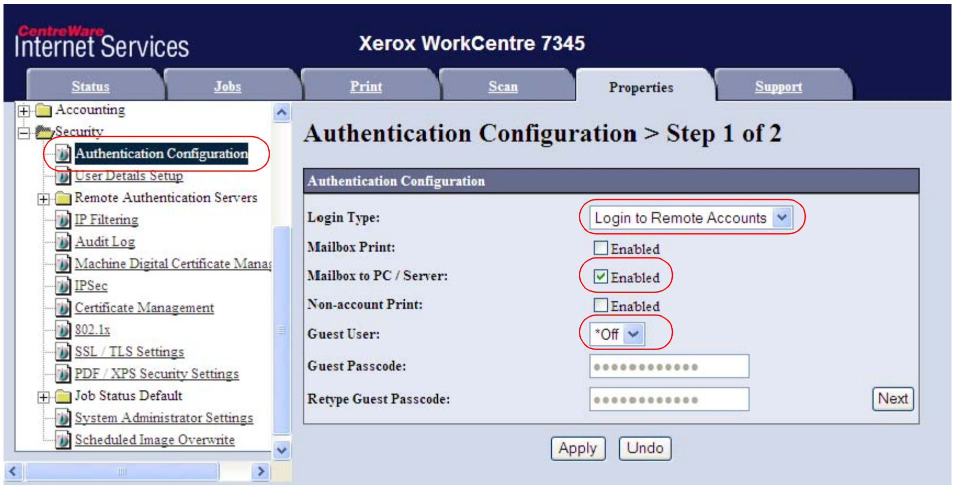
Authentication Type

Authentication System Settings: *Authentication Agent

4. Click the **Reboot Machine** button to apply the settings, and then click **OK** when prompted to reboot.

Set Authentication Configuration Options

1. In the left pane, click the **Security** folder, then select **Authentication Configuration**.
2. On the **Authentication Configuration > Step 1 of 2** screen, set the following options:
   - **Login Type – Login to Remote Accounts**
   - **Mailbox to PC / Server – Enabled**
   - **Guest User – Off**



Authentication Configuration > Step 1 of 2

Authentication Configuration

Login Type: Login to Remote Accounts

Mailbox Print: □ Enabled

Mailbox to PC / Server: ☑ Enabled

Non-account Print: □ Enabled

Guest User: *Off

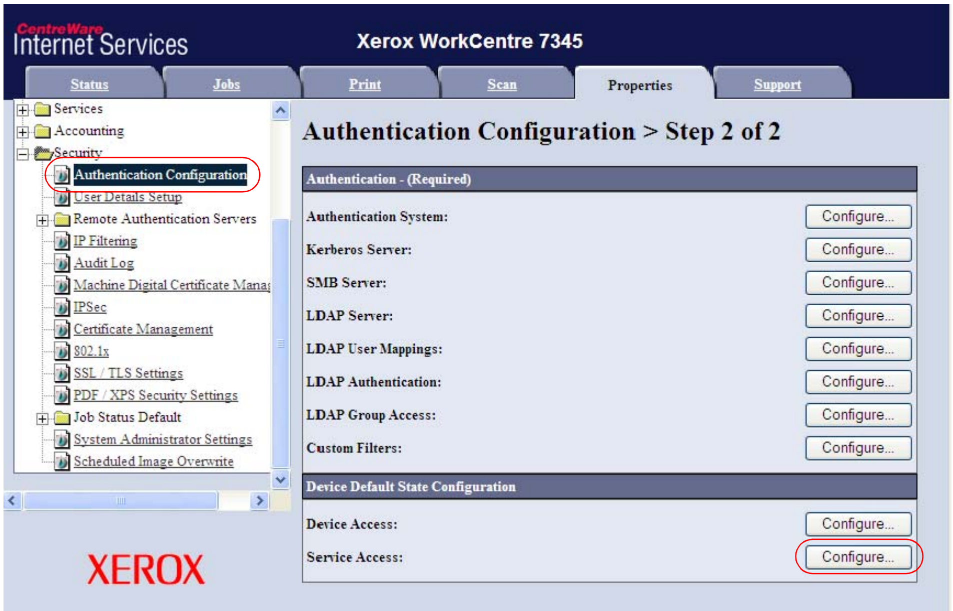
Guest Passcode: ●●●●●●●●●●●●

Retype Guest Passcode: ●●●●●●●●●●●●

CentreWare Internet Services
Xerox WorkCentre 7345
Status
Jobs
Print
Scan
Properties
Support
Accounting
Security
Authentication Configuration
User Details Setup
Remote Authentication Servers
IP Filtering
Audit Log
Machine Digital Certificate Manag
IPSec
Certificate Management
802.1x
SSL / TLS Settings
PDF / XPS Security Settings
Job Status Default
System Administrator Settings
Scheduled Image Overwrite
Next
Apply
Undo

3. Click **Apply** before proceeding to Step 2. You may be required to reboot the machine at this time.
4. Click **Next** to continue to the Step 2 of 2 screen.

5. On the **Authentication Configuration > Step 2 of 2** screen, click the **Configure** button located beside the **Service Access** option at the bottom on the screen.


CentreWare Internet Services
Xerox WorkCentre 7345
Status
Jobs
Print
Scan
Properties
Support
Services
Accounting
Security
Authentication Configuration
User Details Setup
Remote Authentication Servers
IP Filtering
Audit Log
Machine Digital Certificate Manag
IPSec
Certificate Management
802.1x
SSL / TLS Settings
PDF / XPS Security Settings
Job Status Default
System Administrator Settings
Scheduled Image Overwrite
XEROX

Authentication Configuration > Step 2 of 2

Authentication - (Required)

Authentication System:	Configure...
Kerberos Server:	Configure...
SMB Server:	Configure...
LDAP Server:	Configure...
LDAP User Mappings:	Configure...
LDAP Authentication:	Configure...
LDAP Group Access:	Configure...
Custom Filters:	Configure...

Device Default State Configuration

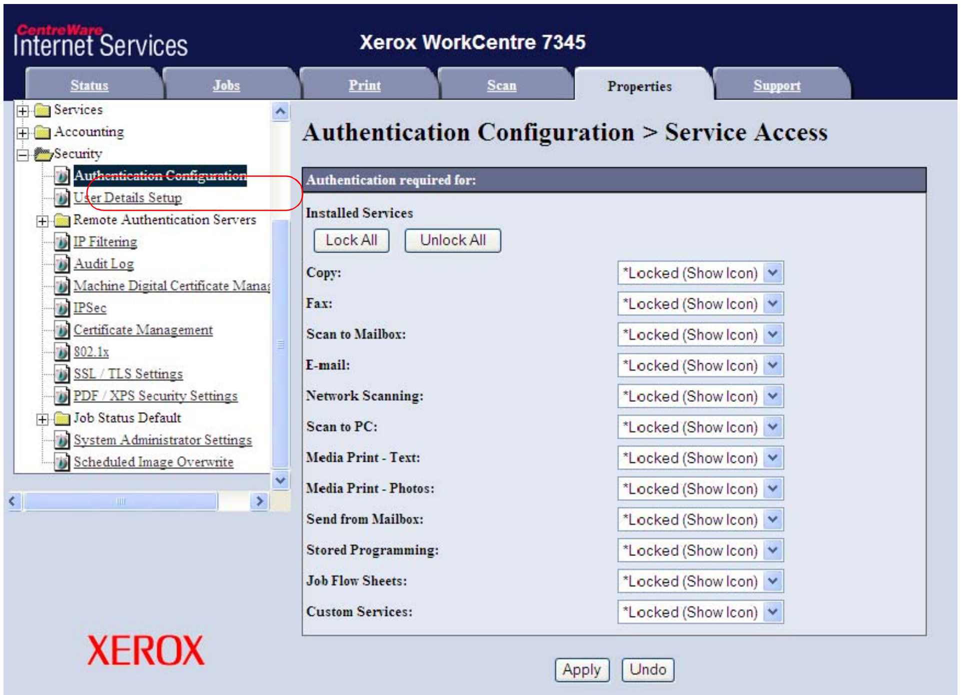
Device Access:	Configure...
Service Access:	Configure...

6. On the **Service Access** screen, choose the services you want to lock.

There are three available options:

- Unlocked
- Locked (Show Icon)
- Locked (Hide Icon)

You can set each service individually, or you can **Lock All** or **Unlock All** services by pressing the corresponding button.


CentreWare Internet Services
Xerox WorkCentre 7345
Status
Jobs
Print
Scan
Properties
Support
Services
Accounting
Security
Authentication Configuration
User Details Setup
Remote Authentication Servers
IP Filtering
Audit Log
Machine Digital Certificate Manag
IPSec
Certificate Management
802.1x
SSL / TLS Settings
PDF / XPS Security Settings
Job Status Default
System Administrator Settings
Scheduled Image Overwrite
XEROX

Authentication Configuration > Service Access

Authentication required for:

Installed Services

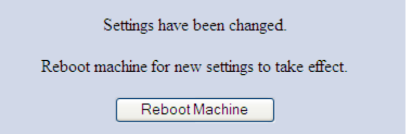
Lock All Unlock All

Copy:	*Locked (Show Icon)
Fax:	*Locked (Show Icon)
Scan to Mailbox:	*Locked (Show Icon)
E-mail:	*Locked (Show Icon)
Network Scanning:	*Locked (Show Icon)
Scan to PC:	*Locked (Show Icon)
Media Print - Text:	*Locked (Show Icon)
Media Print - Photos:	*Locked (Show Icon)
Send from Mailbox:	*Locked (Show Icon)
Stored Programming:	*Locked (Show Icon)
Job Flow Sheets:	*Locked (Show Icon)
Custom Services:	*Locked (Show Icon)

Apply Undo

The user can see any unlocked services when they approach the MFP. The authentication window appears after the user chooses one of these services. If the service is set to Locked, the service does not appear on the front panel until the user authenticates.

7. Click on **Apply** to accept all of the Authentication Configuration settings.
8. Click the **Reboot Machine** button to apply the settings, and then click **OK**.
9. Close the web browser.
10. Click the **Reboot Machine** button to apply the settings, and then click **OK** when prompted to reboot.

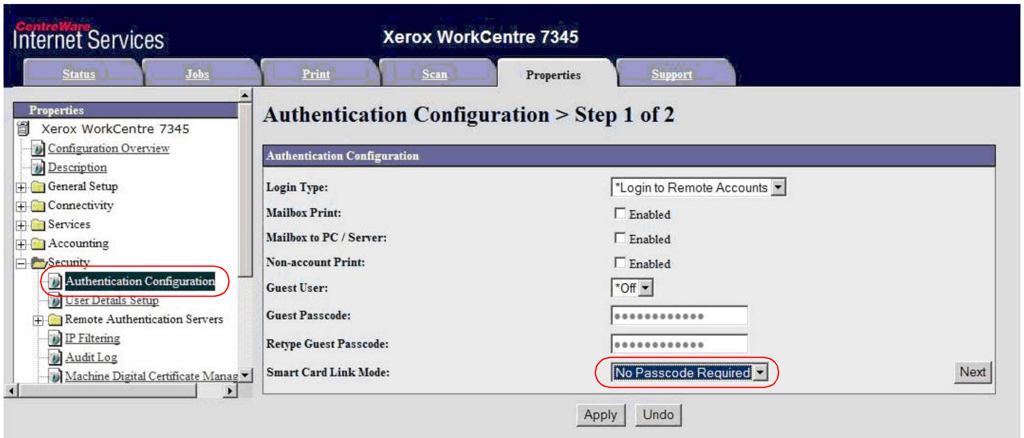


Settings have been changed.

Reboot machine for new settings to take effect.

Configuring Smart Card Through Xerox Authentication

1. Start a web browser, and enter the IP address of the Xerox device in the **Address** field.
2. The Xerox web configuration page opens (CentreWare Internet Services).



Authentication Configuration > Step 1 of 2

Authentication Configuration

Login Type: *Login to Remote Accounts

Mailbox Print: □ Enabled

Mailbox to PC / Server: □ Enabled

Non-account Print: □ Enabled

Guest User: *Off

Guest Passcode: ••••••••••••

Retype Guest Passcode: ••••••••••••

Smart Card Link Mode: No Passcode Required

3. Click the **Properties** tab, expand **the Security folder in the left pane, then select Authentication Configuration.**
4. Select **No Passcode Required** from the **Smart Card Link Mode** drop-down list if only a User ID is required to register the card.

   -Or-
5. Select **Enter Passcode** from the **Smart Card Link Mode** drop-down list if both User ID and Passcode are required to register the card.
6. Click the **Apply** button to save the setting.
7. Close the web browser.

   Note

   The Smart Card link Mode may not be visible until the EPA card reader is configured and the device has been rebooted.

Refreshing a Domain After Restarting a Device

If you are required to enter a user ID or passcode to access the functions of an MFP device, you may also need to make sure that you are logging in as part of a user domain. In particular, after a device has been shut down and restarted, the first user at the device may need to associate the device with a user domain.

Use the following procedure to set a device’s domain:

1. On the device login screen, press the **Domain** button.
2. On the Domain screen, press **Refresh** to update the domain list.
3. Select **Equitrac** from the domain list.
4. Press **Save** to return to the login screen.
5. Log in to the device’s embedded application as normal.

   Note

   Some devices refer to Domain as Realm, and as a result, the Domain button may appear as Realm on the Login screen. If the Realm button is visible, select it to access the Refresh button.

User Workflow

3

Topics

This chapter provides the following information.

- Basic instructions on how users can authenticate and use the Embedded functions at the Xerox MFP
- Procedures for configuring some user workflow functions

Authenticating at a Card Reader

When Xerox Secure Access controls an MFP, users must authenticate with a magnetic stripe card, proximity card or smart card before they can use the device functions.

Authenticating With a Magnetic Stripe Card

To authenticate at a magnetic stripe card reader, do the following:

1. Insert the magnetic 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.

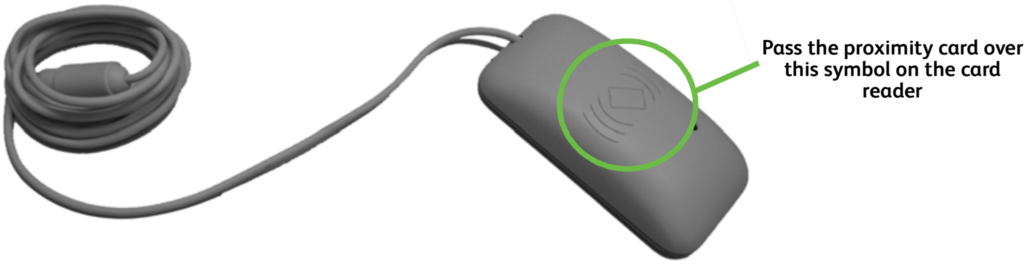
   Note

   Do not run the card through at an angle or the terminal cannot 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 PINs are enabled 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 centimeters of the proximity symbol located on the top of the card reader device or the data reader module.

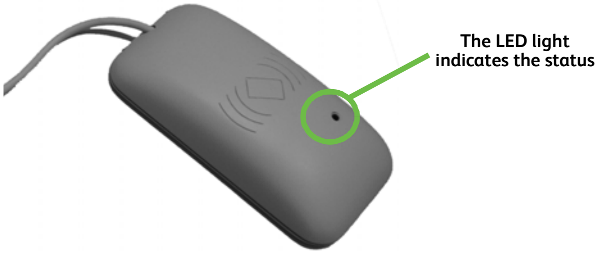


If the swipe is invalid, the LED flashes red.

If secondary PINs are enabled 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, the user can leave the field blank to proceed.

Card Reader Status Messages

Xerox Secure Access displays its authentication messages through an LED light on the card reader module.



The following signals may be displayed on the card reader:

LED Behavior	Meaning
Solid red	MFPAuthentication Device is in Idle mode; it is ready but there is no active session.
Solid green	MFPAuthentication Device is in Ready mode and a session is active.
Slow flashing green	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.
Slow flashing red	No communication between card reader and MFPAuthentication Device.

The MFPAuthentication Device has two functional modes, Idle mode or Ready mode.

Idle Mode

An MFPAuthentication Device 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 MFPAuthentication Device 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.

Card Self-Registration

Card registration enables a user to quickly and conveniently login to the MFP without manually entering user credentials before each session.

1. At the MFP, swipe your card on the attached card reader.

   The following error message appears on the MFP touch screen:

   Login failed
   Incorrect authentication system settings
   See User Guide for information on fault code 016-569

2. Press **Close** on the touch screen, and then press the **Key** button on the control panel to open the **Login** screen.

   Note

   Ensure that the Domain is set to **Equitrac**® on the MFP screen before proceeding with self-registration. If it is not set to Equitrac, see Refreshing a Domain After Restarting a Device on page 25.

3. Enter your primary ID in the **User ID** field, and press **Next**.
4. Leave the **Password field blank, and** press **Enter** on the password login screen.
   - **If the MFP main screen opens, skip to Step 6.**
   - **If login fails, and the main screen does not open, continue with Step 5.**
5. **Key in your secondary ID in the Password field, and then press Enter to open the MFP main screen.**

   A required password depends on which Smart Card Link Mode option is selected in Authentication Configuration. See Configuring Card Self-Registration on page 16 for configuration options.

6. Press the **Log In/Out** (**Key)** button on the control panel and press **Logout** on the touch screen.
7. Swipe your card again to verify that the card has been successfully registered.

   The MFP main screen appears when login is successful.

8. Press the **Log In/Out** button and press **Logout**.

   Note

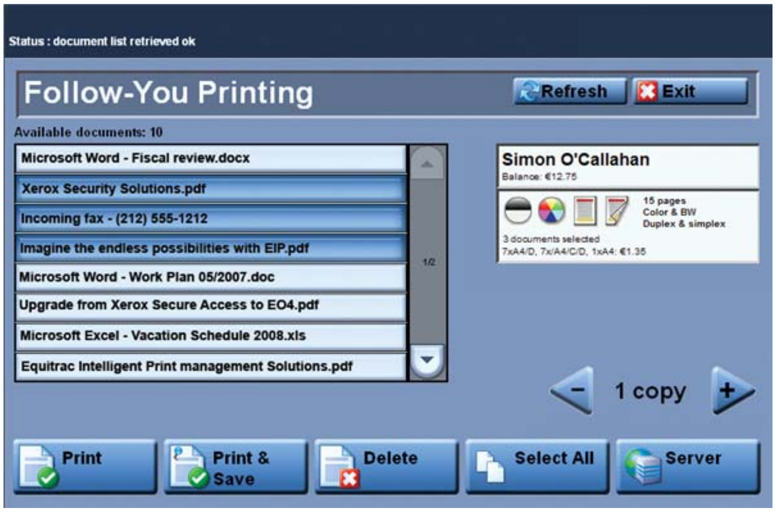
   The ID and password for card registration can be Xerox Secure Access PINs or external user IDs and passwords, such as from Windows or LDAP.

Using Follow-You Printing®

If you configured the Follow-You Printing extension, users can access the Follow-You Printing screen to view their print jobs from one or more secure queues, and then release or delete the jobs as required.

To use the Follow-You Printing feature, do the following:

1. After authenticating, press **All Services**.
2. Press **Custom Services**.
3. Press **Follow-You Printing**.



Status : document list retrieved ok

Follow-You Printing

Available documents: 10

- Microsoft Word - Fiscal review.docx
- Xerox Security Solutions.pdf
- Incoming fax - (212) 555-1212
- Imagine the endless possibilities with EIP.pdf
- Microsoft Word - Work Plan 05/2007.doc
- Upgrade from Xerox Secure Access to EO4.pdf
- Microsoft Excel - Vacation Schedule 2008.xls
- Equitrac Intelligent Print management Solutions.pdf

Simon O'Callahan
Balance: €12.75

15 pages
Color & BW
Duplex & simplex

3 documents selected
7xA4/D, 7x/A4/C/D, 1xA4: €1.35

1 copy

4. All documents on the users' Home print server, default server, or both are shown in the screen. Users can then perform the following functions at the device:

Function	Description
Print	Touch one or more documents in the list, then press **Print** to print the documents and delete the jobs from the list.
Print & Save	Touch one or more documents in the list, then press **Print & Save** to print the documents but keep the jobs in the list.
Delete	Touch one or multiple documents in the list, then press **Delete** to delete the jobs from the queue without printing them.
Select All	Selects all jobs in the list, after which you can press **Print**, **Print & Save**, or **Delete**.
Refresh	Checks 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.

Function	Description
Server	If multiserver Follow-You Printing is enabled on the Xerox Secure Access server, press **Server** 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 only see the local server listed. For multiserver Follow-You Printing configuration information, see the "Advanced Printing Configuration" chapter in the *Xerox Secure Access Administration Guide*.
Exit	Returns to the Custom Services screen.

Ending a Session

To end your user session, press **Log In/Out** on the device control panel.

Copy Enforcement and Configuration

Xerox Secure Access can enforce limits on the number of copies that a user can make based upon their account limit, color quota, and/or copy rule(s) configured in System Manager.

Note

Enforcement only occurs at the start of a session when the user logs in.

Users are denied access if they are out of funds or quota, or if a copy rule is applicable. For information on configuring account limits, color quotas, and copy rules, see the *Xerox Secure Access Administration Guide*.

In addition, when account limits are enabled with Equitrac Express, copy limits are enforced automatically based on users' account balances. Equitrac Express calculates how many pages can be printed based on the default page price for a copy and the remaining balance in the user's account.

Color Quota Enforcement

In-session color quota limits are not enforced in Xerox Secure Access.

Color quotas are configured through System Manager. For instructions on setting and enforcing color quota limits, see the Creating & Managing Accounts chapter in the *Xerox Secure Access Administration Guide*.

4

Troubleshooting

Known Limitations

On some MFPs the User ID of the authenticated user is not available to the EIP session. This may affect the functionality of third party workflow applications.

Symptoms and Solutions

If you experience a problem with your Xerox Secure Access application at a device, refer to the table below for symptoms and solutions that match your problem before contacting Technical Support for help.

Symptom	Possible Solution
The indicator light on the card reader is off	When the light is not lit, this indicates a loss of power to the reader. • Check the NVM Read/Write settings; 850-007 should be set to “10” and 850-001 to “1.” • Check the cable connection to the MFP and ensure that it is firmly seated. • If the light remains unlit, check the power to the MFP. If the MFP does not have power, neither does the card reader.
The card reader indicator light stays red upon swipe	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 see Supported MFPs on page 1-4.
Fault Code, or error 121-333, on the device panel	The card reader was removed without resetting the NVM Read/Write values. To correct the error: • Install the card reader again and restart the device. —Or— • Reset the NVM Read/Write 850-007 to “10” and 850-001 to “1,” and restart. For instructions on resetting NVM Read/Write values and removing a card reader, see Configuring Follow-You Printing® on page 14.
Error message "Login Failed" on the device panel	If a device has been restarted, the first user at the device may need to associate the device with the Xerox Secure Access realm. See to Refreshing a Domain After Restarting a Device on page 25.

xerox®