

USB Card Reader Configuration Guide

Xerox WorkCentre[®] 51xx / Xerox WorkCentre 56xx

Xerox WorkCentre 57xx / Xerox WorkCentre 6400

Xerox WorkCentre 75xx / Xerox WorkCentre 77xx

Xerox ColorQube[®] 87xx / 89xx

Xerox ColorQube 92xx / Xerox ColorQube 93xx

February 2014



©2014 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design®, WorkCentre®, ColorQube®, and Xerox Extensible Interface Platform® are trademarks of the Xerox Corporation in the United States and/or other countries.

Other company trademarks are also acknowledged.

Document Version: 3.0 (February 2014).

dc13cd023

Table of Contents

Overview.....	2
Supported Reader Technology	2
Operation.....	2
Diagnostics	3
Card Reader Software	3
Magnetic Stripe Reader Constraints	3
Prerequisites.....	4
Installation	4
Connecting the USB card reader.....	4
Configuring the machine to use USB card reader for authentication...	5
Create a Device Certificate and Enable SSL.....	5
Appendix A – Supported USB card readers	7
Appendix B Card Reader Configuration Setting	8
Elatec TWN3 Software	8
Magnetic Stripe Reader Configuration.....	8
ID TECH Magnetic Stripe Reader Configuration Upgrade	9
RF IDEas Magnetic Stripe Reader Configuration Upgrade	10
Document Version History	Error! Bookmark not defined.

Overview

This document describes how to configure off box authentication to a Solution Partner Authentication server with a USB card reader using the new open USB standard. The USB card reader is connected directly to the USB port on the Xerox machine. When the USB card reader is connected to the machine, an external card reading controller is no longer required.

This feature is used to control access to the MFP via employee badge to a partner authentication server. Once the server is setup to communicate with the device and selected Services are locked at the LUI, access to those 'locked' services will only be granted to walk up users with valid cards and/or System Administrators.

Supported Reader Technology

Employee badges can contain one or multiple technologies for storing user identity information. The 4 prominent methods in use today are Wireless which is also known as Proximity, Magnetic Stripe, Visual Barcode and Smart Cards. This document addresses support for Proximity, Magnetic Stripe and Visual Barcode readers. There are two classes of proximity readers, those which can read the Card Serial Number (CSN) and those which can read from secure memory segments contained on specific card types. This solution will only support proximity readers which send the CSN.

Smart Card Authentication (CAC / PIV / .NET etc) are addressed in the Smart Card feature documentation.

Operation

This feature is designed to read data from an employee badge and to package that data into a message which is sent to the server running software from a solution provider. This requires that the solution provider has developed their software to be compatible with this feature using the Convenience Authentication API.

This feature enables solution providers to provide authentication, pull printing and accounting which is tied the user associated with the employee's badge. This feature is configured using most of the Xerox Secure Access set up screens but is not compatible with the Xerox Secure Access feature itself. It is not compatible with the white card readers supplied as part of Xerox Secure Access.

Each of the currently approved badge readers has internal intelligence to read a card and to acknowledge success by blinking the LED or creating sound with the beeper on the reader itself. Note that this behavior is different than with the Xerox Secure Access (XSA) solution. With XSA, the authentication server is in control of the LED on the reader. This means users will observe faster acknowledgement that their card has been recognized because that recognition does not require communication with a server. A side effect is that the LED indications will not be consistent with those of the XSA solution.

The card readers will have power applied when the MFP is awake and while it is in Sleep mode. A card swipe will take the MFP out of Sleep mode and will initiate an authentication sequence. To meet EPA

Energy Star requirements, power is removed from the reader when the MFP enters Deep Sleep. In Deep Sleep the card reader will appear to be dead. Since the reader has no power, the LED will not be illuminated. A card swipe in Deep Sleep mode will be ignored. Users must first awaken the MFP using the Energy Saver button. Once the MFP is awake, the card reader will again be functional.

Diagnostics

USB card readers have been chosen which communicate using the Human Interface Device (HID) keyboard emulation mode. The rationale for this decision is primarily to aid in the ability to troubleshoot problems in the field. An HID reader can be plugged directly into any personal computer and tested independent from the MFP. All one need do is open a document application such as Microsoft Notepad which expects Text as input. If an employee badge is swiped across the reader, the CSN will be displayed in the Notepad application. This makes it easy to diagnose reader related problems in the field.

Since this is a relatively new feature we have chosen to start cautiously. As a result the only readers which will be recognized are those which have been tested and found acceptable by engineering. If any reader is connected which is not listed in Appendix A, the MFP will totally ignore it. The Configuration section of this document will address how the MFP will indicate that a non-supported reader is connected.

Card Reader Software

Magnetic Stripe Reader Constraints

There is a wide variety in the factory default behavior of magnetic stripe readers. While all of the tested readers are capable of supporting the applicable ISO standards they do not initially send the card data in exactly the same way. Each of the supported readers can be programmed in the way they send card data and each of the manufacturers provides PC based tools to program the reader. As a result a standard configuration can be defined across all readers.

In our defined standard configuration the reader will emit every line of data which the magnetic stripe card contains. The reader will emit all line sentinels, field separators and line termination characters and will not mask out any data. This will enable solution partners full access to card data which can be processed as they desire.

Appendix B contains directions to properly configure each magnetic stripe reader.

Prerequisites

- The Multi-function Printer software must meet a minimum software level. The supported devices and the minimum software levels are:

WC51xx software - Version 21.120.65.170

WC56xx software - SBC Version 25.54.65.170
- MBC Version 21.120.65.170

WC57xx software - Version 061.132.222.28900

WC6400 software - Version 061.070.102.23501

WC75xx software - Version 061.121.222.21500

WC77xx software – Version 061.090.223.10600

CQ87xx / 89xx software - Version 071.160.222.28900

CQ93xx software - Version 61.180.222.08700

- Must be using supported cards and card readers. See Appendix A.
- The Secure Socket Layer (SSL) must be enabled

Note

- Extensible service setup has to be enabled if the Xerox Extensible Interface Platform® (EIP) application is used.
- The open USB card reader standard cannot be used with Xerox Secure Access branded card readers.

Installation

Connecting the USB card reader

Connect the card reader to one of the available USB ports on the MFP. The reader can be mounted in a number of locations on the MFP. For example, it can be placed on the top panel next to the UI, on the left hand shelf or on the top of the finisher.

Most of the tested readers will indicate that they have power and are operational by illuminating an LED and possibly emitting a sound once the card reader has booted up.

Please insure the card reader software is at the latest level by checking with the particular manufacture web site as outlined in Appendix A. Some readers require a particular configuration to be compatible with the MFP. This is defined in Appendix B. Please be sure the software and configuration are correct before the reader is installed on the MFP.

Configuring the machine to use USB card reader for authentication

Create a Device Certificate and Enable SSL

The following configuration settings can only be completed via CWIS.

Note: Either the existing default certificate can be used or the user can install their own certificate. The steps below use the default certificate.

1. Open a web browser and connect to CWIS by entering the following URL: `http://[enter device IP address]/`
2. Click on the **[Properties] - [Certificates] – [Security Certificates]** (note: SSL must be enabled. If it is not follow the **[Configure SSL]** link on this page to enable SSL, then repeat step 2.)
3. Enter System Administrator credentials if prompted
4. On the Xerox Device Certificate tab, click on **[Create New Xerox Device Certificate]**
5. Select Connection [Enabled] with port 80
6. Select Secure HTTPS [Disabled]
7. Select **[Default Xerox Device Certificate]**
8. Select Device Certificate : **[Default Xerox Device Certificate]**
9. Complete all text fill in fields
10. Select the **{Subject Alternative Name}** checkbox
11. When all entries are complete select [Finish
12. Wait while the new certificate is created.]
13. Select **[Apply]**

Configure the feature via the existing Xerox Secure Access web page

1. Navigate to **[Security] - [Authentication] – [Setup]**
2. Select **[Xerox Secure Access Unified ID System]** as the Authentication method on the machine's touch user interface
3. Under Configuration Setting, select the **[Edit]** button next to **[Xerox Secure Access Setup]**
4. Normally the configuration settings are pushed down from the partner server. If you plan to use this method, select [Close] and consult the particular solution partner's installation and configuration documentation. If you wish to configure these settings manually, select [Manually Configure]
5. Fill in the server Communication details using either IP address or Host Name. Include the path to the server.
6. Verify that the **[Embedded]** box is **NOT** checked. This checkbox enables software which only works with the white egg shaped Xerox Secure Access card readers.
7. Set the **[USB Card Reader Detection Policy]** to either allow or deny access to the MFP if the card reader becomes unplugged. This will cause a Caution screen to appear whenever the card reader is accidentally unplugged and remind the user to plug it back in.
8. Set the **[Device Log In Method]** to either enable only swipe card authentication or whether to also offer Alternate Authentication where the user manually enters their logon credentials in the event they lost or forgot their card.

9. Configure **[Accounting Information]** If the Job Based Accounting option has been purchased, these fields will be available for selection. Choose whether the server will enter the appropriate accounting code or whether the user will be prompted to enter a code.
10. Fill in the **[Device Instructional Blocking Window]** details; the Window Title and Instructional Text. For example “Please swipe your card to log on”.
11. Select **[Save]**

If the USB Card Reader Detection Policy was set to **[Prevent use of device when USB card reader is disconnected]** then when the summary screen appears, it will indicate whether an Approved card reader is **Connected, Not Connected** or **Not Supported**.

Verify Connected Reader

At this point the local UI should show a pop up or message indicating that the card reader is not connected.

1. Insert a qualified card reader into the USB port and observe that the message goes away.
2. Remove the card reader and observe that the pop up reappears.
3. Plug the card reader back in.

Validation

At this point the system is fully configured for authentication. Lock a few services to verify that authentication is required for access.

1. Via CWIS, navigate to **[Properties] –[Security] – [Authentication] – [Tools & Feature Access]**
2. Under Presets, select **[Custom Access]**
3. Select **[Locked]** for any Services, Features, or Pathways that should be secured.
4. Select **[Apply]**

At the local UI, navigate to a locked Service or Pathway. Verify the prompt to swipe a card to log on is displayed.

5. Swipe or scan a valid card with the USB card reader
 - a) Depending on the particular reader you should observe the card reader LED change color or the reader will beep.
 - b) Observe that the user is authenticated and their username appears in the upper right corner of the local user interface display.
6. Swipe or scan the same card with the card reader
 - a) Depending on the particular reader you should observe the card reader LED change color or the reader will beep.
 - b) Observe that the user is logged out and that the Default Walkup Screen is displayed. If the Default Screen is locked, the blocking screen will be displayed.

Appendix A – Supported USB card readers

Proximity readers

These support 125Khz & 13.56Mhz which include HID Prox®, Mifare, HID iCLASS®, LEGIC®, and a variety of other card types.

Elatec TWN3 & TWN4 family USB readers: (<http://www.elatec-rfid.com>)

RF IDEas RDR-XX6081-AKU family USB Prox readers and all other readers from the “USB Enroll” family including pcProx® Plus. (<http://www.rfideas.com>)

YSoft V2 family USB readers: (<http://www.ysoft.com>)

Magnetic Stripe readers:

These support ISO 7813 and ISO 4909 encoding standards for tracks 1, 2 & 3.

RF IDEas MS3-00M1AKU MagStripe reader. (<http://www.rfideas.com>)

ID TECH MiniMag II™ MagStripe reader (<http://www.idtechproducts.com>)

MagTek® Magnetic stripe reader (<http://www.magtek.com>)

YSoft V2 Magnetic stripe reader: (<http://www.ysoft.com>)

Visual Barcode Reader

These support one dimensional visual barcodes

Honeywell® 3800G (<http://www.honeywellaidc.com>)

These support two dimensional visual barcodes.

Motorola® DS457 & DS9208 (<http://www.motorola.com>)

Appendix B Card Reader Configuration Setting

Elatec TWN3 Software

Elatec TWN3 readers must have at least software version V3 03d/4.39 to operate properly on the WorkCentre 53xx, WorkCentre 7120, and WorkCentre 74xx. If connecting an Elatec reader with earlier software to one of these products, the reader software will need to be upgraded first.

Please contact Elatec Customer Support for this software update. (support@elatec-rfid.com)

Magnetic Stripe Reader Configuration

The ISO specification for magnetic stripe cards defines the data format for the 3 possible tracks on a mag stripe card. Each line starts with a unique character called a sentinel which denotes which line of data is being read. The ISO spec specifies characters used to define the data blocks within a line as well as the line termination character.

Shown below are three lines of data contained on a hypothetical 3 track mag stripe card:

```
%B6006493801^XEROX   ^1012110   LQI?  
;6006493801=101211050282809?  
; 6006493801?
```

Xerox MFPs require this data to be concatenated into a single string with only one carriage return as the terminating character.

```
%B6006493801^XEROX   ^1012110   LQI?;6006493801=101211050282809?; 6006493801?
```

In order to determine if the reader conforms to the Xerox standard, the reader can be easily tested using a personal computer.

- 1) Open a text document tool like Microsoft Notepad
- 2) Connect the magnetic stripe reader to a USB port on the computer
- 3) Wait for the card reader driver to be installed.
- 4) Swipe one of the customer's mag stripe cards.
- 5) Observe the data displayed in Notepad.
 - a. If the data is presented in a single line with one carriage return the reader is compatible and no programming is required.
 - b. If the reader sends multiple lines or strips off the line start and end characters, the reader will need to be reprogrammed.

Each of the card readers listed in Appendix A can be reprogrammed to this format using tools supplied by each manufacturer. Below are URLs to the manufacturer's websites where the card reader configuration tool can be retrieved.

Note that the YSoft and ID TECH Magnetic stripe readers listed in Appendix A already conformed to the Xerox standard and did not need to be upgraded.

RF Ideas: pcSwipeConfig.exe <http://www.rfideas.com/Software/>

ID TECH; USB Swipe & Insert Reader programming tool

http://www.idtechproducts.com/index.php?option=com_docman&task=cat_view&gid=298&Itemid=79

MagTek: MiniMag II Configuration Software

http://www.magtek.com/support/software/demo_programs/usb_swipe_insert.asp

ID TECH Magnetic Stripe Reader Configuration Upgrade

Software can be found at: http://www.idtechproducts.com/download/swipe-readers/doc_download/38-configuration-software.html

Select the **IDTech_Xerox_Config.zip** file to access the ID TECH MagStripe Configuration file that will be required later in the setup process. The file is located within the [USB Card Reader Install.zip](#) file mentioned in the Prerequisites section.

Save the file to your PC for later use.

After installing (note: requires a restart) and running the Magstripe Configuration Utility:

1. Select Reader Interface button.
2. Select "USB" (Radio button below USB picture) and then select "Continue":
The reader will beep a few times and the screen will return back to the default view.
3. Select "Change Basic Reader Settings":
4. Select "Load from File":
5. Navigate to where you saved the configuration file, then select it followed by "Open":
You should get a message that loading the file was successful. Select "Ok":
6. Select "Send to MSR":
Reader will beep once or twice and you see a message that the settings were successfully written.
7. You are now done programming the reader. Select "Close" and then 'EXIT':

RF IDEas Magnetic Stripe Reader Configuration Upgrade

RF Ideas magnetic stripe readers can be configured with the pcSwipe tool available from their website (<http://www.rfideas.com>). Select Support / Software & Downloads then scroll down to **pcSwipe® Magnetic Card Reader**. Download and install pcSwipeConfig.exe.

- 1) Connect the reader to the workstation and run the pcSwipe tool.
 - a) Select the Scan/Connect button so the tool will interrogate the reader.

- 2) Once a reader has been recognized, select the Fields tab
 - a) In the Tracks field, enable tracks 1, 2 & 3.
 - b) Select User Field 1, and insure that the checkbox next to “Show Sentinels and Separators” is selected.
 - c) Select User Field 2 and then 3 and insure the “Show Sentinels and Separators” field is selected for those as well.
 - d) Select User Field 4
 - e) Insure the checkbox next to “Enable” is selected.
 - f) Verify that the word <ENTER> appears in the text field adjacent to the User Field 4 button. This is the termination to the data stream.
 - g) If <ENTER> does not appear, select the keyboard icon on the left labeled “Keys”
 - h) Within the pop up which will appear, select <ENTER> and then “Insert”.

- 3) Select the LED/Beep tab.
 - a) Verify that the LED and tone response match the customer’s desired behavior
 - b) When all configuration options have been set, this can be written to the reader.
 - c) From the pcSwipeConfig toolbar, select the Flash icon
 - d) The reader will beep and blink and beep when the new settings have been written.