SHARP

SYNAPPX™

SYNAPPX™ GO

PRODUCTIVITY WHEREVER YOU GO!

Administrator Setup and Configuration Guide for Native Authentication Integrated with Synappx Go

Table of Contents

This page is intentionally left blank.

Synappx Go Integration with MFP Native Authentication: Getting Started

Synappx Go and MFP Native Authentication Integration Overview

Synappx Go is a mobile app that connects to Sharp multifunction printers (MFPs), shares content to Sharp displays and captures workspace locations with mobile check-in. Sharp MFPs can be configured to control user access to selected MFP features via Synappx Go and account for MFP usage by user.

This guide is intended to support customers who want both the control of MFP authentication and authorization with the convenience of Synappx Go mobile scan, copy, print cloud file and/or print release.

System Requirements

For Synappx Go

See the Synappx Go Support site for more detail on specific component system requirements.

Synappx Go Components For Native Authentication Integration	
1. Mobile Application (iOS and Android™) 2. NFC Tags 3. MFP Agent 4. Admin Portal	5. Cloud System (Microsoft® Azure) 6. For Sharp A3 and A4, embedded OSA .emo Synappx Go app 7. For selected Sharp A4 models[1], Synappx-Go_2012a.fls, cardAuth_2012a.fls, keyboardreader-2.4.11.fls embedded apps

[1] MX-C507F, MX-C407F, MX-C357F, MX-B557F, MX-B467F

A stable internet connection is required.

Organizations must have a Microsoft® 365 or Google Workspace™ environment. Provider is designated after sign up.

Important: The user email addresses (user IDs) used in Native Authentication must match the email addresses (Microsoft 365 or Google Workspace) used in Synappx Go. The MFP Native and Go integration is not possible if this condition is not met.

Microsoft 365® Service Plans	
Business	Microsoft 365 Business Basic*/Standard/ Premium
Enterprise	Microsoft 365 Enterprise E1*/E3/E5 Microsoft 365 Enterprise F1
Education	Microsoft 365 Education A1*/A3/A5
Government	Microsoft 365 Government G1*/G3/G5

Google Workspace™ Service Plans
Business Starter
Business Standard
Business Plus
Enterprise

MFP Agent
• Microsoft Windows® 10 or greater or Windows Server 2016 or 2019, 32- or 64-bit • Microsoft .NET Framework 4.7.2 or higher • Minimum 4GB RAM • Minimum 75MB disk space (Requirements can vary based on the number of users and print jobs that the agent supports.) • Internet connectivity

Users and Admins
• Supports 5,000 users • All users must: ○ Have Microsoft 365 or Google Workspace accounts ○ Be in Microsoft Azure Active Directory (AD) or Google Workspace Directory • First administrator to log in requires Azure AD or Google Workspace admin privileges

Supported Mobile Platform
Apple® iPhones®**:** NFC support, iOS 12 or later • 7/7+, 8/8+, X, XR, XS, XS Max, iPhone 11, 11 Pro, 11 Pro Max, and iPhone SE (Second Generation - 2020)
Android™ • 8 to 11, NFC support

*This package offers only the web or mobile version of Microsoft Office applications. Synappx Go requires Office applications to be installed on the display PC for full functionality. Otherwise, the file will open in the web browser.

For MFP Native Authentication and Accounting

Synappx Go can be configured to work with MFPs locked with native authentication, authorization and accounting. Native authentication with local log in is supported on all approved Sharp MFP A3 and A4 models. Native authentication using on-premise AD or LDAP is supported on selected Sharp A3 and A4 MFPs (see MFP support table for details).

This guide will only describe the MFP native authentication settings that are specifically related to supporting Synnapx Go integration. Please see the individual MFP Admin documentation for details on native authentication, authorization and accounting web page configuration.

For rf IDEAS BLE Card Reader

Synappx Go and MFP Native Authentication require integration with rf IDEAS BLE reader Model RDR-30581BKU. Prox and iClass card types are supported.

The reader is attached to the MFP via USB after configuration. Before connection to the MFP, the rf IDEAS reader needs to be configured via a utility to support mobile credentials which are used with Synappx Go mobile. The reader can support up to four configurations including mobile credentials. See the rf IDEAS configuration section for set up details. Other BLE readers may be qualified and supported in the future.

Supported MFPs

Sharp MFPs supporting this Synappx Go integration feature are shown below. Some models have built-in NFC tags that can be used. However, MFP NFC or separate Synappx NFC tag configuration may be required, if not already set up.

Teal model numbers can support the Synappx Go copy feature and optional rf IDEAS reader integration with MFP native authentication feature. The rf IDEAS integration requires installation of a Synappx Go 1.0.0.emo file in the MFP on the models below.

A3 Models	**MX-2651**[1, 3]	MX-3050V[1]	MX-M2630[1]	MX-M4070	MX-M905
	MX-3051[1, 3]	MX-3070V	**MX-M2651**[1, 3]	**MX-M4071**	MX-M654N[2]
	MX-3071	MX-3550V[1]	MX-M3050[1]	MX-M5050[1]	MX-M754N[2]
	MX-3551[1, 3]	MX-3570V	**MX-M3051**[1, 3]	**MX-M5051**[1, 3]	
	MX-3571	MX-4050V[1]	MX-M3070	MX-M5070	
	MX-4051[1, 3]	MX-4070V	**MX-M3071**	**MX-M5071**	
	MX-4071	MX-5050V[1]	MX-M3550[1]	MX-M6050[1]	
	MX-5051[1, 3]	MX-5070V	**MX-M3551**[1, 3]	**MX-M6051**[1, 3]	
	MX-5071	MX-6050V[1]	MX-M3570	MX-M6070	
	MX-6051[1, 3]	MX-6070V	**MX-M3571**	**MX-M6071**	
	MX-6071	MX-6580N	MX-M4050[1]	MX-M6570	
		MX-7580N	**MX-M4051**[1, 3]	MX-M7570	

[1] MX-PK13L Adobe® PostScript® 3™ Expansion Kit and MX-PU10L Direct Print Expansion Kit are required to print cloud files.

[2] Special firmware needed to enable TLS 1.2 support

[3] These models support the Synappx Go copy feature and optional rf IDEAS card reader integration (e.g. for native authentication) but require that the MX-AMX2L Application Communications Module (ACM) option be installed.

A4 Models	**MX-B376W**	**MX-C507F**[1]
	MX-B476W	**MX-C407F**[1]
	MX-C303W[2]	**MX-C357F**[1]
	MX-C304W[2]	**MX-B557F**[1]
	MX-B355W	**MX-B467F**[1]
	MX-B455W	

Printer Models	MX-C607P	MX-B427W
	MX-C507P	MX-B427PW
	MX-C407P	MX-B467F
	MX-B707P	MX-B467P
	MX-B557P	

[1] For document scan, copy and native authentication:

- **Hard Disk Drive** is recommended (standard on MX-B557F and MX-C507F) and required to create searchable PDF scans from Synappx Go.
- **Hard Disk Drive** is required to support job accounting log for native authentication.
- Install the Synappx Go with ID Card embedded applications. For native authentication, all three apps (Synappx-Go_2012a.fls, keyboardreader-2.4.11.fls and cardAuth_2012a.fls) should be installed.

[2] These models support the Synappx Go/native integration feature but require that the MX-AMX2L Application Communications Module (ACM) option be installed.

Overview of Installation and Configuration Steps

The following is the recommended installation sequence when integrating Synappx Go with Native MFP Authentication. Details will be described in subsequent sections.

1. Install and configure Synappx Go system. See Synappx Go Admin Guide for details including normal Go web page setting confirmation and Synappx Go print release driver set up.
2. Configure rf IDEAS BLE Reader with rf IDEAS PC Prox Utility to support mobile credentials.
3. For Sharp A3 and A4 MFPs: Connect rf IDEAS Reader and configure each MFP
   a. Register and configure rf IDEAS Reader on MFPs to support ID cards
   b. Set up users for native authentication/log in locally, on-premise AD integration or LDAP integration (same as normal MFP configuration process)
   c. Configure MFP to support anonymous user printing (if users will be printing cloud files via Synappx Go)
   d. Install Synappx Go eOSA app in Sharp A3 and A4 OSA enabled MFPs *(note: goal is to support download eOSA app via App Portal at launch)*
4. For selected[1] Sharp A4 MFPs: Connect rf IDEAS Reader and configure each MFP
   a. Download and install three embedded apps on MFPs
   b. Configure A4 MFPs to support rf IDEAS and support ID Cards
   c. Add users for local log In
   d. Configure card authentication (for user authentication)
   e. User registration for local log in at A4 MFPs

   [1] A4 models: MX-C507F, MX-C407F, MX-C357F, MX-B557F, MX-467F
5. Complete user ID card number set up:
   a. Admin imports user and card ID CSV via the Admin Portal Users page or
   b. Manually enters user card numbers via the Users page or
   c. Users enter their own card numbers via Synappx Go mobile
6. Synappx Go and MFP native authentication integration complete and ready for use

Detailed Installation and Configuration Steps

1. Install and Configure Synappx Go System

See the Synappx Go Admin Guide for details on setting up the full Synappx Go system including agent installation, user and workspace configuration and NFC tag set up. See the Synappx Go User Guide for user mobile app set up and configuration.

Ensure the following web page setting are confirmed.

Configure MFP Web Page for Copy

To use Synappx Go for copying on a supported MFP, check the following MFP web page settings.

1. Go to **System Settings** > **Sharp OSA Settings** > **Condition Settings** on the MFP web page.
2. The following items must be checked.
   a. **Accept remote access request from application.**
   b. **Accept UI operation request from application.**
3. All other items on the **Condition Settings** page must be unchecked.
   a. Approve remote access request on operation panel.
   b. Display dialog of connection in Sharp OSA mode.
   c. Accept secondary send request from Sharp OSA application.

For MFP Embedded NFC Tags:

1. If using built-in NFC tags, modify the following MFP web page settings:
   - **Network Connections** > **Easy Connections Setting**: Enable NFC tag
   - **Network Settings** > **Quick Settings** > **Wireless Settings:** Set **Connection Type** to either **Wireless (Infrastructure Mode)** or **Wired + Wireless (Access Point Mode)**

   There are no MFP web page network setting changes for external NFC tags.

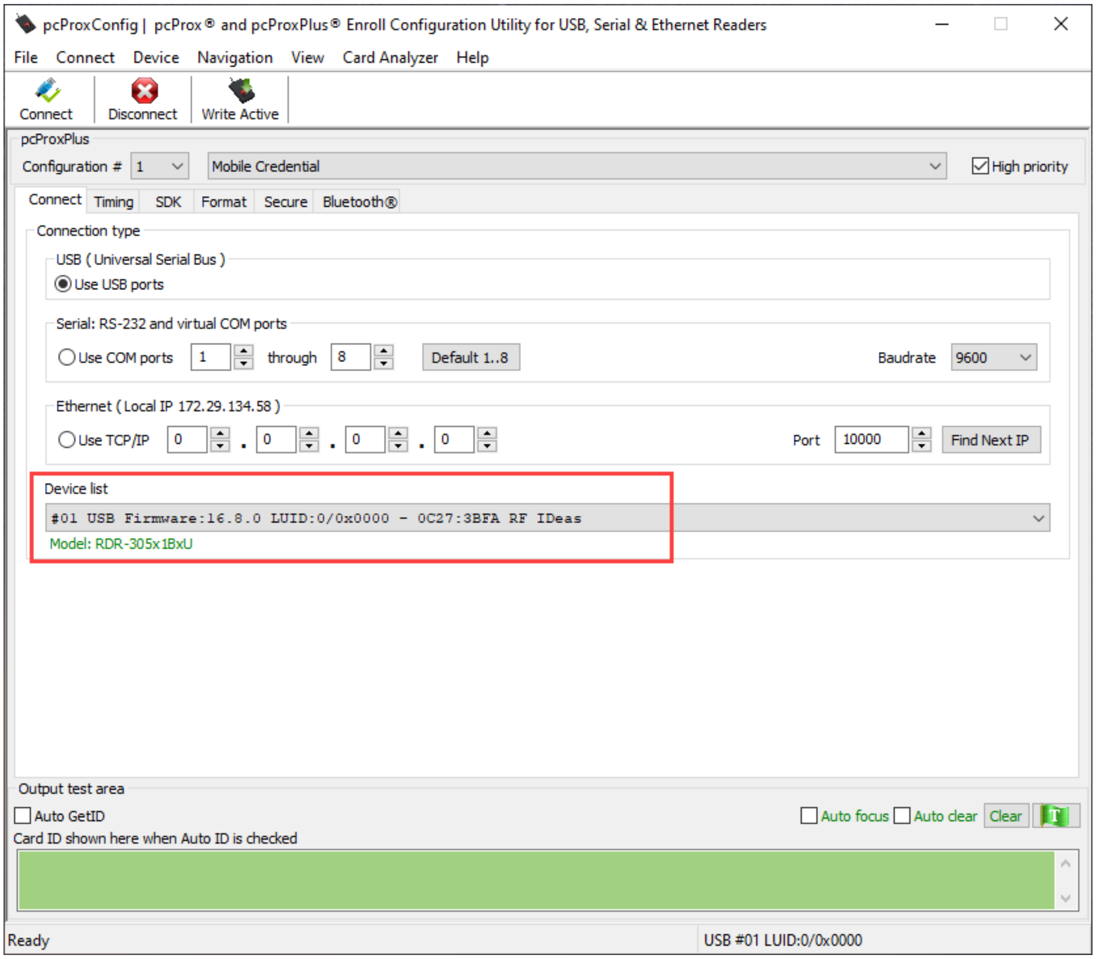
2. Configure rf IDEAS BLE Reader

The native authentication and Synappx Go integration relies on use of the BLE card reader from rf IDEAS. The supported model is RDR-30581BKU. The first step is to configure the rf IDEAS reader using their PC Prox Config Utility reader to support mobile credentials.

RF IDEAS BLE Reader Configuration

Configure the rf IDEAS reader with the following steps. The configuration utility can be found at RFID Reader Software Downloads | RF IDEAS.

1. Plug rf IDEAS card reader, model RDR-30581 BKU, into the USB port of the PC running the pcProxConfig utility.
2. Start **pcProxConfig.exe**
3. If reader is now shown under the **Device list**, select **Connect**.


pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers

File Connect Device Navigation View Card Analyzer Help
Connect
Disconnect
Write Active
Connect Timing SDK Format Secure Bluetooth®

pcProxPlus

Configuration # 1 | Mobile Credential | ☑ High priority

Connection type

USB (Universal Serial Bus)
● Use USB ports

Serial: RS-232 and virtual COM ports
○ Use COM ports 1 through 8 | Default 1..8 | Baudrate 9600

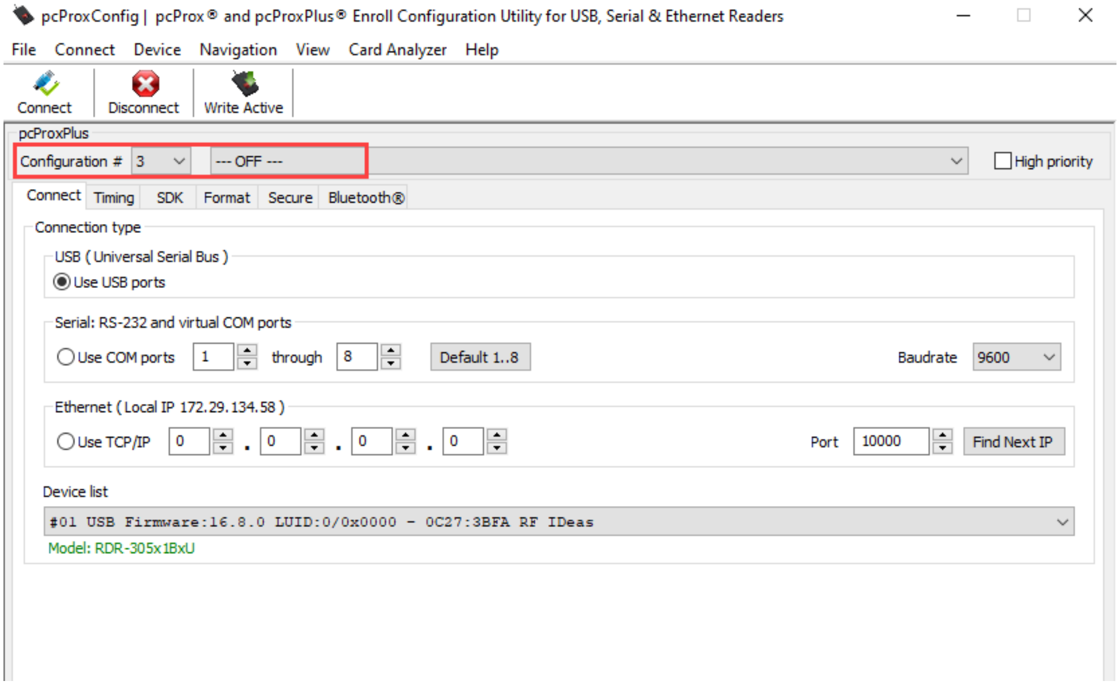
Ethernet (Local IP 172.29.134.58)
○ Use TCP/IP 0 . 0 . 0 . 0 | Port 10000 | Find Next IP

Device list
#01 USB Firmware:16.8.0 LUID:0/0x0000 - 0C27:3BFA RF IDeas
Model: RDR-305x1BxU

Output test area
□ Auto GetID | □ Auto focus □ Auto clear | Clear
Card ID shown here when Auto ID is checked

Ready | USB #01 LUID:0/0x0000

4. Turn **OFF** all configurations.


pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers

File Connect Device Navigation View Card Analyzer Help
Connect
Disconnect
Write Active
Connect Timing SDK Format Secure Bluetooth®

pcProxPlus

Configuration # 3 | --- OFF --- | □ High priority

Connection type

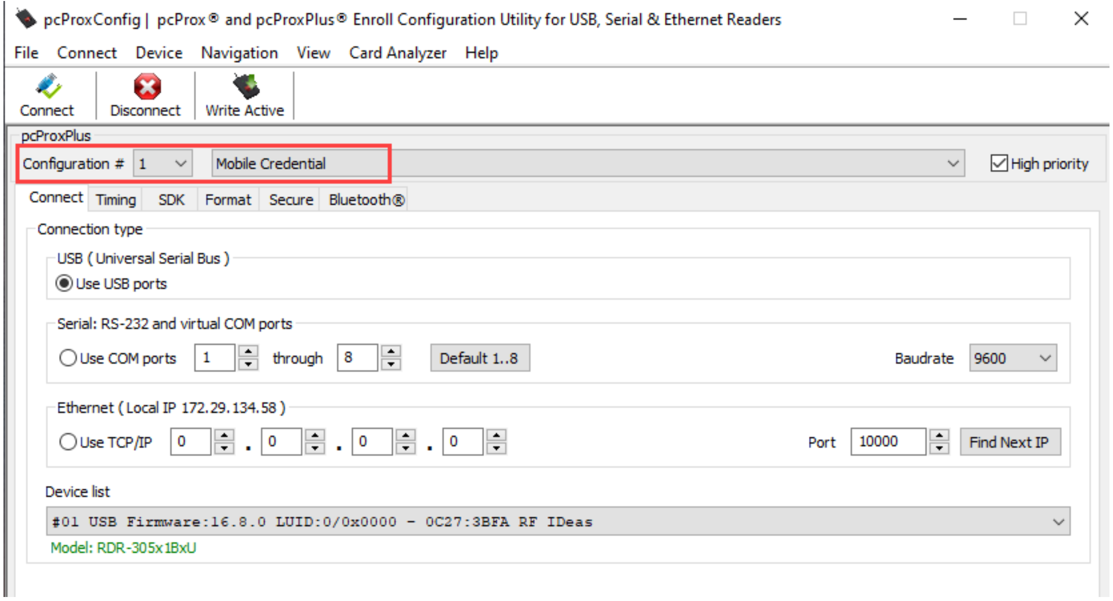
USB (Universal Serial Bus)
● Use USB ports

Serial: RS-232 and virtual COM ports
○ Use COM ports 1 through 8 | Default 1..8 | Baudrate 9600

Ethernet (Local IP 172.29.134.58)
○ Use TCP/IP 0 . 0 . 0 . 0 | Port 10000 | Find Next IP

Device list
#01 USB Firmware:16.8.0 LUID:0/0x0000 - 0C27:3BFA RF IDeas
Model: RDR-305x1BxU

5. Set Configuration #1 to **Mobile Credential.**



pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers

File Connect Device Navigation View Card Analyzer Help

Connect | Disconnect | Write Active

pcProxPlus

Configuration # 1 Mobile Credential ☑ High priority

Connect | Timing | SDK | Format | Secure | Bluetooth®

Connection type

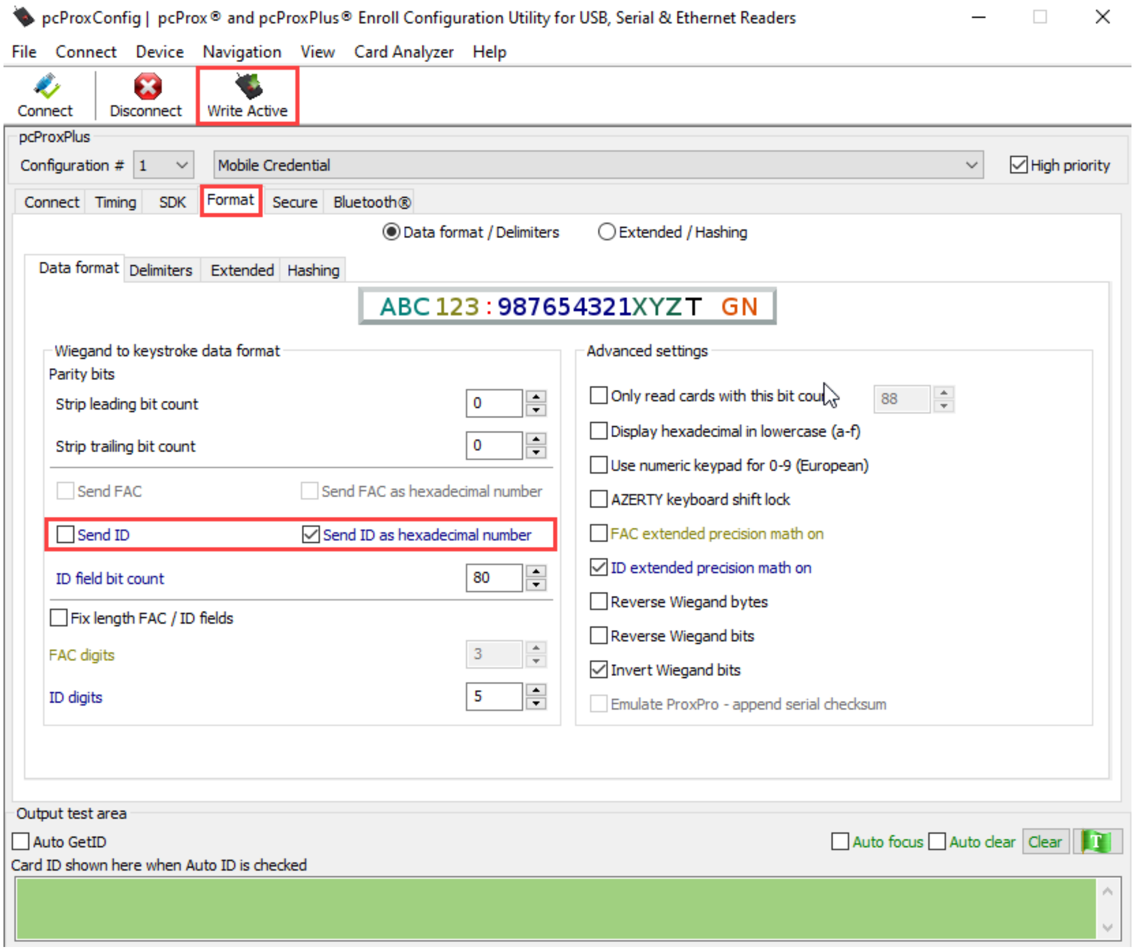
USB (Universal Serial Bus)
● Use USB ports

Serial: RS-232 and virtual COM ports
○ Use COM ports 1 through 8 Default 1..8 Baudrate 9600

Ethernet (Local IP 172.29.134.58)
○ Use TCP/IP 0 . 0 . 0 . 0 Port 10000 Find Next IP

Device list
#01 USB Firmware:16.8.0 LUID:0/0x0000 - 0C27:3BFA RF IDeas
Model: RDR-305x1BxU

6. Select Format tab.
7. Unselect **Send ID** then confirm that **Send ID as hexidecimal number** is selected. Select **Write Active.**



pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers

File Connect Device Navigation View Card Analyzer Help

Connect | Disconnect | Write Active

pcProxPlus

Configuration # 1 Mobile Credential ☑ High priority

Connect | Timing | SDK | Format | Secure | Bluetooth®

● Data format / Delimiters ○ Extended / Hashing

Data format | Delimiters | Extended | Hashing

ABC 123 : 987654321XYZT GN

Wiegand to keystroke data format
Parity bits
Strip leading bit count 0
Strip trailing bit count 0
□ Send FAC □ Send FAC as hexadecimal number
□ Send ID ☑ Send ID as hexadecimal number
ID field bit count 80
□ Fix length FAC / ID fields
FAC digits 3
ID digits 5

Advanced settings
□ Only read cards with this bit cou 88
□ Display hexadecimal in lowercase (a-f)
□ Use numeric keypad for 0-9 (European)
□ AZERTY keyboard shift lock
□ FAC extended precision math on
☑ ID extended precision math on
□ Reverse Wiegand bytes
□ Reverse Wiegand bits
☑ Invert Wiegand bits
□ Emulate ProxPro - append serial checksum

Output test area
□ Auto GetID □ Auto focus □ Auto clear Clear
Card ID shown here when Auto ID is checked

8. Select **Disconnect**. Card reader is now ready to add to MFP.

Notes:

- **To support multiple credential/card types for the rf IDEAS card reader, other configurations can be enabled in addition to the Mobile Credential. For instance, HID cards can be added on Configuration #2.** Some configurations may be incompatible with Mobile Credential. Please refer to rf IDEAS documentation.
- If desired, an optional harness can be ordered to attach the reader to the MFP.

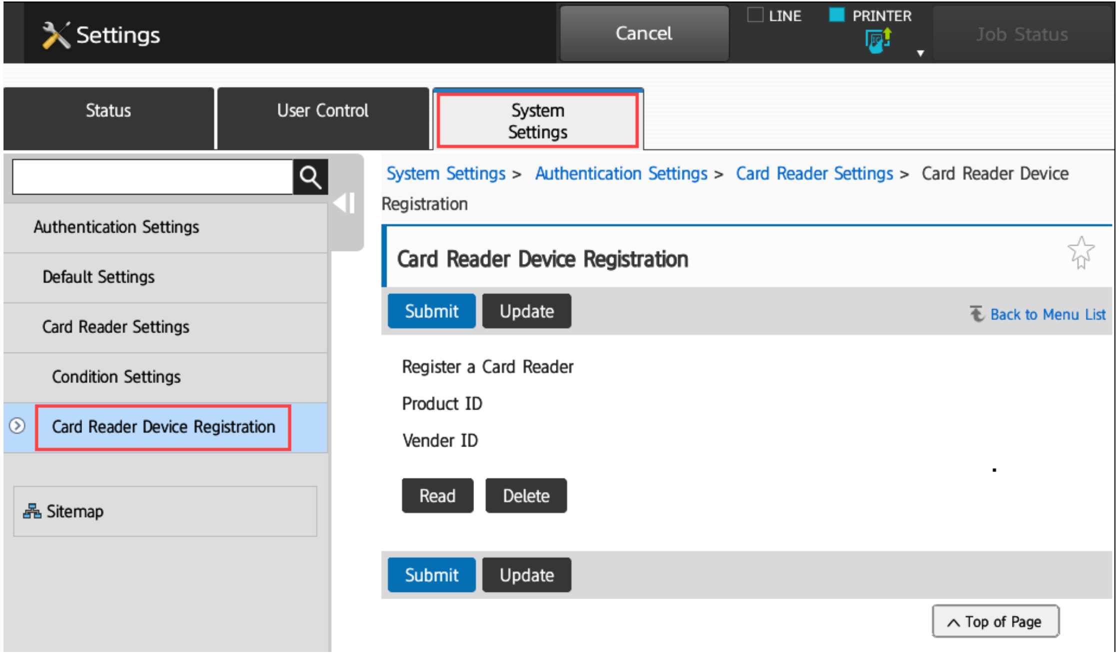
3. For Sharp A3/A4 MFPs: Connect rf IDEAS Reader and Configure Each MFP

Register and Configure rf IDEAS Reader

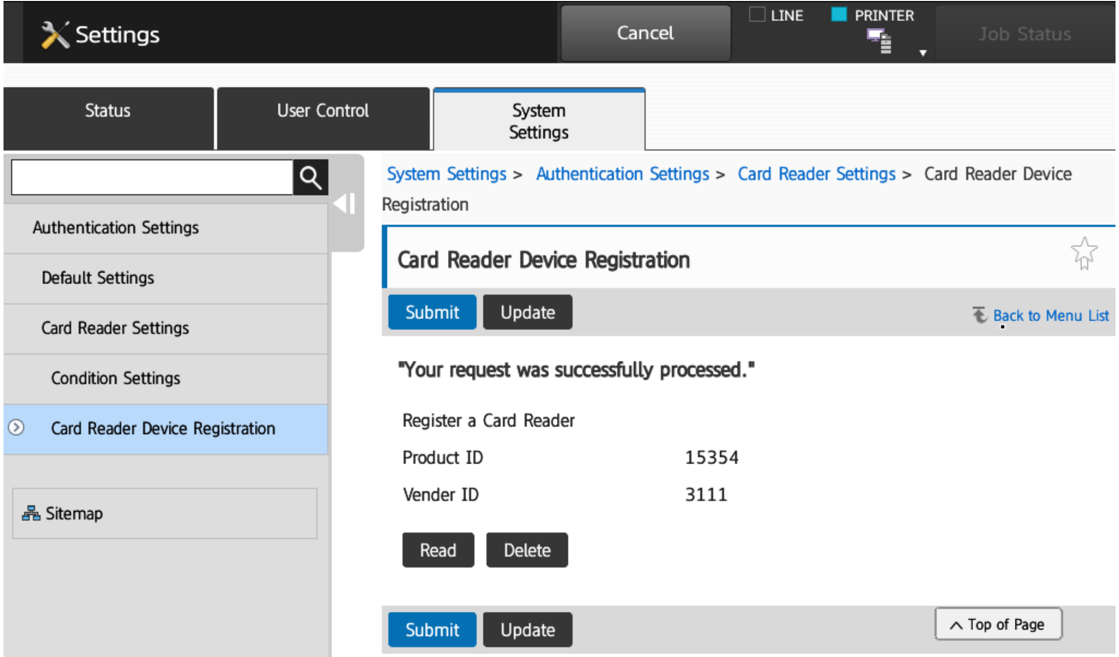
Once the rf IDEAS BLE card reader is configured, check to see if an existing or old card reader is registered to the MFP. If so, delete the existing reader registration.

Follow the steps below to connect the rf IDEAS BLE card reader, configure each MFP and register users.

1. Card registration can be done at the front panel. Login to MFP with Admin credentials. Navigate to **System Settings > Authentication Settings > Card Reader Settings > Card Reader Device Registration**.



2. Select **Read.** Connect rf IDEAS Card Reader to the USB port of the Sharp MFP. Verify **Product ID** and **Vendor ID** have identified themselves from the card reader. If okay, select **Submit.**



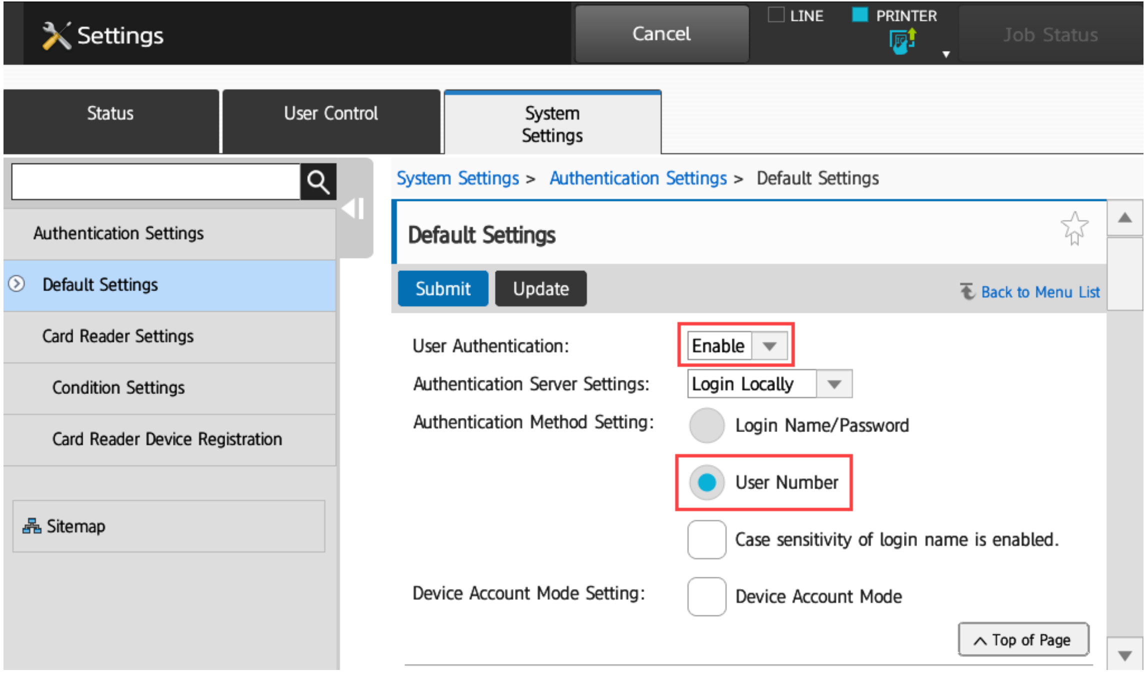
"Your request was successfully processed."

Register a Card Reader

Product ID 15354

Vender ID 3111

3. Navigate to **System Settings > Authentication Settings > Default Settings.** Set **User Authentication: Enable.** Select **Authentication Setting Method: User Number.**



User Authentication: Enable

Authentication Server Settings: Login Locally

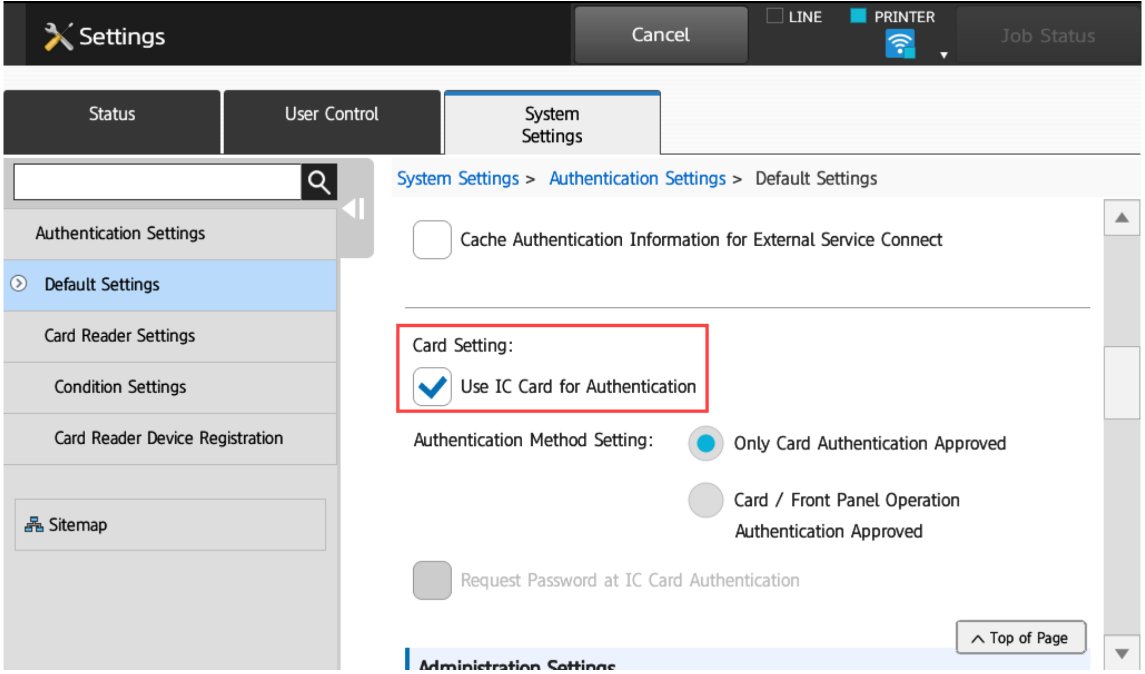
Authentication Method Setting: ○ Login Name/Password

● User Number

□ Case sensitivity of login name is enabled.

Device Account Mode Setting: □ Device Account Mode

4. Scroll down page and select **Use IC Card for Authentication**. Set **Card ID Registration/Change Authority: Enable**



□ Cache Authentication Information for External Service Connect

Card Setting:

☑ Use IC Card for Authentication

Authentication Method Setting: ● Only Card Authentication Approved ○ Card / Front Panel Operation Authentication Approved

□ Request Password at IC Card Authentication

The Card reader and ID card support are now configured.

Configure Native User Authentication Options and Users

The Admin needs to configure each MFP to support the native authentication and authorization. Refer to MFP documentation for details for setting up users for native authentication (1) local login (2) on-premise AD integration and (3) on-premise LDAP integration.

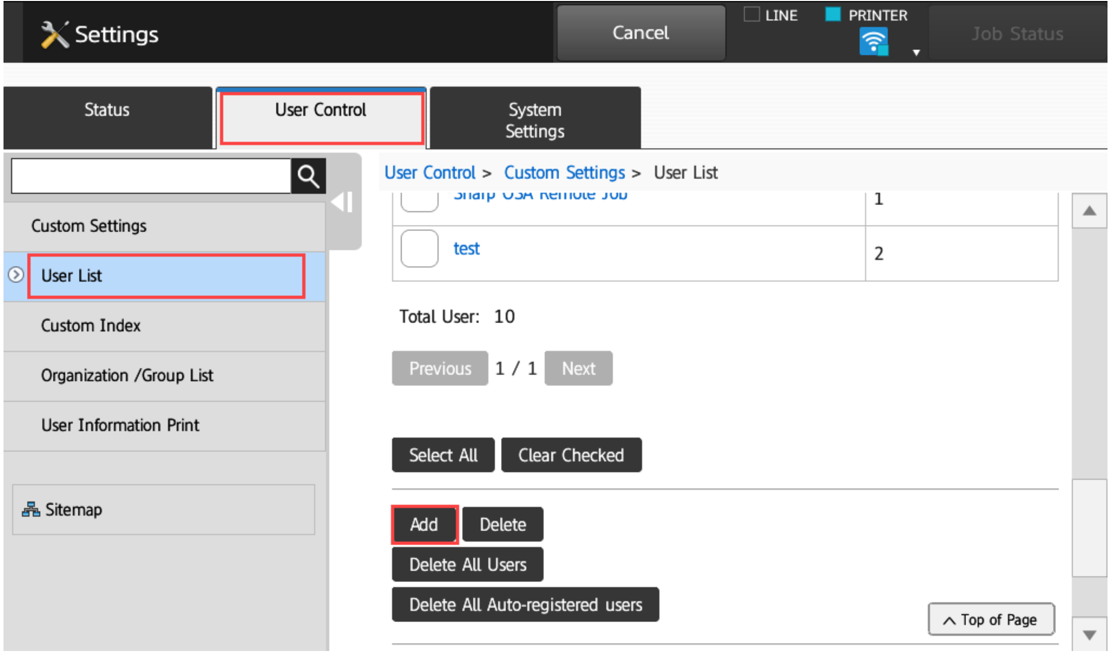
> Note: Local login can be configured on all supported Sharp MFPs. AD and LDAP integration is only available on Sharp A3 and A4 (OSA 5.5) models. Some A4 models (MX-C507F, MX-C407F, MX-C357F, MX-B557F, MX-467F) do not support AD or LDAP authentication with Synappx Go.

The following steps show an example of user card registration for native authentication/local log in.

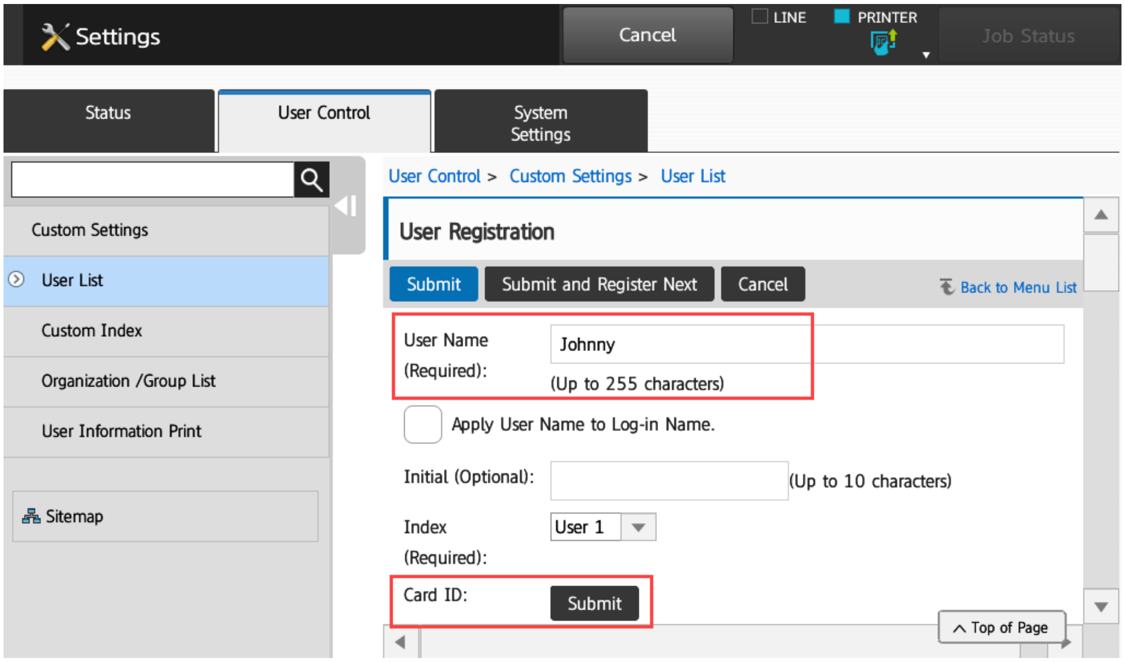
Reminder: The Synappx Go user ID (email) must match the user ID used for native authentication of any kind for Synappx Go integration.

To register each user and card ID at the front panel.

1. Navigate to **User Control > Custom Settings > User List.** Select **Add.**



2. Create user - enter value for **User Name**. Select Card ID: **Submit**



User Name (Required): Johnny (Up to 255 characters)

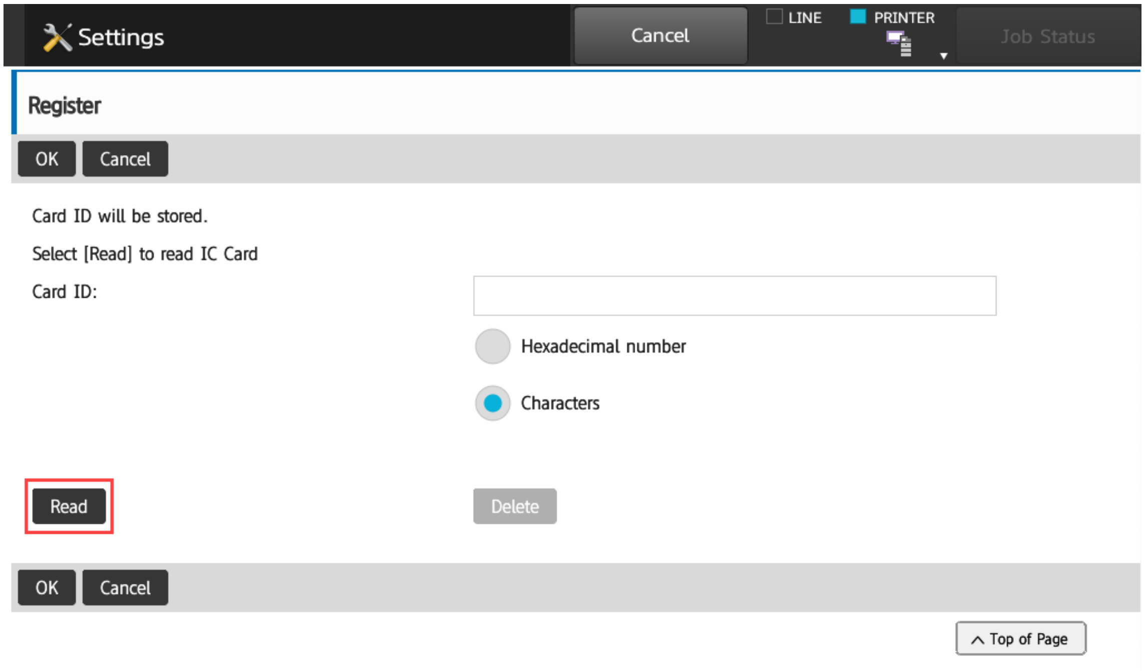
□ Apply User Name to Log-in Name.

Initial (Optional): (Up to 10 characters)

Index (Required): User 1

Card ID: Submit

3. Select **Read.**



Card ID will be stored.

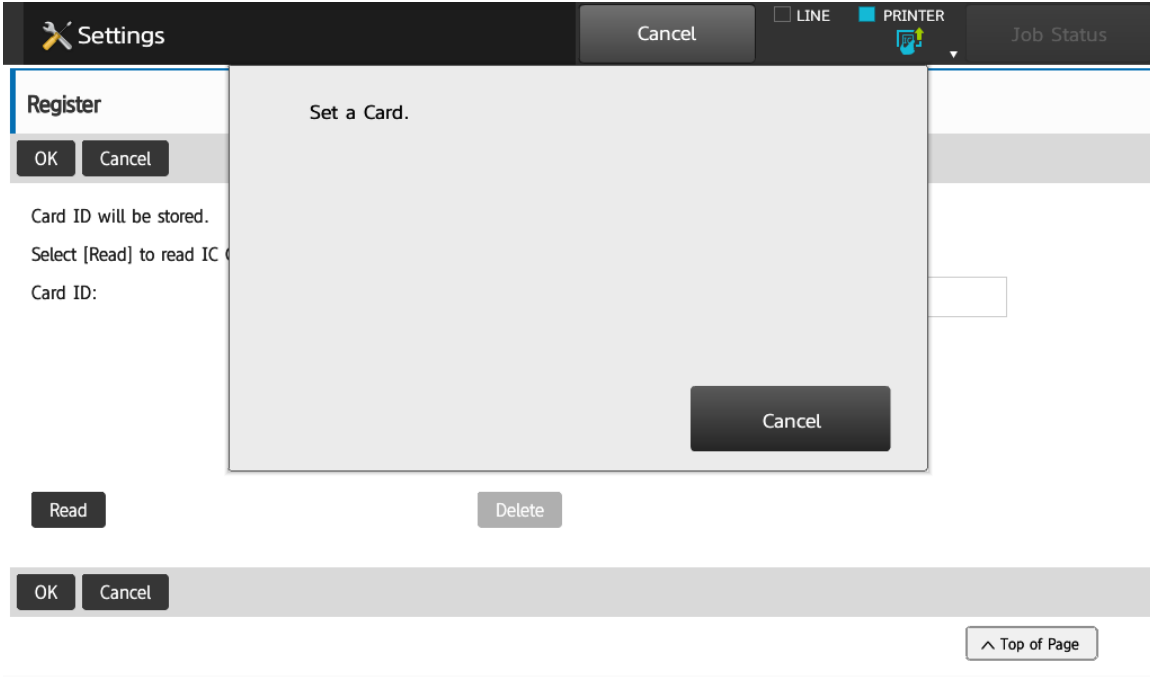
Select [Read] to read IC Card

Card ID:

○ Hexadecimal number

● Characters

4. Engage card reader using rf IDEAS BLE Reader by selecting **Unlock** on Synappx Go Mobile OR swipe user ID card to set card. Note: Native authentication requires card numbers with a minimum of five characters and a maximum of eight characters.



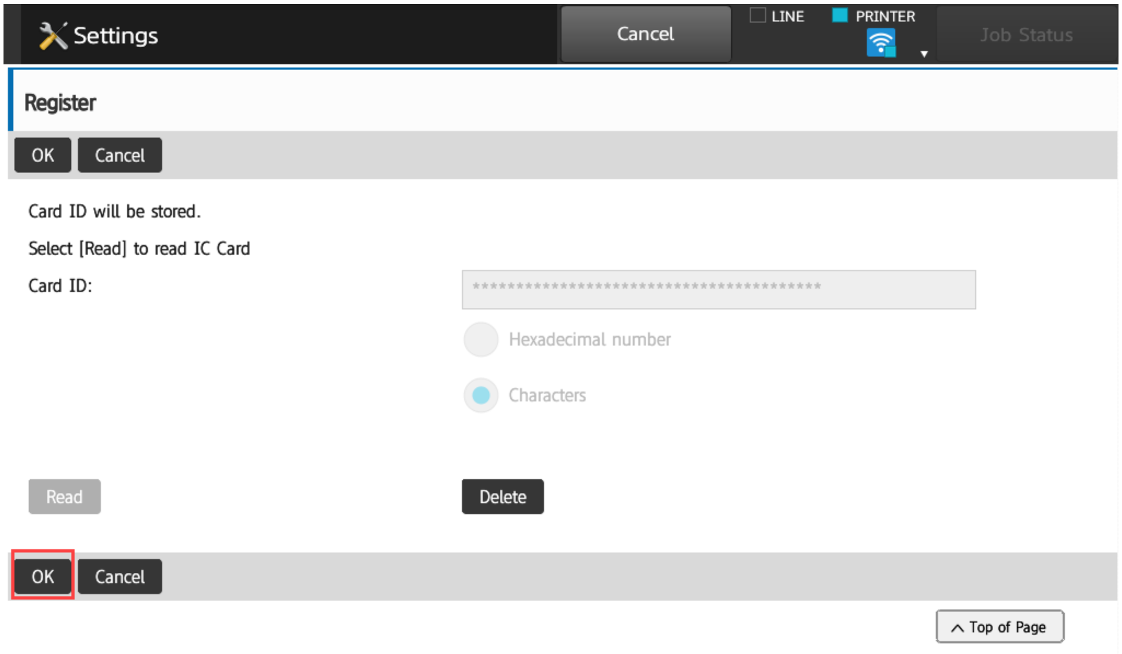
Set a Card.

Card ID will be stored.

Select [Read] to read IC

Card ID:

5. Select **OK.**



Card ID will be stored.

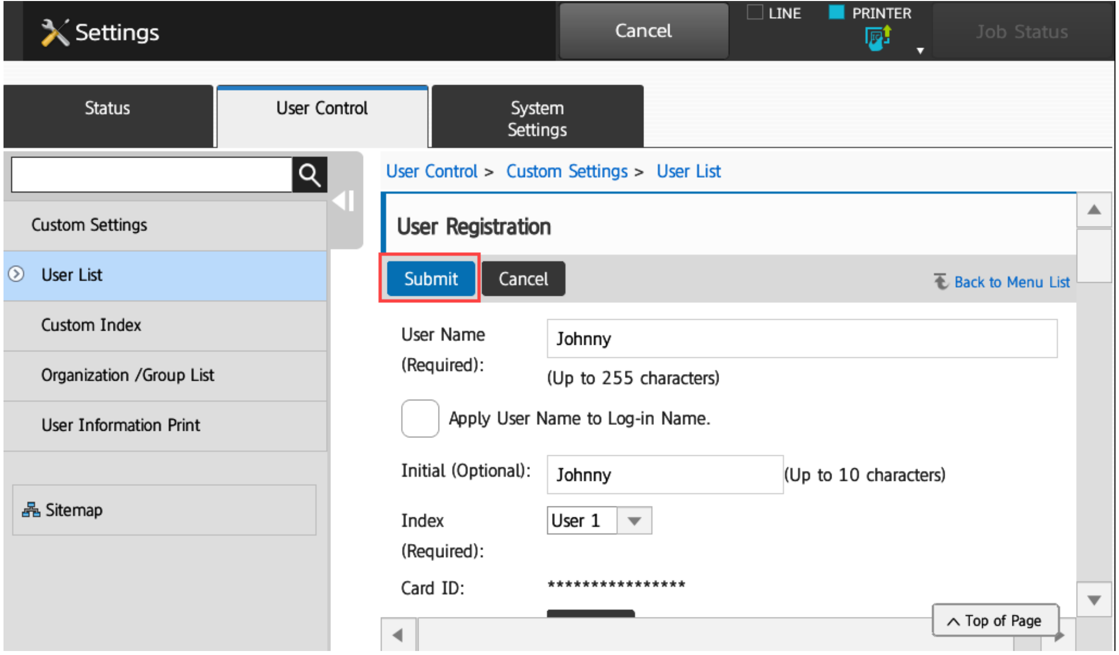
Select [Read] to read IC Card

Card ID: **

○ Hexadecimal number

● Characters

6. Select **Submit** to save. Repeat for other users.



User Name (Required): Johnny (Up to 255 characters)

□ Apply User Name to Log-in Name.

Initial (Optional): Johnny (Up to 10 characters)

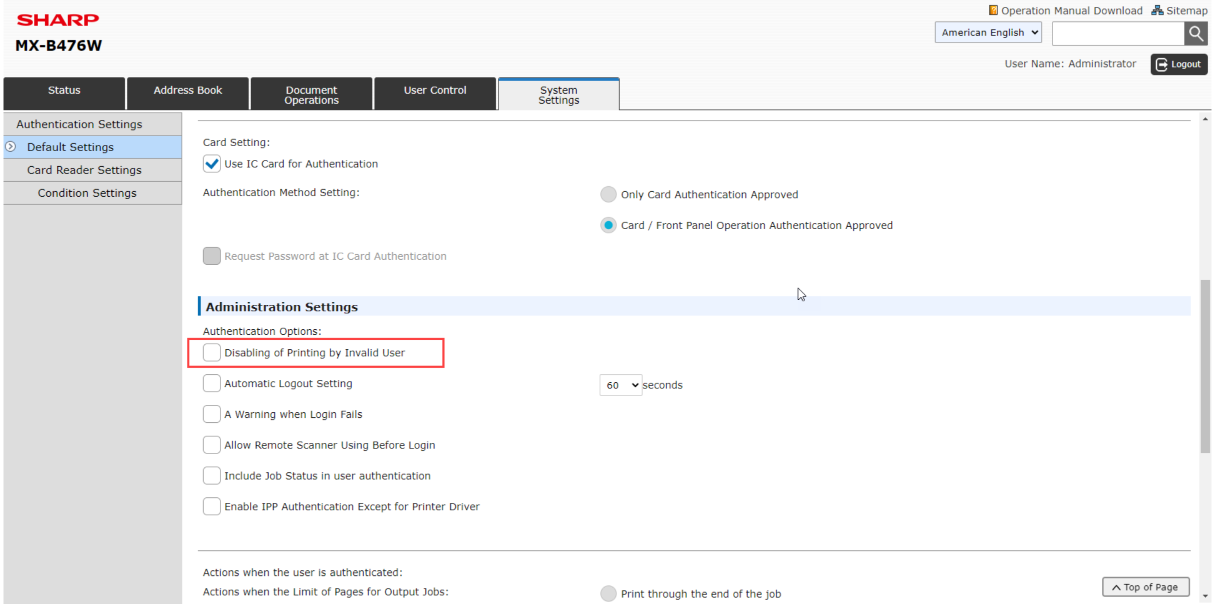
Index (Required): User 1

Card ID: ****************

Configure Support for Anonymous Printing

To support printing cloud files via Synappx Go, enable support for anonymous printing on the MFP web page. Note: Cloud print files will be accounted as untracked (not associated with Go user).

1. Log into MFP web page. **Browse to System Setting > Default Settings**. Ensure **Disabling of Printing by Invalid User** is unselected (unchecked).



Card Setting:

☑ Use IC Card for Authentication

Authentication Method Setting: ○ Only Card Authentication Approved ● Card / Front Panel Operation Authentication Approved

□ Request Password at IC Card Authentication

Administration Settings

Authentication Options:

□ Disabling of Printing by Invalid User

□ Automatic Logout Setting 60 seconds

□ A Warning when Login Fails

□ Allow Remote Scanner Using Before Login

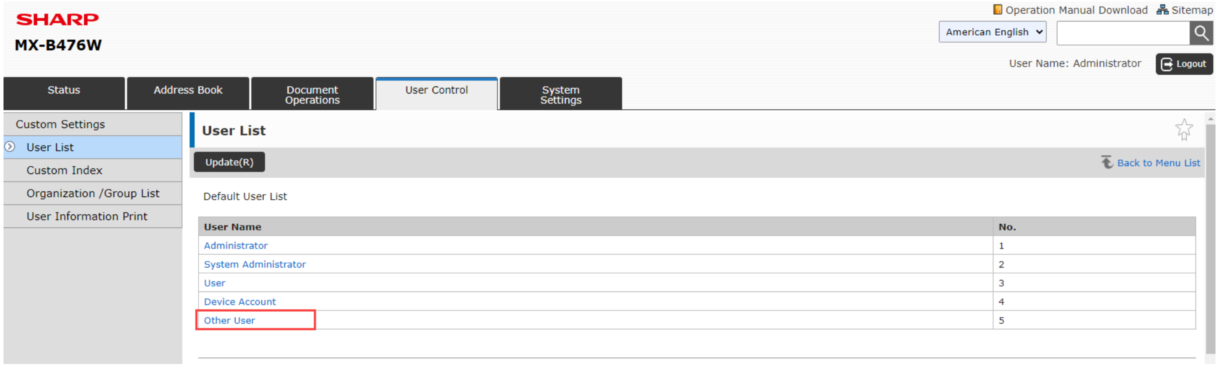
□ Include Job Status in user authentication

□ Enable IPP Authentication Except for Printer Driver

Actions when the user is authenticated:

Actions when the Limit of Pages for Output Jobs: ○ Print through the end of the job

2. Select **Other User.**

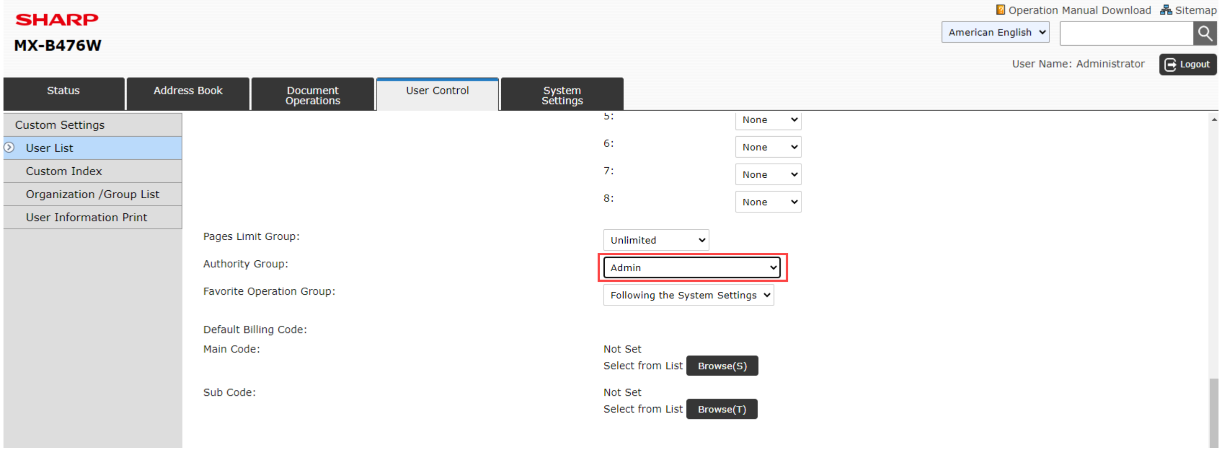


User List

Default User List

User Name	No.
Administrator	1
System Administrator	2
User	3
Device Account	4
Other User	5

3. For Authority Group, select **Admin.**



5: None

6: None

7: None

8: None

Pages Limit Group: Unlimited

Authority Group: Admin

Favorite Operation Group: Following the System Settings

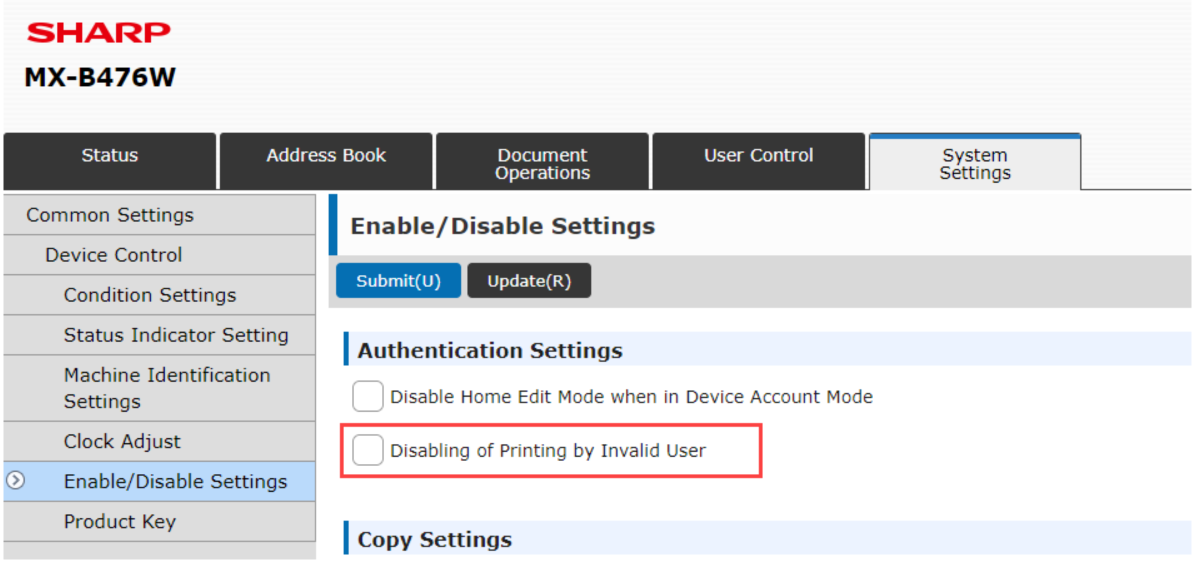
Default Billing Code:

Main Code: Not Set Select from List

Sub Code: Not Set Select from List

4. Reboot MFP.

Note: The setting to permit Synappx Go printing of cloud files can also be done on the **System Settings > Common Setting > Device Control > Enable/Disable Settings** web page. Process is the same as above (**Disabling of Printing by Invalid User** must be unchecked).


SHARP
MX-B476W

Status | Address Book | Document Operations | User Control | System Settings

Common Settings
Device Control
Condition Settings
Status Indicator Setting
Machine Identification Settings
Clock Adjust
Enable/Disable Settings
Product Key

Enable/Disable Settings

Submit(U) Update(R)

Authentication Settings

□ Disable Home Edit Mode when in Device Account Mode

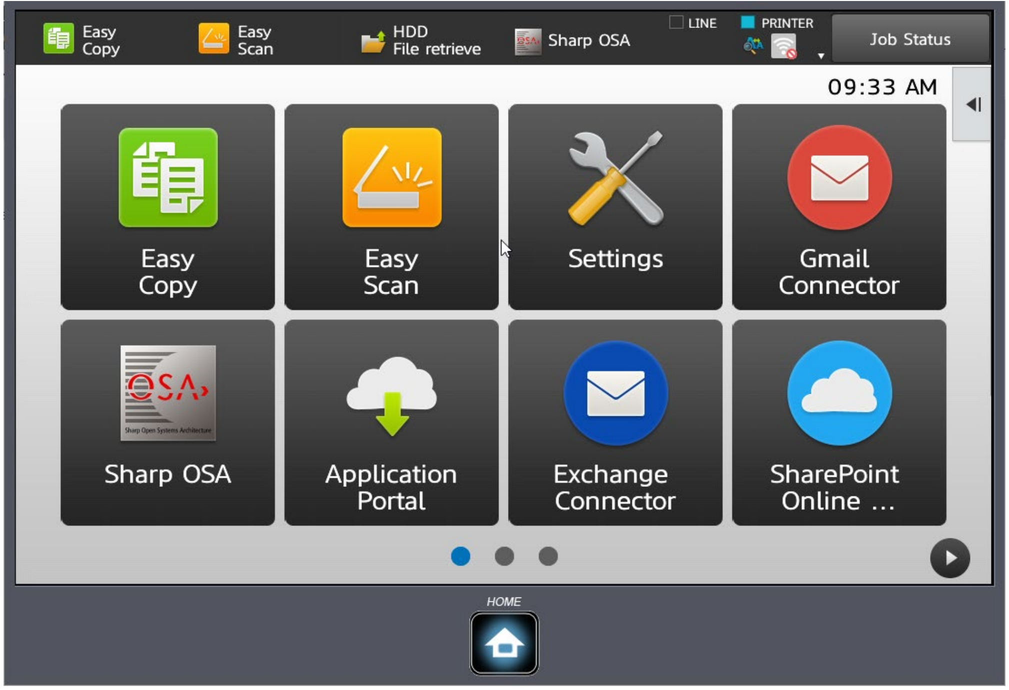
□ Disabling of Printing by Invalid User

Copy Settings

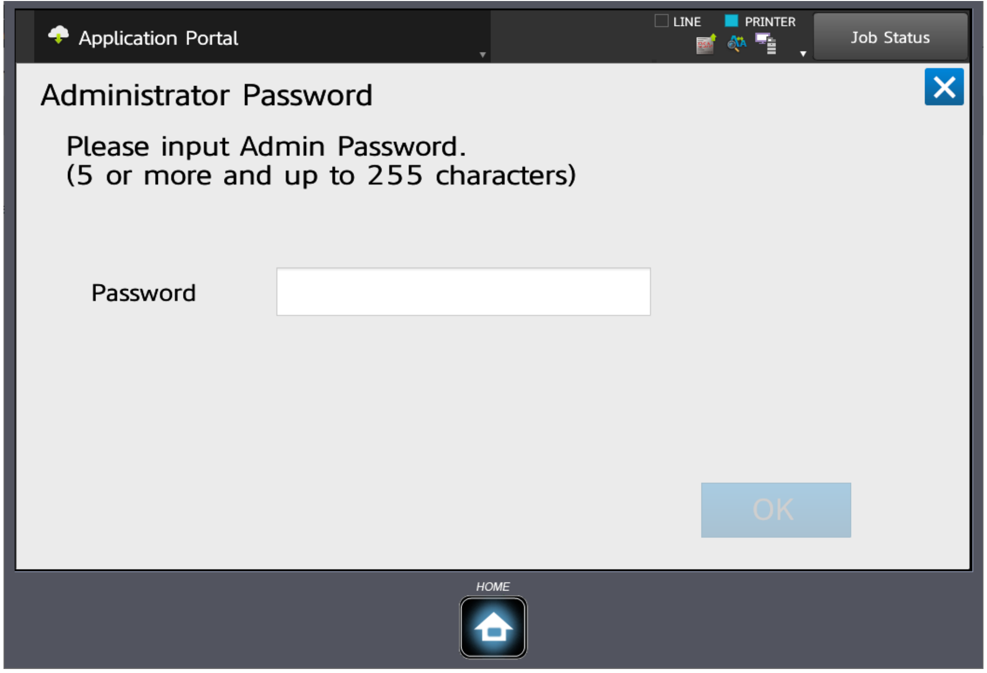
Install Synappx Go Embeded App

To support native integration with Synappx Go via the rf IDEAS reader, an embedded OSA app needs to be installed in each Synappx enabled A3 and selected A4 MFPs (OSA 5.5 support required).

1. From the MFP front panel, navigate to and **select Application Portal**.



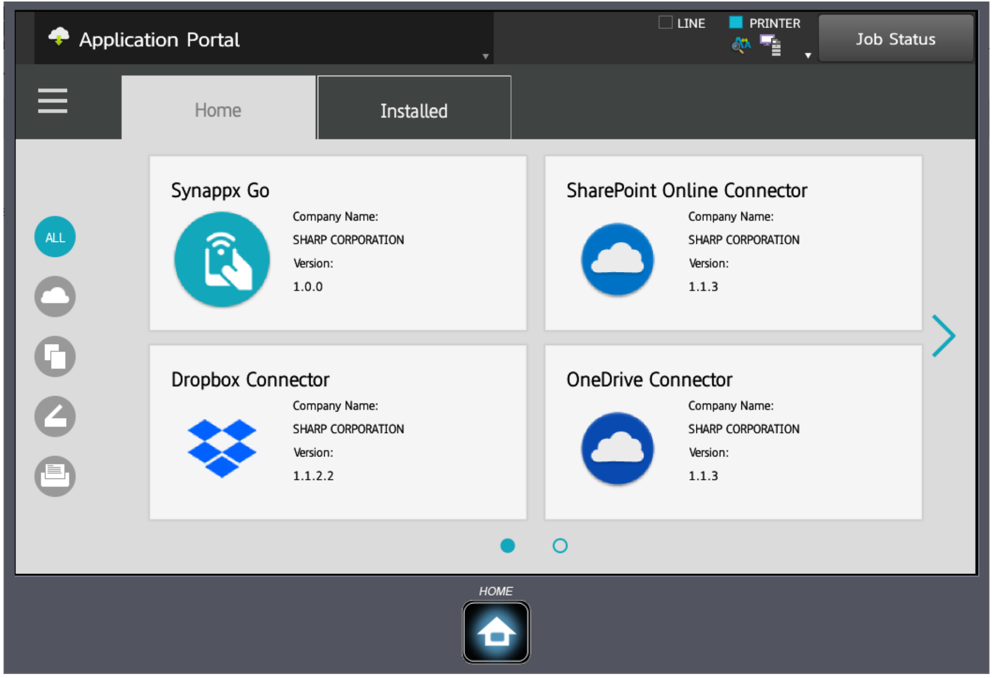
2. Enter Administrator password and select **OK.**



Administrator Password

Please input Admin Password.
(5 or more and up to 255 characters)

3. Browse to Synappx Go application and select.



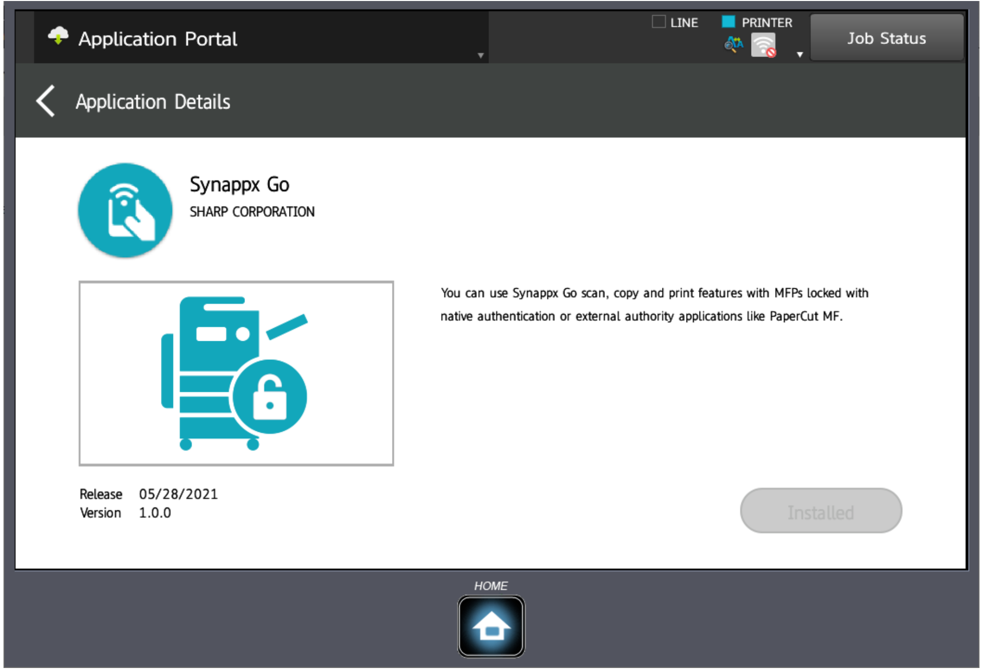
Synappx Go
Company Name:
SHARP CORPORATION
Version:
1.0.0

SharePoint Online Connector
Company Name:
SHARP CORPORATION
Version:
1.1.3

Dropbox Connector
Company Name:
SHARP CORPORATION
Version:
1.1.2.2

OneDrive Connector
Company Name:
SHARP CORPORATION
Version:
1.1.3

4. Confirm app and select **Install**.



You can use Synappx Go scan, copy and print features with MFPs locked with native authentication or external authority applications like PaperCut MF.

Release 05/28/2021
Version 1.0.0

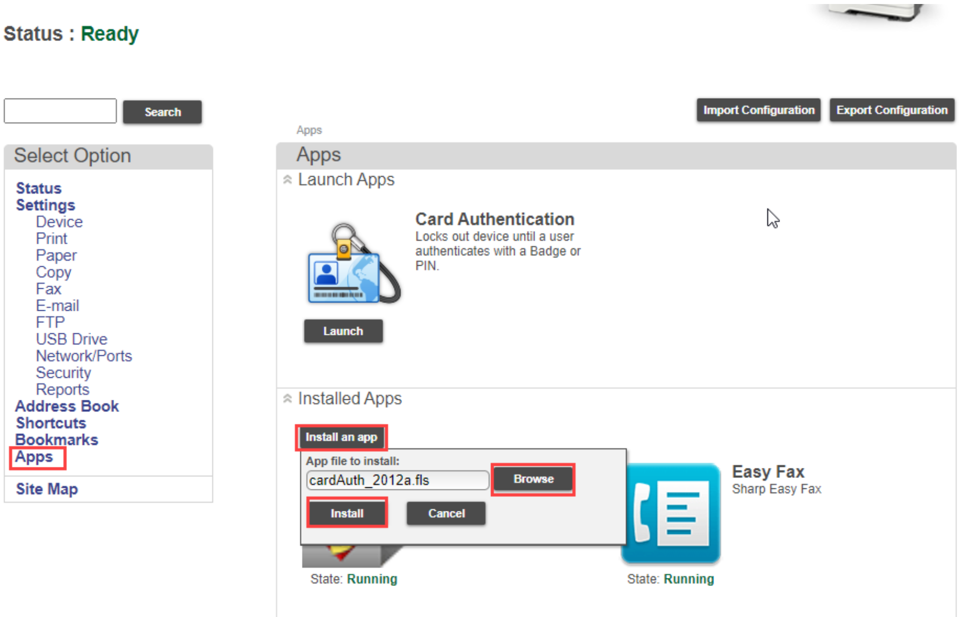
5. Synappx Go eOSA is ready to use with native authentication.

4. For Selected[1] Sharp A4 MFPs: Connect rf IDEAS Reader and Configure Each MFP

[1] MX-C507F, MX-C407F, MX-C357F, MX-B557F, MX-B467F

Download and Install A4 MFP Embedded Applications

1. Download the following MFP embedded apps from the Sharp web site to a local PC.
   a. Synappx Go 1.3.0. fls
   b. CardAuth_2012a.fls
   c. keyboardreader-2.4.11.fls
2. Log into the MFP web page and select **Apps**.
3. Select **Install** an app. Browse to location of the card authentication flash file, cardAuth_2012a.fls. Select **Install.**



Card Authentication: Locks out device until a user authenticates with a Badge or PIN.

App file to install: cardAuth_2012a.fls

State: Running

State: Running

4. Following the same installation steps, install the keyboard emulation card reader driver, (keyboardreader-2.4.11.fls) and Synappx Go 1.3.0.fls.

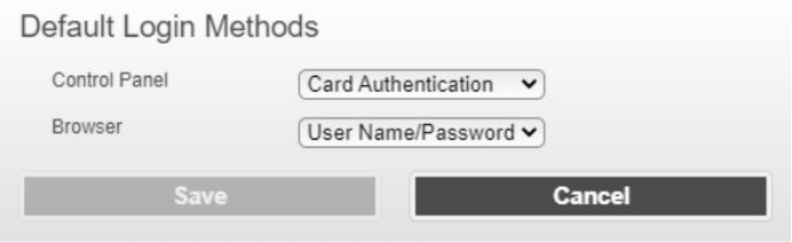
Note: If Omnikey 5427ck Reader Driver is installed, uninstall the Omnikey 5427ck Reader Driver app.

Configure A4 MFPs to Support rf IDEAS and ID Card Support

The Admin needs to configure each A4 MFP to support the native authentication/local login. Note: Native authentication via AD and LDAP integration is only available on Sharp A3 and other A4 models.

Set Default Login Methods

1. Browse to **Security > Login Methods**.
2. Select **Change** beside Default Control Panel Login Method.
3. In the Control Panel menu, select **Card Authentication.**



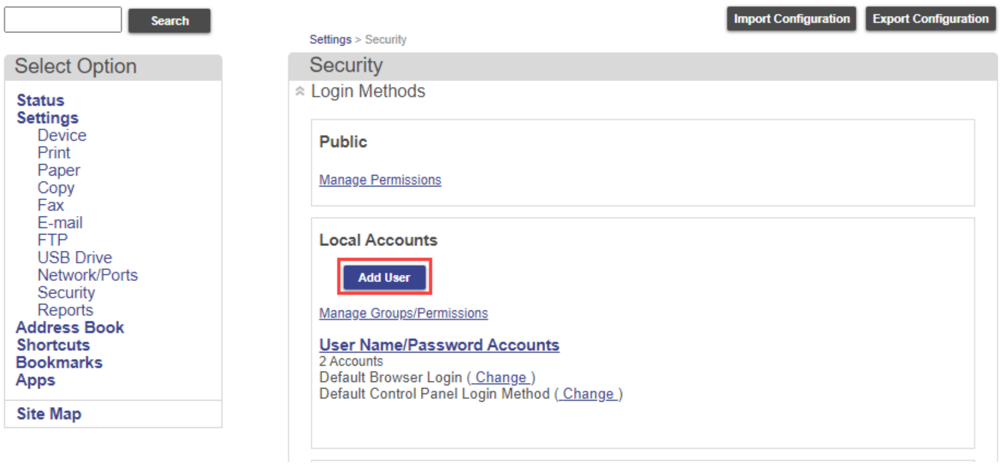
Control Panel: Card Authentication

Browser: User Name/Password

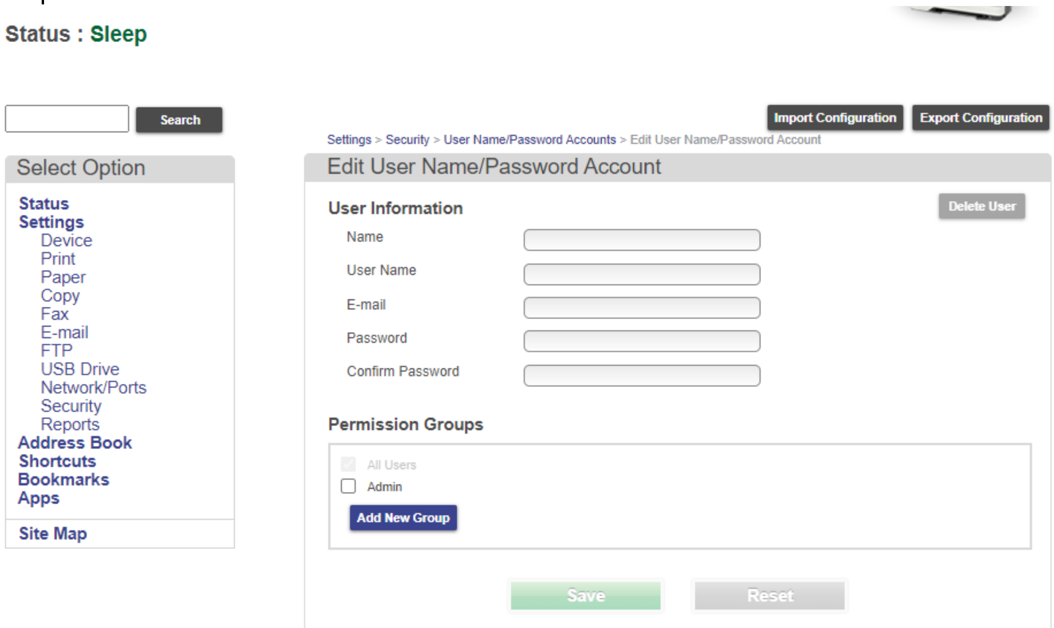
4. Click **Save.**

Add Users for Local Log In

1. Settings **Settings** > **Security.**
2. Under Local Accounts select **User Name/Password Accounts**.
3. Select **Add User**.



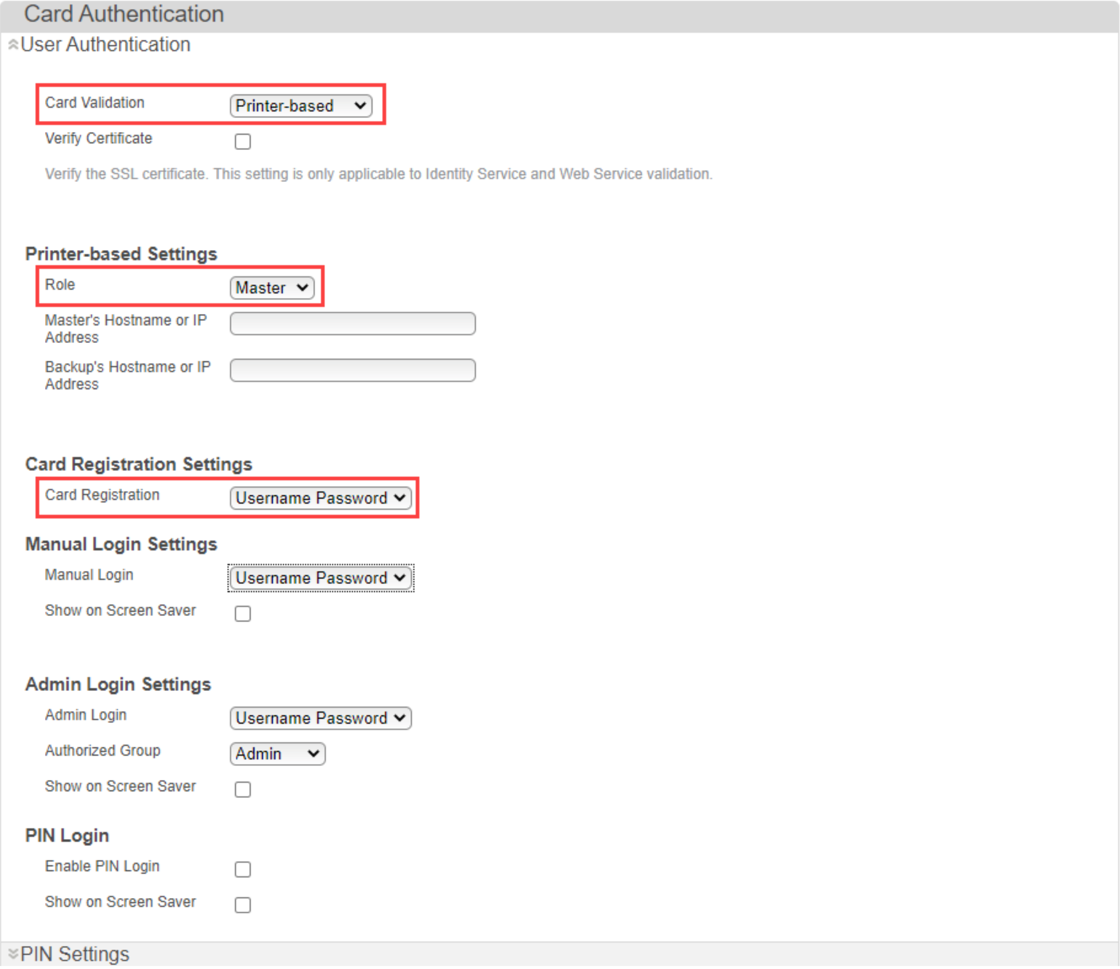
4. Complete user information and select **Save**.



5. User is ready to self-registration card info at the A4 MFP front panel.
6. Repeat for other users.

Configure Card Authentication (User Authentication)

1. Browse to **Card Authentication** > **User Authentication** page. For Card Validation, select **Printer-based**.
2. For Printer-based Settings, select Role: **Master.**
3. For Card Registration Settings, select **Username Password.**



Card Authentication

User Authentication

Card Validation: Printer-based

Verify Certificate □

Verify the SSL certificate. This setting is only applicable to Identity Service and Web Service validation.

Printer-based Settings

Role: Master

Master's Hostname or IP Address:

Backup's Hostname or IP Address:

Card Registration Settings

Card Registration: Username Password

Manual Login Settings

Manual Login: Username Password

Show on Screen Saver □

Admin Login Settings

Admin Login: Username Password

Authorized Group: Admin

Show on Screen Saver □

PIN Login

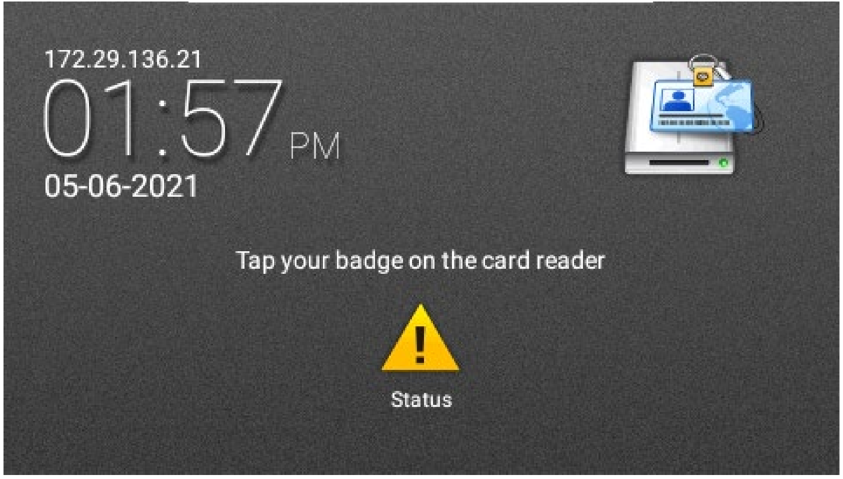
Enable PIN Login □

Show on Screen Saver □

PIN Settings

User Registration for Local Log In at A4 MFPs

1. User unlocks the MFP using Synappx Go mobile app in proximity to A4 MFP.



172.29.136.21

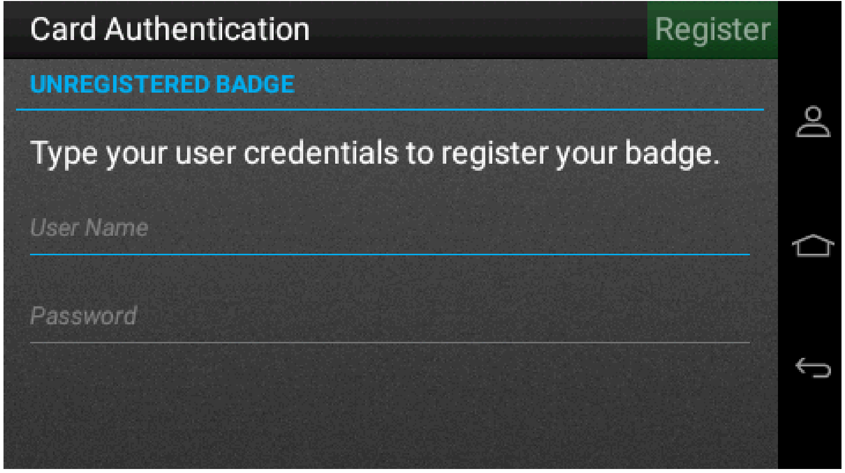
01:57 PM

05-06-2021

Tap your badge on the card reader

Status

2. To register, user enters username and password. Select **Register.**



Type your user credentials to register your badge.

5. Complete User ID Card Number Set Up

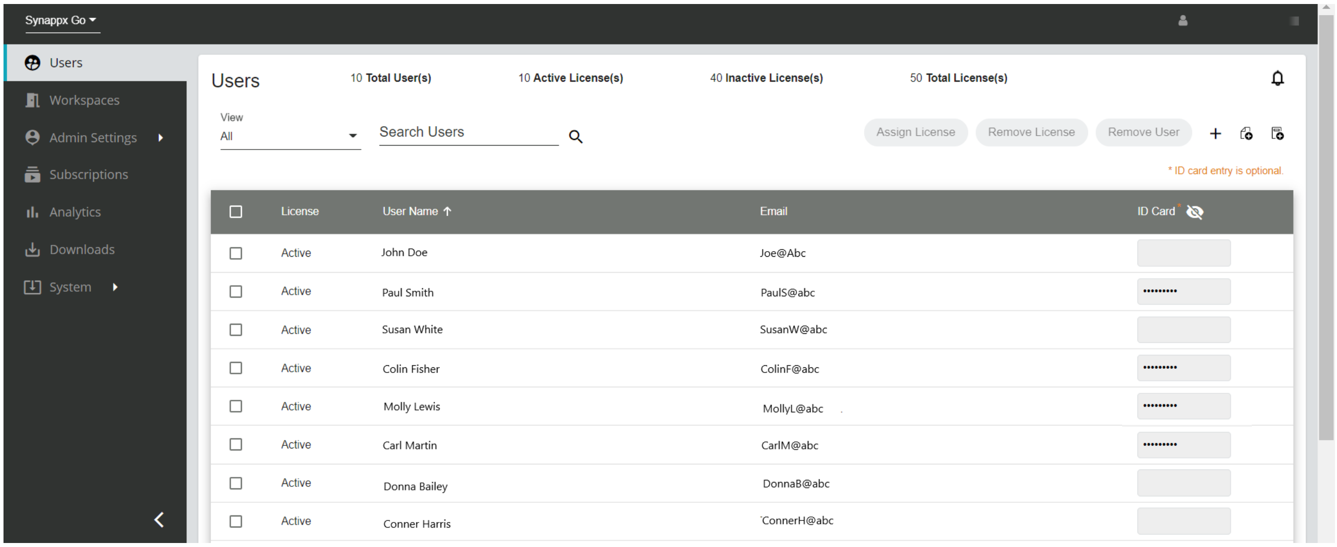
There are three ways that user ID card numbers can be added to the Synappx system to enable MFP Native Authentication and Synappx Go integration.

1. Admin manually enters user card numbers via the Users page OR
2. Admin imports a CSV file with the user names, user ID (email addresses) and ID card numbers via the Admin Portal Users page OR
3. Users enter their own card numbers via Synappx Go mobile (also included in User Guide)

Reminder: The user ID (email address) used in Native Authentication and Synappx Go must be the same.

Admin Portal User ID Card Entry (Manual or Import Via CSV)

The Synappx Admin Portal Go Users page now includes a “ID Card” column with entry fields for user ID card numbers. The card numbers are hidden by default but can be viewed by selecting the “eye” icon at the top of the column or during entry. If an Admin views the ID card number(s), there is an entry in the Admin Log.

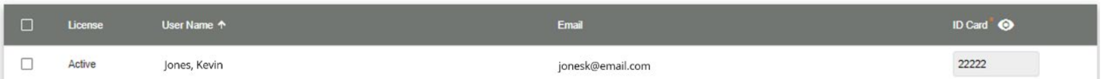


* ID card entry is optional.

☐	License	User Name ↑	Email	ID Card
☐	Active	John Doe	Joe@Abc	
☐	Active	Paul Smith	PaulS@abc	•••••••••
☐	Active	Susan White	SusanW@abc	
☐	Active	Colin Fisher	ColinF@abc	•••••••••
☐	Active	Molly Lewis	MollyL@abc	•••••••••
☐	Active	Carl Martin	CarlM@abc	•••••••••
☐	Active	Donna Bailey	DonnaB@abc	
☐	Active	Conner Harris	ConnerH@abc	

Card numbers can be manually entered, changed and/or deleted via direct entry in the field for each user. To enter a card manually:

1. Select the **eye icon** at the top of the column to see the text as you type.
2. Type in the card number (limit of 38 characters except for local login which has a limit of 5 to 8 character limit). **Select the check mark icon** to save the entry.



☐	License	User Name ↑	Email	ID Card
☐	Active	Jones, Kevin	jonesk@email.com	22222

3. Repeat for each user ID card number.

To edit a card number, backspace to correct or change the number. **Select the check mark icon** to save the change. To revert to previous entry before saving, select the x icon.

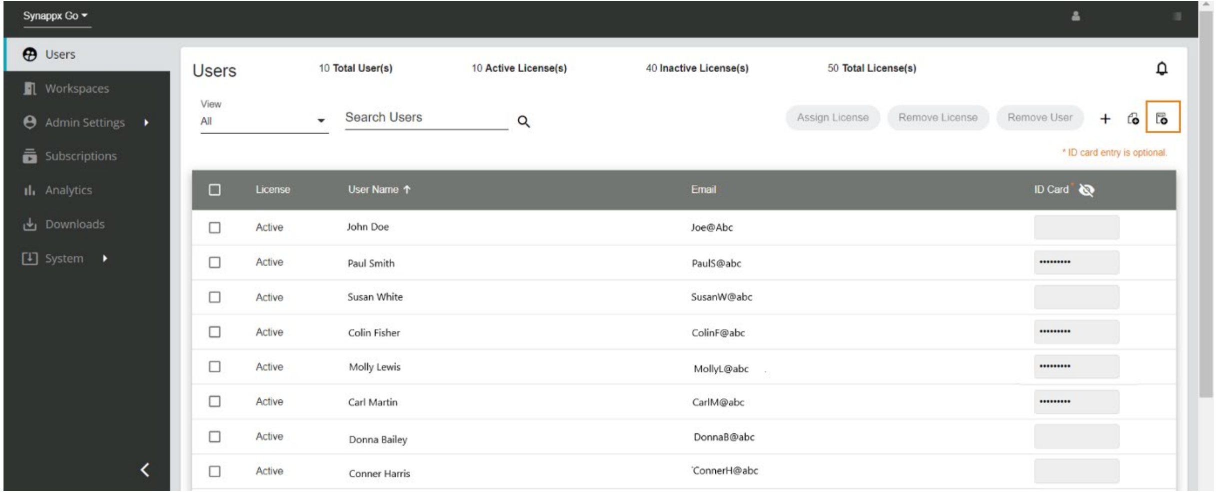
To delete a card number, backspace to empty the field and **select the check mark icon** to save the change.

Alternatively, the Admin can import a csv file with the user names, email addresses and card IDs. **The csv file name should be named "user_list.csv" and should contain columns called "Full Name," "Email" and "Primary Card Number."** In addition, the file to be imported cannot have any records for any of the three required columns that are blank. Before importing, remove any records with blank content.

The Admin must have already added Synappx users to the Admin Portal Users page via import from either Azure AD or Google.

To import the **user_list.csv** file:

1. Select the new “Import card numbers for users” icon.



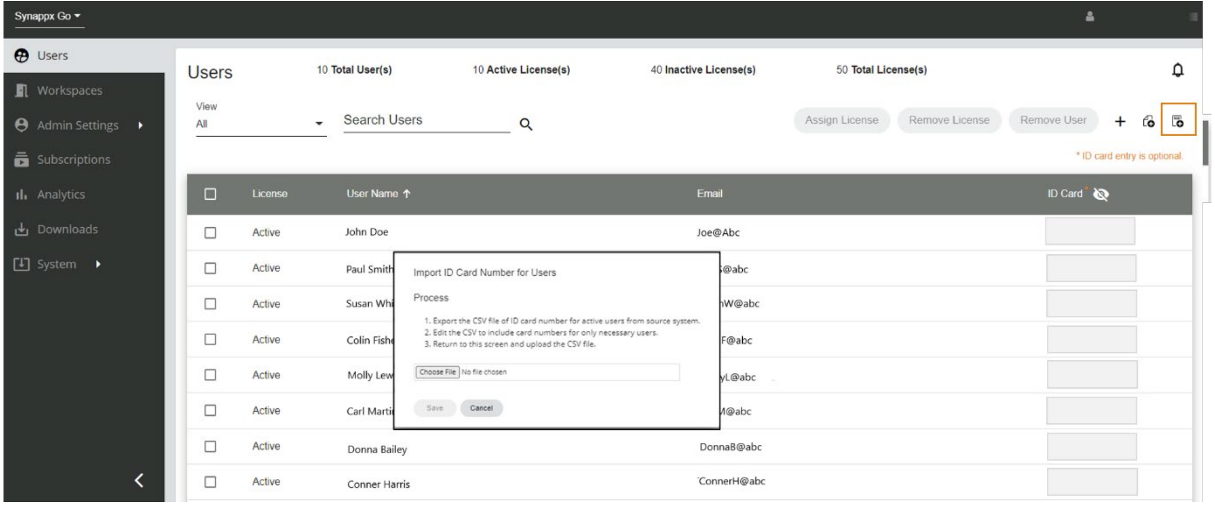
Users 10 Total User(s) 10 Active License(s) 40 Inactive License(s) 50 Total License(s)

View All | Search Users

* ID card entry is optional.

□	License	User Name ↑	Email	ID Card
□	Active	John Doe	Joe@Abc	
□	Active	Paul Smith	PaulS@abc	•••••••••
□	Active	Susan White	SusanW@abc	
□	Active	Colin Fisher	ColinF@abc	•••••••••
□	Active	Molly Lewis	MollyL@abc	•••••••••
□	Active	Carl Martin	CarlM@abc	•••••••••
□	Active	Donna Bailey	DonnaB@abc	
□	Active	Conner Harris	ConnerH@abc	

2. Browse to the location with the csv file and select **Save** to begin the content import.



Users 10 Total User(s) 10 Active License(s) 40 Inactive License(s) 50 Total License(s)

View All | Search Users

* ID card entry is optional.

Import ID Card Number for Users

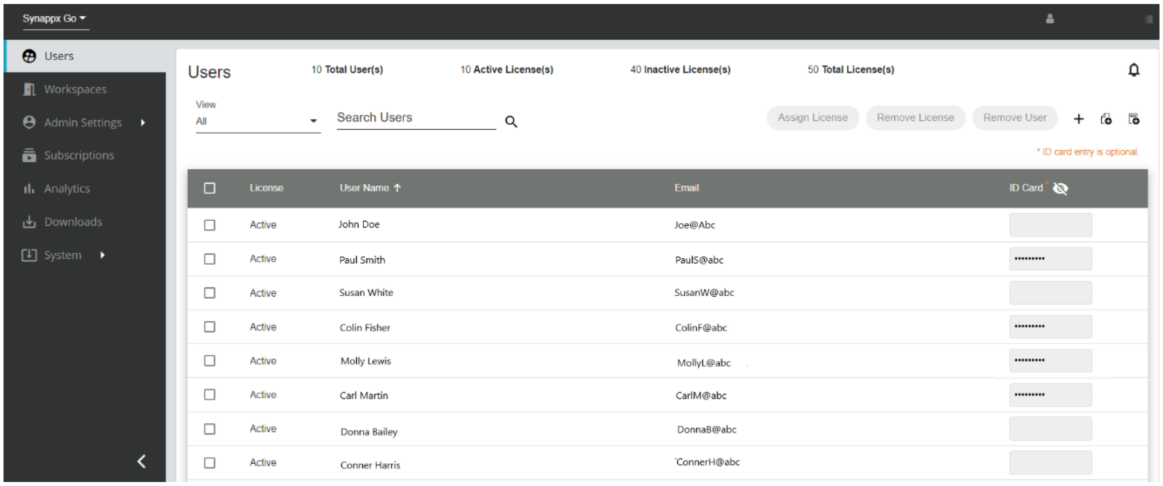
Process

1. Export the CSV file of ID card number for active users from source system.
2. Edit the CSV to include card numbers for only necessary users.
3. Return to this screen and upload the CSV file.

Choose File No file chosen

□	License	User Name ↑	Email	ID Card
□	Active	John Doe	Joe@Abc	
□	Active	Paul Smith	S@abc	
□	Active	Susan Whi	hW@abc	
□	Active	Colin Fishe	F@abc	
□	Active	Molly Lew	yL@abc	
□	Active	Carl Marti	M@abc	
□	Active	Donna Bailey	DonnaB@abc	
□	Active	Conner Harris	ConnerH@abc	

3. The import operation will add the card ID numbers to the page for all matched users. Note: users in the csv file that are not Synappx Go users will not be added to the Users page.



Users

10 Total User(s) | 10 Active License(s) | 40 Inactive License(s) | 50 Total License(s)

View: All

Search Users

* ID card entry is optional.

☐	License	User Name ↑	Email	ID Card *
☐	Active	John Doe	Joe@Abc	
☐	Active	Paul Smith	PaulS@abc	•••••••••
☐	Active	Susan White	SusanW@abc	
☐	Active	Colin Fisher	ColinF@abc	•••••••••
☐	Active	Molly Lewis	MollyL@abc	•••••••••
☐	Active	Carl Martin	CarlM@abc	•••••••••
☐	Active	Donna Bailey	DonnaB@abc	
☐	Active	Conner Harris	ConnerH@abc	

The card numbers entered, updated or deleted by manual or csv import will be sent to each user's mobile device for local storage and will be visible to the user under the following three conditions:

- Mobile user logs in the Synappx Go app
- Mobile user restarts the Synappx Go app
- Within 60 minutes after Admin entry

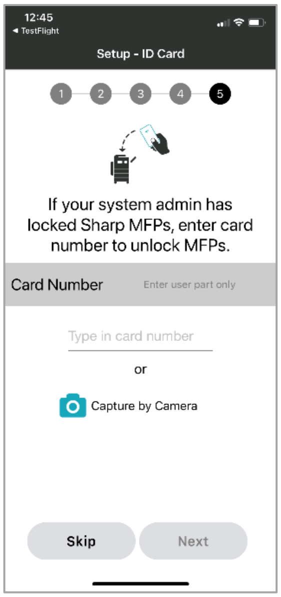
Alternative: User Entry of ID Card Numbers

To use Synappx Go mobile features with native locked MFPs, users can also enter their ID card numbers via the Synappx Go Mobile App. There are two ways for users to enter the card numbers:

- During initial Synappx Go wizard set up
- After initial set up via the **ID Card** page under **Settings**

After installing the Synappx Go mobile app, the user has the option to enter the ID card number as the last step of the wizard. The user can also skip this page if they don't need or want to access native locked MFPs.

1. After completing (or skipping) other wizard steps, enter the ID card number either by manual entry with the keyboard or via camera capture.



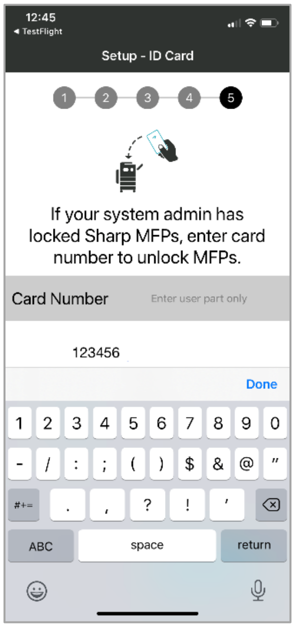
If your system admin has locked Sharp MFPs, enter card number to unlock MFPs.

Card Number Enter user part only

Type in card number

or

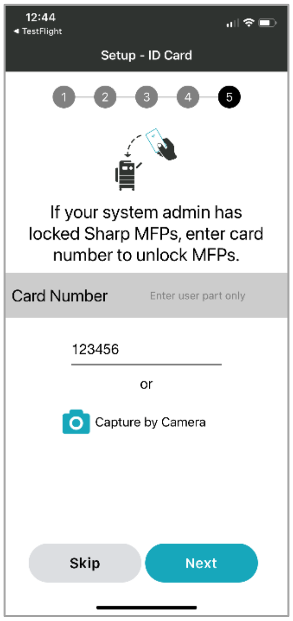
2. Manual entry: Touch the entry field and type user ID card number from Prox or iClass ID card via the keyboard. A maximum of 38 characters can be supported except native local login supports only five to eight characters.
   Note: Only include the user portion of the card number. Press **Next** to accept the number and finish the wizard set-up. Press **Skip** if no card number is needed.



If your system admin has locked Sharp MFPs, enter card number to unlock MFPs.

Card Number Enter user part only

123456



If your system admin has locked Sharp MFPs, enter card number to unlock MFPs.

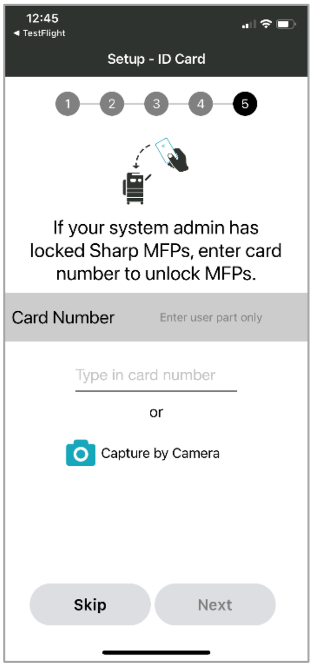
Card Number Enter user part only

123456

or

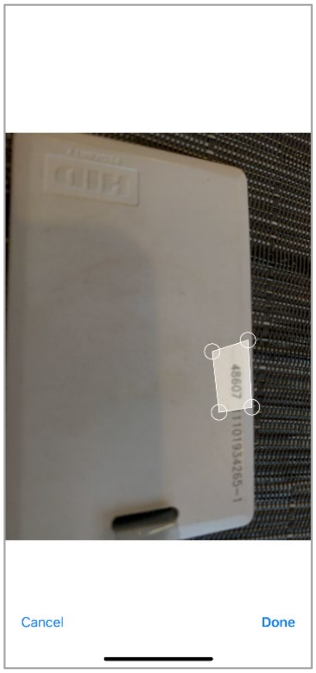
3. Camera capture entry: Select Capture by Camera and accept Synappx Go being able to access the camera. Take a close up picture of the card number, check and **Save** image. The number should be entered into the Card ID field.

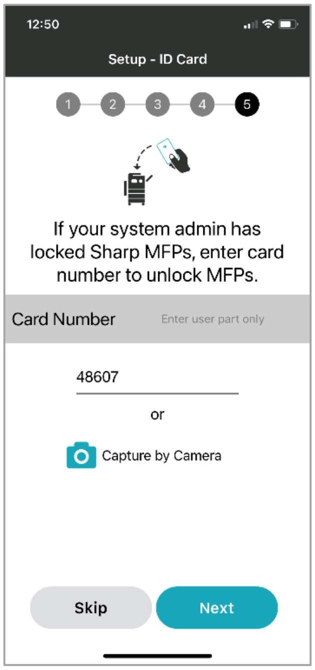
Note: User should check the results and confirm the card number is correct based on the OCR.



If your system admin has locked Sharp MFPs, enter card number to unlock MFPs.

Card Number: Type in card number (Enter user part only)





If your system admin has locked Sharp MFPs, enter card number to unlock MFPs.

Card Number (Enter user part only): 48607

Setting or editing the ID card number can also be done via the **Settings** menu under **ID Card**. The card number can be edited and saved by selecting the top left back arrow.

Note: Users cannot delete the ID card number from this page. User card numbers can be deleted from the Admin Portal only for v2.7.

6. Native Authentication and Go Integration Complete/Ready for Use

Upon completion of the installation and configuration steps, users can now use Synappx Go with Native locked MFPs. See the Synappx Go v2.7 User Guide for more details on the user experience at the MFP.

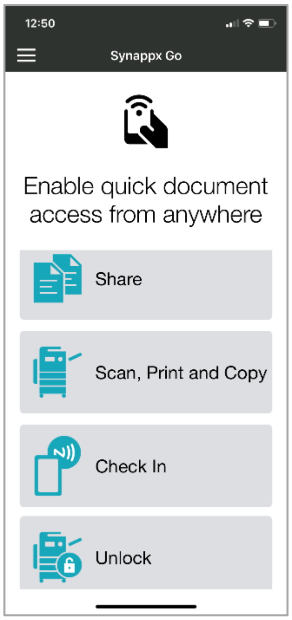
User Registration of ID Card with Native

Users who plan to use their ID Cards and/or use Synappx Go mobile to unlock the native A4 locked MFPs, first need to self-register their ID cards with each A4 MFP. Sharp A3 and some A4 MFP card setup must be done by Admins.

Synappx Go Mobile Use with Native Locked MFPs

Once the user has registered their card on the MFPs and the ID card number has been saved on their mobile (either by user or Admin entry), a new Unlock button is shown on the Synappx Go mobile home page.

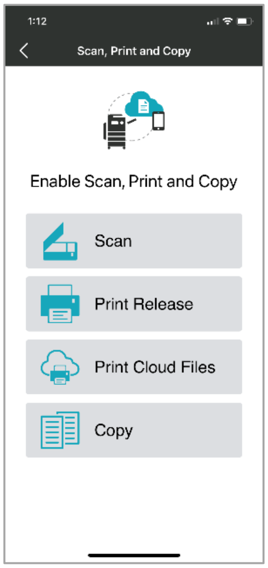
1. Place the mobile in proximity to the RF IDEAS BLE reader and press **Unlock.**



Enable quick document access from anywhere

2. The mobile automatically transfers the user's card ID number through the reader to the native (local database, AD, LDAP) to validate the user identity and confirm the card has a valid ID.
3. The mobile screens show the status of the confirmation process. Once the card ID is validated by the native MFP database, the MFP is unlocked and the MFP home page is displayed. The user can now use the Synappx Go features:
    - Tap the NFC tag first and then select Scan, Print Release, Print Cloud Files or Copy to perform the job OR
    - Select the Synappx Go MFP feature of interest and tap after selection

Note: Ensure the MFP home screen is showing before tapping the NFC tag.

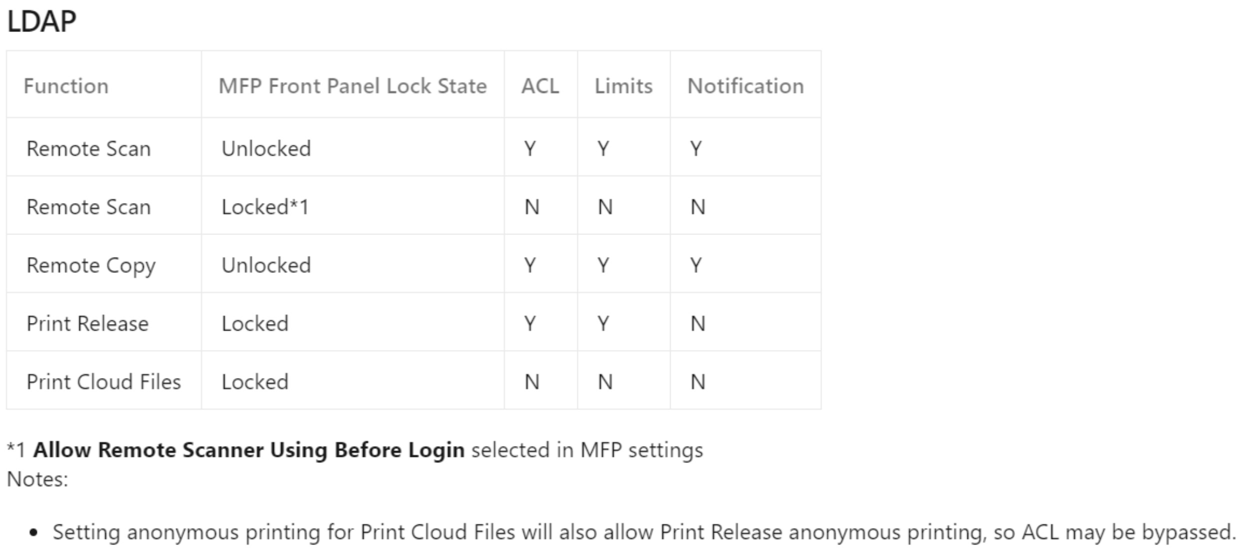


Enable Scan, Print and Copy

4. When finished with MFP remote actions, log out from the front panel or the front panel will time out based on MFP settings.

Synappx Go Integration with Native MFP Authentication Capabilities and Limitations

- Synappx Go scan, copy and print release are accounted to the correct user with valid credentials. Synappx Go Cloud Print files are not accounted to a specific user and are shown as untracked/anonymous.
- Synappx Go scan and copy require the user to select **Unlock** on the mobile device before tapping NFC tag at the MFP to scan or copy jobs.
- Synappx Go print release files can be sent to the locked MFP with a NFC tap without first selecting the Unlock button on Synappx Go mobile.
    - If a valid user, print release jobs will be correctly accounted to the user.
    - If the user is not valid:
        - If **Disabling of Printing by Invalid User** web page setting is unchecked, user print release job will be printed but accounted to anonymous user.
        - If **Disabling of Printing by Invalid User** web page is checked, user print release job will not be printed.
- For Synappx Go Print Cloud Files use, user does not need to select Unlock on the mobile before tapping the NFC tag to release the print job
    - If **Disabling of Printing by Invalid User** web page setting is unchecked, user job will be printed but accounted to anonymous user
    - If **Disabling of Printing by Invalid User** web page is checked, user job will not be printed
- Some interaction by the user with the MFP front panel "may" be required if the Native Authentication requires PIN and password entry in addition to user card ID
    - If Native Authentication requires extra PIN or password entry in addition to card number, user must enter PIN via the MFP front panel
- For OSA 5.5 enabled Sharp A3 and A4 models, Synappx Go integration abides by native authentication access control and limit features for Copy, Scan and Print Release. See the LDAP and AD A3 support tables below.



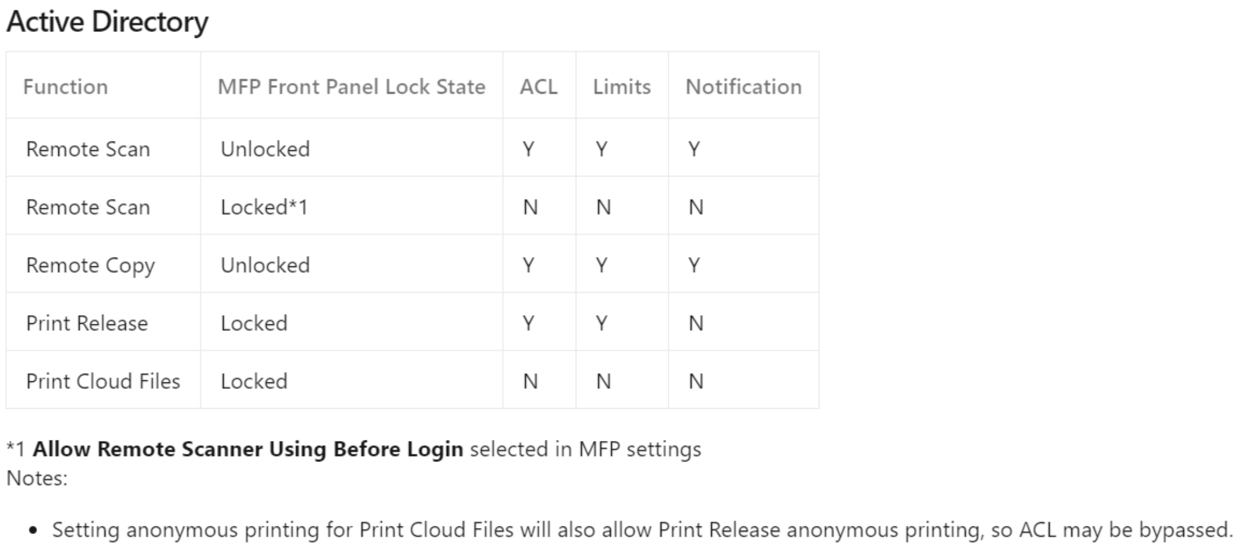
LDAP

Function	MFP Front Panel Lock State	ACL	Limits	Notification
Remote Scan	Unlocked	Y	Y	Y
Remote Scan	Locked*1	N	N	N
Remote Copy	Unlocked	Y	Y	Y
Print Release	Locked	Y	Y	N
Print Cloud Files	Locked	N	N	N

*1 **Allow Remote Scanner Using Before Login** selected in MFP settings

Notes:

- Setting anonymous printing for Print Cloud Files will also allow Print Release anonymous printing, so ACL may be bypassed.



Active Directory

Function	MFP Front Panel Lock State	ACL	Limits	Notification
Remote Scan	Unlocked	Y	Y	Y
Remote Scan	Locked*1	N	N	N
Remote Copy	Unlocked	Y	Y	Y
Print Release	Locked	Y	Y	N
Print Cloud Files	Locked	N	N	N

*1 **Allow Remote Scanner Using Before Login** selected in MFP settings
Notes:

- Setting anonymous printing for Print Cloud Files will also allow Print Release anonymous printing, so ACL may be bypassed.

- At the end of the user jobs, user may touch the front panel to return to locked condition OR allow time-out (no touch needed for time-out option) to return to locked state.

This page is intentionally left blank.

SYNAPPX™

For more information, visit the Synappx support site.

Access the Synappx Terms of Use at https://business.sharpusa.com/synappx-support/about/termsofuse.
Access the Synappx Privacy Policy at https://business.sharpusa.com/synappx-support/About/Privacy.
Access the Synappx End User License Agreement at https://business.sharpusa.com/synappx-support/about/EULA.