

SHARP

Synappx Cloud Print Administrator Guide.

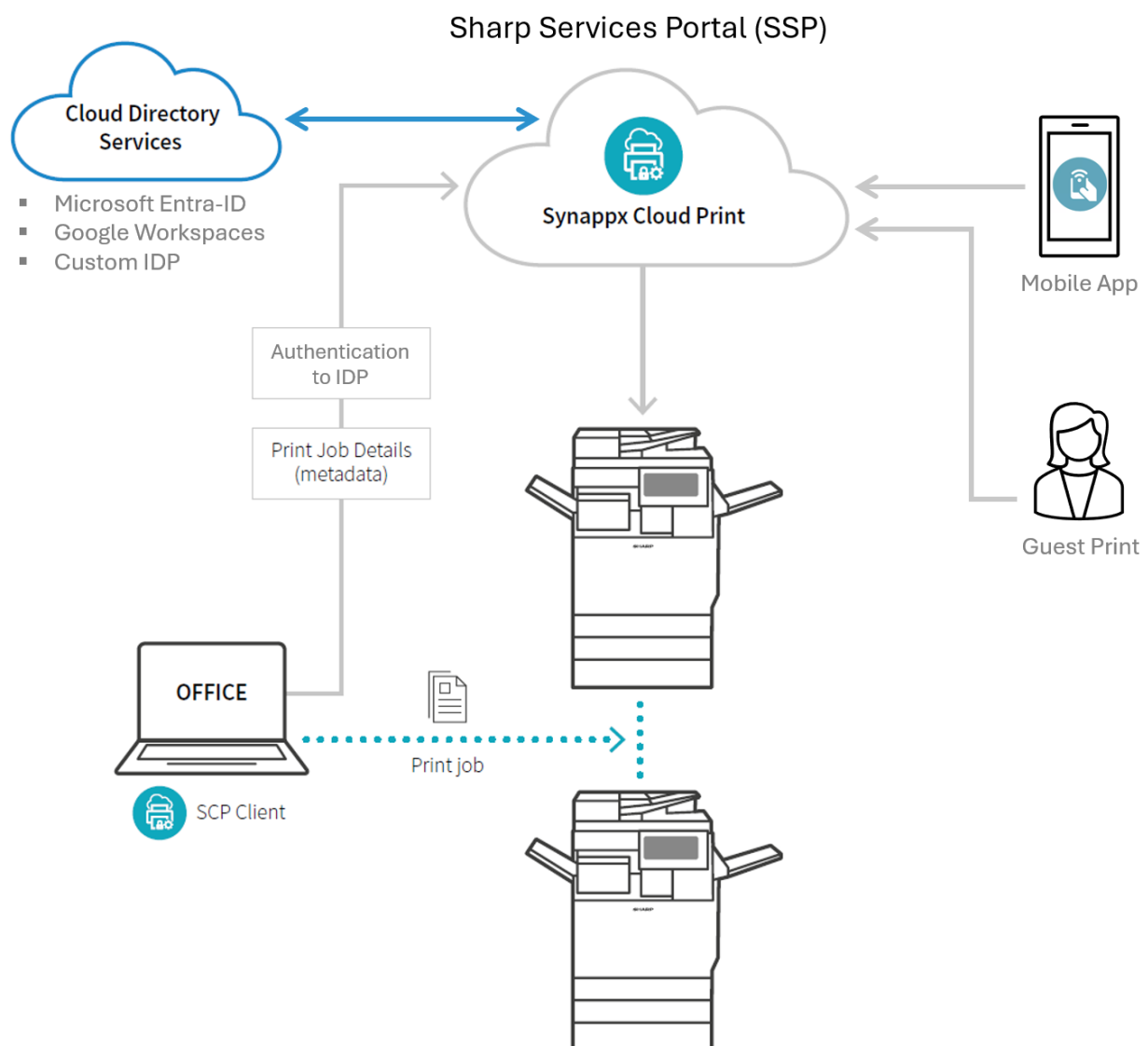
V1.8.

Table of Contents

System Requirements	5
Initial Sign Up and Selecting Provider	7
Custom Identity Provider (IDP) Support	8
Client PC Setup.....	14
Windows Print Logging	14
Print Driver Installation.....	16
Installing and Configuring the Synappx Cloud Print Client	19
The Administrator Portal	22
The Dashboard	24
Users and Groups.....	28
Devices (MFP Search and Registration)	41
Jobs	48
Reports.....	50
Creating Custom Reports	52
Creating Scheduled Reports.....	55
Settings.....	56
Security	56
Admin Users.....	61
Tenant	63
Subscriptions.....	64
System.....	65
What's New – Notification.....	68
User Portal	69
Configure MFP settings - Group 1 Device	72
Configure MFP Settings - Group 2 Device.....	80
Installing the Keyboard Emulation driver for USB Card Readers for Group 2 Devices	82
Using the SCP app on the MFP.....	83
Troubleshooting.....	96
Addendum A – Settings for Google WorkSpace	97
Addendum B – Direct Print	98
Addendum C – Guest Printing.....	105
Addendum D – 3 rd Party Printer Support.....	116
Addendum E – Red Firmware Upgrade	124
Addendum F - PC Client Deployment using MSI file.....	127

Overview of Synappx Cloud Print

The Sharp Synappx Cloud Print solution has been developed as a 'true' cloud-based print management solution. In use the customer only requires an SCP client on the PC they wish to print from, a Sharp Group 1 or 2 MFP and an internet connection, no other infrastructure such as print servers or network connection devices are required.



System Requirements

MFP Device

- A Sharp Group 1 MFP running OSA version 5.5 or above with EAM (AMX3 or BP-AM11) and (AMX2 or BP-AM10) keys installed
- A Sharp Group 2 MFP with firmware version 230.207 and above
- Internet Connectivity

Client PC

- Processor: 1 gigahertz (GHz) or faster with two or more cores - 64-bit
- Memory: 4 gigabytes (GB) or greater
- Storage: 64 GB or greater available disk space
- Internet connectivity
- Microsoft Windows 10 or Windows 11

Browser/s

- Chrome v117 or above
- Firefox v118 or above
- Edge v 117 or above

For the purpose of this Administrator Manual the various Sharp MFP models have been placed into two groups, Group 1 & Group 2

Sharp MFP Groups

Group 1 Devices:

MX-2651 MX-3051 MX-3551 MX-4051 MX-5051 MX-6051 MX-3061 MX-3561 MX-4061 MX-3061S
MX-3561S MX-4061S MX-3071 MX-3571 MX-4071 MX-5071 MX-6071 MX-3071S MX-3571S
MX-4071S MX-5071S MX-6071S MX-M2651 MX-M3051 MX-M3551 MX-M4051 MX-M5051
MX-M6051 MX-M3071 MX-M3571 MX-M4071 MX-M5071 MX-M6071 MX-M3071S MX-M3571S
MX-M4071S MX-M5071S MX-M6071S MX-C303W MX-C304W MX-C303WH MX-C304WH
MX-B356WH MX-B356W MX-B456WH MX-B456W BP30C25 MX-7081 MX-8081 BP30M28 BP30M31
BP30M35 MX-M1056 MX-M1206

BP-50C26 BP-50C31 BP-50C36 BP-50C45 BP-50C55 BP-50C65 BP-55C26 BP-60C31 BP-60C36
BP-60C45 BP-70C31 BP-70C36 BP-70C45 BP-70C55 BP-70C65 BP-90C70 BP-90C80 BP-50M26
BP-50M31 BP-50M36 BP-50M45 BP-50M55 BP-50M65 BP-70M31 BP-70M36 BP-70M45 BP-70M55
BP-70M65 BP-C533WR BP-C533WD BP-C542WD BP-B537WR BP-B547WD BP-70M75 BP-70M90
BP-51C26 BP-51C31 BP-51C36 BP-51C45 BP-51C55 BP-51C65 BP-56C26 BP-61C31 BP-61C36
BP-61C45 BP-71C31 BP-71C36 BP-71C45 BP-71C55 BP-71C65 BP-51M65 BP-71M31 BP-71M36
BP-71M45 BP-71M55 BP-71M65

Group 2 Devices:

MX-C407P MX-C507P MX-C428P MX-C607P MX-C357F MX-C358F MX-C428F MX-C528F MX-C557F
MX-C607F MX-B467F MX-B468F MX-B557P MX-707P MX-B557F MX-B707F

Ports and Firewall – Settings

Bidirectional traffic must be enabled on ports 443 and 57100, if there is a gateway or bridge where Synappx Cloud Print needs to pass data then these ports need to be open on those as well

The following Synappx domains must be allowed through the customers firewall:

- .cloudprint.synappx.sharp.eu
- .adminportal.synappx.sharp.eu
- .synappx-sharp-eu.eu.auth0.com

Access Token Lifetimes – Entra ID

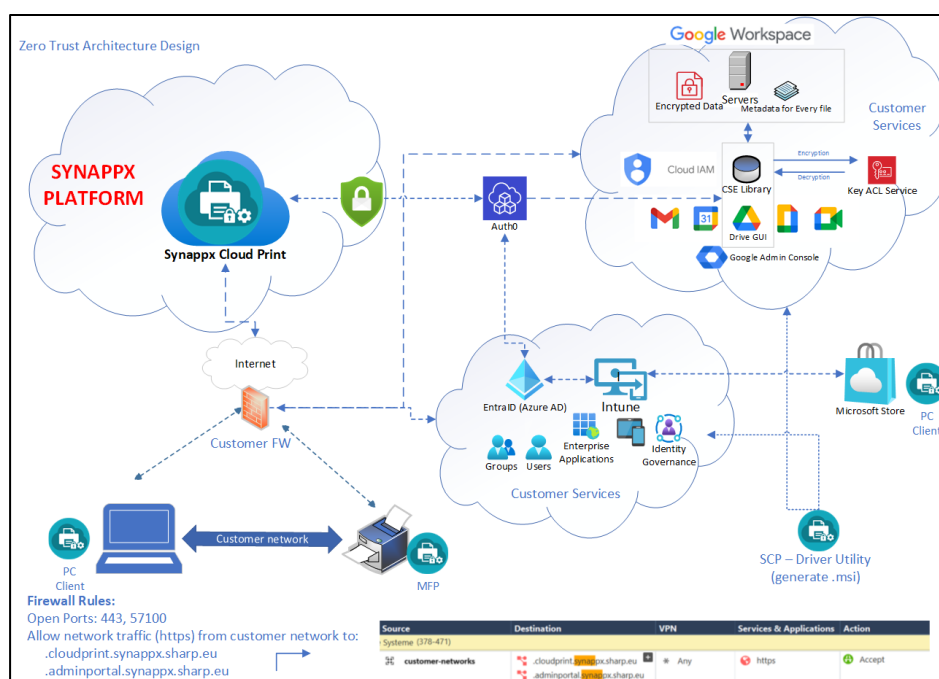
The Synappx Cloud Print PC client was created using OpenID Connect (OIDC) to support single sign-on (SSO) to your Microsoft Entra tenant. In order to extend the default token life there are options to extend in Entra-ID

To learn more about access tokens in Microsoft Identity Platform please see: [Access tokens in the Microsoft identity platform](#)

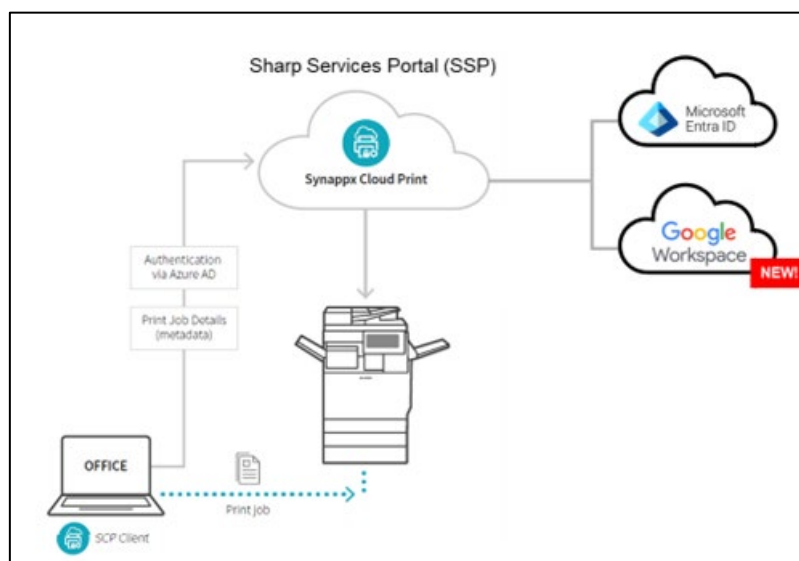
The default lifetime of an access token is variable. When issued, the Microsoft identity platform assigns a random value ranging between 60-90 minutes (75 minutes on average) as the default lifetime of an access token. The variation improves service resilience by spreading access token demand over a time, which prevents hourly spikes in traffic to Microsoft Entra ID.

Adjust the lifetime of an access token to control how often the client application expires the application session, and how often it requires the user to reauthenticate (either silently or interactively). To override and increase the default access token lifetime variation, use [Configurable token lifetime \(CTL\)](#).

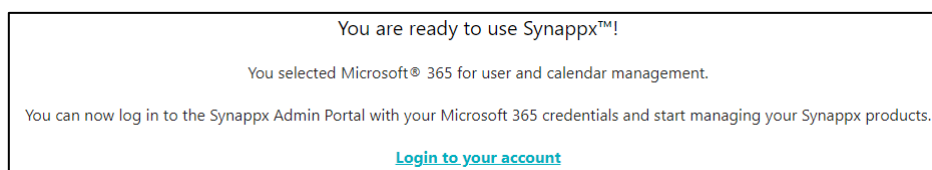
Zero Trust Architecture Design



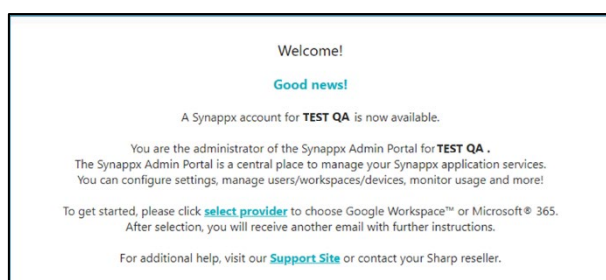
Initial Sign Up and Selecting Provider



After signing up for Synappx Cloud Print, the assigned administrator will receive an email asking to choose either Google Workspace or Microsoft 365 as a cloud service provider.



After the admin chooses a service provider, a second welcome email will arrive in the admin mailbox with instructions to log in to the Synappx Admin Portal.



From here they can log in to the Synappx Admin Portal and start adding users and devices.

SYNAPPX™

Enter your email address or Cloud Portal username

Note: The assigned administrator for Microsoft 365 or Google Workspace must have administrator privileges for that service. For Google Workspace, there may be additional settings required. Please see Addendum A at the end of the guide

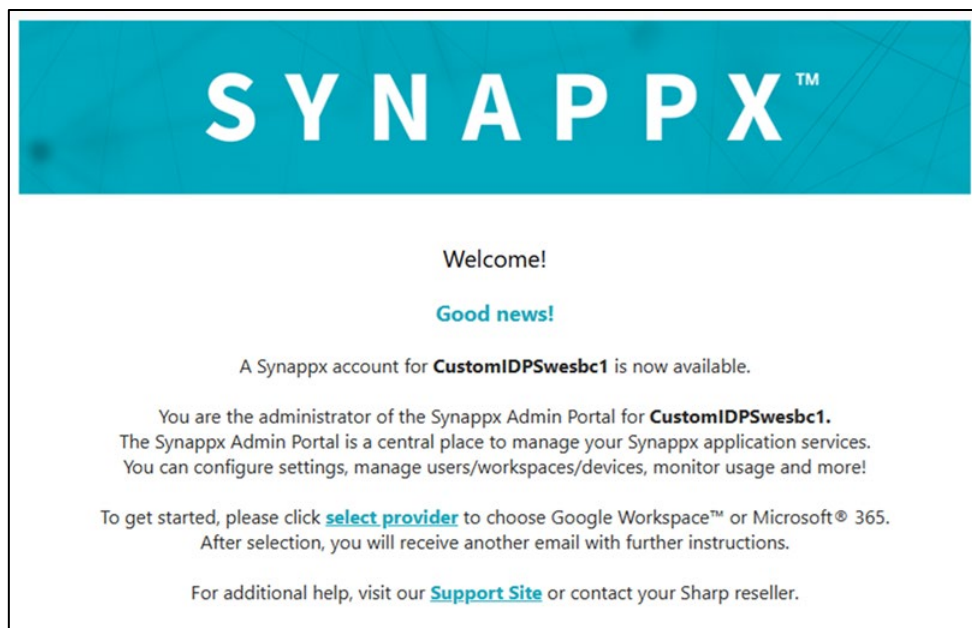
Custom Identity Provider (IDP) Support

In cases where customers have not migrated to cloud directory services (Microsoft Entra-ID or Google Workspaces) Synappx Cloud print provides a Custom Identity Provider (IDP) option. Using this option users can be onboarded and managed within the application.

Since cloud print creates a custom tenant outside of the customers IT environment there are some limitations:

- Scan to cloud folder (embedded scan) is not available
- Authenticate to MFP using QR code is not available
- Guest Printing is not available
- Mobile application is not compatible

Creation of custom tenants are initiated in License Manager and made available to customers via a welcome email and sign-up link



Clicking the 'select provider' link in the welcome email provides the option to create a new sign-in account for Synappx

Select organization sign-in option

Sign-in with:

- ☐ Microsoft 365 account
- ☐ Google Workspace account
- ☒ Create a new Sign-in account for Synappx

OK

Provider

You selected to create new sign-in account.

OK Cancel

Set your password

ID : swesbc1@outlook.com

Password :

You must enter a value

Confirm :

OK Cancel

Success! We will send you an email with a login link to Synappx Admin Portal.

A welcome email is received with a link to login to your custom IDP "Admin" account

SYNAPPX™

You are ready to use Synappx™!

You selected Custom Account for user management.

If you want to add others as administrators, go through all steps explained in [the support site](#).

Then, log in to the Synappx Admin Portal with your Custom Account credentials and start managing your Synappx products.

[Login to your account](#)

For additional help, visit our [Support Site](#) or contact your Sharp reseller.

You can now login to the admin portal by clicking the link

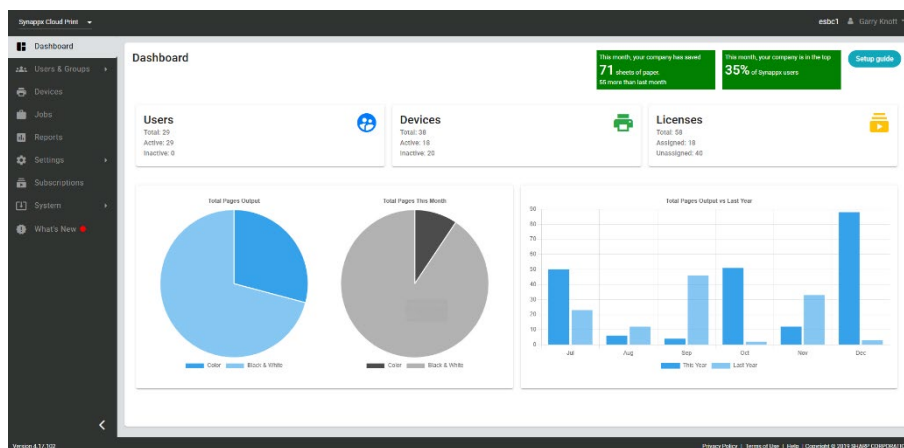
After following the link and entering your email address select [Log in with custom account]

The first screenshot shows the Synappx login page with the email address swesbc1@outlook.com entered and the 'Log in with custom account' button highlighted. The second screenshot shows the password entry screen with the email address swesbc1@outlook.com and a 'Log In' button. The third screenshot shows the 'Authorize App' screen for SYNAPPX ADMIN, requesting access to the synappx-sharp-euqa tenant, with a green checkmark indicating successful authorization.

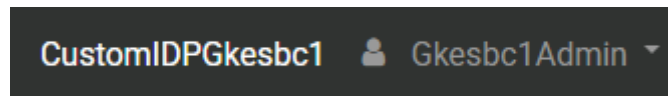
On first use please authorise the app and agree to the Terms & Conditions and Privacy Policy

The screenshot displays the 'Terms & Conditions of Use - for Synappx™' document, effective 11/07/2023. It outlines the agreement between Sharp Corporation and the customer, covering access to Synappx services and related documentation. The document is scrollable, with a scrollbar visible on the right side.

The IDP Admin will now be logged into the Admin Portal dashboard



The default IDP Tenant name will show as “CustomIDPGkesbc1” as shown below



Adding IDP Users

From the [Users & Groups] tab, select the [+] button

Add User

New Users

Import Multiple Users

To add a new user, provide their details by entering the first name, last name, and email address in the required fields.

First Name

Garry

Last Name

Knott

Email

gkesbc2@outlook.com

☒ Activate Users ⓘ

User Grouping

Create Group & Map User(s) ⓘ

☐

Map User(s) to Group ⓘ

☐

Cancel

Save

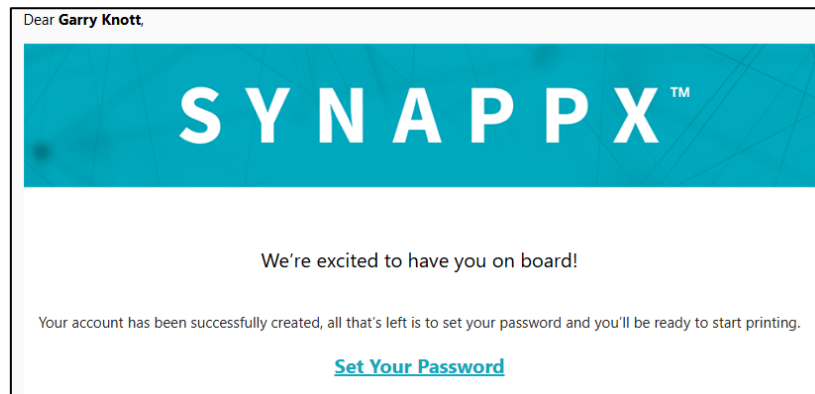
Insert user details, email address and actions required. The new user will receive an activation email invitation which will allow them to setup their account

If [Activate Users] is selected they will also receive a valid PIN code once the email invitation has been accepted

In the Admin Portal you can see that an invitation has been sent but not yet accepted via the email symbol and red inactive user symbol

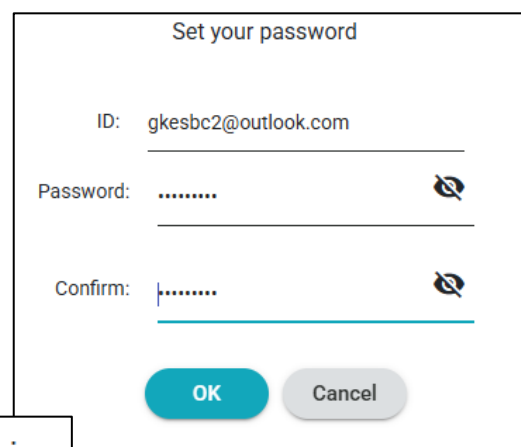


The new user will receive the email invitation asking them to set their password for the account



Users set password details by clicking the link in the invitation

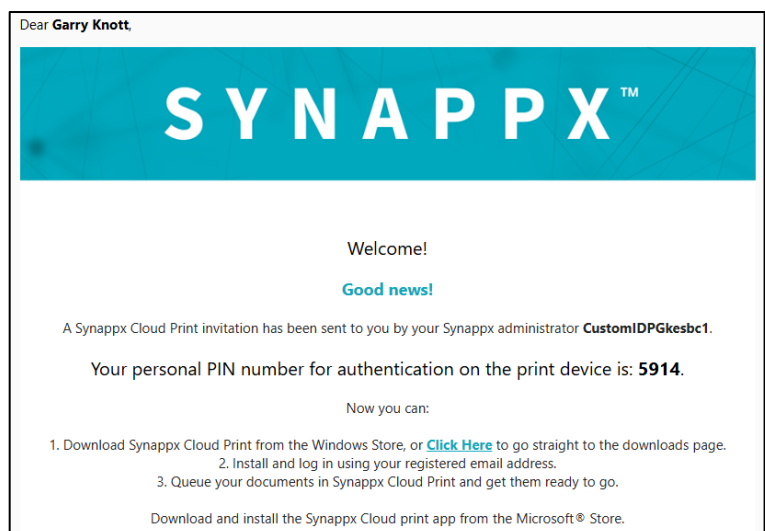
A message will inform the user that a link to the Admin Portal has been sent to them

A "Set your password" form. It includes fields for "ID:" (gkesbc2@outlook.com), "Password:" (masked with dots), and "Confirm:" (masked with dots). There are "OK" and "Cancel" buttons at the bottom.

Success! We will send you an email with a login link to Synappx Admin Portal.

The received welcome email will inform the user of:

- Their personal device PIN login
- A link to download the PC Client App
- Setup Instructions
- A link for the Support Site
- A link for the Admin Portal site



Administrators can see when user(s) have accepted the email invitation via the [Users] tab



The ticked email icon shows as verified and the green user icon shows as active

There is also an option to “bulk” import users via the [Import Multiple Users] tab and using a .csv file

Add User

New Users

Import Multiple Users

Process

1. Export the CSV file of Active users from Microsoft 365 admin center.

2. Edit the CSV to include only necessary users.

3. Return to this screen and upload CSV file.

Choose file

No file chosen

☒

Activate Users

For more information see page 31 “Import multiple users via a CSV file

Client PC Setup

The Client PC Setup consists of ...

- Enabling Windows Print Logging
- Installing a Sharp Printer Driver
- Installing the Synappx Cloud Print Client Software

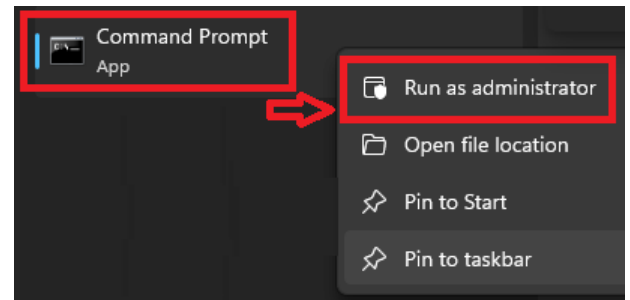
Windows Print Logging

So that the Portal correctly logs the number of print pages, Windows Print Logging needs to be enabled on any PC that will be running the Client software

Enabling Windows Print Logging

On the client PC open a Command Prompt as Administrator

- From the search box type CMD
- Right click on [Command Prompt] and select "Run as administrator"



In the command prompt type the following:

wevtutil sl Microsoft-Windows-PrintService/Operational /e:true then press [Enter]

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32 wevtutil sl Microsoft-Windows-PrintService/Operational /e:true
C:\Windows\system32>
```

The printer driver needs to be a suitable Sharp PCL 6 Driver. These are available from the Global Sharp website:

https://global.sharp/restricted/products/copier/downloads/select_us_driver.html

The screenshot shows the Sharp Global website's 'Driver Downloads' page. The header includes the Sharp logo and navigation links: 'About Sharp', 'Investor Relations', 'Social & Environmental Activities', and 'Brand'. The main content area is titled 'Digital MFPs / Printers' and features a 'Downloads' tab. A language selector is set to 'English(US) / English'. The page is titled 'Driver Downloads' and includes a search bar. Below the search bar, there are four steps for selecting a driver: (1) Select Country/Region (set to Europe), (2) Select Category (set to Drivers for Color Models), (3) Enter Product Name (set to BP-60C45), and (4) Select Language of Driver/Software (set to UK English). A 'NEXT >' button is at the bottom.

SHARP
Be Original.

About Sharp Investor Relations Social & Environmental Activities Brand

Digital MFPs / Printers

Downloads

Choose your language English(US) / English

Driver Downloads

Search drivers.

(1) Select Country/Region Europe

(2) Select Category Drivers for Color Models

(3) Enter Product Name BP-60C45

(4) Select Language of Driver/Software UK English

NEXT >

Products Downloads

Downloads

- Brochures
- Drivers
- Software
- Applications
- AR Markers

The Synappx Cloud Print Client software can be downloaded from the Microsoft Store

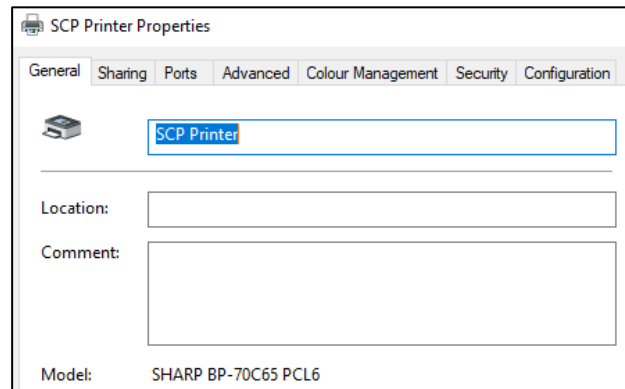
Search for “[Synappx Cloud Print](#)”



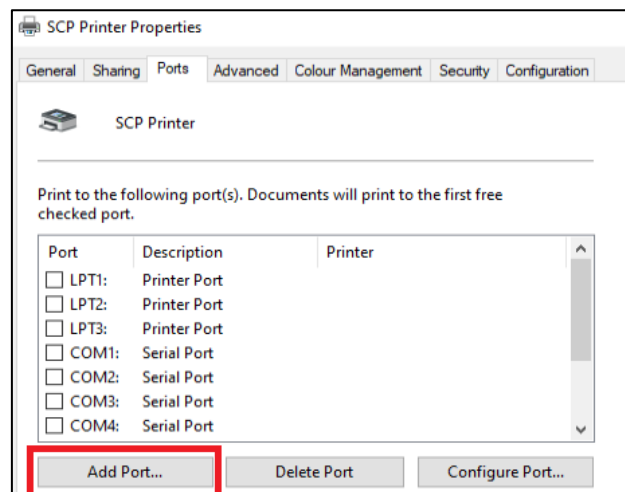
Print Driver Installation

A suitable Sharp PCL Print Driver must be installed on to the client PC using a downloaded Sharp driver installer application, (see client PC setup on page 5).

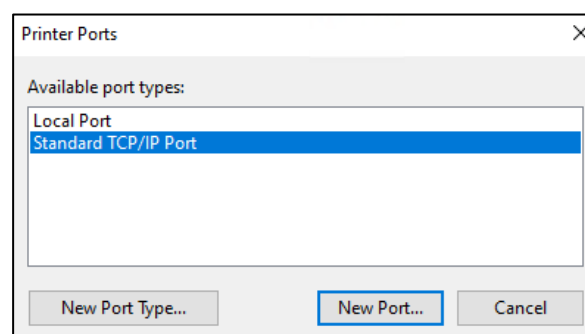
Once installed, give the printer a suitable name, (from [Printer Properties] – [General] tab).



Synappx Cloud Print uses a specific port to print from; you must now add this port to the printer driver. From [Printer Properties] – [Ports] - select [Add Port](#)



Select - [Standard TCP/IP Port](#) > [New Port](#)



On the “Welcome to the Add Standard TCP/IP Printer Port Wizard,” click [\[Next\]](#)

Set IP Address to [127.0.0.1](#) – Click [Next](#)

The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window. The title bar says 'Add Standard TCP/IP Printer Port Wizard'. The main heading is 'Add port' with a subtext 'For which device do you want to add a port?'. Below this, it says 'Enter the Printer Name or IP address, and a port name for the desired device.' There are two input fields: 'Printer Name or IP Address:' with the value '127.0.0.1' and 'Port Name:' with the value '127.0.0.1'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

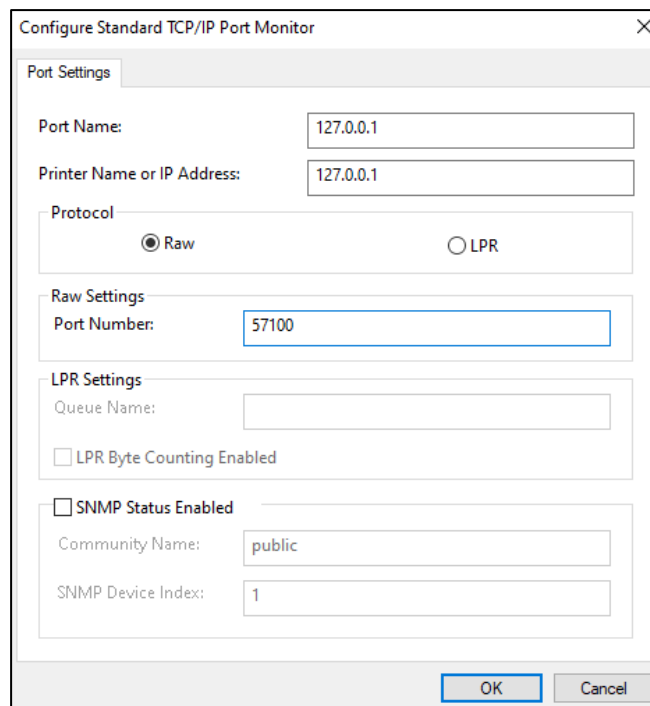
For the “Detecting TCP/IP Port” you may have to wait up to 30 seconds for it to detect the port

The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window. The title bar says 'Add Standard TCP/IP Printer Port Wizard'. The main heading is 'Detecting TCP/IP port' with a subtext 'Windows is detecting the TCP/IP port and will move to the next page when finished.' Below this, it says 'Detecting the TCP/IP port...' and 'Windows will automatically move to the next page when the detection is complete.' There is a small icon of a magnifying glass over a document. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

On the “Additional Port Information” select [\[Custom\]](#) then click [\[Settings\]](#)

The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window. The title bar says 'Add Standard TCP/IP Printer Port Wizard'. The main heading is 'Additional port information required' with a subtext 'The device could not be identified.' Below this, it says 'The device is not found on the network. Make sure that:' followed by a list of four items: 1. The device is turned on. 2. The network is connected. 3. The device is properly configured. 4. The address on the previous page is correct. Below the list, it says 'If you think that the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure that the address is correct, select the device type below.' There are two radio buttons: 'Standard' and 'Custom'. The 'Custom' radio button is selected. Below the radio buttons, there is a dropdown menu labeled 'Device Type' with 'Generic Network Card' selected. To the right of the 'Custom' radio button is a button labeled 'Settings...'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Change the [Port Number] to 57100

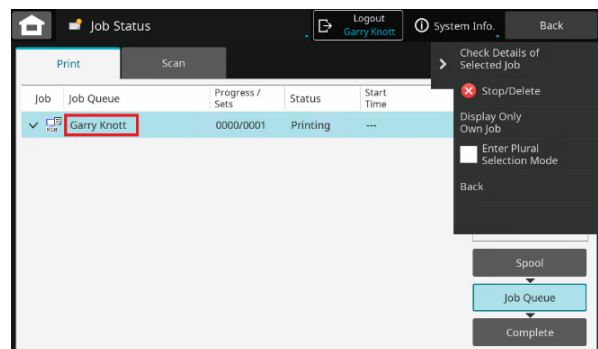


Click **OK** – Next – Finish

Close Settings

No further information is required to be input to the driver as the PC Client will assign the print jobs to the user who is currently logged in, (to the PC Client)

The user who is logged in to the PC Client is used for easily identifying job owners on the MFP screen (and in the portal job history pages)



To use the feature [Direct Print], please refer to Addendum B – Direct Print

To use the feature [Guest Printing], please refer to Addendum C – Guest Printing

To use the feature [3rd Party Printing], please refer to Addendum D – 3rd Party Printing

All of the above Addendums are at the end of this manual

Installing and Configuring the Synappx Cloud Print Client

The Client software communicates with the Print Driver, the Print Device and Synappx Cloud Print for authentication and discovery.

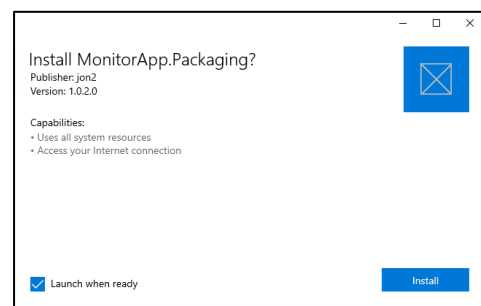
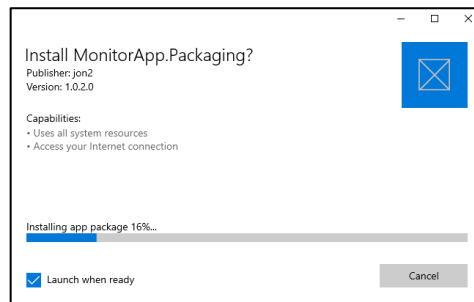
The client software will need to be installed on a Windows PC that is on the same local network as the MFPs. This is for the device discovery, (if admin), and also for printing purposes

Please note: The Client installation will set a Firewall rule to open port 59080

The Synappx Cloud Print Client software is available from the Microsoft Store



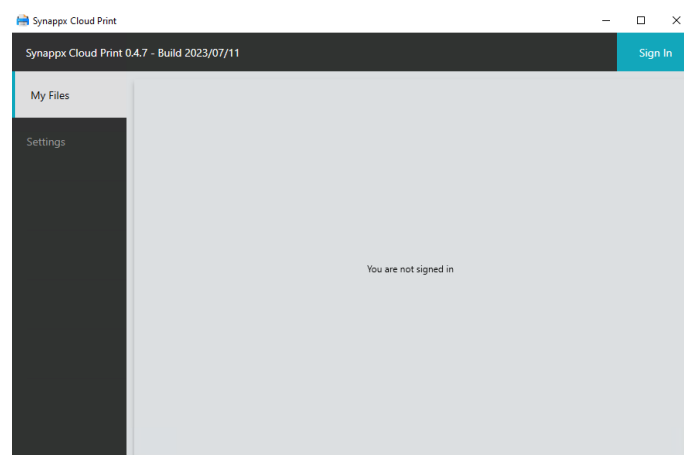
Click Install →

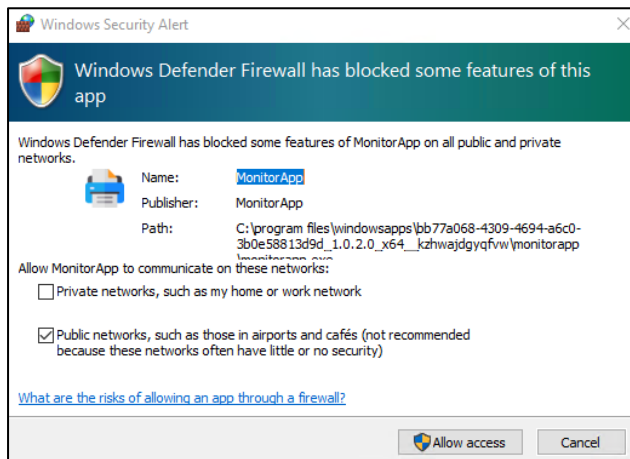


← The client will automatically install

When the Client has installed the Client screen will be displayed

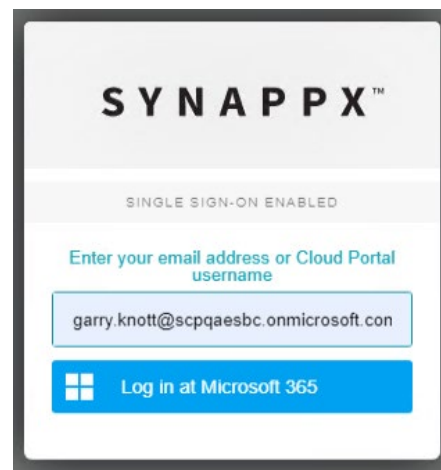
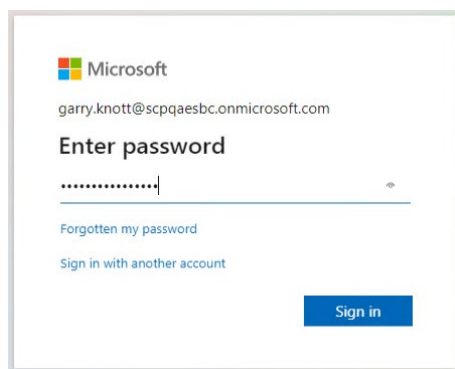
Please sign in using your supplied tenant account





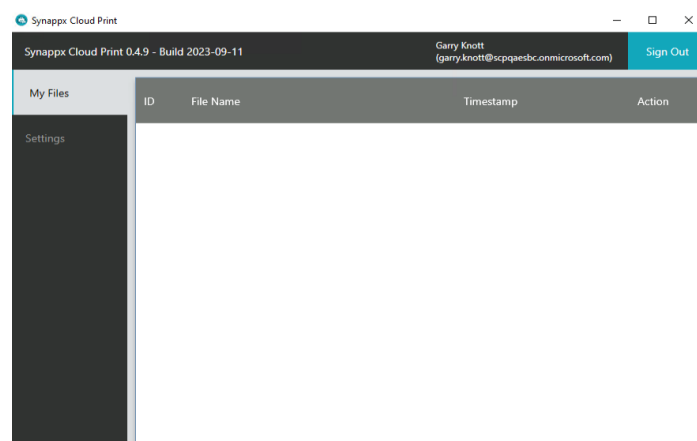
On first sign in you will receive a Firewall message, please allow access so that firewall rules can be implemented for the Client

Login using your username and password login credentials



When logged in you will see the Client main page [My Files] which will be empty.

Once logged in, click on the [Settings] tab



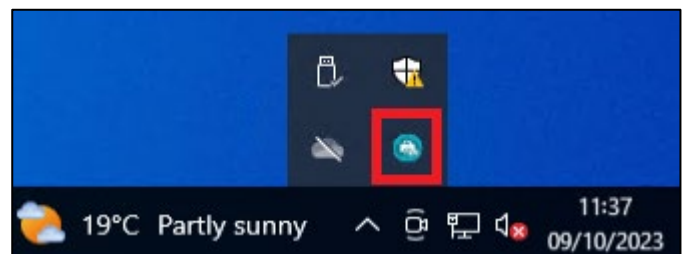
Select the printer being used for printing to Synappx Cloud Print

Click [\[Restart\]](#) to restart the Client

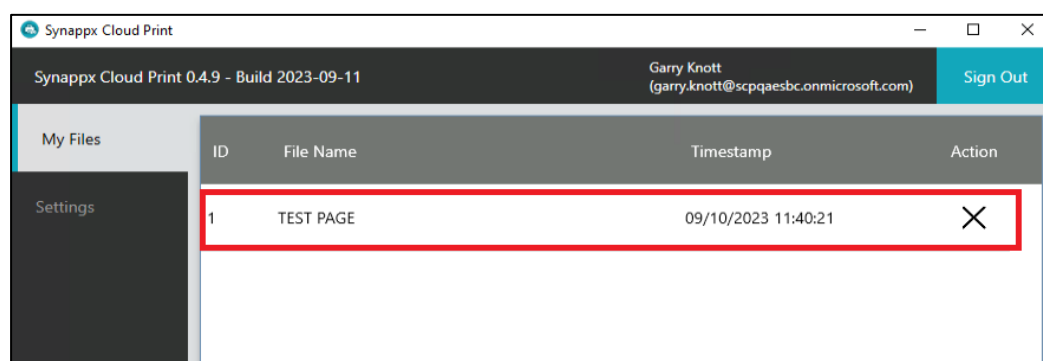


Once restarted, you will need to sign in again by clicking [\[Sign In\]](#), (you will be automatically signed in). You can check you are successfully signed in by checking the username displayed.

Check that the MonitorApp is running by checking for its icon in the hidden items menu of the system tray in the task bar



At this point you can send a test print from your Print Driver and the print job should be displayed in the client software by clicking the “My Files” tab



Note: Setting up Client software, Driver installation with configuration and Print Logging command can be made via Microsoft Intune. Please contact ESBC Support for further instructions.

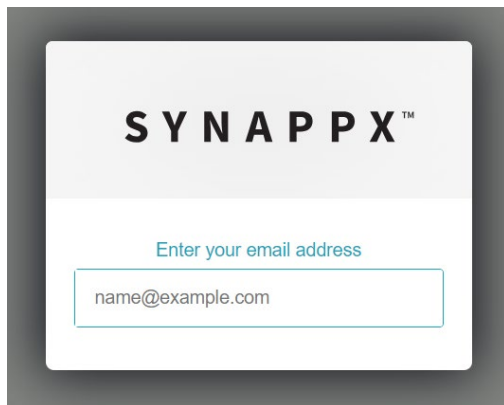
The Administrator Portal

The style and layout of the admin and user portals have been designed following the Synappx design guide.

Note:

Before you can login to the Administrator Portal you must have received a “Welcome” E-Mail in which you are requested to select your provider, (Google Workspace or Microsoft 365).

After you have made a selection, you will receive a confirmation E-Mail with the link to login to the Administrator Portal.

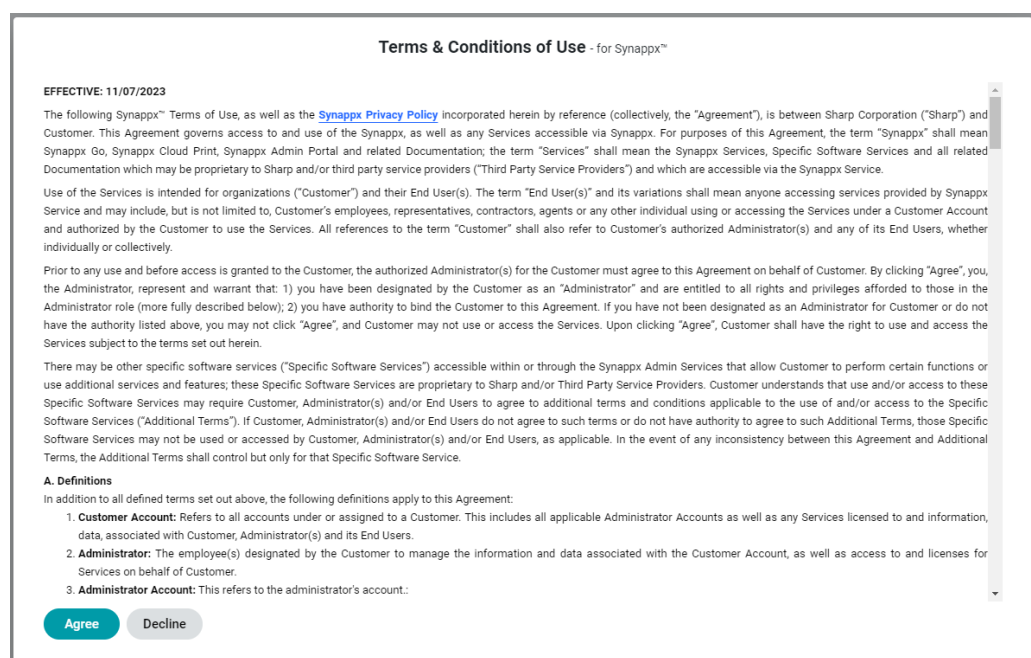
A login form for the Synappx Administrator Portal. It features the 'SYNAPPX™' logo at the top. Below the logo, the text 'Enter your email address' is displayed in a light blue font. Underneath this text is a text input field containing the placeholder 'name@example.com'.

To log into the administrator portal, go to the following url:

<https://adminportal.synappx.sharp.eu>

Enter your Admin credentials

On the first login the admin or user will see the [Terms & Conditions of Use] screen
You must click [Agree] to continue, (if you decline you will be logged out)

A screenshot of the 'Terms & Conditions of Use - for Synappx™' screen. The title is centered at the top. Below the title, the text 'EFFECTIVE: 11/07/2023' is displayed. The main body of the document contains several paragraphs of text, including a section titled 'A. Definitions' which lists three items: 'Customer Account', 'Administrator', and 'Administrator Account'. At the bottom of the screen, there are two buttons: 'Agree' (highlighted in blue) and 'Decline' (in grey).

After the Terms & Conditions screen, you will be shown the [Initial Setup] pop-up. This takes you through all the steps required to setup Synappx Cloud Print if required.

Initial Setup Steps of Synappx Cloud Print

Step 1

Download and install the SCP Client here:



Step 2

Configure your MFPs using this guide:

[SCP MFP Configuration](#)

Step 3

Discover & License your MFPs here:

[Devices](#)

Step 4

Import & Invite your users here:

[Users](#)

Step 5

Set up your SCP preferences here:

[Settings](#)

For further information see the on-line guides here:

[SCP Help](#)

Do you wish to see this guide again?

[Yes](#)[No](#)

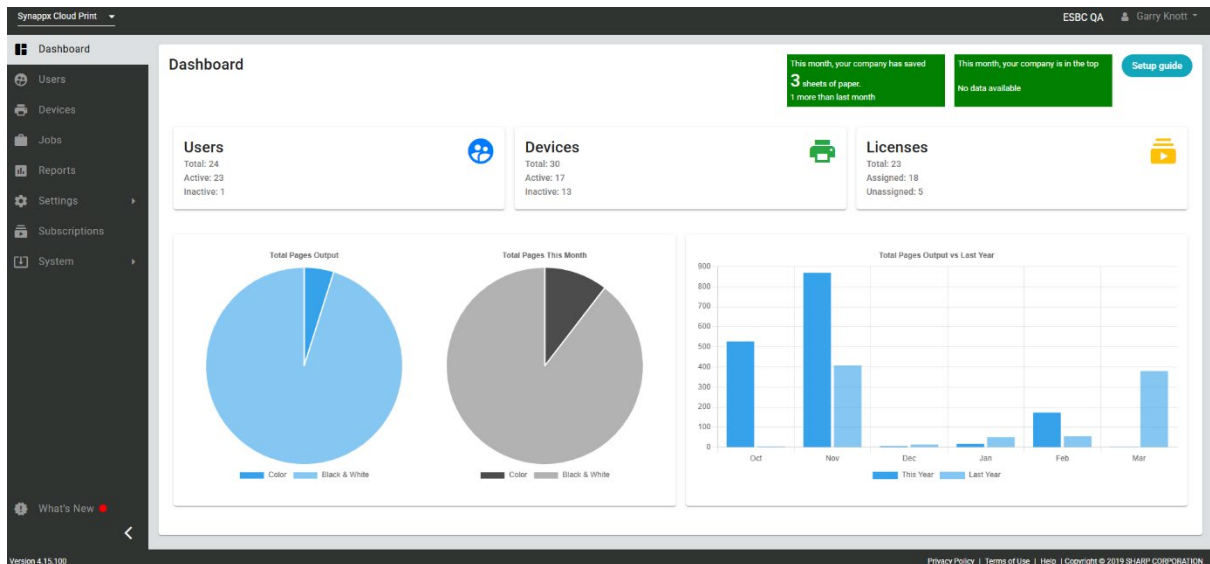
If you do not wish to see this screen each time you login select [No] at the bottom of the screen, where asked “Do you wish to see this guide again?”

Once logged in, from the Dashboard you are always able to get back to the [Initial Setup Steps] by clicking the button [Setup Guide](#)



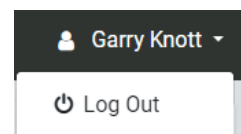
The Dashboard

The admin portal home page will now be displayed showing the Synappx Cloud Print Admin Dashboard with the navigation menu on the left of the screen



The logged in user details are displayed in the top right-hand corner of the screen

Clicking on the user details displays the option to [log out](#)



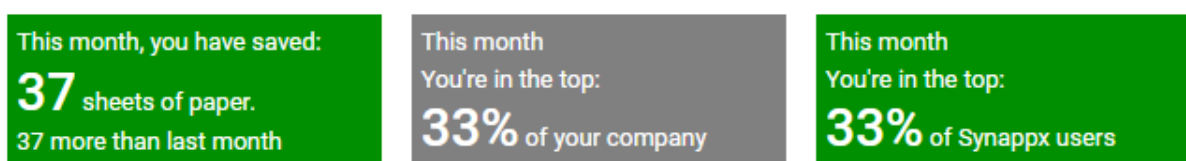
The Dashboard screen area displays several “green” values

In the top right-hand area of the screen is information regarding environmental credentials

If you login as “Admin” you will see company information



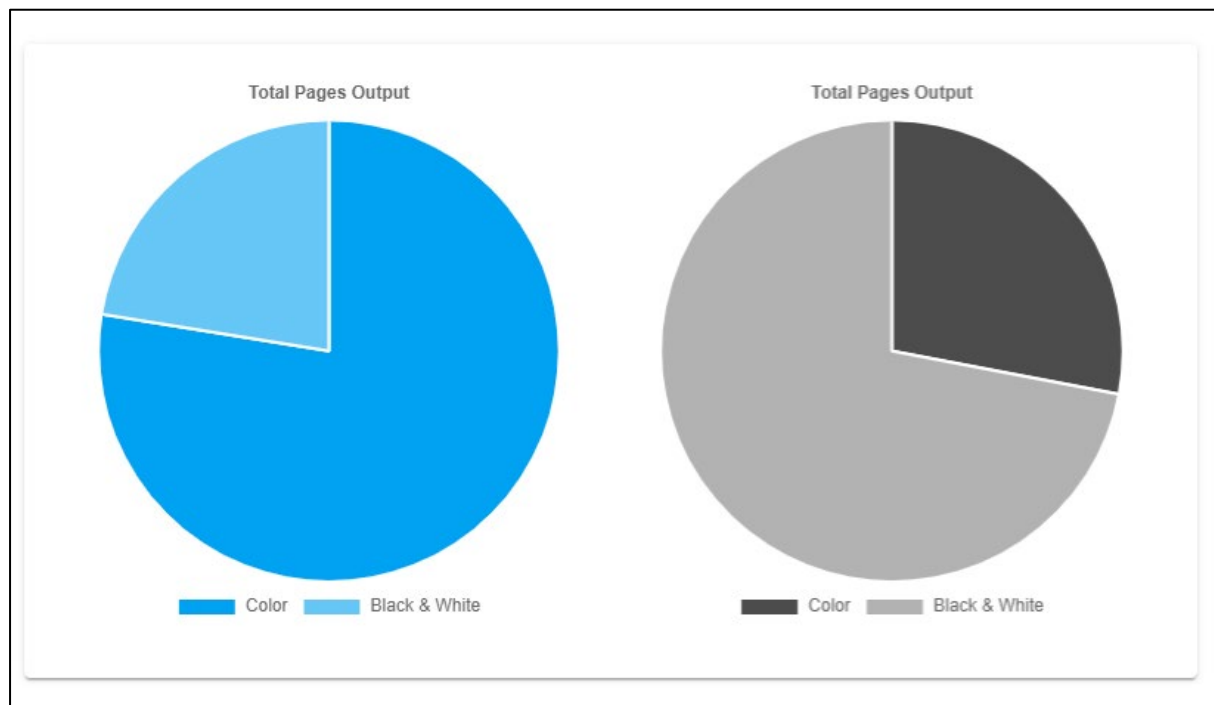
If you log in as a “user” you will see your own personal information



Displayed in the lower left section of the Dashboard is Total Pages Output in Colour and B&W

Logging in as Admin will display the total for the [organisation](#)

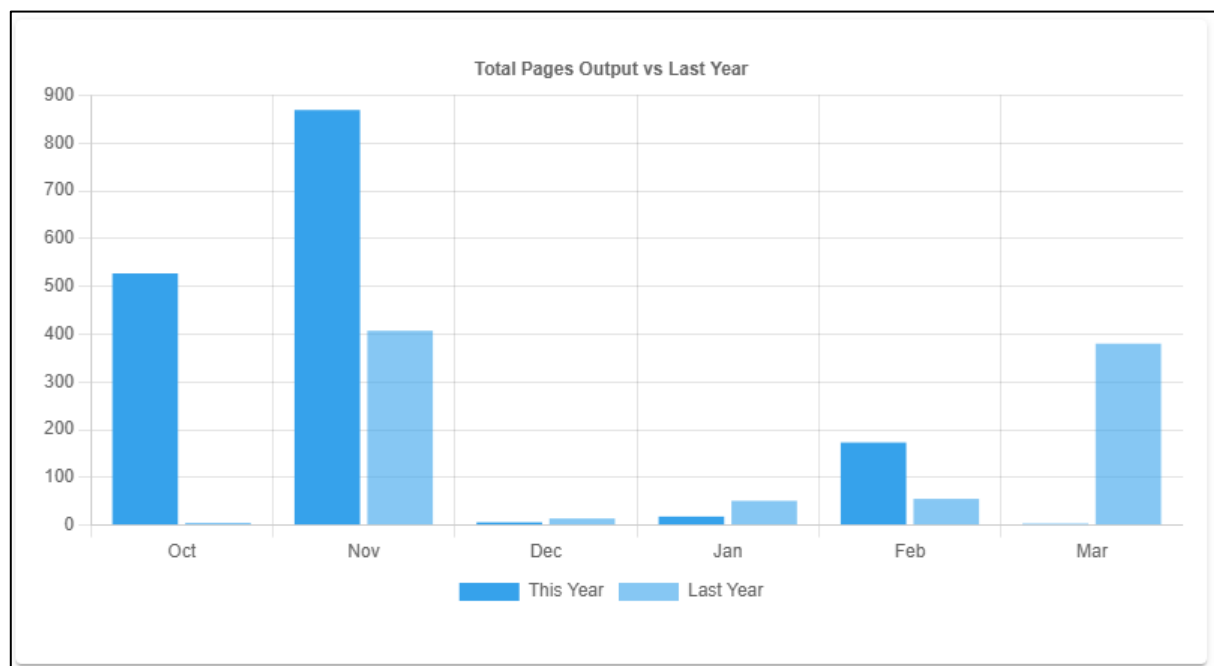
Logging in as a User will display the totals for that user



In the lower right section of the Dashboard is the Total Pages output compared to 1 year ago

For an Admin login this will display the total for the Organisation

For a user login this will display the total for that User



Across the centre of the Dashboard is information regarding Users, Devices and Licenses

Users Total: 9 Active: 8 Inactive: 1		Devices Total: 23 Active: 2 Inactive: 21		Licenses Total: 5 Assigned: 2 Unassigned: 3	
--	---	--	---	---	---

Users: Displays the total number of Users added to Synappx Cloud Print and how many have been activated

Users

Total: 9
Active: 8
Inactive: 1



Devices: Displays the number of Devices discovered on the network and how many have been activated

Devices

Total: 23
Active: 2
Inactive: 21



Licenses: Displays the number of licenses you have available in total; how many have been assigned and how many are unassigned

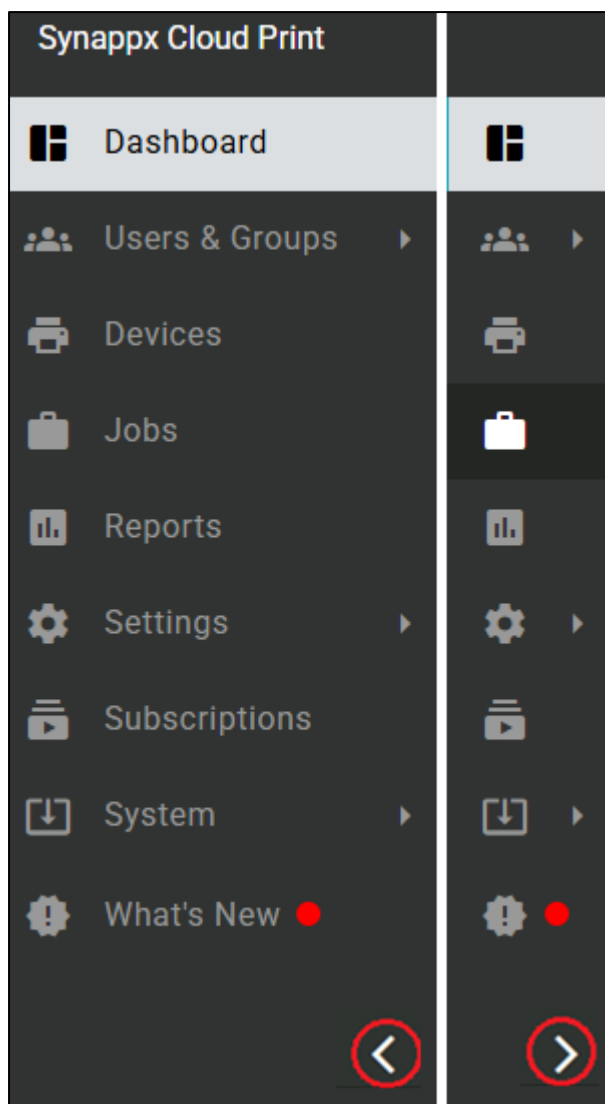
Licenses

Total: 5
Assigned: 2
Unassigned: 3



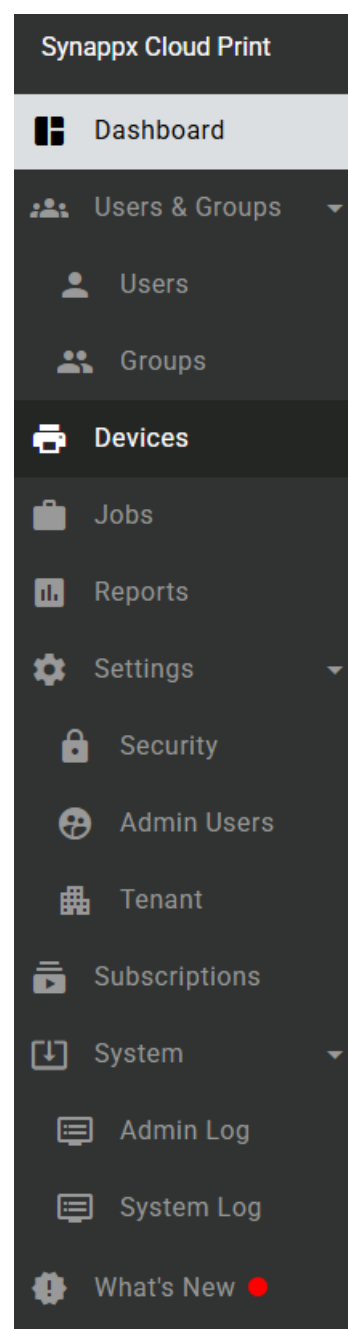
Clicking on any of the Icons next to Users, Devices or Licenses will link to the appropriate area in the Admin Portal





The Menu Bar

On the left-hand side is the menu bar, where there are several options for administrative functions. Selecting one of these will open the appropriate option window or expand the selection



Selecting the arrow at the bottom of the page will collapse or expand the menu bar as shown

Some selections expand to reveal “child” sections, such as [System] which expands to show the log screens and [Settings] which expands to show further administrative options

At the foot of the Admin Portal are links to Synappx Cloud Print

- Privacy Policy
- Terms of Use
- Help

Users and Groups

Users

The Users area is where users from your Cloud Tenant can be added to the Synappx Cloud Print system

You can quickly see your user Status, User Role, Username, Email Address and possible Actions
You are able to add users, remove users, activate/deactivate users, assign & unassign groups, search for users and filter users

Users

Users: 29

+

-

Activate user(s)

Deactivate user(s)

Assign Group

Unassign Group

Filter users

☐	User Name ↑	User Role	Status	Actions
☐	Admin1 Admin1@esbc1.onmicrosoft.com	Tenant Admin		
☐	admin3 admin3@esbc1.onmicrosoft.com	Tenant User		
☐	Artur artur@esbc1.onmicrosoft.com	Tenant Admin		
☐	Auto Test autotest@esbc1.onmicrosoft.com	Tenant Admin		
☐	Claudio Roselli Claudio.Roselli@esbc1.onmicrosoft.com	Tenant Admin		
☐	Deepak Kumar Deepak.Kumar@esbc1.onmicrosoft.com	Tenant Admin		
☐	email test email.test@esbc1.onmicrosoft.com	Tenant User		
☐	Garry Knott garry.knott@esbc1.onmicrosoft.com	Tenant Admin		
☐	IT Inspection1 ITInspection1@esbc1.onmicrosoft.com	Tenant Admin		
☐	Jugal Trivedi Jugal.Trivedi@esbc1.onmicrosoft.com	Tenant Admin		

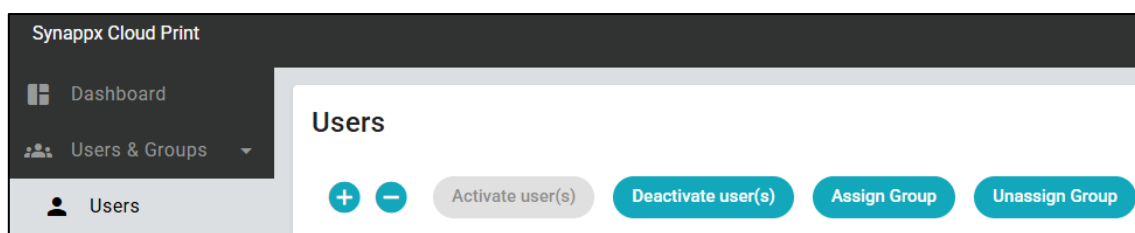
User icons quickly allow you to see if a user is activated or not, if they have a swipe card registered to the account, delete the card, edit the user or to delete the user



Adding Users

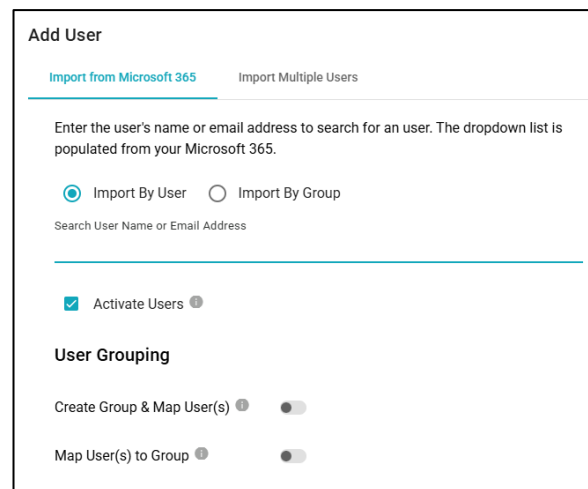
When you first log in, you will only have the initial logged in Admin user available

From the Users screen click the **[+]** button, (as you hover the mouse over the button it will display "Add User")



The options available are to:

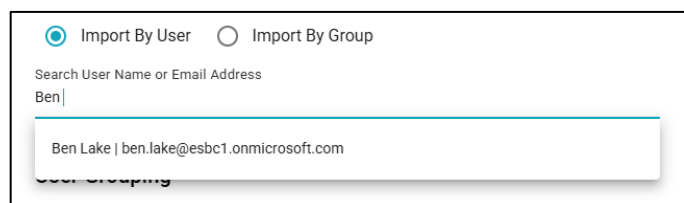
- Import users individually from Microsoft 365 or Google Workspace
- Import users by group
- Auto Activate Users
- Import multiple users via a .csv file



The 'Add User' form has two tabs: 'Import from Microsoft 365' (active) and 'Import Multiple Users'. Below the tabs, there is a text input field for 'Search User Name or Email Address'. Below this, there are two radio buttons: 'Import By User' (selected) and 'Import By Group'. Below the radio buttons, there is a checkbox for 'Activate Users' which is checked. Below the checkbox, there is a section titled 'User Grouping' with two toggle switches: 'Create Group & Map User(s)' and 'Map User(s) to Group', both of which are currently turned off.

Importing Users Individually

Users can be selected by Username or Email address. When characters are typed you will be presented with a list of users from your tenant who match the typed string



This screenshot shows the search dropdown in the 'Add User' form. The 'Import By User' radio button is selected. The search input field contains the text 'Ben'. A dropdown list is open, showing a single result: 'Ben Lake | ben.lake@esbc1.onmicrosoft.com'.

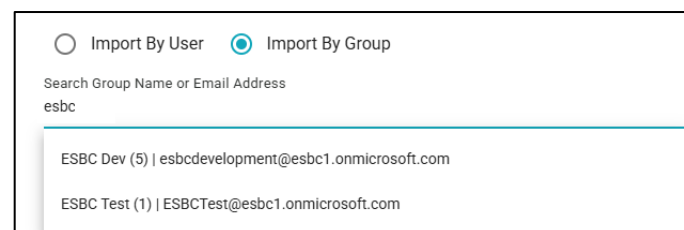
Clicking [Save] will add that user to your Admin Portal

Note: Newly added users are not yet activated

Importing Users by Group

Users can be [Imported by Group] by selecting that option

Start typing the group name and existing groups will be displayed, along with number of users in that group



This screenshot shows the search dropdown in the 'Add User' form with the 'Import By Group' radio button selected. The search input field contains the text 'esbc'. A dropdown list is open, showing two results: 'ESBC Dev (5) | esbcdevelopment@esbc1.onmicrosoft.com' and 'ESBC Test (1) | ESBCTest@esbc1.onmicrosoft.com'.

Selecting the particular group and then selecting [Save] will add all users from that group to the Portal

Note: Newly added users are not yet activated

Auto Activating Users

If enabled, users are automatically activated once imported

If [Generate Pin on User Activation] is enabled in [Settings], users will automatically receive a welcome email and PIN number

PIN Login

Enable PIN Login

Generate PIN on User Activation

User Grouping

When new users or groups of users are added to the portal, it is possible via [User Grouping] to:

- Create a new group on the portal & map users to that group
- Use the imported group name to create a new group & map users to that group
- Map users to an already existing group on the portal

User Grouping

Create Group & Map User(s)

Map User(s) to Group

Create a new group on the portal and add users to that group

- Select [Import by User]
- A single user or a group of users is discovered
- The option [Create Group & Map User(s)] is selected
- Enter the new group name
- Selected user or group of users will be added to the new group

☒ Import By User ☐ Import By Group

Search User Name or Email Address

Bob Benson

User Grouping

Create Group & Map User(s)

Map User(s) to Group

Enter Group Name
Group 1

☐	Name ↑	Description	# of Members
☐	Group 1	Group 1	1

Use the imported group name to create a new group & map users to that group

- Select [Import by Group]
- Search for and select the required group
- Select [Create Group & Map User(s)]
- Use pre-existing group name or change the name
- Users will be imported into the portal and added to the new group

☐ Import By User ☒ Import By Group

Search Group Name or Email Address
ESBC

ESBC Dev (5) | esbcdevelopment@esbc1.onmicrosoft.com

ESBC Test (1) | ESBCTest@esbc1.onmicrosoft.com

User Grouping

Create Group & Map User(s) ☒ ☐

Enter Group Name
ESBC Dev

☐	Name ↑	Description	# of Members
☐	ESBC Dev	ESBC Dev	5

Map users to an already existing group on the portal

- Select [Import by User] or [Import by Group]
- Select [Map User(s) to Group]
- Select existing group
- Click [Save] to add users to that group

☒ Import By User ☐ Import By Group

Search User Name or Email Address
Scott Wells

User Grouping

Create Group & Map User(s) ☐ ☒

Map User(s) to Group ☒

Select Group
Administration Staff

Search

Administration Staff

ESBC Dev

Save

Import Multiple Users via CSV file

By selecting **[Import Multiple Users]** you can import multiple users from an exported CSV file

Please note that the CSV file must be exported from active users within the MS365 or Google Workspace admin centres

The CSV file, once exported, can be edited before importing to the Synappx Cloud Print Admin Portal

Add User

Import from Microsoft 365

Import Multiple Users

Process

1. Export the CSV file of Active users from Microsoft 365 admin center.

2. Edit the CSV to include only necessary users.

3. Return to this screen and upload CSV file.

Choose file

No file chosen

Editing a User

Once imported, a Username can be edited for correction of [Displayed Name] and for ease of identification if required

To do this click on the [Pencil Icon] to the right of the username and select [Edit]



Edit User

User Name

Kevin Yip

From the [Edit User] screen type the required username and click [Save]

Please note the user, even with a changed Username will still log in with their normal email address

Activating Users

Initially the new user status will show as “inactive” via a red user icon
(unless auto activate is selected when adding users)

Claudio Roselli

Claudio.Roselli@esbc1.onmicrosoft.com

Select the user and click **[Activate user]** to activate the user. Active users can be set to inactive by selecting **[Deactivate user]**

Activate user(s)

Claudio Roselli

Claudio.Roselli@esbc1.onmicrosoft.com

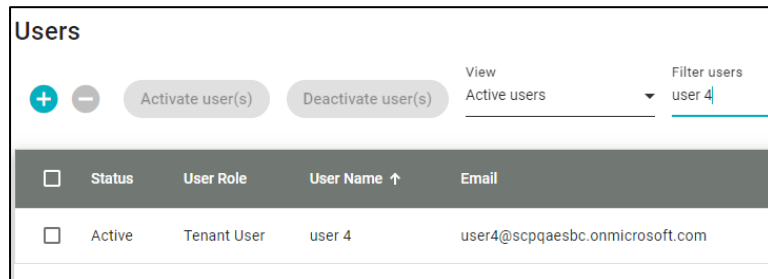
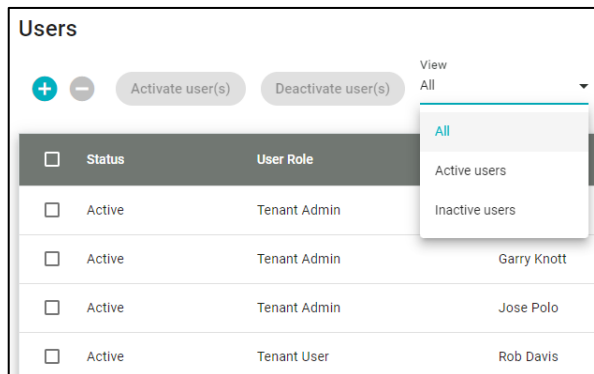
For both activating and deactivating users, multiple users can be selected by using the check boxes to the left of their Username

Filtering Users

You may soon have too many users to easily manage. For this reason, there are two additional tools available in the Users area, the [\[View\]](#) tool and the [\[Filter Users\]](#) tool.

The [\[View\]](#) tool lets you select to display a list of

- [\[All\]](#) Users
- [\[Active Users\]](#)
- [\[Inactive Users\]](#)

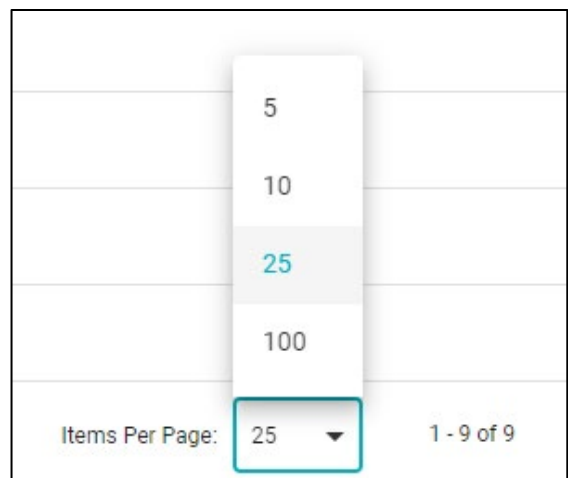


The [\[Filter Users\]](#) tool can be used in conjunction with the [\[View\]](#) tool to further filter users by inputting any part of their username or email address

At the bottom of the user list is an [\[Items per Page\]](#) option

This can be set to 5, 10, 25 or 100 to show as many users as is preferable

The choice you make is remembered for the next time you return to this screen



Unregistering a Swipe Card

If a user has a swipe card registered against their name, they can remove it from the [Users] screen. Any user with a card registered will show this icon against their name:



To unregister the card simply click this icon



On the top right-hand side of the Users screen you are shown how many total users you have available in the Admin Portal.

9 User(s)

You are also able to refresh the data on the Users screen by clicking the [Refresh] button

Refresh data



Deleting a User

Users can be deleted by clicking the [Trash Can] icon



Successfully deleted selected user(s).

Be warned, there is no confirm step, as soon as the trash can is clicked the user is deleted

Groups

Groups and the Group Admin role allow for more granular and distributed management of users and easy control of access to devices

Managing Groups

The creation and management of groups is controlled by Admin Portal administrators. They can:

- Create Groups
- Delete Groups
- Edit Groups
- Add / Move / Remove users from groups
- Assign access to groups for devices

The user role called [Group Admins] gives a user all of the above control, (except device access control). This is a step above a regular user but without the full administrator capabilities.

Assign a User the Group Admin Role

To assign a user the role of Group Admin go to [Settings] – [Admin Users]

Click the [+] button to add a user

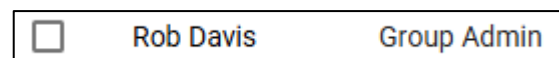


Select the User

From the dropdown menu select the [Role] of [Group Admin]

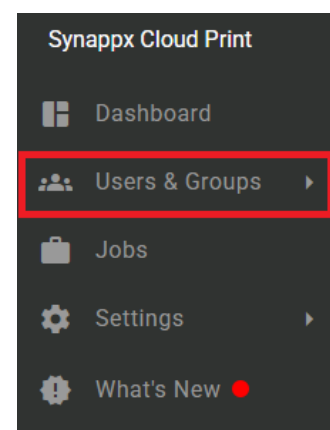
A form titled "Add Admin" with a search bar set to "Admin Name" and "Email". Below, the "Admin Name" field contains "Rob Davis". The "Role" dropdown menu is open, showing "Admin" and "Group Admin", with "Group Admin" highlighted by a red box.

This user now has the ability to manage Groups



A user assigned as [Group Admin] now has an additional section, [Users & Groups], on their Portal menu

The [Group Admin] user can also manage users



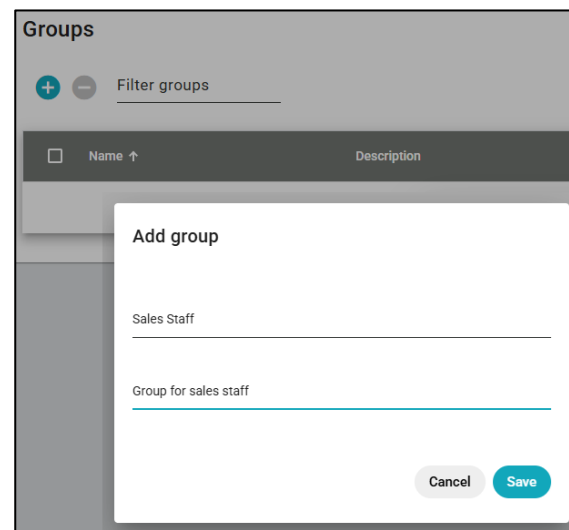
Creating a Group

From the Admin Portal, [Users & Groups] – [Groups], select the + button

Name the group (optional)

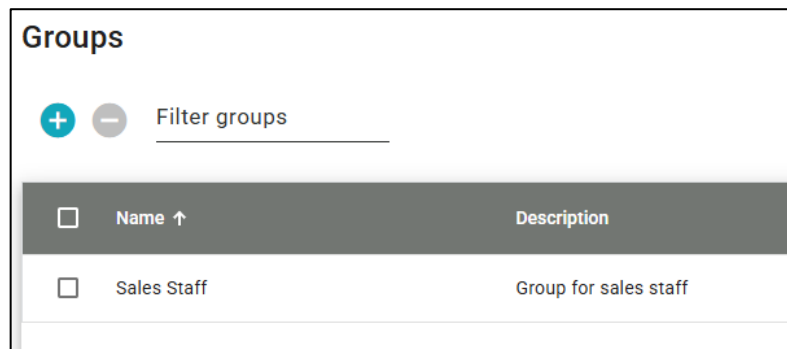
Add a description for the group

Click [Save] to create the group



The screenshot shows the 'Groups' management interface. At the top, there are '+', '-' buttons and a 'Filter groups' search bar. Below is a table with columns 'Name' and 'Description'. An 'Add group' modal is open, showing a form with two fields: 'Sales Staff' and 'Group for sales staff'. At the bottom of the modal are 'Cancel' and 'Save' buttons.

The group is created

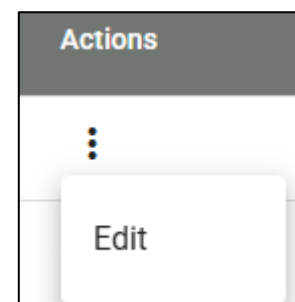


The screenshot shows the 'Groups' page after the group has been created. The table now contains one entry:

☐	Name ↑	Description
☐	Sales Staff	Group for sales staff

To add users to the group click the 3 dots under [Actions] and then click [Edit]

The Edit Group page is displayed



From here you are able to add existing users to your group

Edit group

Sales Staff

Group for sales staff

User Mapping

Select the users that should be allocated to the group

Available Users (0/12)

Search User

☐	Name ↑	Group
☐	Admin1	
☐	Admin2	
☐	Artur	
☐	Bob Benson	
☐	Claudio Roselli	

Items Per Page: 5 1 - 5 of 12 |< < > >|

Selected Users (0/0)

Search User

No selected users

Items Per Page: 5 0 of 0 |< < > >|

→

←

Cancel

Save

Adding Users to a Group

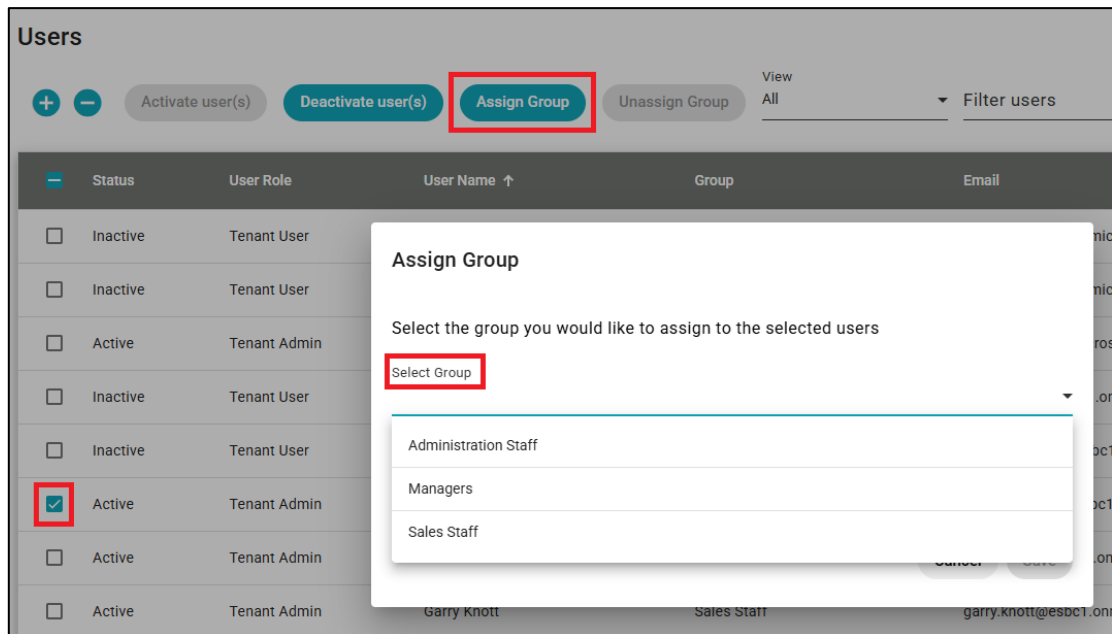
To add users to the group, select the users using the checkbox next to the username, then click the [right arrow] to add them

Once added, users can be removed from the group by selecting them and using the [left arrow]

When happy with your group membership, click the [Save] button to save the users into that group

Users can also be added to groups via the [Users] page

From the [Users] page, select one or multiple users via the checkbox next to their name, click on [Assign Group], and select the group from the dropdown list



The screenshot shows the 'Users' management interface. At the top, there are buttons for '+', '-', 'Activate user(s)', 'Deactivate user(s)', 'Assign Group' (highlighted with a red box), and 'Unassign Group'. Below these is a table with columns: Status, User Role, User Name ↑, Group, and Email. The table lists several users, with one user (Active, Tenant Admin) selected via a checkbox (also highlighted with a red box). An 'Assign Group' dialog box is open, prompting the user to 'Select the group you would like to assign to the selected users'. It features a 'Select Group' dropdown menu (highlighted with a red box) showing a list of groups: Administration Staff, Managers, and Sales Staff.

Then click [Save]

If one or more of the selected users is already in a group, you will receive a warning before confirming the change

Confirmation

2 of the selected users are already assigned to a group. Are you sure you want to continue?

CancelOk

From the [Users] page you are able to see which users are in which groups

☐	Status	User Role	User Name ↑	Group
☐	Active	Tenant Admin	Deepak Kumar	Sales Staff

Users can also be removed from groups by selecting them via the checkbox and clicking [Unassign Group]

In this example you can see that three groups are setup

Groups

+

-

Filter groups

-	Name ↑	Description	# of Members	Actions
☐	Administration Staff	Group for admin staff	2	⋮
☐	Managers	Group for managers	2	⋮
☐	Sales Staff	Group for sales staff	2	⋮

Existing groups can easily be edited to add or remove users by clicking the 3 dots under the [Actions] menu and selecting [Edit]

Note: Please be aware that any user can only ever belong to a single group. If a user already belongs to a group but is added to a new group, they will be removed from their original group

Deleting a Group

Groups can easily be deleted by selecting the check box next to a group and clicking the [-], (delete), button

+

-

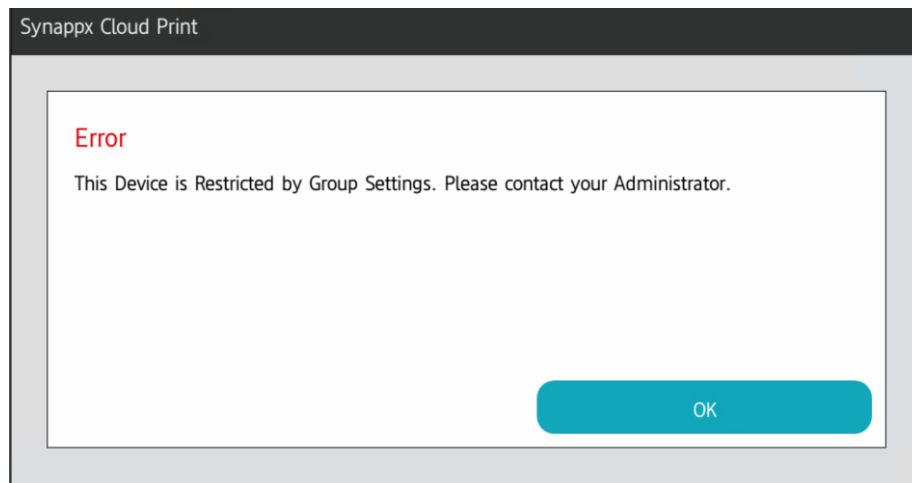
Filter groups

✓	Name ↑
✓	Administration Staff
☐	Managers
☐	Sales Staff

Using Groups to control Device Access

Devices that are activated in your Tenant can be restricted to a certain group, so that only users from within that group are allowed to use Synappx Cloud Print on that device.

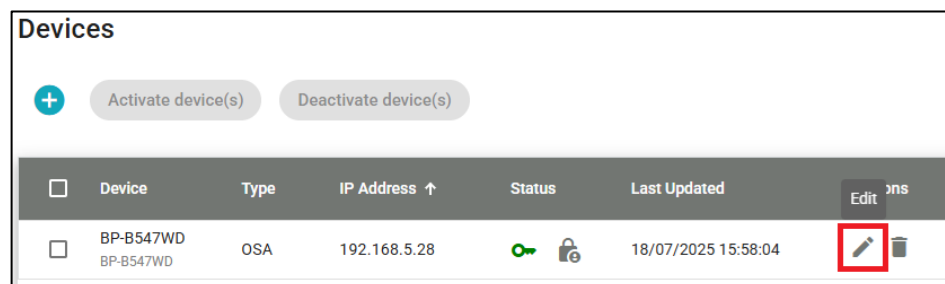
If the device is set to allow access to a particular group and your account does not belong to that group, you will see this message on the device screen:



Setting Device Access

From the Admin Portal – [Devices] – select the device that you wish to control access to

Click the [Edit] icon

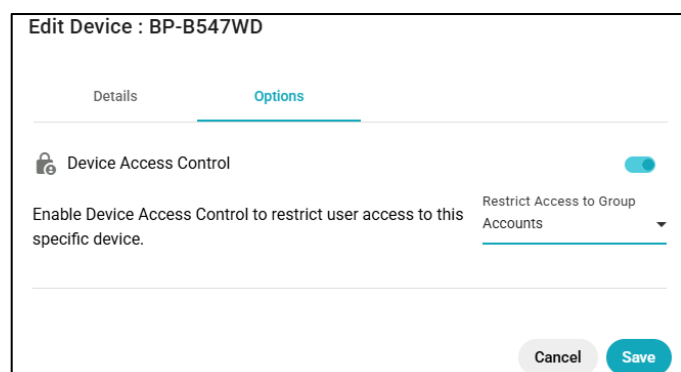


From the [Edit Device] screen:

Select to enable [Device Access Control]

From the [Restrict Access to Group] dropdown menu

Select [Your Group]



Click [Save] to save the settings

Access to that device is now set for the selected group only

Devices (MFP Search and Registration)

The Devices tab displays all of the print devices on your network that you have successfully imported into the Admin Portal. From here you are able to apply your licenses to any devices that you will be using with Synappx Cloud Print

Before searching for devices, ensure that you are running the Windows Client App on a PC on the same network as your MFPs and are logged in to that as the same admin user that is logged in to the Admin Portal

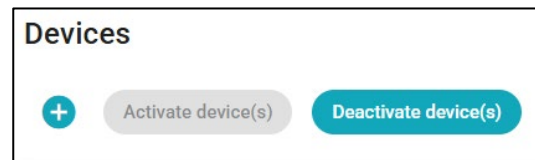
On first login you will have no devices available



Your license information is displayed here. One activated device = 1 license

0 Device(s) 0 Active License(s) 5 Inactive License(s) 5 Total License(s)

To discover MFPs on the network click [+] (Add device)



From [Smart Search]

If you have a single MFP then enter the IP address of that device

If you have multiple devices It is recommended to enter an IP address that will search the local network, such as 192.168.5.0

Add Device

[Smart Search](#) [Add Manually](#)

To start Smart Search, enter any IP address from the network where the printers are connected.

192.168.5.0

[Cancel](#) [Search](#)

To begin searching click [Search]

The smart search will now begin, click OK and wait up to 3 minutes before refreshing the devices page using the [\[refresh\]](#) button



Smart Search

Your MFP search request has been submitted, any newly discovered MFPs will appear in the device list shortly.

OK

The devices List will now be populated

Devices

+

Activate device(s)

Deactivate device(s)

☐	Device	Type ↑	IP Address	Status	Last Updated
☐	BP-30C25 BP-30C25	OSA	192.168.5.22		18/07/2025 10:50:57
☐	BP-70M31 BP-70M31	OSA	192.168.5.46		10/07/2025 10:35:07
☐	BP-B537WR BP-B537WR	OSA	192.168.15.140		16/07/2025 14:36:45
☐	BP-C131PW BP-C131PW	OTHERS	192.168.15.157		15/07/2025 10:18:28
☐	BP-C131PW BP-C131PW	OSA	192.168.15.150		16/07/2025 14:36:47
☐	BP-C533WR BP-C533WR	OSA	192.168.5.52		10/07/2025 10:35:08

To Delete a Device

To delete an existing device, click on the 3 dots, (action), to the right of the device, select [Delete] and confirm

BP-B547WD	192.168.5.28	3301383500	ESBC	Disabled	Edit Delete
BP-B537WR	192.168.5.29	3301382500		Disabled	
MX-C557F	192.168.5.40	75649250E18X5		Disabled	

Confirmation

Are you sure you want to delete device - BP-B547WD?

CancelOk

To Apply a License to a Device, (Activating the Device)

Once devices have been discovered, they will need to be activated. This action assigns a license to a device.

Select the device you wish to activate, select the check box next to the device and click [\[Activate device\]](#) (multiple devices can be selected and activated together).

Note: a green key icon symbolises an [Activated] devices where a red key is for a [Deactivated] device



+

Activate device(s)

Deactivate device(s)

☐	Device	Type ↑	IP Address	Status	Last Updated
☐	BP-30C25 BP-30C25	OSA	192.168.5.22		18/07/2025 10:50:57
☐	BP-70M31 BP-70M31	OSA	192.168.5.46		10/07/2025 10:35:07
☒	BP-B537WR BP-B537WR	OSA	192.168.15.140		16/07/2025 14:36:45

This will activate the device/s and assign a license to that device.

Successfully activated selected device(s).

Your license usage will be reflected depending how many MFPs are licensed

16 Device(s) 16 Active License(s) 4 Inactive License(s) 20 Total License(s)

If an MFP is not licensed, you are not able to run Synappx Cloud Print on that device

Error

This device has not been licensed to use Synappx Cloud Print. Please contact your administrator.

OK

To Deactivate a device, (which will remove the license from that device), select the device by using the check box to the left of the device, then click [[Deactivate Device](#)]

Activate device(s) Deactivate device(s)				
☐	Device	Type ↑	IP Address	Status
☐	BP-30C25 BP-30C25	OSA	192.168.5.22	
☒	BP-70M31 BP-70M31	OSA	192.168.5.46	
☐	BP-B537WR BP-B537WR	OSA	192.168.15.140	

A message will be displayed confirming the deactivation

Successfully deactivated selected device(s).

The device will now show as deactivated

☐	BP-70M31 BP-70M31	OSA	192.168.5.46	
--------------------------	----------------------	-----	--------------	--

You are not able to activate more devices than you have lincenes

An error occurred while activating selected device(s). Please try again.

Filtering Devices

When all of your devices are listed, to assist in finding certain devices you can use filtering.

To filter devices use the [Filter Devices] text entry

Filter devices

esbc

Using the [Filter Devices] text entry area will search all devices listed for any string that you enter which appears in:

- Device
- Type
- IP Address
- Location
- Device Alias
- MAC Address
- Serial Number

☐	Device	Type	IP Address	Status
☐	BP-30C25 BP-30C25	OSA	192.168.5.22	

Naviagting Devices

Devices shown per page can be set using the selector in the bottom right hand side of the Devices screen

Any value set here will be remembered when you next visit this page

If the number of devices is greater that the number reuester per page, you are able to navigate pages with left, right, start and end icons

5

10

25

100

25

1 - 17 of 17

<<

<

>

>>

Deleting a Device

A device can be removed from the Tenant by clicking on the delete button to the right.

☐	Device	Type	IP Address	Status	Last Updated	Actions
☐	BP-30C25 BP-30C25	OSA	192.168.5.22		18/07/2025 10:50:57	

Before deletion a confirmation message is displayed

Confirmation

Device will be deleted. Are you sure?

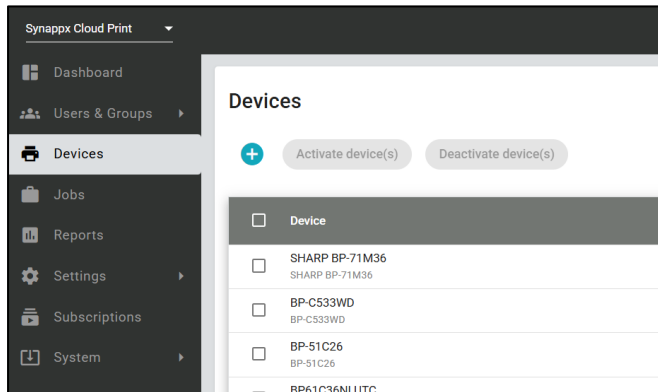
Cancel

Ok

Adding MFPs using 'Direct Connect' method (Group 1 devices only)

In addition to discovering MFPs the 'direct connect' method can also be used. This is particularly useful if the administrator's PC client is not running on the target network.

Navigate to the devices tab and select the '+' button to add a new device:



Select the 'direct connect' option:

A screenshot of the 'Add Device' dialog box. It has three tabs: 'Smart Search', 'Direct Connect' (selected), and 'Add Manually'. The 'Direct Connect' tab contains instructions to copy URLs into the device's configuration portal. There are three URL entries, each with a copy icon to its right. The first entry is for 'MFP Address Application UI (Standard Application Settings)' with URL 'https://qa-cloudprint.synappx.sharp.eu/mfp/home.jsp' and is marked with a blue square '1'. The second entry is for 'MFP Address Application UI (External Accounting Application Settings)' with a long URL and is marked with a blue square '2'. The third entry is for 'MFP Address WebService (External Accounting Application Settings)' with URL 'https://qa-cloudprint.synappx.sharp.eu/mfp/SharpService' and is marked with a blue square '3'. Below the URLs, it shows an 'Expiration' date of '21/04/2026 13:50:12'. A 'Cancel' button is at the bottom right.

Use the 'copy' buttons to copy and paste each URL into the MFPs admin settings

Note: the URLs must be copied to the target MFP before the token expiration setting shown

Status	Address Book	Document Operations	User Control	System Settings
Sharp OSA Settings Condition Settings Standard Application Settings External Accounting Application Settings Embedded Application Settings Polling Setting External Service Connect Standard Application Registration Submit(U) Cancel(C) Back to Menu List				
Standard Application Registration Application Name: Synappx Cloud Print P (Up to 36 characters) Address for Application UI: https://cloudprint.synappx.sharp.eu/mfp (Up to 127 characters) Timeout: 20 seconds(1-60) ☒ Extended Platform Data Size Wide-SVGA ☒ Use Custom Icon File Name: SCP_Icon.png Select File: Browse Notice: The supported file types:JPEG with file extensions jpeg, jpg, jpe and jfif. GIF with file extensions gif. PNG with file extensions png. Submit(U) Cancel(C) Top of Page				

Status	Address Book	Document Operations	User Control	System Settings
Sharp OSA Settings Condition Settings Standard Application Settings External Accounting Application Settings Embedded Application Settings Polling Setting External Service Connect External Accounting Application Settings Submit(U) Update(R) Back to Menu List				
External Accounting Application Settings External Account Control: Enable Server 1 ☐ Use Embedded Application Application Name: SCP Prod (Up to 36 characters) Address for Application UI: https://cloudprint.synappx.sharp.eu/mfp (Up to 127 characters) Address for Web Service: https://cloudprint.synappx.sharp.eu/mfp (Up to 127 characters) Timeout: 20 seconds(1-60) ☒ Extended Platform Data Size: Wide-SVGA Find My Address Search from LDAP Server 2 Disable Application Name: (Up to 36 characters) Top of Page				

After entering the External Accounting Application URLs, select [Update] and reboot the MFP.

The MFP will now be visible in the devices section of the Administrator Portal

Jobs

The Jobs tab displays a list of all currently queued jobs submitted to Synappx Cloud Print. There are tabs to swap between the display of currently queued jobs and a history of processed jobs.

Statistics are also displayed for the logged in user/admin.

Jobs

This month, you have saved:
8 sheets of paper.
19 more than last month

This month
You're in the top:
100% of your company

This month
You're in the top:
50% of Synappx users

Queue

History

Filter jobs

Date/Time ↓	User	Job Name	Job Location	Page Count	Colour Mode	Duplex	Actions
10/11/2023 7:54:11 AM	Scott Wells	SW_4_PAGE_TEST.PDF	Office	4	AUTO	Yes	
10/09/2023 10:40:21 AM	Garry Knott	TEST PAGE	Office	0	AUTO	Yes	
10/02/2023 11:47:14 AM	Scott Wells	AA1-INTERACTIVE-CLAIM-FORM.PDF	Office	0	AUTO	Yes	
09/28/2023 8:10:17 AM	Jose Polo	PRINTTEST.TXT - NOTEPAD	Office	1	AUTO	Yes	

Items Per Page: 100

1 - 4 of 4

<

>

There are a number of administrative actions against jobs available:

- List jobs
- Delete Jobs
- Search jobs
- Job History

Job Queue

The Job Queue displays current jobs that have been submitted but not yet printed. There are seven columns that can be used to “order” the jobs.

Date/Time ↑	User	Job Name	Job Location	Page Count ↓	Colour Mode	Duplex	Actions
-------------	------	----------	--------------	--------------	-------------	--------	---------

- Date / Time
- User
- Job Name
- Job Location
- Page Count
- Colour Mode
- Duplex

To the right of each job, under “Actions,” is a waste bin icon. Clicking this will delete the job from the queue, (and will also remove the job from the users Client).



When you delete a Job you are given a “sustainable” message



Thank you for making sustainable print choices.

Job History

The Job History tab lists all jobs that have passed through the system, including finished, cancelled, or deleted jobs. All Print, Scan and Copy jobs are included in history.

Date/Time	User	Job Name	Job Location ↑	Status
-----------	------	----------	----------------	--------

As with the Job Queue, jobs can be ordered by clicking on the appropriate column, which includes

- Date / Time
- User
- Job Name
- Job Location
- Status

Filtering Jobs

On both Job Queue and Job History pages there is an option for filtering jobs. Admins & Users can filter jobs based on text entry and Start / End dates

Once text entry begins, the jobs are filtered to display only those jobs that match any part of the string entered

Queue	History	
Filter jobs	Start date 17/7/2025	End date 24/7/2025

Items Per Page can be set on Job Queue and Job History pages to show that number of jobs per page. The setting is remembered on the next page visit.

You can switch between multiple pages by using the left, right, start and end icons next to the Items Per Page setting

Items Per Page:	100	1 - 2 of 2	<< < > >>
	5		
	10		
	25		
	100		

On both Job Queue and Job History pages you are presented with your current sustainability credentials.

This applies to any logged in Admin / User

This month, you have saved: 8 sheets of paper. -19 more than last month	This month You're in the top: 100% of your company	This month You're in the top: 50% of Synappx users
--	---	---

Reports

Reports

Execute

Schedule

Filter reports

Report Name ↑	Type	Actions
RPT01 - Usage Overview Report	Predefined	
RPT02 - Usage Per User Report	Predefined	
RPT03 - Device Usage Report	Predefined	
RPT04 - Detailed Job Report	Predefined	

Items Per Page: 25

1 - 4 of 4

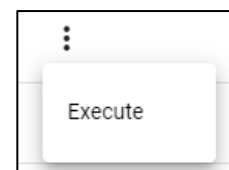
The Reports tab displays a list of available pre-defined, custom, and scheduled reports. Reports are available in PDF or XLS format and cover a wide range of reporting points.

Pre-Defined reports

There are four pre-defined reports

- Usage Overview
- Usage Per User
- Device Usage
- Detailed Job Report

To run a Pre-Defined Report, select the [\[Actions\]](#) button next to the report



You are now able to select a [\[Date Range\]](#) for the report, (default is 10 days), by clicking on the [\[Calendar\]](#) icon

You can also decide to generate the report in PDF or Excel (xlsx) format

Execute Report

RPT01 - Usage Overview Report

Date range
10/1/2023 - 10/10/2023

Export format: ☒ PDF ☐ Excel(xlsx)

Cancel Export

The four pre-defined reports will give the following information:

Usage Overview Report:

- Total Job Page Count
- Page Count Mono
- Page Count Colour
- Page Count Single
- Page Count Duplex
- Page Count Print
- Page Count Copy
- Page Count Scan

Usage Per User Report:

- Usernames
- Page Count Output per user
- Page Count Mono per user
- Page Count Colour per user
- Job Count per user

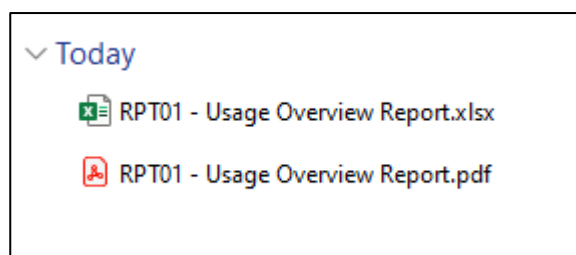
Device Usage Report

- Device Name
- Device IP
- Page Count Output
- Page Count Mono
- Page Count Colour
- Job Count
- Page Count Print
- Page Count Copy
- Page Count Scan

Detailed Job Report

- Job Timestamp
- Job Status
- Department Name
- User Full Name
- Job Type
- Job Filename
- Page Count
- Page Count Mono
- Page Count Colour
- Page Count Single
- Page Count Duplex
- Device Name
- Device IP

When the [\[Export\]](#) button is clicked, the selected report is downloaded to your [\[Downloads\]](#) folder



Once Downloaded the reports can be opened to view

Synapp Cloud Print
Page 1 of 1

RPT01 - Usage Overview Report

Export Date: 10/11/2023 10:58:48
Report Date: 10/1/2023 to 10/10/2023

Totals

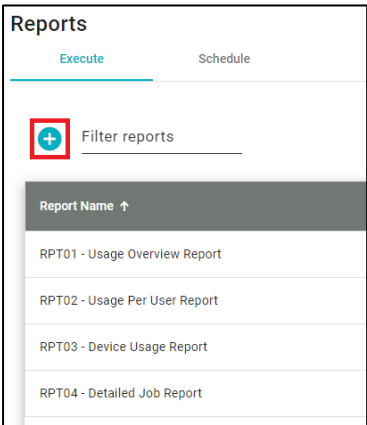
Job Page Count	Job Page Count - Mono	Job Page Count - Colour	Job Page Count - Single	Job Page Count - Duplex	Job Page Count - Print	Job Page Count - Copy	Job Page Count - Scan
51	36	15	9	42	51		0

Top Users

User Full Name	Job Page Count - Output	Job Page Count - Print	Job Page Count - Copy	Job Page Count - Scan
Garry Knott	17	17		0
Scott Wells	34	34		0

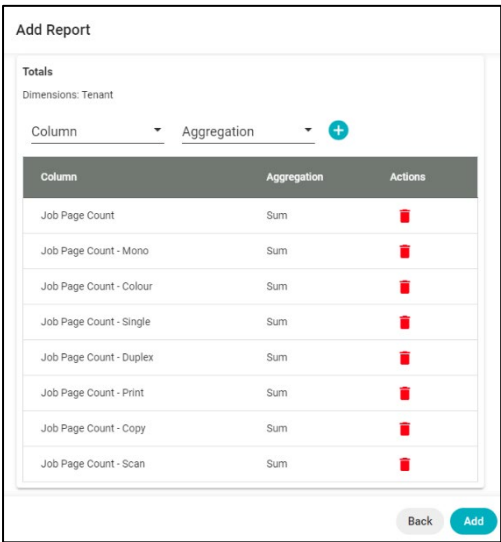
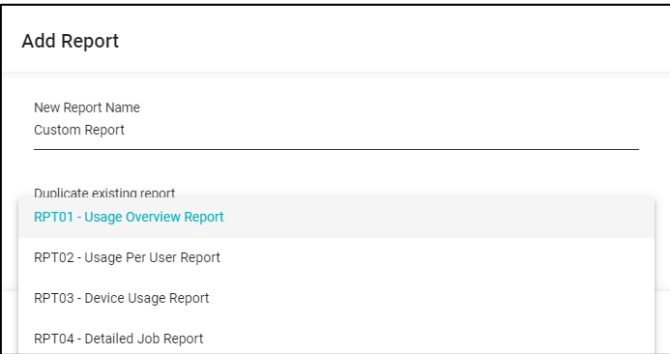
Creating Custom Reports

Custom Reports can be created where you are able to select any of the currently available parameters which will then be used to generate a custom report. The output of custom reports, as with the pre-defined reports, can be in PDF document or Excel format

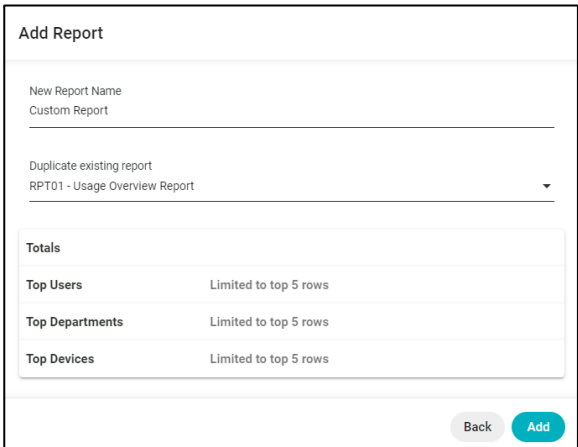


Custom reports can be created by selecting the + button in Reports

The custom report requires a report name, and an existing report selected that it will duplicate



Once a Duplicate existing report has been selected, the new custom report parts can be edited

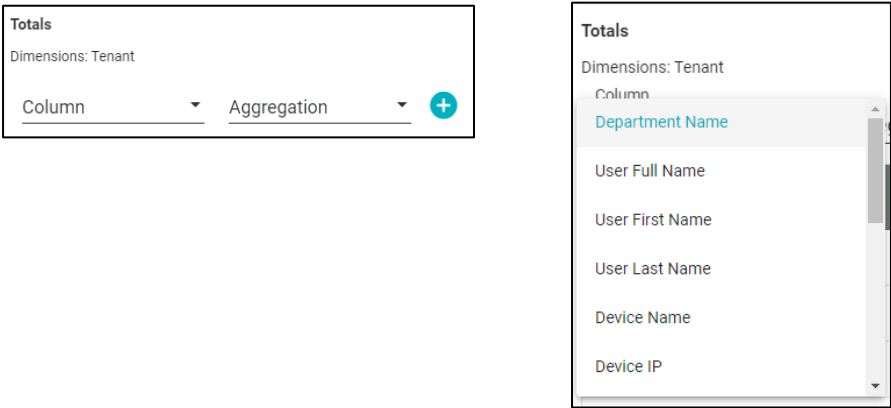


For each section you are able to remove and add all available report parameters

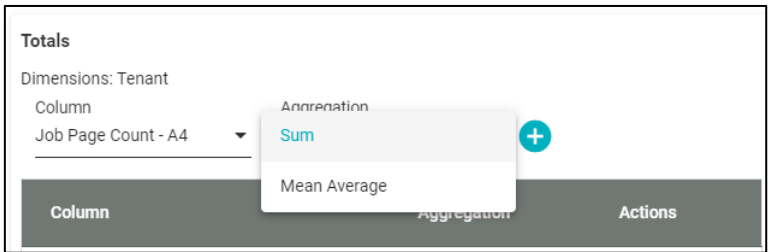
In this example, the parameters are already selected from the existing report, but each one can be easily removed by clicking on the “Trash” icon



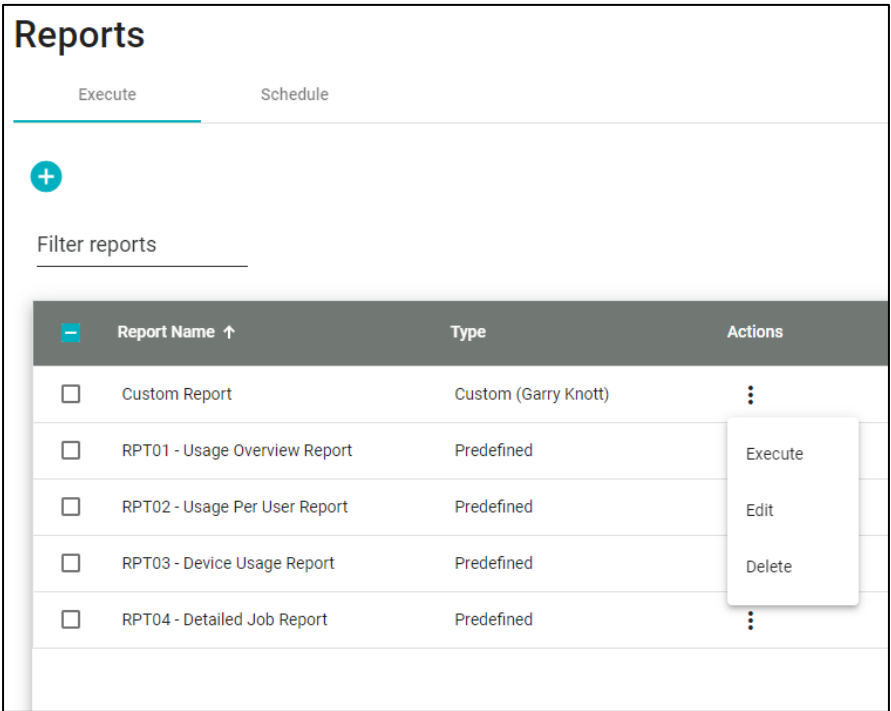
To add report parameters click on [Column](#) to see the list of available parameters, (that are not already selected)



Once selected, some parameters have additional requirements under the [Aggregation](#) column



Each parameter you select for the custom report can be added by using the [Plus](#) button 
When happy with the custom report, click the [Add](#) button to add it to existing reports 
The custom report is now available to be Executed, Edited or Deleted by clicking the [Actions](#) button



When executing the custom report, you are able to select a date range and export format as with regular reports

Execute Report

Custom Report

Date range

01/05/2023 – 31/07/2023



Export format:

☒ PDF

☐ Excel(xlsx)

Back

Export

Synappx Cloud Print

Page 1 of 1

Custom Test Report

Export Date: 10/11/2023 14:21:22

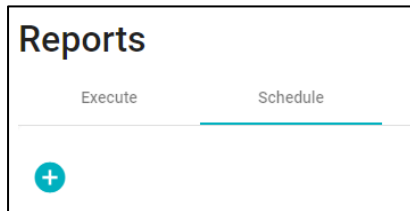
Report Date: 10/1/2023 to 10/10/2023

Detailed Jobs

Job Timestamp	Job Status	Department Name	User Full Name	Job Type	Job Filename	Job Page Count	Mono	Colour	Single	Duplex	Device Name	Device IP
10/05/2023 09:39:18	Completed	ESBC	Jose Polo	Print	*PRINTTEST.txt - Notepad	1	1	0	1	0	CR5-27	192.168.5.27
10/10/2023 08:45:13	Completed	ESBC	Jose Polo	Copy		1	1	0	1	0	theName	192.168.5.6

Creating Scheduled Reports

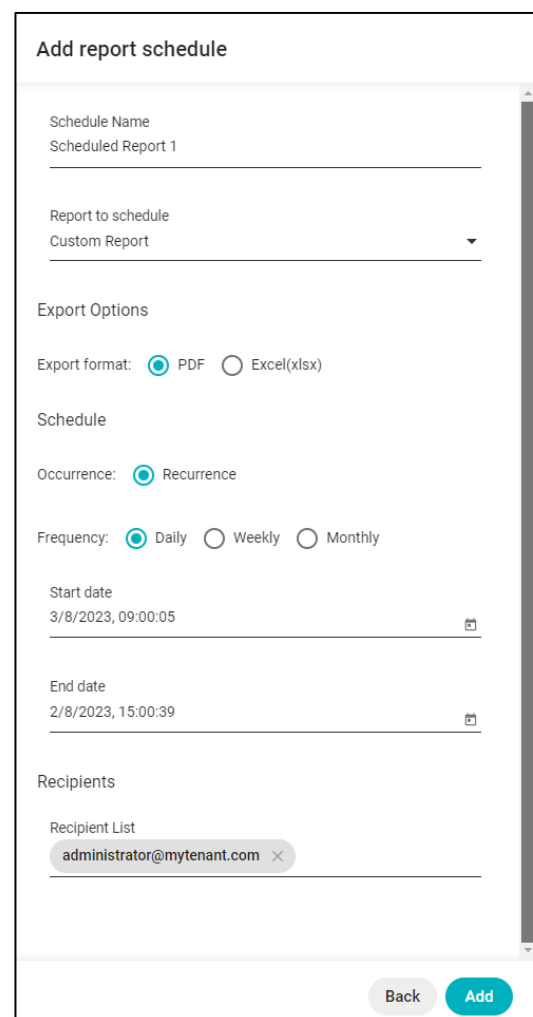
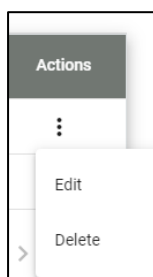
Existing reports can be scheduled to execute at a date & time of your choice. To create a scheduled report click the [Schedule] button in reports then click the [Plus] button



From "Add report schedule" you are able to do the following:

- Give the schedule a name
- Select the report to schedule
- Select Export Options (PDF or Excel)
- Select Occurrence Frequency - (Daily, Weekly or Monthly)
- Select a Start date
- Select an End Date
- Add email Recipients

Click [Add] to add the schedule

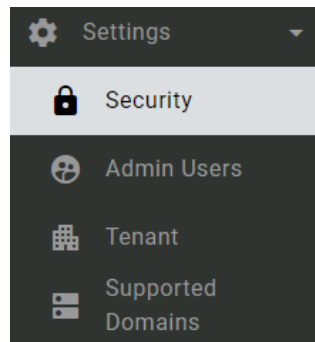
A screenshot of a form titled "Add report schedule". The form contains several sections: "Schedule Name" with the text "Scheduled Report 1"; "Report to schedule" with a dropdown menu showing "Custom Report"; "Export Options" with "Export format" set to "PDF" (selected) and "Excel(xlsx)"; "Schedule" section with "Occurrence" set to "Recurrence" (selected) and "Frequency" set to "Daily" (selected); "Start date" set to "3/8/2023, 09:00:05"; "End date" set to "2/8/2023, 15:00:39"; and "Recipients" with a "Recipient List" containing "administrator@mytenant.com". At the bottom right are "Back" and "Add" buttons.

Scheduled reports can be Edited or Deleted by selecting the three dots at the right-hand side of each schedule

Settings

The Settings option displays a list of SCP settings and provides a number of administrative actions for them. These include:

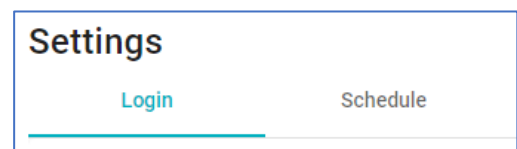
- Security
- Admin Users
- Tenant
- Supported Domains



There are two areas of the Settings Page, Login and Schedule

Login covers device login settings

Schedule covers Job Retention settings

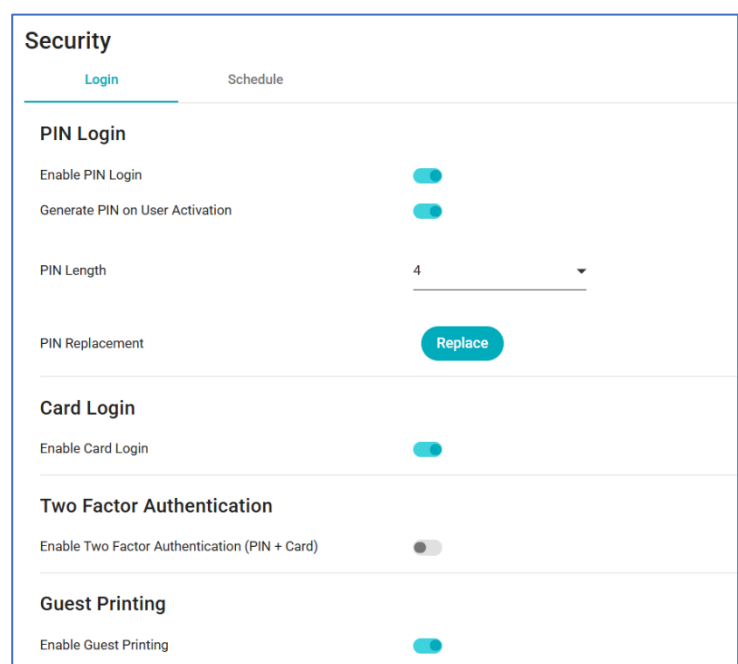


Security

The Security tab is where Device login and job handling options are managed

From this page you can manage:

- PIN Login settings
- Card Login
- Two Factor Authentication
- Guest Printing



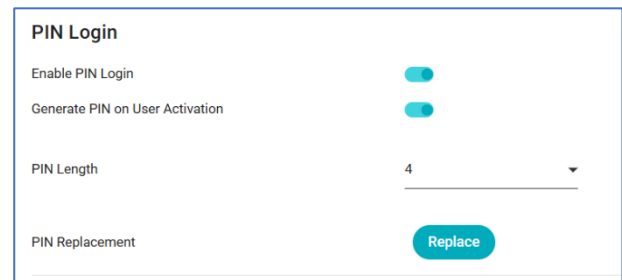
PIN Login

When pin login is enabled, users are able to login to the device using a pin number

A PIN can be generated on User Activation

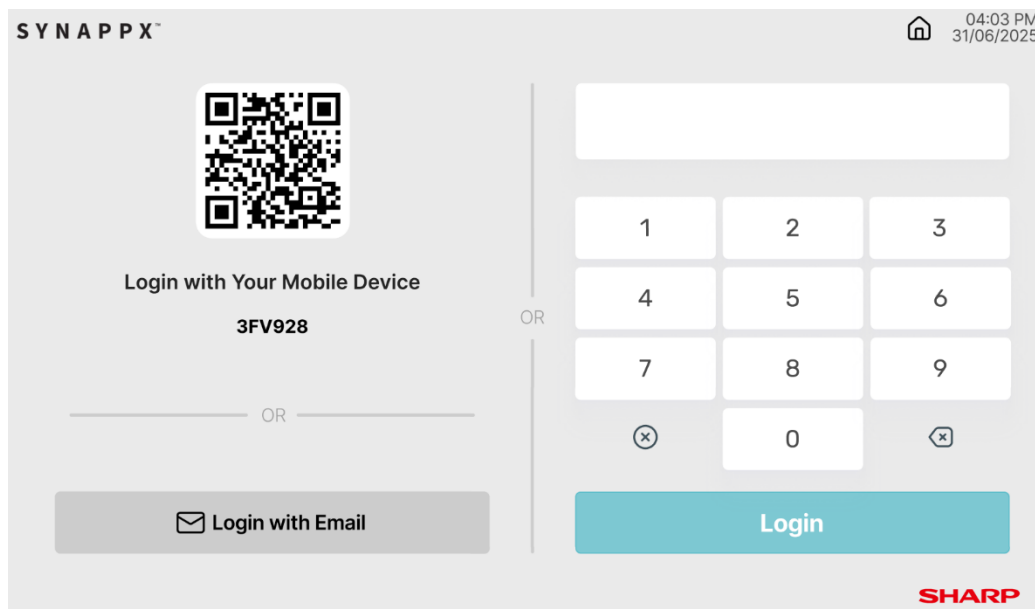
PIN length can be set from 4 to 6 numbers

PIN Replacement can be used by current logged in user to change their Pin number



The screenshot shows the 'PIN Login' configuration page. It includes two toggle switches: 'Enable PIN Login' and 'Generate PIN on User Activation', both of which are turned on. Below these is a 'PIN Length' dropdown menu currently set to '4'. At the bottom, there is a 'PIN Replacement' section with a teal 'Replace' button.

MFP Screen with Pin Login Enabled (Note: Mobile login and Login with email always visible, login with email only displayed on OSA 6 devices and later)



The screenshot displays the MFP login interface. On the left, there is a QR code and the text 'Login with Your Mobile Device' followed by the alphanumeric code '3FV928'. Below this is a horizontal line with 'OR' in the center. At the bottom left is a button with an envelope icon and the text 'Login with Email'. On the right side, there is a numeric keypad with buttons for digits 1-9, 0, a backspace button (X), and a 'Login' button. The top right corner shows the time '04:03 PM' and date '31/06/2025'. The 'SHARP' logo is in the bottom right corner.

Clicking the [[PIN Replacement](#)] button will give the logged in user a choice of up to five different randomly generated PIN numbers.

If the number shown is not acceptable the [[New PIN](#)] button can be used to select another PIN, (up to five tries)

Clicking [[Confirm](#)] will confirm that PIN number for the admin / user

PIN Replacement

5268

Here is your new PIN (5268) and your old PIN will be disabled.
Are you sure to update your PIN?

Cancel

New PIN

Confirm

Generate PIN on User Activation

Selecting to generate a PIN on user activation will trigger the system to email the newly activated user with a PIN code that they can use for login to their account on the device

Generate PIN on User Activation



Good news!

A Synappx Cloud Print invitation has been sent to you by your Synappx administrator **Garry Knott**.
Now you can:

- Send and retrieve your print jobs Securely
- Use any of your Synappx Cloud Print enabled devices to retrieve your print jobs
- Monitor your print sustainability profile

Download and install the Synappx Cloud print app from the Microsoft Store

This PIN can be used to authenticate to your MFPs:

1098

Card Login

Enabling Card Login will allow users to register and login to the device/s with swipe cards

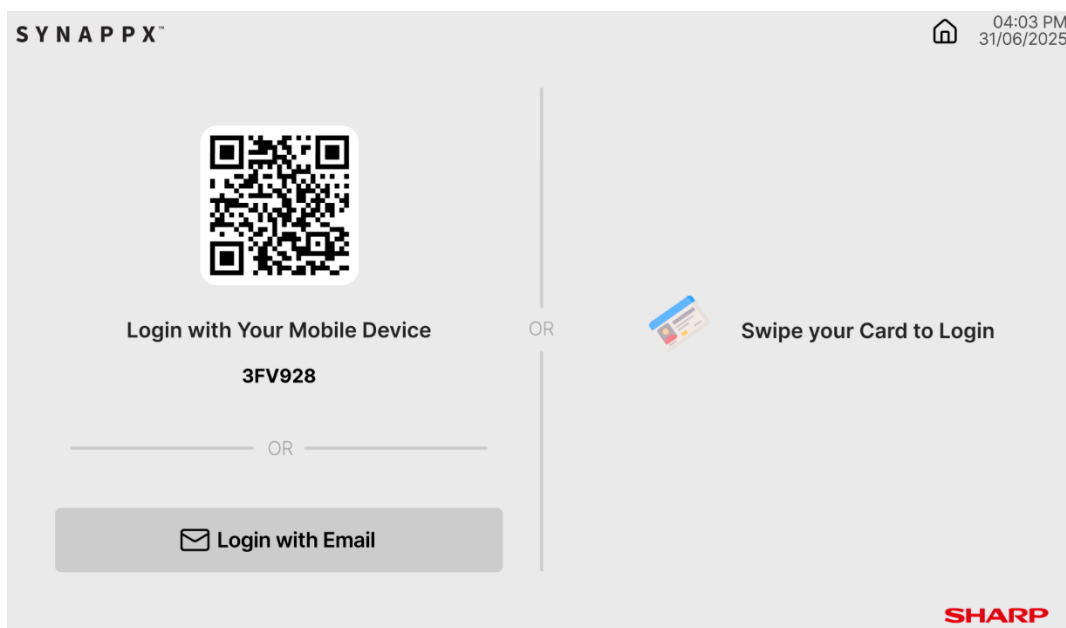
Maximum Unsuccessful Attempts can be set from 1 to 10

Card Login

Enable Card Login



MFP Screen with Card Login enabled (Note: Mobile login and Login with email always visible, login with email only displayed on OSA 6 devices and later)



Two Factor Authentication

Enabling Two Factor Authentication will require users to login to the MFP using their PIN and Card swipe

Two Factor Authentication

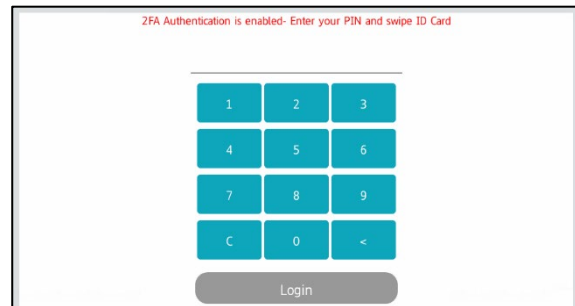
Enable Two Factor Authentication (PIN + Card)



Any change on the Security page will require the [\[Update\]](#) button to be clicked to save the changes

Update

Once Two Factor Authentication is enabled, the login screen defaults to PIN code entry and users will be informed that they need to enter a PIN and then swipe their ID Card



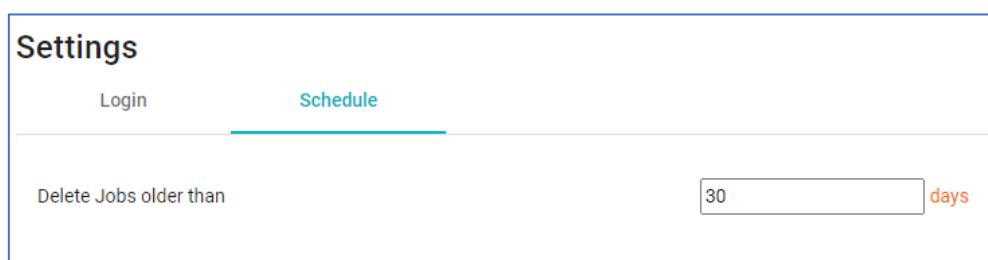
Guest Printing

Guest printing is described in detail in Addendum C at the end of this guide



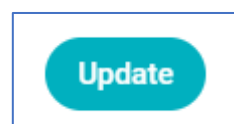
Settings – Schedule

Under the Settings – Schedule tab is the setting for Job Retention



The setting [[Delete Jobs Older Than](#)] can be set from 1 to 365 days. Any jobs older than the set number of days will be automatically deleted. Jobs are deleted at midnight on the qualifying day.

When the setting is changed, the [[Update](#)] button must be clicked to save the change

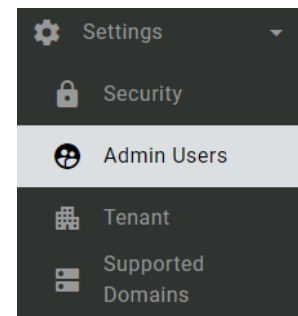


Any changes made in the settings – Security pages will affect ALL Devices

Admin Users

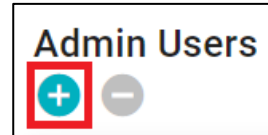
Admin user management is managed from [Settings – Admin Users]

From here you are able to add an existing user as an Admin for the Portal



Admin Users			
+ -			
☐	Admin Users ↑	Role	Email Address
☐	Admin1	Admin	Admin1@esbc1.onmicrosoft.com
☐	Deepak Kumar	Admin	Deepak.Kumar@esbc1.onmicrosoft.com
☐	EU Admin	Primary Admin	philip.chow@esbc1.onmicrosoft.com
☐	Garry Knott	Admin	garry.knott@esbc1.onmicrosoft.com

To add an Admin, click the **[+]** button



Users can be searched by Username or Email address

Add Admin

Search by ☒ Admin Name ☐ Email

Admin Name
Rob Davi

Rob Davis | Rob.Davis@esbc1.onmicrosoft.com

When selected, clicking **[Save]** will bring up a confirmation box

Clicking **[OK]** will add that user as an Admin for the Portal

Add Admin

Search by ☒ Admin Name ☐ Email

Admin Name
Rob Davis

Save

Add Admin User

Are you sure you want to add: Rob Davis ?

OK **Cancel**

Admin added successfully

OK

The selected user will now show in the list of Portal Admins

Admin Users			
+ -			
☐	Admin Users ↑	Role	Email Address
☐	Artur	Admin	artur@esbc1.onmicrosoft.com
☐	Claudio Roselli	Admin	Claudio.Roselli@esbc1.onmicrosoft.com
☐	Rob Davis	Group Admin	Rob.Davis@esbc1.onmicrosoft.com
☐	philip.chow@esbc1.onmicrosoft.com	Primary Admin	philip.chow@esbc1.onmicrosoft.com

To remove an Admin from [Admin Users] click the [\[trash\]](#) can button next to the admin name

Remove Admin

Are you sure you want to remove: Rob Davis ?

OK

Cancel



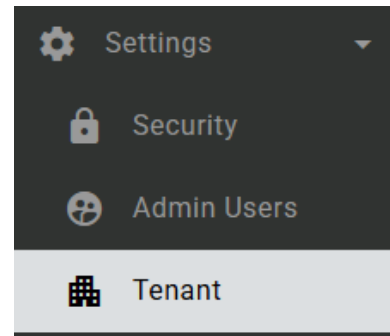
Admin Users		
+ -		
☐	Admin Users ↑	Role
☒	Jon Breen	Admin

This can also be achieved by selecting the admin check box and then using the [\[-\]](#) button

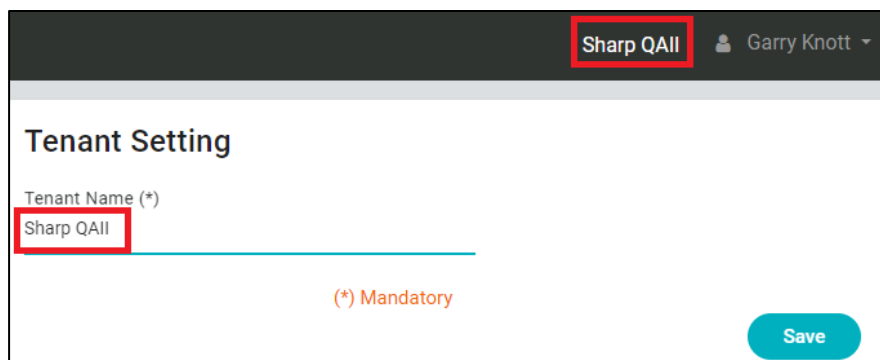
The role of [Group Admin] is covered in the section [\[Groups\]](#)

Tenant

The Tenant area of [Settings] currently displays the current saved Company Tenant



This can be changed and saved, and will then be displayed on all Admin portal screens next to the logged in User/Admin name

A screenshot of a 'Tenant Setting' form. The form has a dark grey header bar with the text 'Sharp QAll' and a user profile icon labeled 'Garry Knott'. The main content area is white and contains the title 'Tenant Setting'. Below the title is a label 'Tenant Name (*)' and a text input field containing 'Sharp QAll'. The input field is highlighted with a red border. Below the input field is a red text label '(*) Mandatory'. At the bottom right of the form is a blue 'Save' button.

Subscriptions

The Subscriptions tab shows licenses and subscriptions for the various Synappx products assigned to the admin's company's tenant.

There is no functionality other than information display

The screenshot displays the Synappx Cloud Print management interface. On the left is a dark sidebar with navigation options: Dashboard, Users, Devices, Jobs, Reports, Settings, Subscriptions (highlighted), and System. The main content area is divided into two sections. The top section, titled 'Synappx Cloud Print Device License', provides a summary of license status: Total License(s): 25, Assigned License(s): 7, Unassigned License(s): 18, License(s) in Archive Period: 0, and License(s) in Grace Period: 1. The bottom section, which has a light gray background, displays details for a specific subscription: E-ID: 8fc1d16d-a438-44cc-baa6-ad25863bf8a7, Reference Source ID: ahdzc87je06kf87qu3lzp1as, License(s): 1, and Auto-renewal set for 11/1/2023.

Synappx Cloud Print

- Dashboard
- Users
- Devices
- Jobs
- Reports
- Settings
- Subscriptions**
- System

Synappx Cloud Print Device License

Total License(s): 25

Assigned License(s): 7

Unassigned License(s): 18

License(s) in Archive Period: 0

License(s) in Grace Period: 1

E-ID: 8fc1d16d-a438-44cc-baa6-ad25863bf8a7

Reference Source ID: ahdzc87je06kf87qu3lzp1as

License(s): 1

Auto-renewal set for 11/1/2023

System

Admin Log

The Admin Log is available so that there is visibility over the actions of all Portal Admins

Admin Log

Synappx Cloud Print

Start dateEnd dateExport

ViewGarry Knott

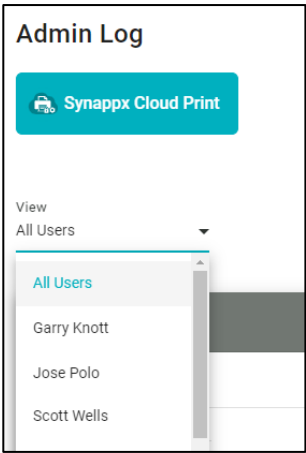
Log Date ↓	User Name	Service Name	Category	Action
10/13/2023 11:52 AM	Garry Knott	Cloud Print	Login	Login
10/11/2023 4:16 PM	Garry Knott	Cloud Print	Login	Login
10/11/2023 4:11 PM	Garry Knott	Cloud Print	Logout	Logout
10/11/2023 4:07 PM	Garry Knott	Cloud Print	Tenant	Tenant name changed
10/11/2023 4:07 PM	Garry Knott	Cloud Print	Tenant	Tenant name changed
10/11/2023 4:07 PM	Garry Knott	Cloud Print	Login	Login
10/11/2023 4:06 PM	Garry Knott	Cloud Print	Logout	Logout

The default view shows all recent actions. Each column can be sorted in ascending or descending order by clicking on the column header.

You are able to select all Admins or filter just a single Admin action

Currently the Admin actions are logged are:

- Logout
- Login
- Add Admin User
- Remove Admin User
- Export Admin Log
- Change Tenant Name



Log Date ↓	User Name	Service Name	Category	Action
------------	-----------	--------------	----------	--------

The admin log page displays:

- Date of logged action
- Admin Username
- Cloud Service Name
- Category
- Action

The Admin Log can be exported by selecting a [start date], [end date] and clicking the [Export] button

Start date	End date	
10/4/2023	10/12/2023	<button>Export</button>

You are informed that the download has started and when it is completed

Download will start now

1 file(s) will be downloaded.

It will take 1 minute(s) to complete the download.

Please don't leave the page and don't click the export button till the download is complete.

1 file(s) have been downloaded.

OK

The exported file is a zipped .csv file that can be opened with Excel

The csv file gives more information on each action than is displayed on the Admin Log screen

The csv file includes:

- Local Date & Time
- Tenant
- Device Type
- Hostname
- Role
- Detail
- Category
- IP Address
- Application
- Log Date & Time
- Device Name
- Action
- Username
- User ID
- App Version
- Service Name

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	No.	Local date time	Tenant	Device Type	Hostname	Role	Detail	Category	IP address	Application	Log Date/Time	Device name	Action	User Name	User ID	App Version	Service name	
2	1	08/04/2023, 04:45:14.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	182.72.144.36:4	Admin Portal	2023-08-04T09:15:14+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
3	2	08/04/2023, 05:28:15.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T09:58:15+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
4	3	08/04/2023, 05:32:02.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:02:02+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
5	4	08/04/2023, 05:53:35.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:23:35+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
6	5	08/04/2023, 05:54:49.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	182.72.144.37:2	Admin Portal	2023-08-04T10:24:49+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
7	6	08/04/2023, 05:55:07.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:25:07+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
8	7	08/04/2023, 05:55:42.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:25:42+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
9	8	08/04/2023, 05:56:31.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	182.72.144.37:2	Admin Portal	2023-08-04T10:26:31+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
10	9	08/04/2023, 05:57:43.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:27:43+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
11	10	08/04/2023, 05:58:26.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:28:26+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
12	11	08/04/2023, 05:59:00.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:29:00+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
13	12	08/04/2023, 06:00:13.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	203.197.160.37:2	Admin Portal	2023-08-04T10:30:13+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
14	13	08/04/2023, 06:00:37.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	182.72.144.37:2	Admin Portal	2023-08-04T10:30:37+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
15	14	08/04/2023, 06:01:05.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Admin	Tenant na	Tenant		203.197.160.37:2	Admin Portal	2023-08-04T10:31:05+05:30		Tenant name	test admin	testadmin@4.7-SNAPSHO'	Go		
16	15	08/04/2023, 06:01:16.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Admin	Tenant na	Tenant		203.197.160.37:2	Admin Portal	2023-08-04T10:31:16+05:30		Tenant name	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		
17	16	08/04/2023, 06:01:27.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Admin	Tenant na	Tenant		203.197.160.37:2	Admin Portal	2023-08-04T10:31:27+05:30		Tenant name	test admin	testadmin@4.7-SNAPSHO'	Go		
18	17	08/04/2023, 06:03:15.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Admin	Login	Login	Login	182.72.144.37:2	Admin Portal	2023-08-04T10:33:15+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Go		
19	18	08/04/2023, 06:05:11.	esbcl-onmicl	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	Tenant Admin	Login	Login	Login	182.72.144.37:2	Admin Portal	2023-08-04T10:35:11+05:30		Login	test admin	testadmin@4.7-SNAPSHO'	Cloud Print		

System Log

The System Log will display events related to the system and its components. Generally these events will be errors, such as a failed login or a list not displayed.

System Log

S Admin Portal

Start date

▼

End date

▼

View
All Users / Agents

▼

Log Date ↓	User Name / Agent Name	Application	Category	Error
10/11/2023 1:14 PM	Rob Davis	Admin Portal	Login	Failed to Login
10/11/2023 11:56 AM	admin3	Admin Portal	Login	Failed to Login
10/11/2023 9:14 AM	Rob Davis	Admin Portal	Login	Failed to Login
10/1/2023 8:07 AM	test admin	Admin Portal	Admin	Failed to get Admin list
10/1/2023 8:07 AM	test admin	Admin Portal	Admin	Failed to get Admin list

The

System Log page displays:

- Log Date
- Username / Agent Name
- Application
- Category
- Error

Each column can be sorted in ascending or descending order by clicking on the column header.

The System Log can be exported by selecting a [start date], [end date] and clicking the [Export] button

Start date
10/4/2023

▼

End date
10/12/2023

▼

Export

You are informed that the download has started and when it is completed

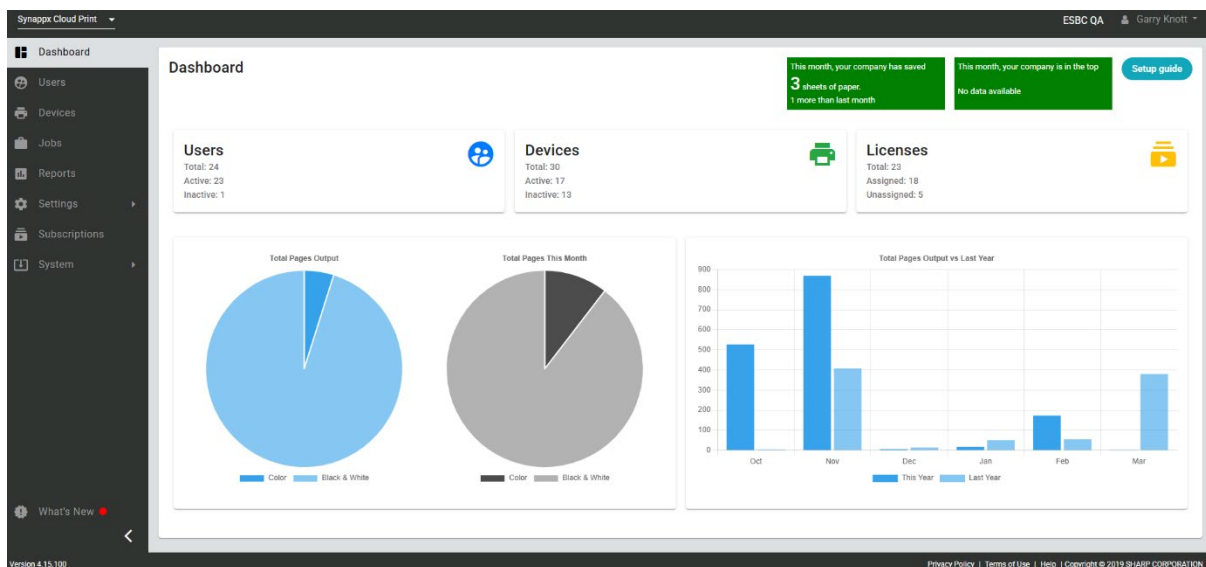
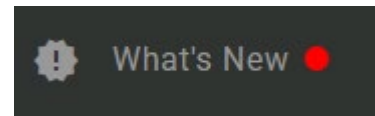
The exported file is a zipped .csv file that can be opened with Excel

The csv file gives more information on each action than is displayed on the Admin Log screen

What's New – Notification

New features and improvements are made available to users and administrators in every new software release. The what's new notification in the menu bar immediately notifies of new features and provides an easy and convenient way to learn more

When new features are available a red dot is visible next to the What's New notification.



Clicking the What's New notification will take users to the Synappx Cloud Print support website where further information is available.

SHARP
Be Original.

Synappx Cloud Print | Synappx Collaboration Hub | Synappx Go | Synappx Meeting | Synappx FAQs | What's New | Contact Us

What's New
Discover the features and benefits of each version of Synappx.

Version 3.4

Synappx Collaboration Hub

- QR code for easy meeting start is now supported.
- Kiosk Mode helps simplify and control the meeting experience for users.
- In-Room PC Security helps secure the meeting in-room PC by providing IT Admins access to Windows security settings.

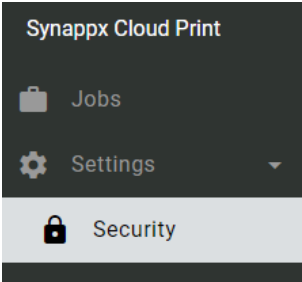
Synappx Meeting

- Start meetings from the Windows application by using the pairing code.
- Control the In-room PC microphone, camera, and volume within the Synappx meeting launcher.
- Bug fixes and usability improvements

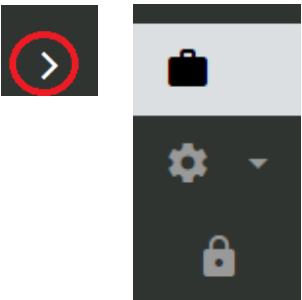
User Portal

When a Synappx Cloud Print User logs into the Portal, they are able to see the following screens:

- Jobs
- Security - Pin Login

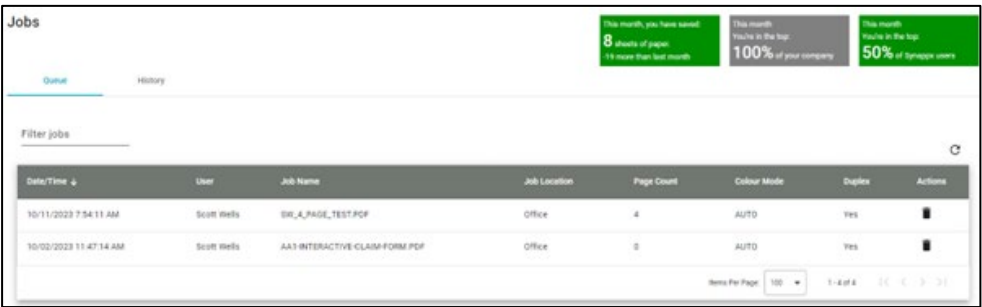


The user is able to minimise the menu by using the [Hide] icon



Jobs

The Jobs page displays a list of currently available queued print jobs



There are a number of user actions against jobs available:

- List jobs
- Delete Jobs
- Search jobs
- Job History

Job Queue

The Job Queue displays current jobs that have been submitted but not yet printed. These are:

Date/Time ↑	User	Job Name	Job Location	Page Count ↓	Colour Mode	Duplex	Actions
-------------	------	----------	--------------	--------------	-------------	--------	---------

- | | |
|----------------|---------------|
| • Date / Time | • Page Count |
| • User | • Colour Mode |
| • Job Name | • Duplex |
| • Job Location | |

To the right of each job, under “Actions,” is a waste bin icon. Clicking this will delete the job from the queue, (and will also remove the job from the users Client).



When you delete a Job you are given a “sustainable” message



Thank you for making sustainable print choices.

Job History

The Job History tab lists all jobs that have passed through the system, including finished, cancelled, or deleted jobs. All Print, Scan and Copy jobs are included in history.

Date/Time	User	Job Name	Job Location ↑	Status
-----------	------	----------	----------------	--------

As with the Job Queue, jobs can be ordered by clicking on the appropriate column, which includes

- Date / Time
- User
- Job Name
- Job Location
- Status

Filtering Jobs

On both Job Queue and Job History pages there is an option for filtering jobs

Once text entry begins, the jobs are filtered to display only those jobs that match any part of the string entered

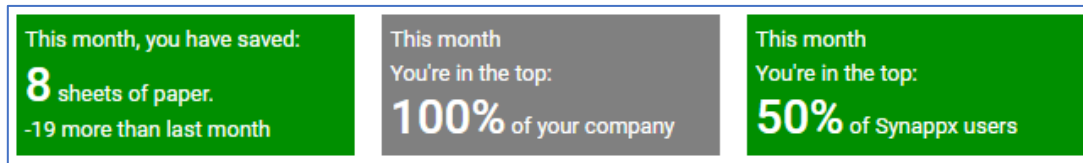
Filter jobs scott			
Date/Time	User	Job Name	
10/11/2023 7:54:11 AM	Scott Wells	SW_4_PAGE_TEST.PDF	
10/02/2023 11:47:14 AM	Scott Wells	AA1-INTERACTIVE-CLAIM-FORM.PDF	

Items Per Page can be set on Job Queue and Job History pages to show that number of jobs per page. The setting is remembered on the next page visit.

You can switch between multiple pages by using the left, right, start and end icons next to the Items Per Page setting

Items Per Page:	100	1 - 2 of 2	< > < >
	5		
	10		
	25		
	100		

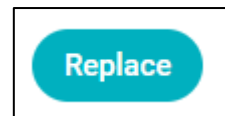
On both Job Queue and Job History pages you are presented with your current “Green” credentials.



PIN Login

From [Settings] – [Security] the user is able to change their PIN for PIN login on the MFP

Clicking the [Replace] button will give the logged in user a choice of up to five different randomly generated PIN numbers.



If the number shown is not acceptable the [New PIN] button can be used to select another PIN, (up to five tries)

Clicking Confirm will confirm that PIN number for the admin / user

PIN Replacement

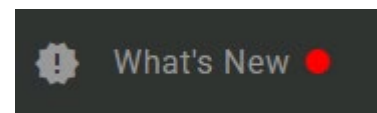
0860

Here is your new PIN (0860) and your old PIN will be disabled.
Are you sure to update your PIN?

Cancel New PIN Confirm

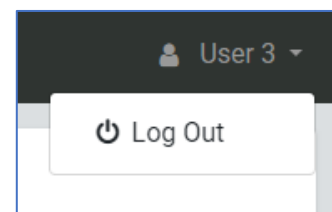
What's New

New features and improvements are made available to users and administrators in every new software release. The what's new notification in the menu bar immediately notifies of new features and provides an easy and convenient way to learn more



Logout

The user can logout by clicking the [Logout] button



Configure MFP settings - Group 1 Device

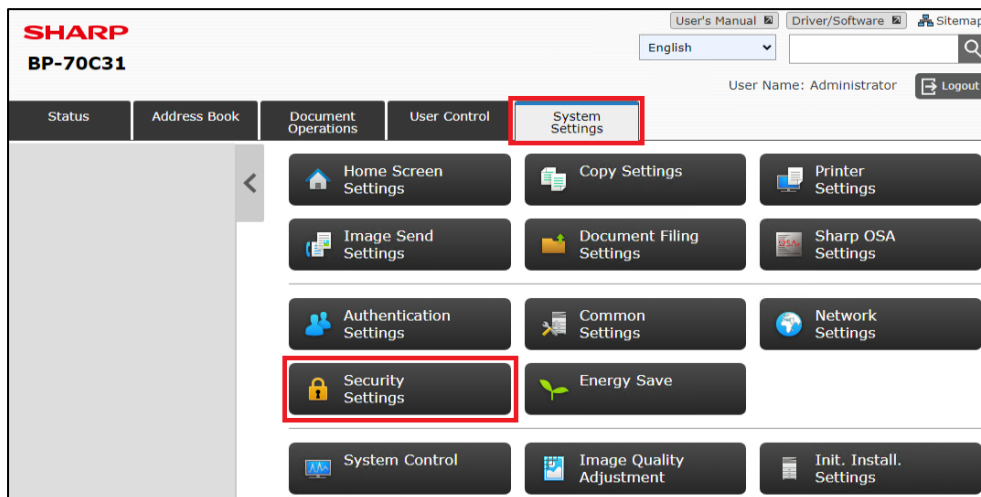
Note: If the MFP you are setting up does not appear in the [Synappx Cloud Print Portal] – [Devices] list, you will receive an Error 500 message when trying to connect the MFP to the service

Minimum MFP Requirements:

- A Sharp Group 1 MFP running OSA version 5.5 or above
- EAM (AMX3) key installed

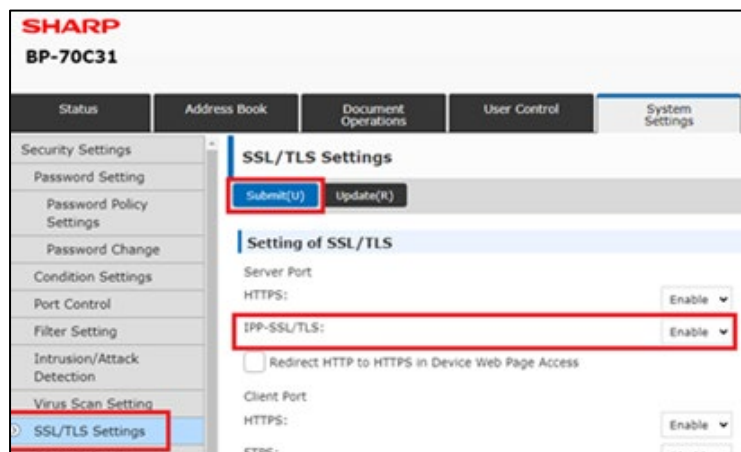
Input the [IP address] of the MFP into a web browser to navigate to the configuration page of the MFP. The default Username and password is [admin](#).

Step 1. Security Settings



Go to [System Settings](#) then [Security Settings](#)

Select [SSL/TLS Settings](#) in the left-hand menu bar, change [IPP-SSL/TLS](#) setting is set to [Enable](#) then select [Submit](#) and [Reboot](#)



Step 2. Active Directory Settings

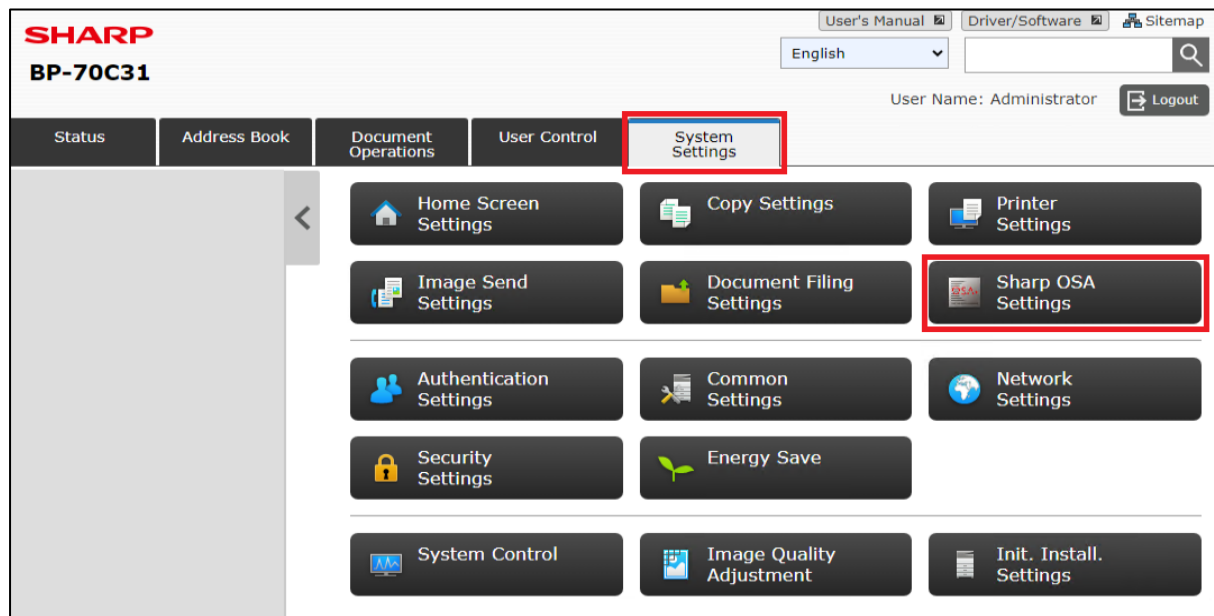
Once Rebooted, Go to [System Settings](#) then [Network Settings](#) then [Active Directory](#)

Ensure that [Domain Name] is **blank**

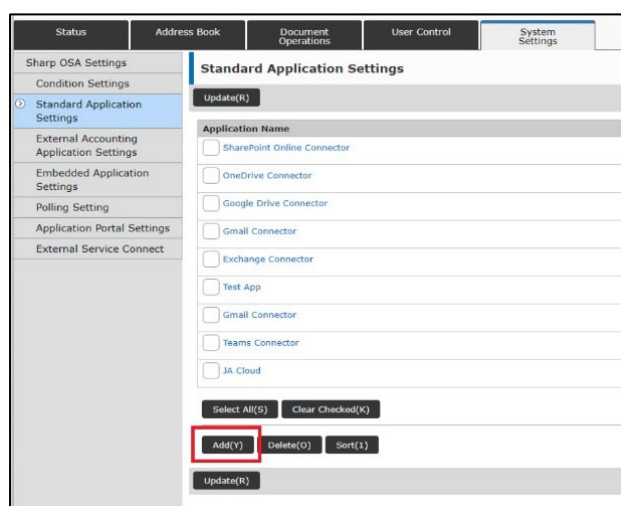
Domain Name:

Step 3. Standard OSA Settings

Click on the [System Settings](#) tab and select [Sharp OSA Settings](#)



Click [Standard Application Settings](#) then [Add](#)



Enter the following information:

- Application name: [Synappx Cloud Print](#)
- Address for Application UI: <https://cloudprint.synappx.sharp.eu/mfp/home.jsp>
- Check the 'Extended Platform' box.
- Ensure Data Size is set to: Wide-SVGA
- Click [Submit](#)

(this can be placed anywhere in the list of Standard Applications)

Standard Application Registration

Application Name: SCP Production

Address for Application UI: <https://cloudprint.synappx.sharp.eu/mfp>

Timeout: 20 seconds(1-60)

☒ Extended Platform

Data Size: Wide-SVGA

Step 4. External Accounting Application Settings

Now go to [External Accounting Application Settings](#):

External Accounting Application Settings

[Submit\(U\)](#) [Update\(R\)](#)

External Account Control: Enable

Server 1: Enable

☐ Use Embedded Application Not Set

Application Name: Synappx Cloud Print (Up to 36 characters)

Address for Application UI: <https://cloudprint.synappx.sharp.eu/mfp> (Up to 127 characters)

Address for Web Service: <https://cloudprint.synappx.sharp.eu/mfp> (Up to 127 characters)

Timeout: 20 seconds(1-60)

☒ Extended Platform

Data Size: Wide-SVGA

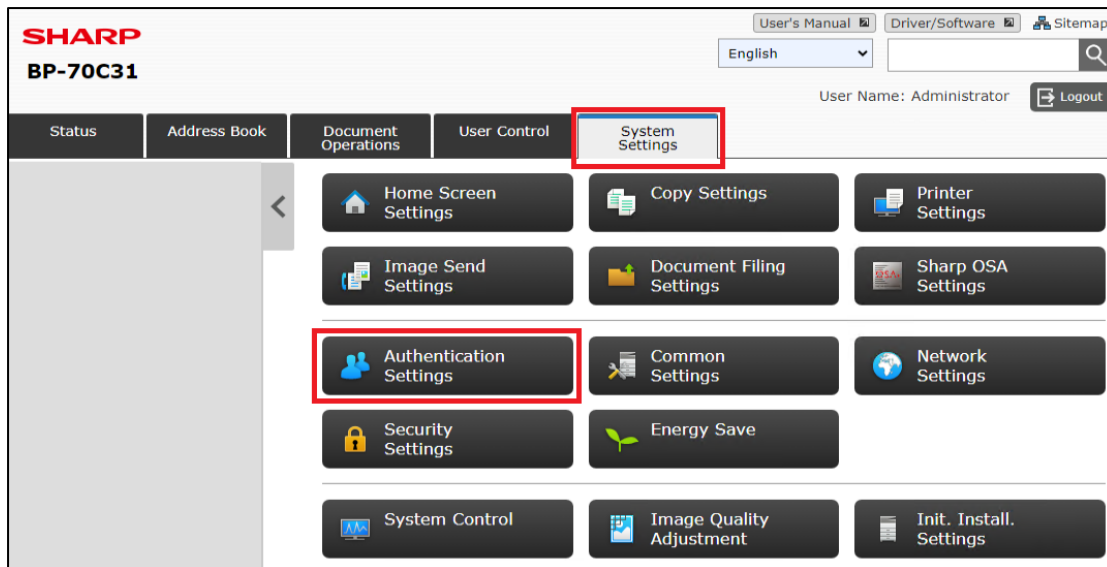
Enter the following information:

- External Account Control: [Enable](#)
- Server 1: [Enable](#)
- Application name: [Synappx Cloud Print](#)
- Address for Application UI: https://cloudprint.synappx.sharp.eu/mfp/login_credentials.jsp
- Address for Web Service: <https://cloudprint.synappx.sharp.eu/mfp/SharpService>
- Check the 'Extended Platform' box.
- Ensure Data Size is set to "Wide-SVGA"
- Click [Submit](#)
- Click [Reboot Now](#) - The MFP will now reboot

Step 5. Authentication Settings

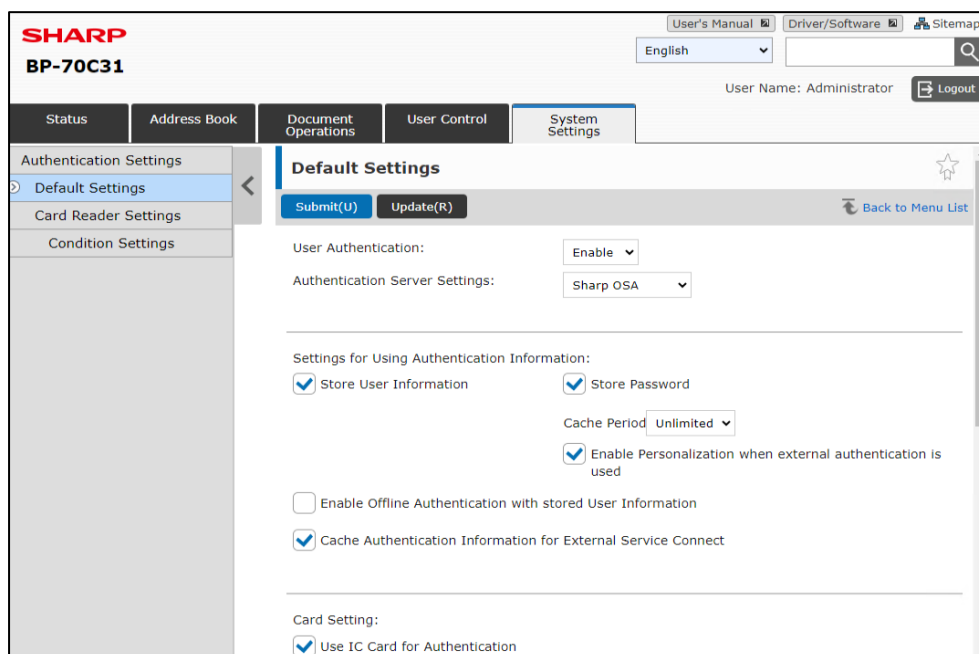
Go back into the MFP Admin web pages

Go to [System Settings](#) then [Authentication Settings](#)



Enter the following information:

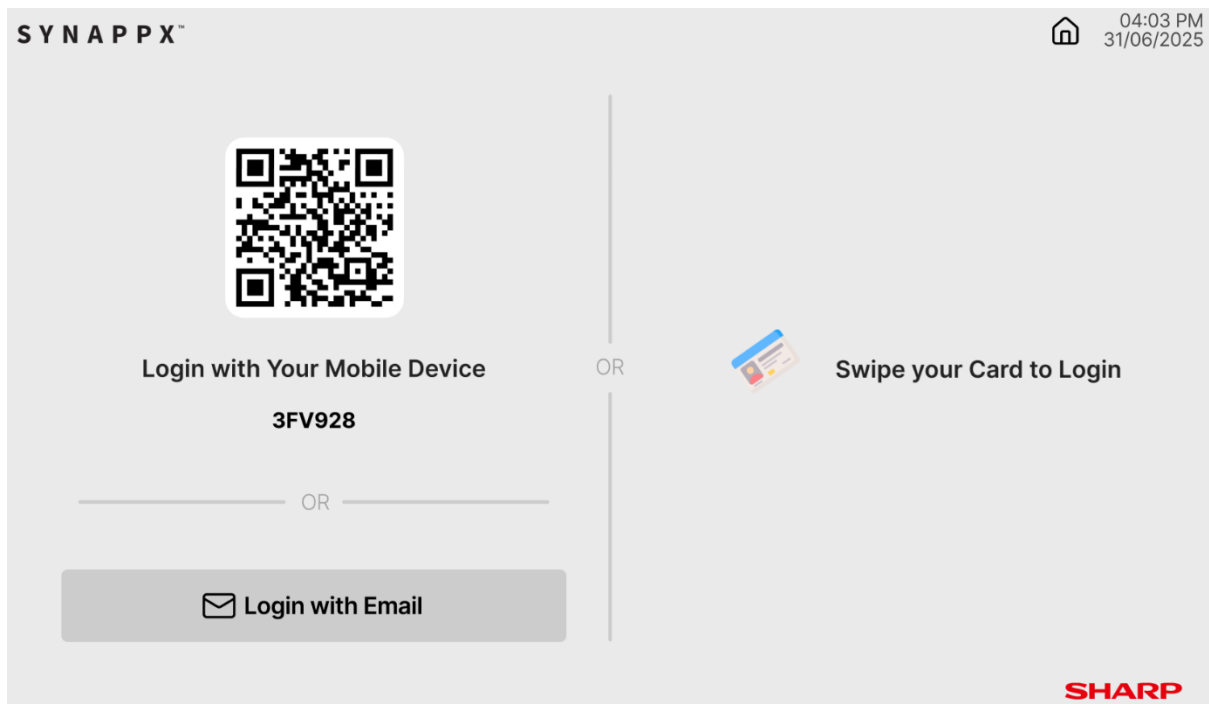
- User Authentication: [Enable](#)
- Authentication Server Settings: [SHARP OSA](#)
- If a card reader is fitted check the '[Use IC Card for Authentication](#)' box
- Click [Submit](#)
- Click [OK](#)



Adding a

The MFP will reboot

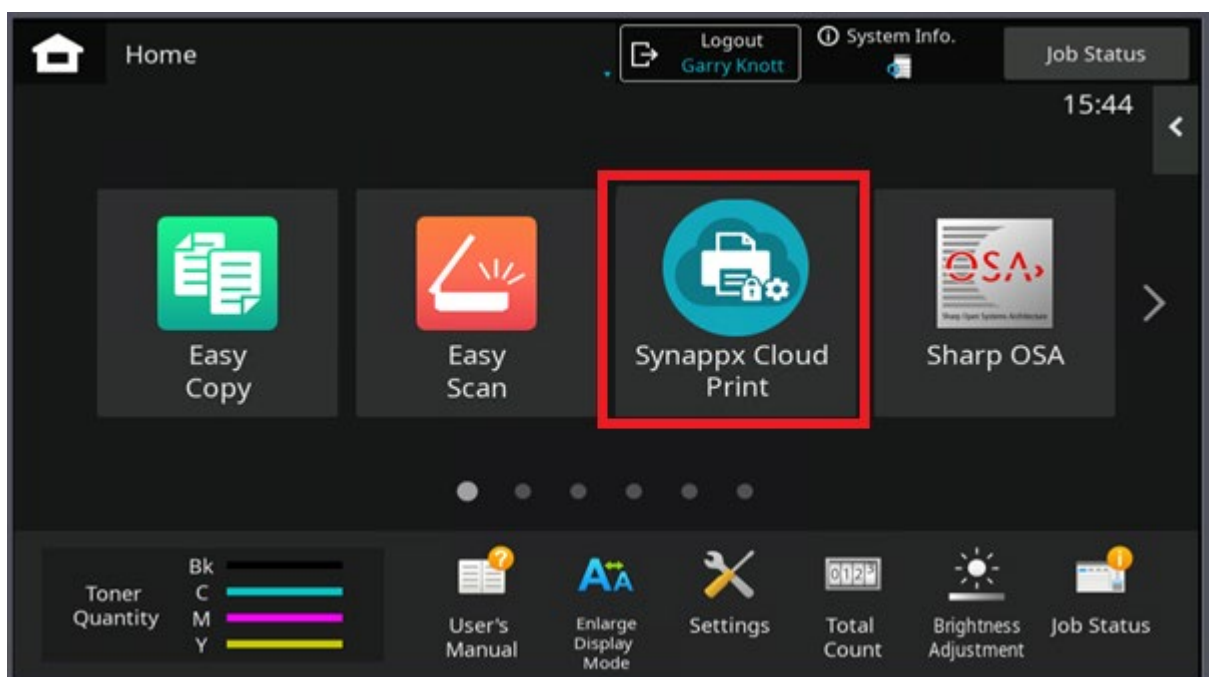
At this point, the MFP will have rebooted and will display the Synappx Cloud Print QR Code and menu items on the main screen



Step 6. Add a Standard OSA Application button to the MFP native screen

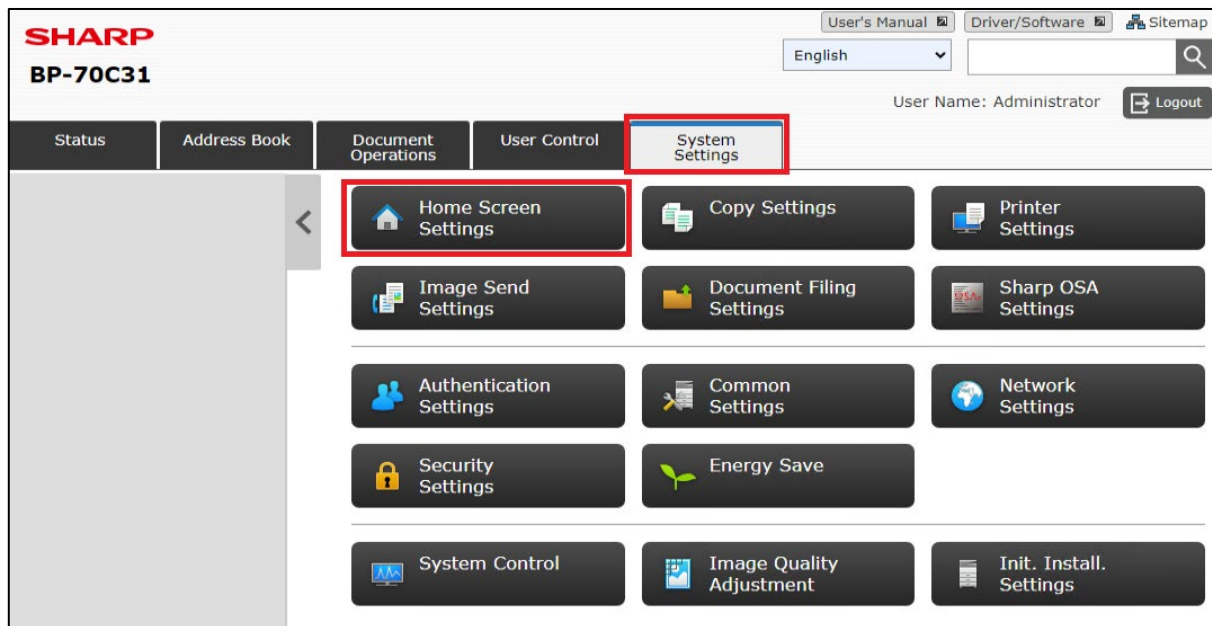
For convenience, it is recommended to add an additional button to the MFP native screen that will assist users in getting back to Synappx Cloud Print

The following pages explain how to do that and also how to add the Synappx Cloud Print icon

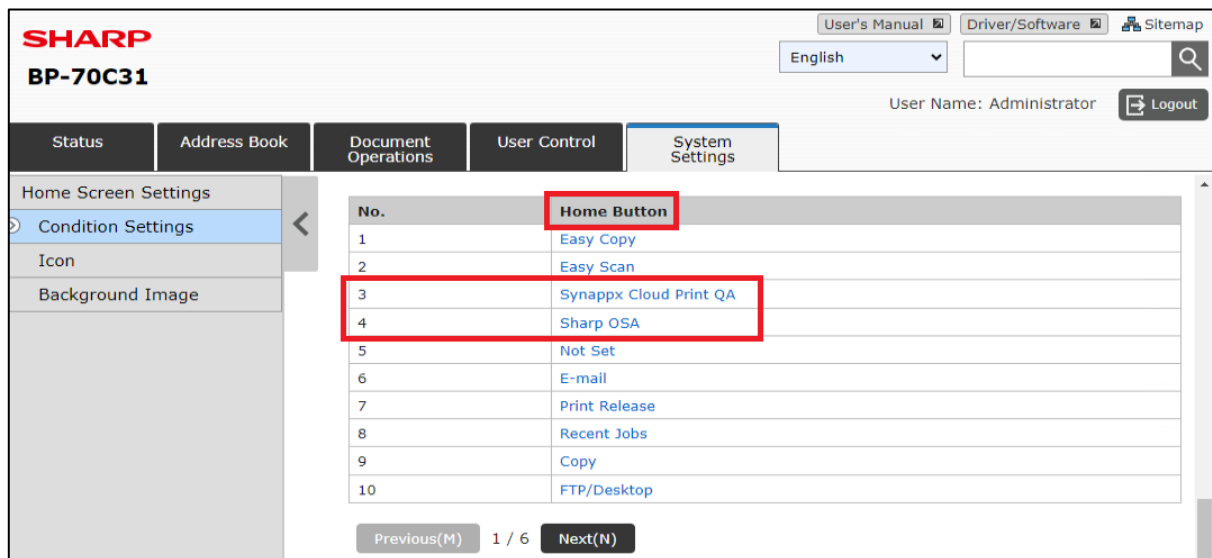


Go back into the MFP admin pages

Select [System Settings] – [Home Screen Settings]



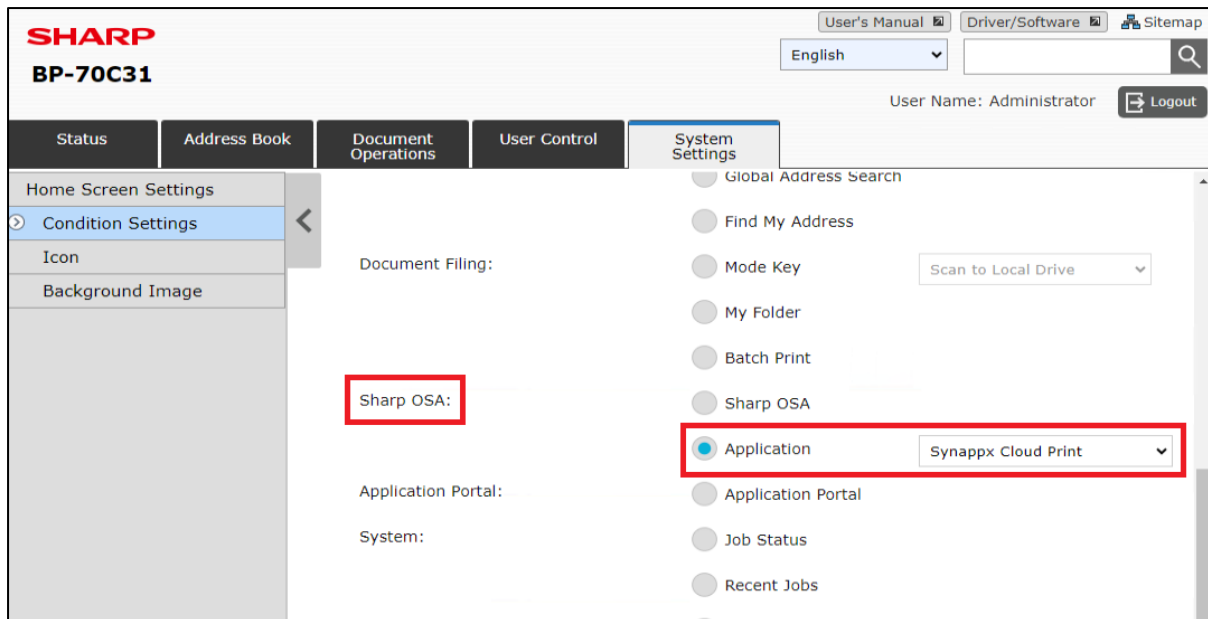
Select one of the first four entries that is either free or that you would like to use



Once you click one of the home screen entries, you will see the [Home Screen Registration Screen]

Scroll down until you see the [Sharp OSA] section

From there, next to [Application], select [Synappx Cloud Print]



Adding the Synappx Cloud Print Icon to the Application

The Synappx Cloud Print icon can be downloaded from the ESBC Jira Software Downloads site at:

<https://sharpesbc.atlassian.net/servicedesk/customer/portal/5/SD-147>

The icon file name is "SCP_Icon.png"



To upload to the associated application, connect to the MFP web page and login as [admin]

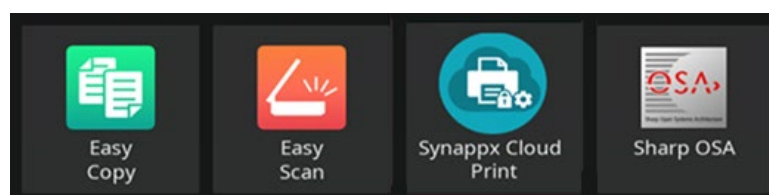
Go to [System Settings] – [Sharp OSA Settings] – [Standard Application Settings] and select the Synappx Cloud Print application

From there select to [Use Custom Icon]

Select the icon path by using the [Browse] button

Click [Submit] to apply the icon to the application

☒ Use Custom Icon	
File Name:	Not Set
Select File:	C:\fakepath\SCP_Icon.png Browse
(Up to 200 characters)	





Login with Your Mobile Device
3FV928

OR



Swipe your Card to Login

OR

 Login with Email

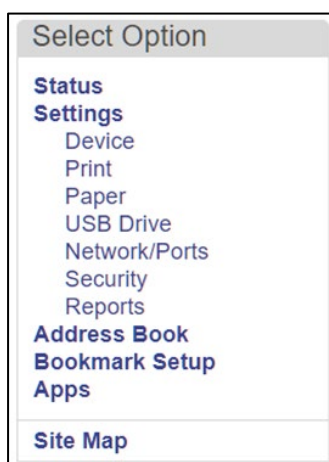
Configure MFP Settings - Group 2 Device

Minimum Group 2 Device Requirements

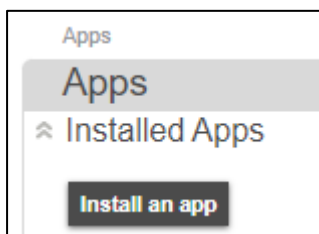
- Firmware version 230.207 and above

Note: You will need to have added the Sharp Group 2 device to [Synappx Cloud Print Portal] – [Devices] list, and assigned a license to it before continuing

Input the [IP address] of the Group 2 Device into a web browser to navigate to the configuration page of the MFP.



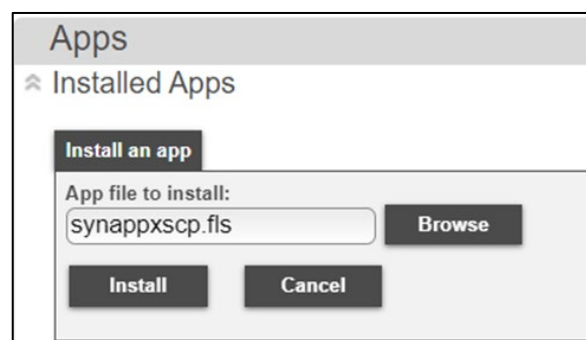
From the web page options, select [Apps]



From the [Apps] page, select [Install an App]

Use the [Browse] button to browse for the supplied .fls file and then click [Install]

This will install the embedded application [Synappx Cloud Print] on to the Group 2 device



Once installed, the Synappx Cloud Print login screen should be displayed on the MFP panel



14 minute(s) and 5 seconds remaining



LBJB-SMFN

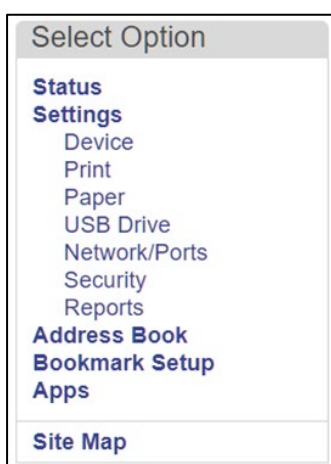
Scan QR code to login

Installing the Keyboard Emulation driver for USB Card Readers for Group 2 Devices

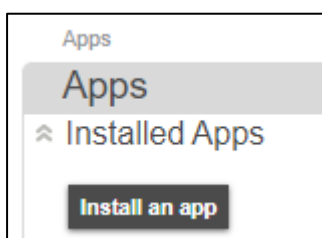
Sharp Group 2 A4 devices can work with most USB card readers that support keyboard emulation mode once the keyboard emulation driver is installed.

To Install:

Input the [IP address] of the Group 2 Device into a web browser to navigate to the configuration page of the MFP.



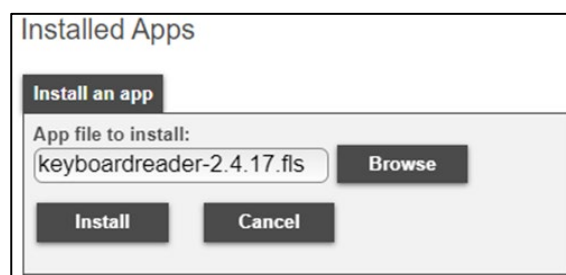
From the web page options, select [Apps]



From the [Apps] page, select [Install an App]

Use the [Browse] button to browse for the supplied .fls file and then click [Install]

This will install the embedded application [Keyboard Reader] on to the Group 2 device



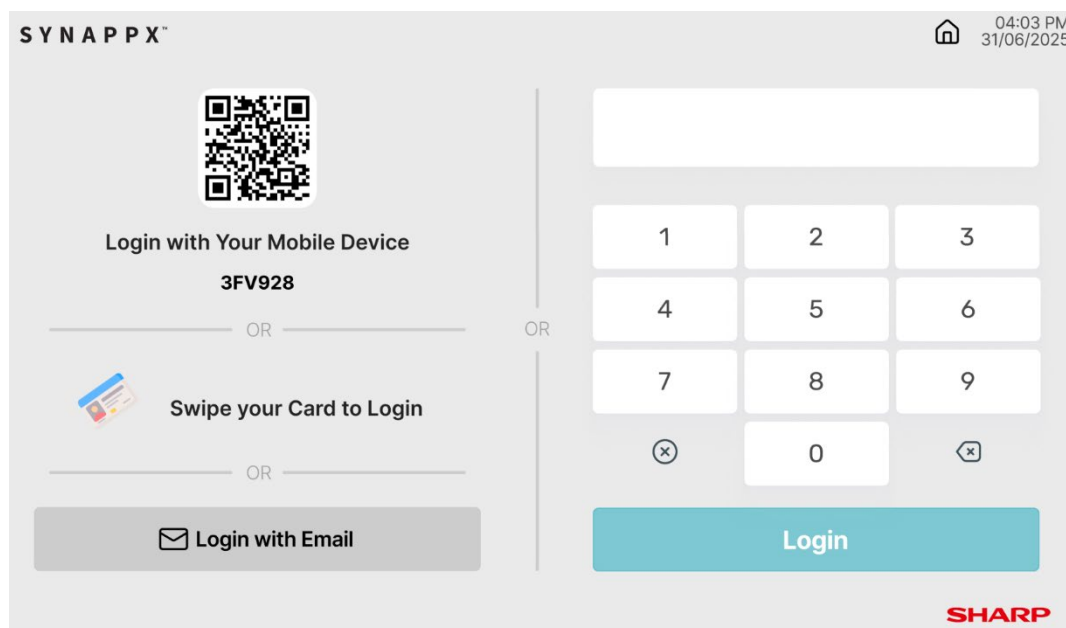
A supported USB card reader can now be plugged into the Group 2 device USB port and used for card login

To support **Lexmark RFID card reader**, you also need to install the OmniKey driver. Please follow the steps above and install **omnikey5427ckdriver-1.2.15.fls**.

Using the SCP app on the MFP

The available log in options PIN, Card or two factor can be enabled/disabled in the admin portal under settings

Once the MFP has been set up to work with Synappx Cloud Print the device will be locked and the following screen with available login options will be displayed.



Note: If users have already been activated and received a PIN code, they will be able to login via the PIN code screen

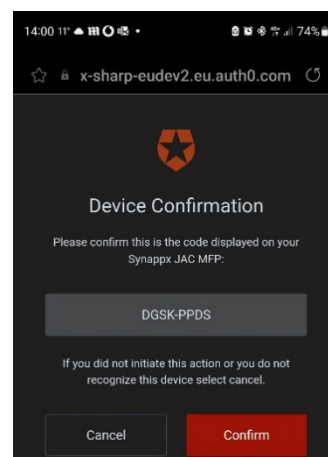
(Group 1 OSA 6.0 and above devices only)

As a one-time-only requirement, the user will need to either scan the QR code on a mobile phone app, or login using username and password

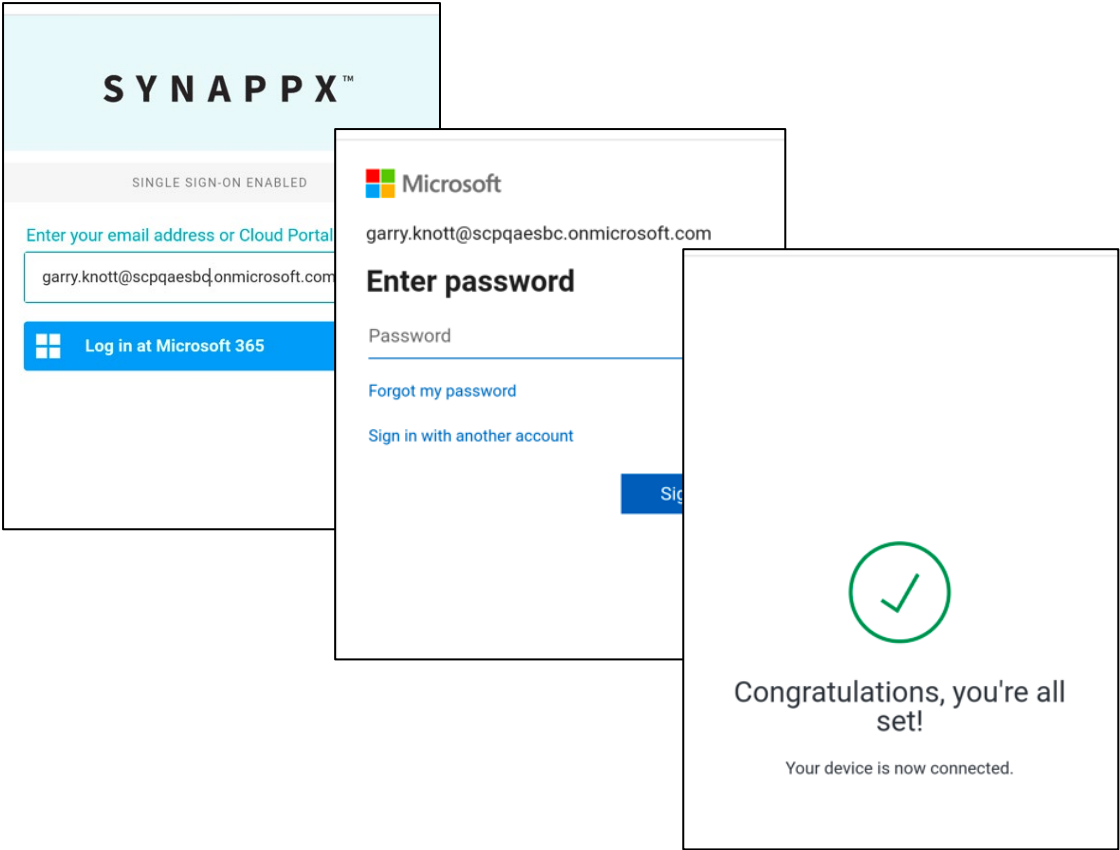
QR Code first login:

Once scanned, the user will be taken to the Microsoft Authentication page where they will enter their account username and password.

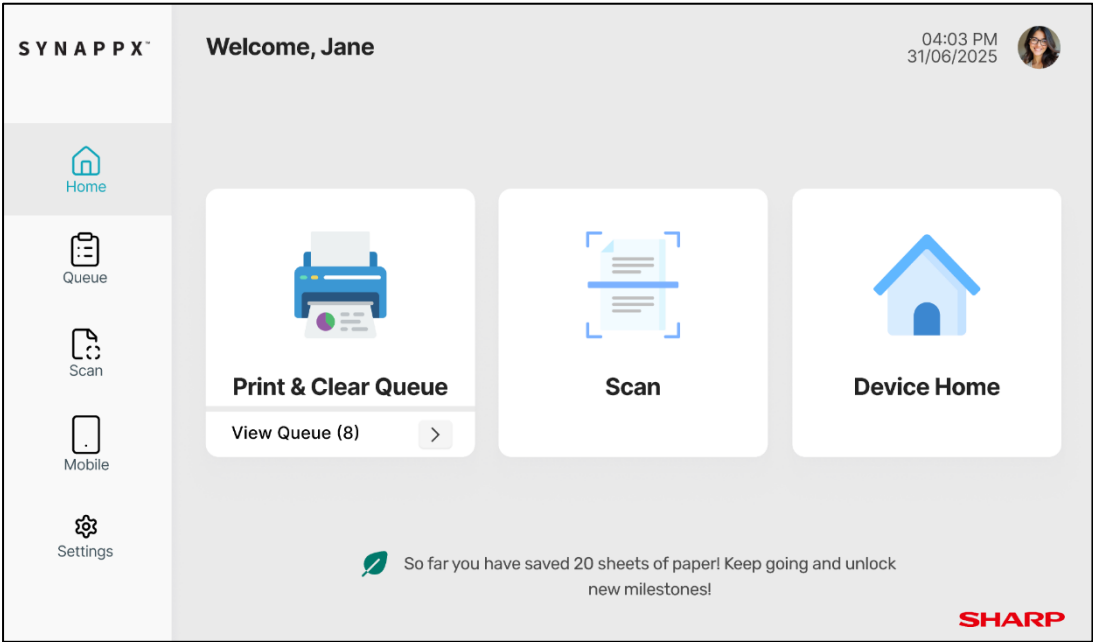
The Microsoft authentication process will ask for Device Confirmation (*ensure that the code shown matches the one displayed on the device*)



Go through each screen on the mobile device



Once past the “Congratulations” screen you will be logged into the device



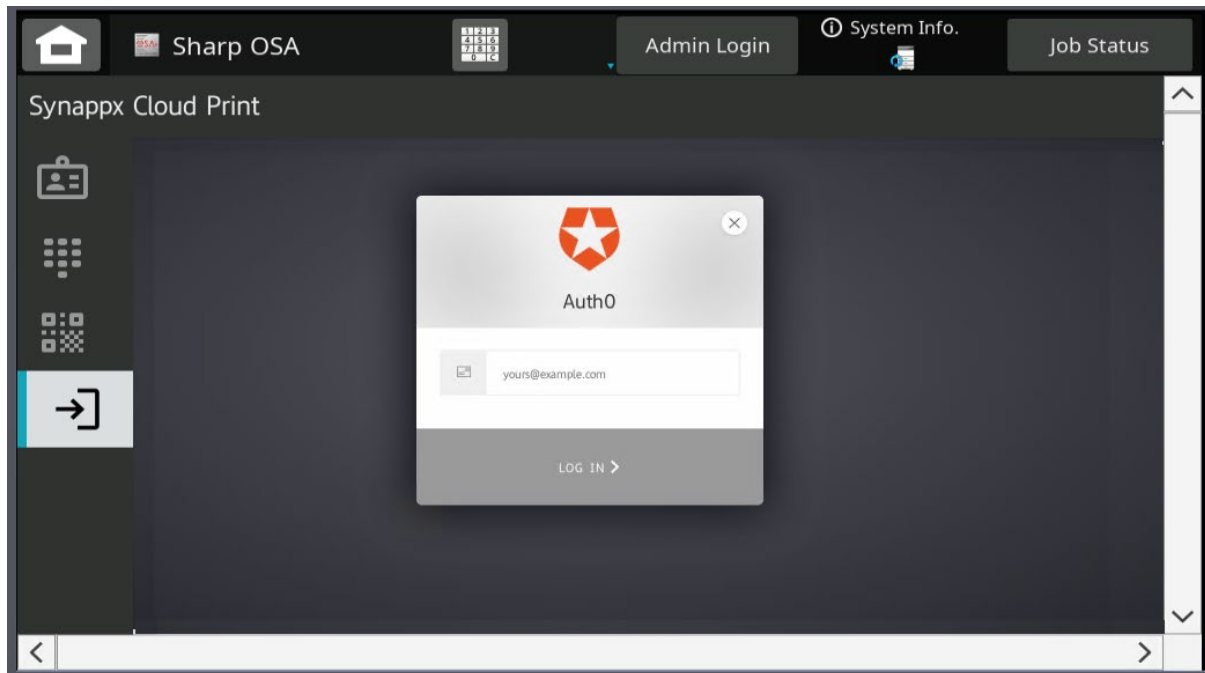
Having used the QR code to provide authentication details the user will be able to subsequently log in to the device using the QR code via the same phone without having to enter the authentication details again.



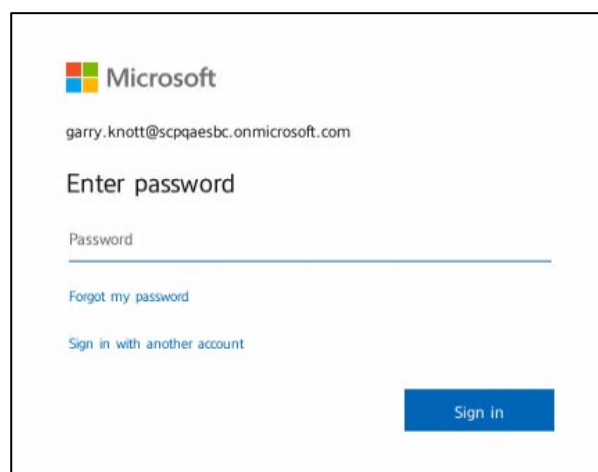
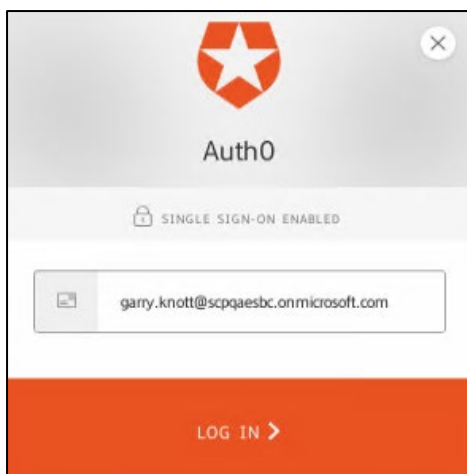
Username & Password First Login

Please note this is only available on Group 1 devices running OSA 6.0 and above

Press the [[Manual Login Icon](#)] to see the manual login screen

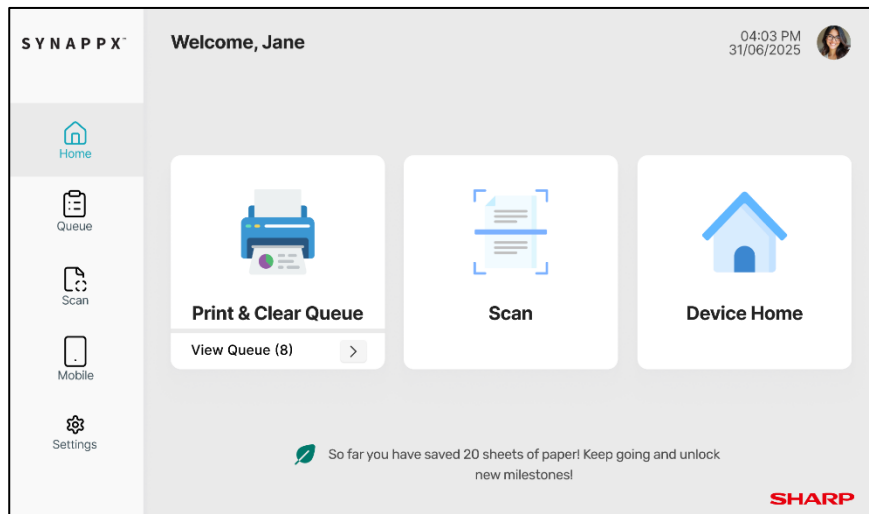


Follow the MFP on screen prompts



Once successfully logged in, you will see the Device welcome screen

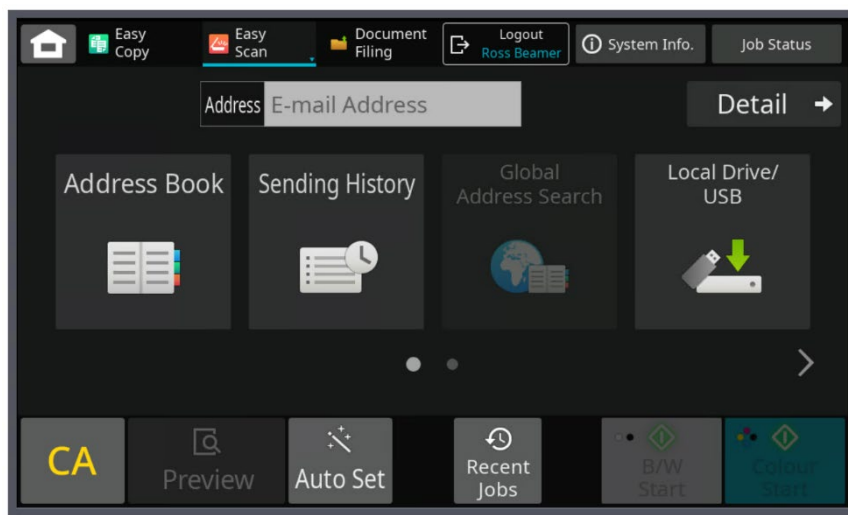
Once logged in, the Synappx Cloud Print home screen will be displayed. Users will be logged out either when a timeout occurs or another user presents their card, the user can also log out by selecting the [\[Logout\]](#) button on top of the screen



If the [Fast Print and Delete](#) option is selected, then all the user's queued jobs will be printed and deleted with no further input required from the user

Note When there are no print jobs available, Fast Print & Delete is greyed out

If the [Copy](#) option is selected, then the user will be taken into the MFP native device screen



If [Scan](#) is selected, users will be taken to the [Embedded Scan function](#) which is described after file printing in this manual

When finished the user can either log out of the device using the [Logout](#) button or select the [Synappx Cloud Print Home](#) button from the MFP front screen, (if the FP is setup according to "Configure MFP Settings" area of setup)



Selecting the [My Files] button will display a list of your print jobs that are queued for printing

SYNAPPX™

Home

Queue

Scan

Mobile

Settings

Queue

04:03 PM
31/06/2025

Sync

☐	Name	Submitted	Finishing	Copies
☒	Invoice_April2025.pdf 13 Pages	2 mins ago		- 1 +
☒	Roadmap_product.xlsx 2 Pages	53 mins ago		- 1 +
☐	Lease_Agreement.docx 8 Pages	1 hour ago		- 1 +
☐	Marketing Proposal.pdf 7 Page	2 days ago		- 1 +
☐	Team Meeting Notes.docx 3 Pages	1 month ago		- 1 +

1-5 of 5

Print (2)

Print & Clear (2)

Clear (2)

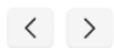
<

>

☐ Lease_Agreement.docx 8 Pages	1 hour ago
☐ Marketing Proposal.pdf 7 Page	2 days ago

Print Jobs with the same name will display with automatically incremented names

The various buttons available to the following:



Page navigation buttons, (where you have more than five jobs available)



Select all jobs & unselect all jobs

Print (2)

Will print the selected job/s

Print & Clear (2)

Will print the selected job/s & delete them from the queue

Clear (2)

Will delete the selected job/s from the queue

By clicking on the check marks next to a print job, you can select which jobs will be printed or deleted when the [Print] buttons are used

☒	Invoice_April2025.pdf 13 Pages	2 mins ago	  	 1 
☒	Roadmap_product.xlsx 2 Pages	53 mins ago	  	 1 



To the right of each print job are three additional job options which are available to allow you to change the job output values. The three values are:

- Duplex
- Black & White
- Staple

You are able to select any, some or all of the values for each print job available



Selecting duplex will enable you to print your job double sided instead of single sided



Selecting Black & White will enable you to print your job in B&W instead of colour



Selecting Staple will add a staple to your output, (assuming more than one sheet)



When you make sustainable choices in your printing process, you are shown a green leaf symbol next to your print job which is also reflected on your home screen:



So far you have saved 20 sheets of paper! Keep going and unlock new milestones!



The - & + buttons to the right of each print job allow you to change the number of copies of that print job are output

When print job/s are selected and sent to print, you will receive confirmation and will need to press the [OK] button

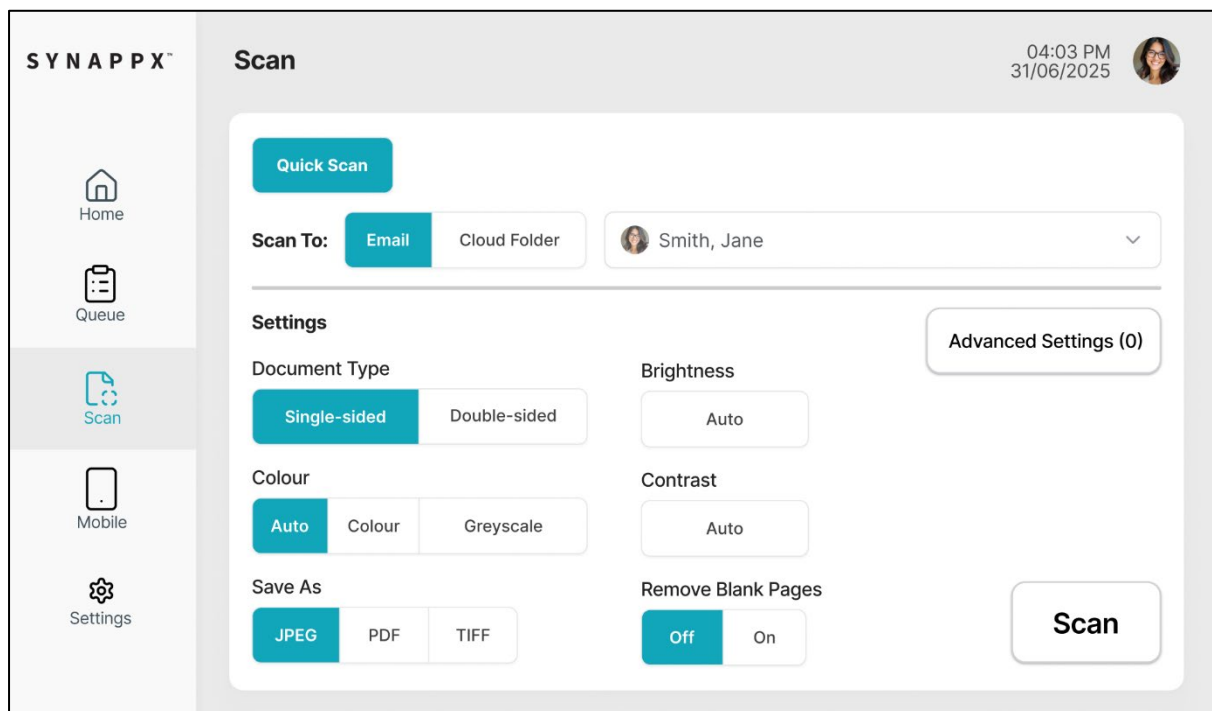
Printing the selected files.

OK

Embedded Scanning

The embedded scanning feature gives users easy access to the MFPs advanced scanning capabilities all within the Synappx Cloud Print app

- Embedded scanning UI provides access to scan to email & scan to cloud folder within the embedded application
- Options include scan settings and secure scan (password protected PDF)
- This feature is not available for custom IDP users



There are two scan destination types, [Scan to Email](#) and [Scan to Cloud Folder](#)

Scan to Cloud Folder can be enabled or disabled by an Administrator via the Admin Portal [Security] – [Scanning] - (this setting affects all devices)



If disabled 'scan to cloud folder' option will be greyed out on the MFP

Scan to Email

Scanning to email will send the scan job to the logged in users email address

The users email address is displayed in the [Email:] area

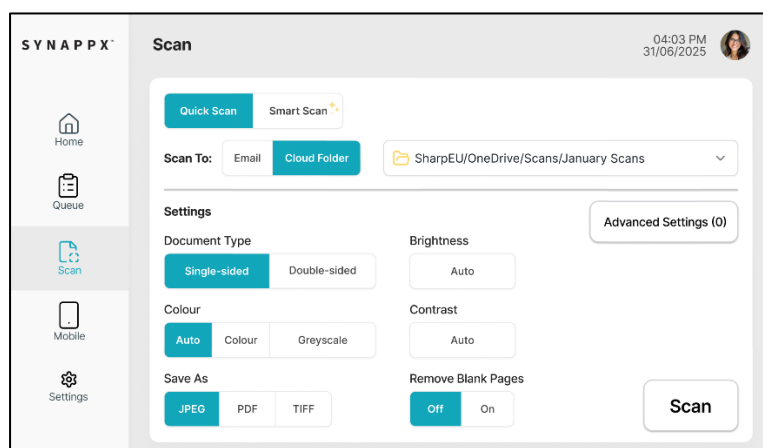
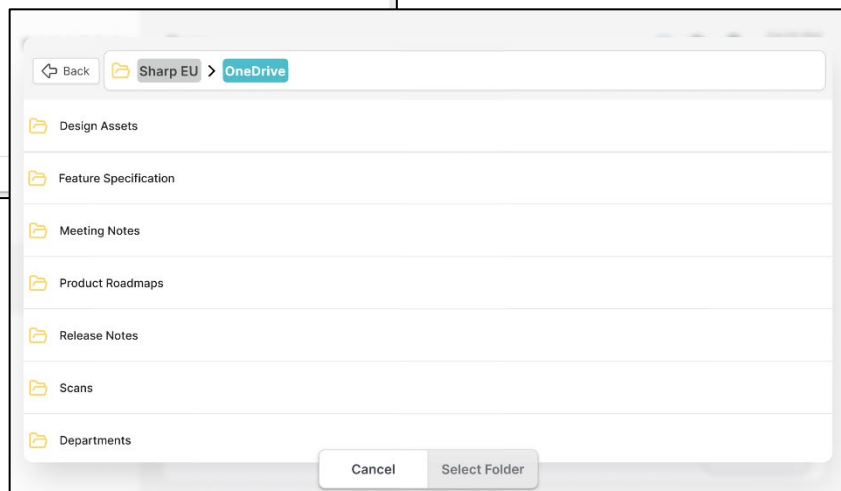
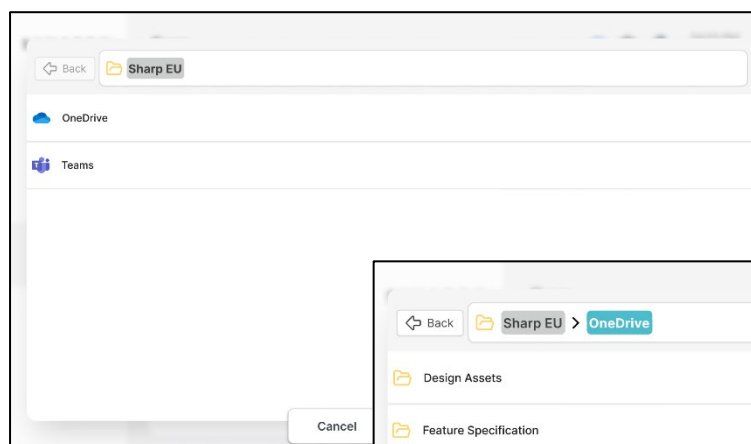
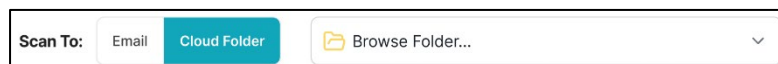


The email address displayed cannot be modified

Scan to Cloud Folder

Available cloud folder storage locations are displayed based on the users' permissions to tenant-wide cloud-based storage services, of which the user is then able to browse the structures

The user can choose an output folder by selecting the [Browse] button



Scan Settings

There are two types of scan settings, [Basic](#) and [Advanced](#)

Advanced includes 'password protect' which provides an additional layer of security:

- A password must be provided for the file
- Only PDF output format is supported (basic scan allows other document types)

Additional scan settings that are available for both Quick Scan and Secure Scan are:

- Document Type
- Rotation
- Resolution
- Colour
- Remove Blank Pages

Settings

Document Type

Single-sided

Double-sided

Brightness

Auto

Colour

Auto

Colour

Greyscale

Contrast

Auto

Save As

JPEG

PDF

TIFF

Remove Blank Pages

Off

On

Advanced Scan Settings (0) ✕

Rotation

0

90 degrees

Resolution

200

400

600

800

Password Protect (PDF Only)

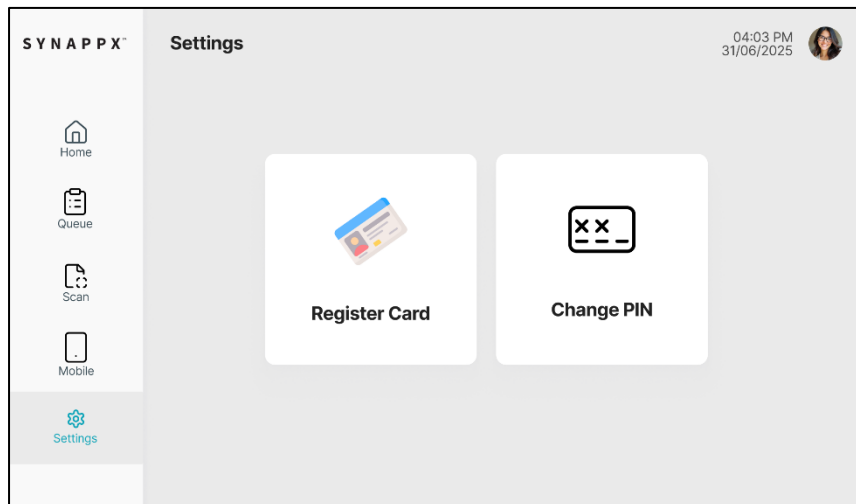
No

Yes

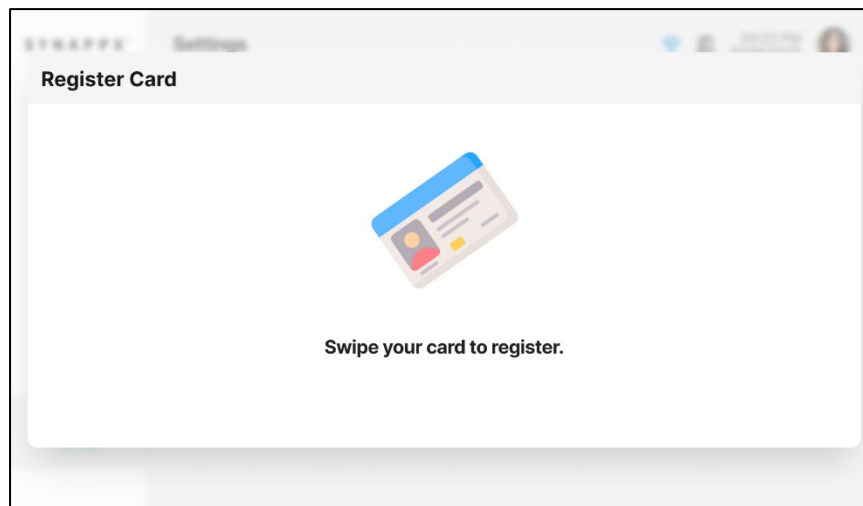
Registering a Card or Generating a PIN Code

To generate a PIN or register a card the user will need to select the Settings icon in the menu bar, they will then have the option to register a card or generate a new PIN

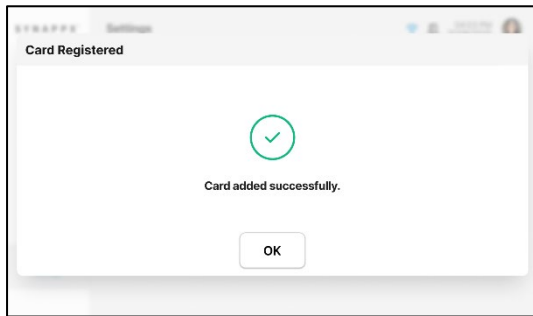
Note: The user must have logged in via QR Code or Username/Password to be able to register a card or change the PIN



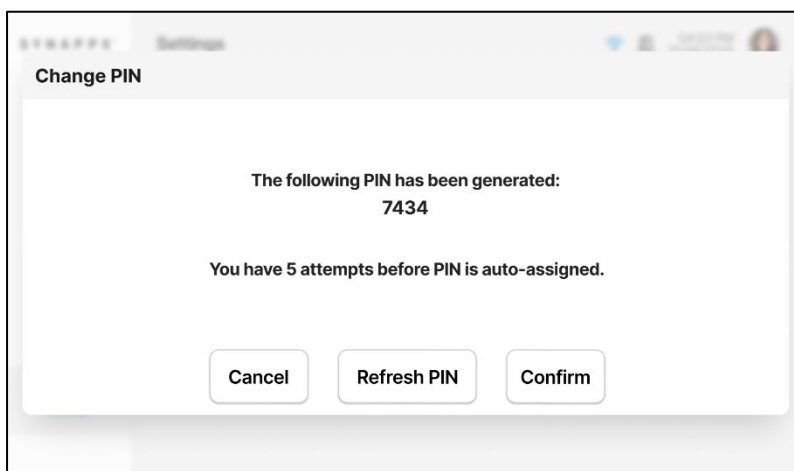
If they select [Register a Card](#), then a prompt to swipe the card will be displayed



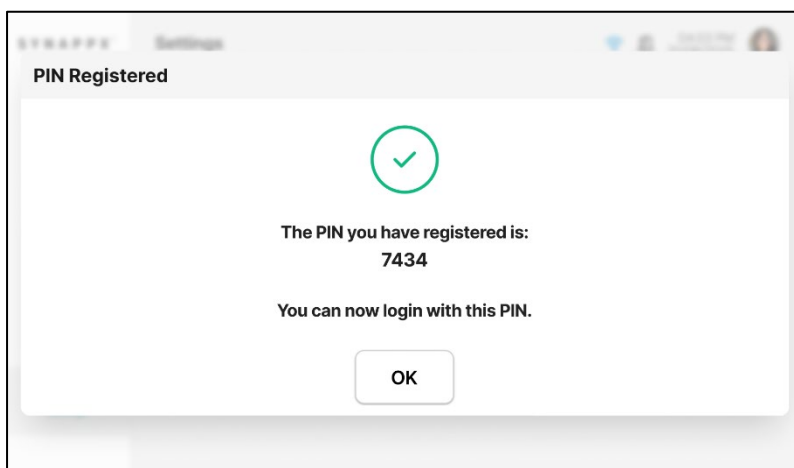
There will be confirmation that the card was successfully registered



If [Generate a PIN](#) is selected then a new PIN will be displayed with the option to accept it ([Confirm](#)), [Cancel](#) the operation, or generate a different one ([Refresh PIN](#))



Users can then Use PIN to log in



Or if a card reader has been fitted and a card registered, by using their card

When fully configured, users are able to login using:

- Card Swipe
- PIN Number
- QR Code
- Email (Group 1 OSA 6.0 and above devices only)

SYNAPPX™



Login with Your Mobile Device
3FV928

OR

 Swipe your Card to Login

OR

 Login with Email

 04:03 PM
31/06/2025

123

456

789

 0 

Login

SHARP

SYNAPPX™

Welcome, Jane

04:03 PM
31/06/2025



Home



Queue



Scan



Mobile



Settings



Print & Clear Queue

View Queue (8)



Scan



Device Home



So far you have saved 20 sheets of paper! Keep going and unlock new milestones!

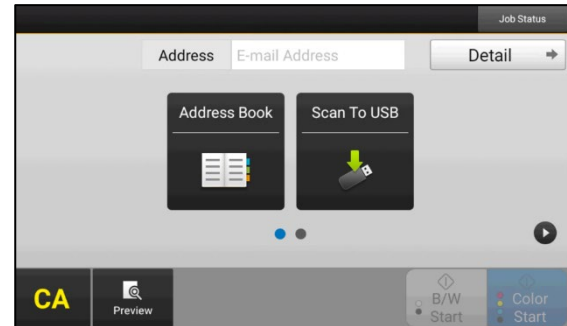
SHARP

Troubleshooting

This section is to help with any simple issues that you may come across when Using Synappx Cloud Print.

Type 2 device not auto logging out after Easy Scan being made

An updated firmware has been requested and should be in place before Synappx Cloud Print v1.6 is released



MFP Showing HTTP Status 500 Error Message

This is displayed if the MFP is attempting to connect to Synappx | Cloud Print but is not registered in the Portal, [Devices].

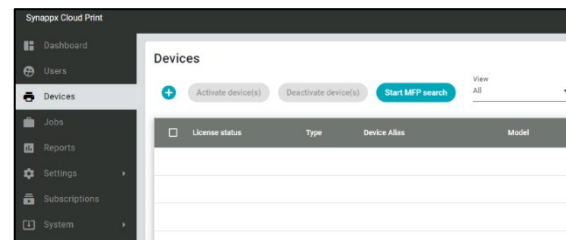
Please add the device to the portal, activate it and reboot the device



Cannot discover any Devices from the Portal

If you are unable to search for devices from the Admin Portal, this may be because you do not have a client running on the local network. It is the Client that runs the search.

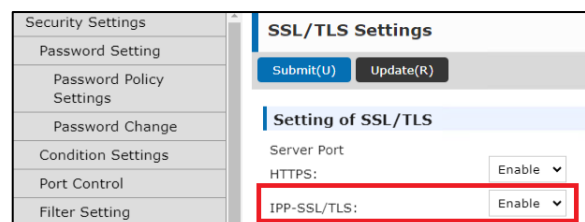
You must be logged into the Client as the same Admin user as on the Admin Portal to successfully search for Devices.



Unable to release Print Jobs from MFP

If you can see print jobs listed on the MFP but are unable to release them successfully, you may need to check that IPP-SSL/TLS is **enabled** on your device.

Check from System Settings – Security Settings – SSL/TLS Settings



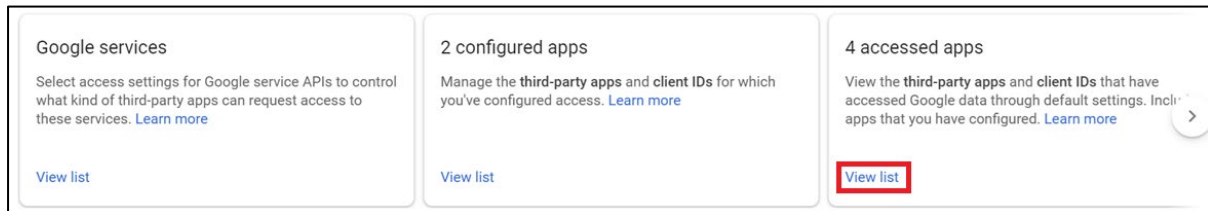
Addendum A – Settings for Google WorkSpace

When using Google WorkSpace as a Provider it may be necessary to make some changes in settings to allow the App to be trusted by Google. Generally production apps are trusted but these steps are included just in case this is not correct for your organisation:

Access the API controls of the Google WorkSpace admin console: <https://admin.google.com/ac/owl>

Click "MANAGE THIRD-PARTY APP ACCESS"

Click "View list" of Accessed apps



Google services

Select access settings for Google service APIs to control what kind of third-party apps can request access to these services. [Learn more](#)

[View list](#)

2 configured apps

Manage the **third-party apps** and **client IDs** for which you've configured access. [Learn more](#)

[View list](#)

4 accessed apps

View the **third-party apps** and **client IDs** that have accessed Google data through default settings. Include apps that you have configured. [Learn more](#)

[View list](#)

Click the correct App name

Accessed apps

[Download list](#)

[Bulk update list](#)

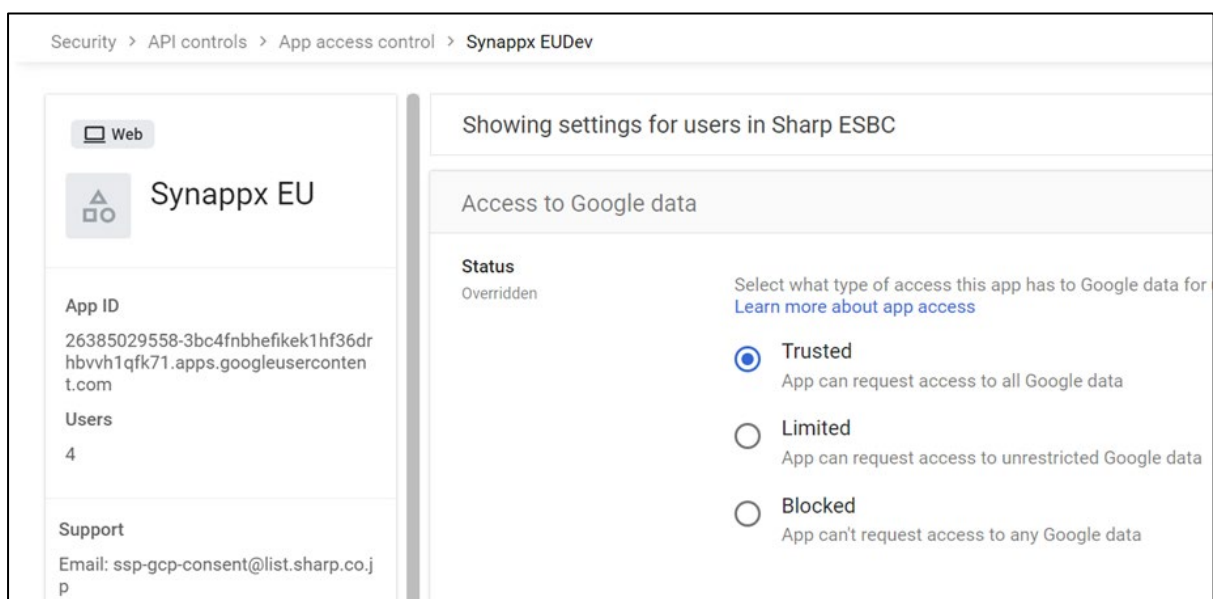
+

Add a filter

☐	App name	Type	ID	Users	Requested services ?	Access
☐	Synappx EU	Web	629070885227-dvh8fu...	3	Google Workspace Admin, Google sign-in	Configured

Click "Access to Google data" of the app

Click "Trusted" and then "Save"



Security > API controls > App access control > Synappx EUDev

Web

Synappx EU

App ID
26385029558-3bc4f9b9f1f36dr
hbvvh1qfk71.apps.googleusercontent.com

Users
4

Support
Email: ssp-gcp-consent@list.sharp.co.jp

Showing settings for users in Sharp ESBC

Access to Google data

Status
Overridden

Select what type of access this app has to Google data for [Learn more about app access](#)

☒ **Trusted**
App can request access to all Google data

☐ **Limited**
App can request access to unrestricted Google data

☐ **Blocked**
App can't request access to any Google data

Addendum B – Direct Print

[Direct Print] refers to the ability to print directly to either Group 1 or Group 2 printers without the use of the Synappx Cloud Print app. When printing directly, the printers will print the document automatically after they have received them. The direct print job will not appear in the Synappx Cloud Print queue on the PC app or in the printers “waiting print jobs queue”.

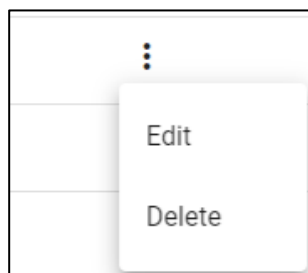
Any successful direct print jobs will appear in the job history in the admin portal.

Setup

Enable the Printer in Admin Portal

To use direct printing, we first need to ensure that the required printers have direct printing enabled. This can be done via the Admin Portal.

- Login to the Admin Portal using an account on the same tenant as the printers
- Navigate to ‘Devices’, and select the 3 dots to the right of the selected printer, from there select [Edit]



- In the [Edit Device] area, scroll to the bottom where you will see [Allow Direct Printing]
- Toggle this to [On] and then [Save]



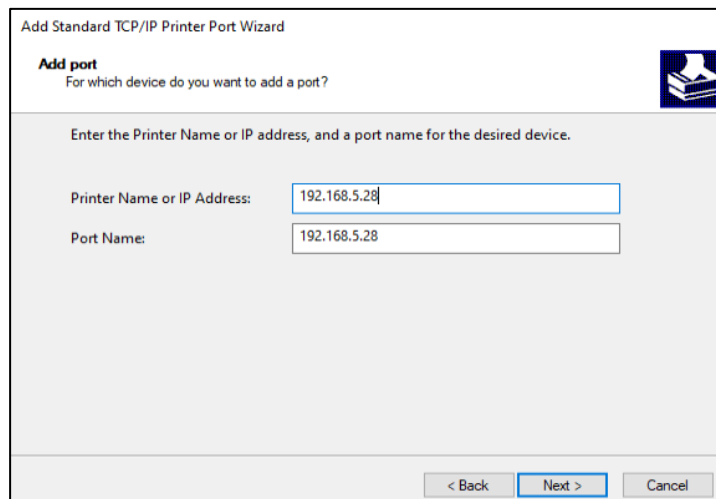
The next step is setting up the print driver correctly to print directly to the printer with user credentials included.

Configuring the Print Driver for Group 1 Devices

Install the Group 1 device Print Driver

Once the print driver has been installed, go to the print driver properties and select the [Ports] tab

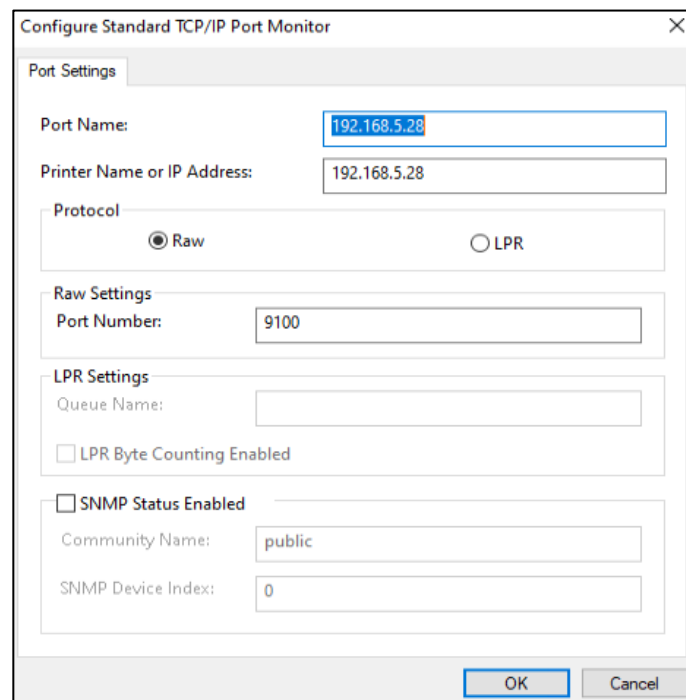
Select [Add Port] and add a [Standard TCP/IP Port] using the Printers IP address as shown



The image shows the 'Add Standard TCP/IP Printer Port Wizard' dialog box. It has a title bar with the text 'Add Standard TCP/IP Printer Port Wizard' and a printer icon. The main area is titled 'Add port' with the subtitle 'For which device do you want to add a port?'. Below this, it says 'Enter the Printer Name or IP address, and a port name for the desired device.' There are two input fields: 'Printer Name or IP Address:' with the value '192.168.5.28' and 'Port Name:' with the value '192.168.5.28'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Once added, select the port and click [Configure Port]

Ensure it is printing directly to the printer on port 9100



The image shows the 'Configure Standard TCP/IP Port Monitor' dialog box. It has a title bar with the text 'Configure Standard TCP/IP Port Monitor' and a close button. The 'Port Settings' tab is selected. The 'Port Name:' field contains '192.168.5.28'. The 'Printer Name or IP Address:' field contains '192.168.5.28'. Under the 'Protocol' section, the 'Raw' radio button is selected. The 'Raw Settings' section has a 'Port Number:' field with the value '9100'. The 'LPR Settings' section has a 'Queue Name:' field that is empty. There are checkboxes for 'LPR Byte Counting Enabled' and 'SNMP Status Enabled', both of which are unchecked. The 'SNMP Status Enabled' section has a 'Community Name:' field with the value 'public' and an 'SNMP Device Index:' field with the value '0'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Now the user authentication needs to be input to the driver

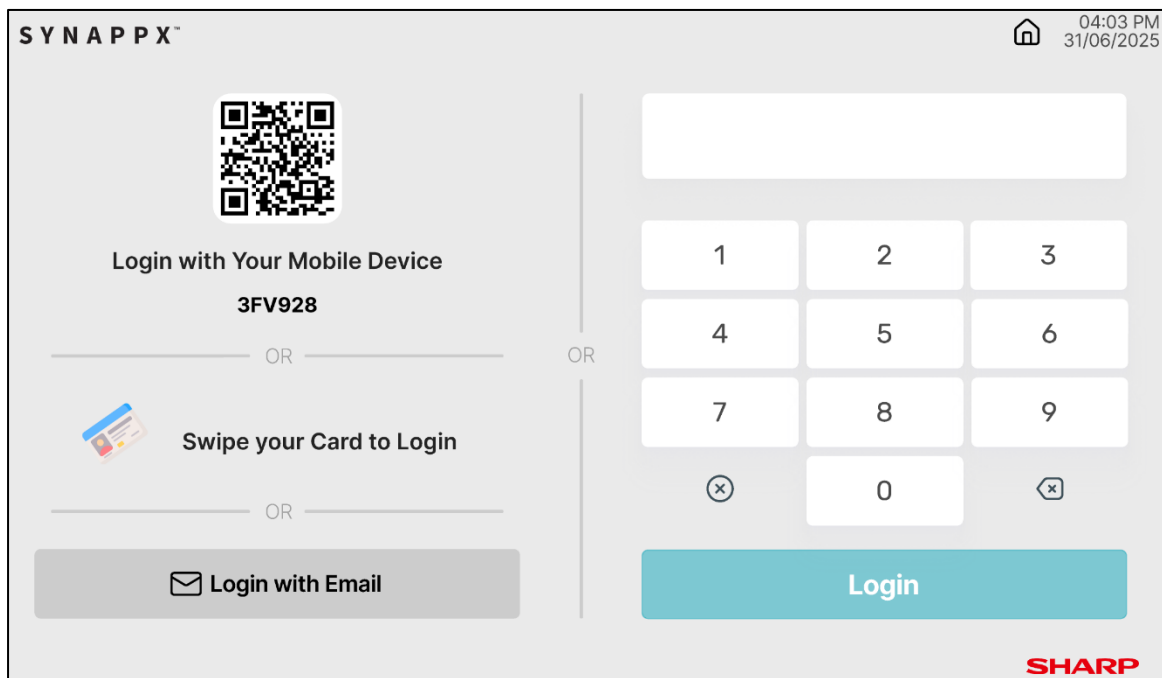
Go to [Printing Preferences] and select the [Job Handling] tab



- Change [Authentication] to “Login Name”
- In [Login Name] type the users “email address”
- Activate [Username] and insert the users name (this is not required unless you want to see who is printing at the MFP)

The image shows a form for authentication settings. On the left, under the heading 'Authentication:', there is a dropdown menu with a person icon and the text 'Login Name'. Below this is a checkbox labeled 'User Name' which is checked, followed by a text input field containing 'Garry Knott'. At the bottom left is a checkbox labeled 'Auto Job Control Review'. On the right, under the heading 'Login Name:', there is a text input field containing the email address 'garry.knott@esbc1.onmicrosoft.com'. Below this is a checkbox labeled 'Job Name' which is unchecked, followed by an empty text input field.

Now any print jobs sent via that print driver to the device will print out directly



Configuring the Print Driver for Group 2 Devices

A separate driver will need to be installed for a group 2 printer. This can be downloaded here:

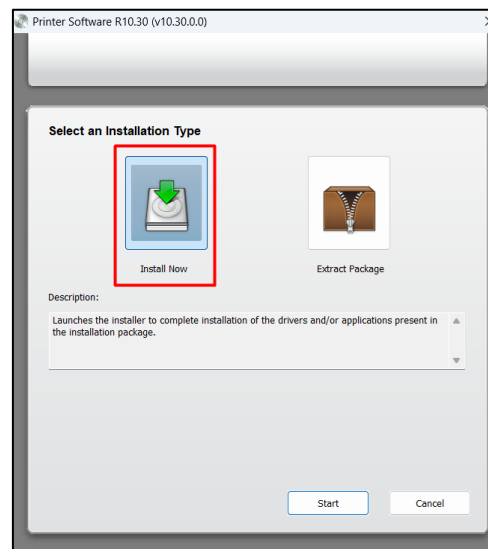
https://global.sharp/restricted/print/select_os.html?view=2&lang=3&pid=413®ion=8

On the page, confirm the correct operating system is shown and select 'Next'

Select and install the 'Generic Installation Package'



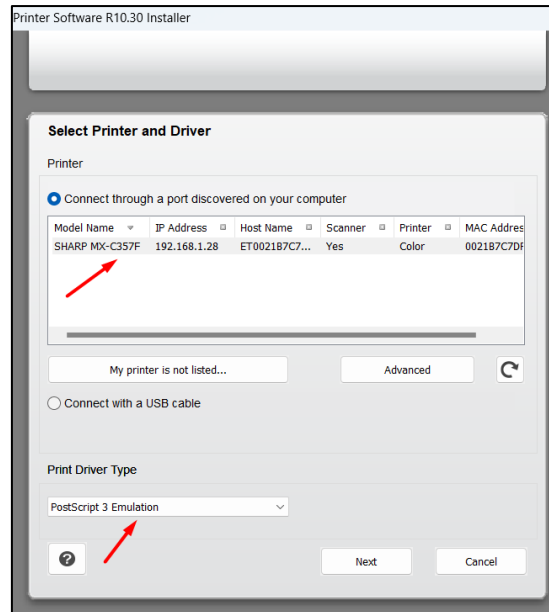
Run the installer and select the 'Install Now' option



Accept the license agreement and select 'Next'

Ensure the Group 2 printer is turned on and the installer should find it

Select the printer from the list and ensure the 'Print Driver Type' is 'PostScript 3 Emulation'

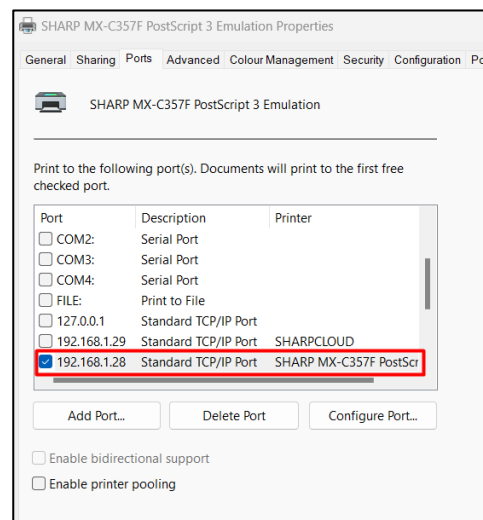
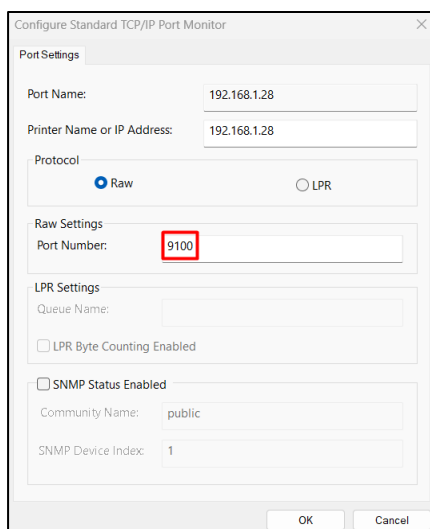


Select 'Next' and the installation should complete OK, (do not install additional software if prompted)

Locate the newly installed driver and navigate to 'Printer properties'

Select 'Change properties' and navigate to 'Ports' then locate the port matching the printer IP address

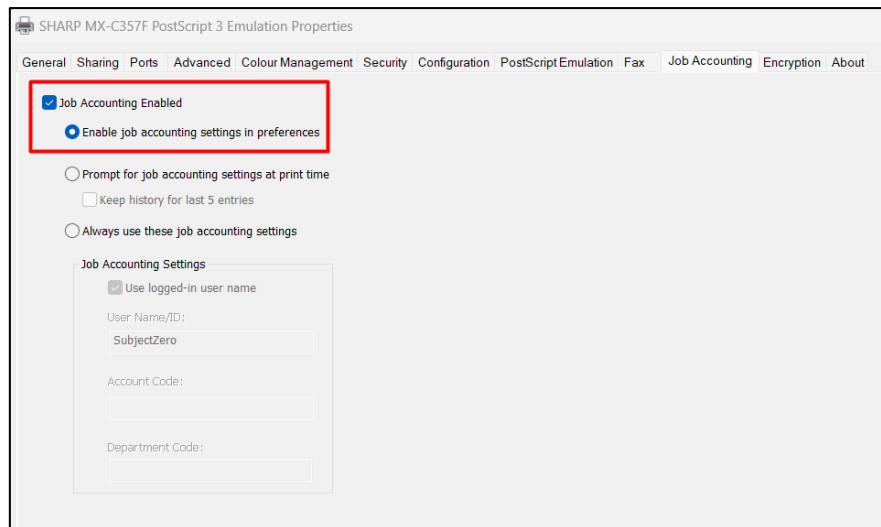
Select 'Configure Port' and ensure the port number is 9100, then click 'OK'



Navigate to the 'Job Accounting' tab

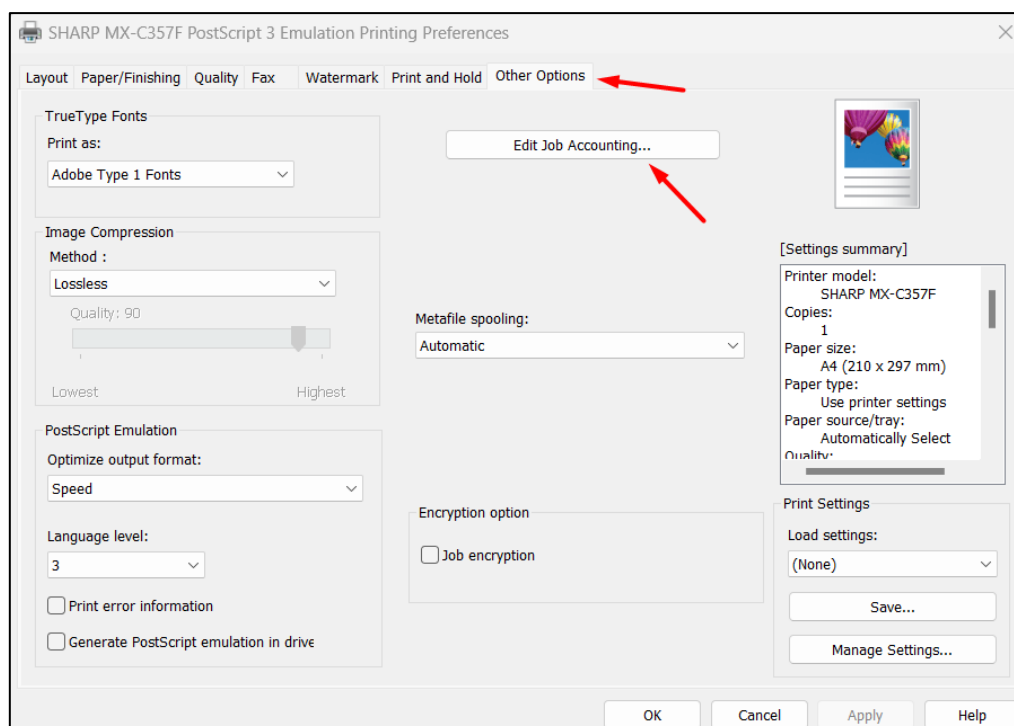
Tick 'Enable Job Accounting'

Ensure 'Enable job accounting settings in preferences' is selected



Click 'Apply' and 'OK' then close 'Printer properties'

Navigate to 'Printing preferences' - Select 'Other Options' - Select 'Edit Job Accounting'



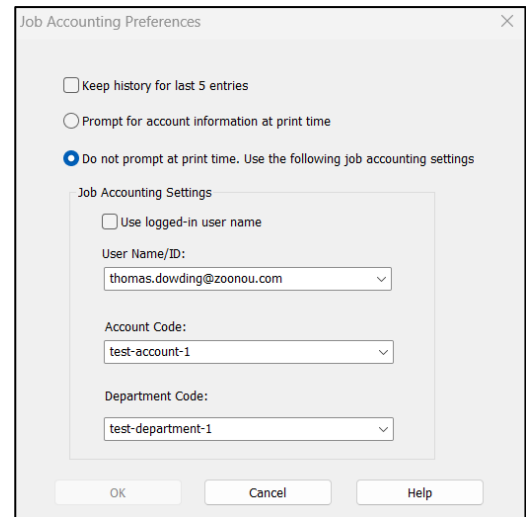
Select 'Do not prompt at print time. Use the following job accounting settings'

Untick 'Use logged-in user name'

In 'Username/ID', input the email address of the user who is logged into Windows

In 'Account Code', type 'test-account-1'

In 'Account Department', type 'test-department-1'



The screenshot shows the 'Job Accounting Preferences' dialog box. It has a title bar with a close button (X). Inside, there are three radio buttons: 'Keep history for last 5 entries' (unchecked), 'Prompt for account information at print time' (unchecked), and 'Do not prompt at print time. Use the following job accounting settings' (checked). Below the radio buttons is a section titled 'Job Accounting Settings' which contains a checkbox 'Use logged-in user name' (unchecked). Under this checkbox are three dropdown menus: 'User Name/ID:' with the value 'thomas.dowding@zonou.com', 'Account Code:' with the value 'test-account-1', and 'Department Code:' with the value 'test-department-1'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Click 'OK' and then click 'Apply' and then 'OK' to close out of printing preferences

Print a document to the newly setup driver

So long as direct printing is enabled, it will print to the Luna printer

Addendum C – Guest Printing

Introduction

Guest printing which is available from Synappx Cloud Print v1.5 to allows guests visiting a business to be able to print to a Synappx Cloud Print controlled MFP without having an account on the tenant.

Upon request guests can upload print files and are given a unique PIN code which allows them to retrieve their print jobs from the Synappx Cloud Print enabled MFP.

Please see the notes on Guest Print Security Information at the end of this section

Pre-Requisite

For Guest Printing to work correctly on a Type 1 device it will need to have the Office Direct Print Expansion Kit installed (MX-PU10) and the PS3 Expansion Kit (MX-PK13)

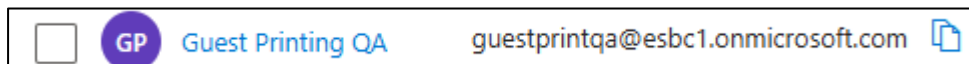
To Activate Guest Printing

Step 1: Create an email for guests to contact for access

A dedicated email account on the customers tenant is required so that guests can request access by emailing that address. This email address is connected to Synappx Cloud Print via the Admin Portal.

In this example the tenant is esbc1.onmicrosoft.com, and the email account that has been created is guestprintqa, so the email address for requesting access to Guest Printing is guestprintqa@esbc1.onmicrosoft.com

Here is the account on the Entra ID portal



Step 2: Enable and setup Guest Printing on the Admin Portal

Login to Synappx Cloud Print Admin Portal as Admin

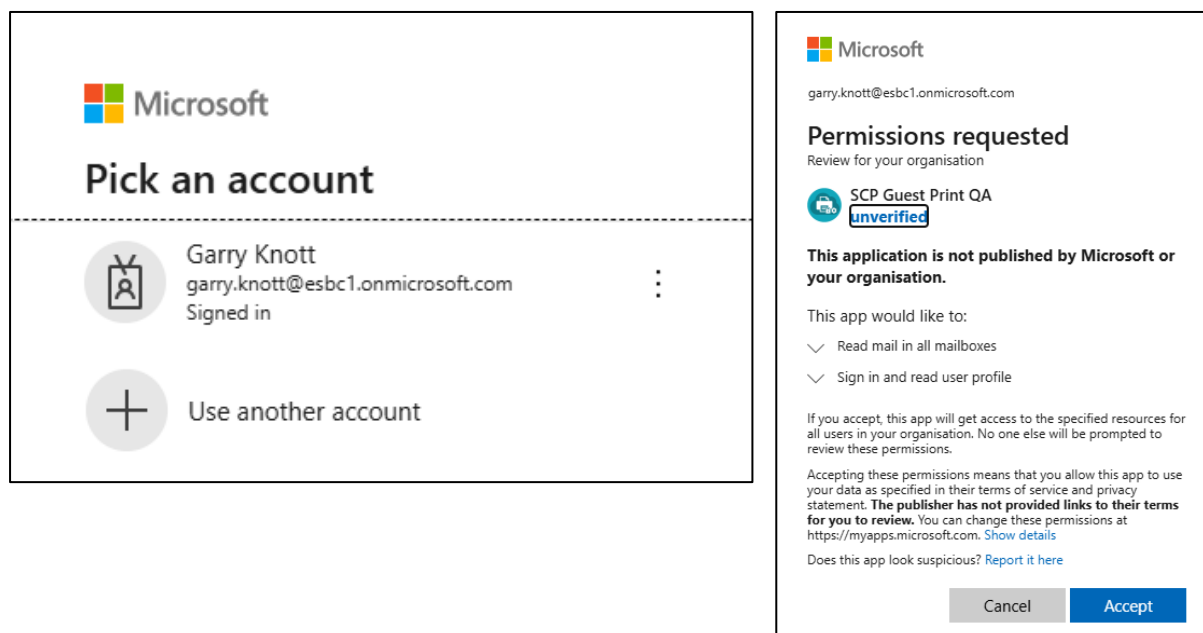
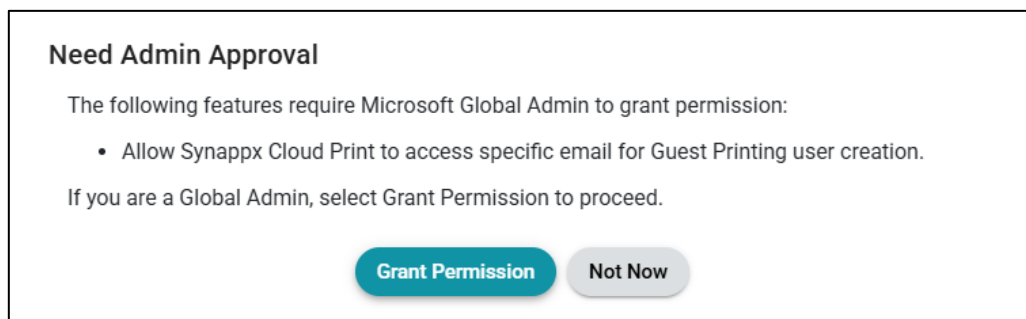
Go to [Settings] – [Security] – Guest Printing

By default Guest Printing will be disabled



Click the slider to the right to enable

You will be prompted to grant permission as a Microsoft Global Admin and required to input your admin credentials then asked to accept permissions.



Please also refer to documentation from Microsoft:

Limiting application permissions to specific Exchange Online Mailboxes

<https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access>

First, set the guest printing Session Period. The Session Period applies to all tenant guests, once the period has expired, they will no longer have access, and their files will be automatically deleted.

Next, enter the email address of the dedicated email setup to allow Guest Printing

Guest Printing

Enable Guest Printing

Guest Printing Session Period

7 Days

Guest Email Account

Connect

Disconnected

Populate Guest Email Account with the dedicated email created earlier

Guest Printing

Enable Guest Printing

Guest Printing Session Period

7 Days

Guest Email Account

guestprintqa@esbc1.onmicrosoft.com

Connect

Disconnected

Then click [Connect]

If the email address is valid, the connection will be successful and [Connection Established] will be displayed – this may take a short while

Guest Printing

Enable Guest Printing

Guest Printing Session Period

7 Days

Guest Email Account

guestprintqa@esbc1.onmicrosoft.com

Disconnect

Connection Established

Expire at: 01/03/2025 23:59:59 (Auto Renew Enabled)

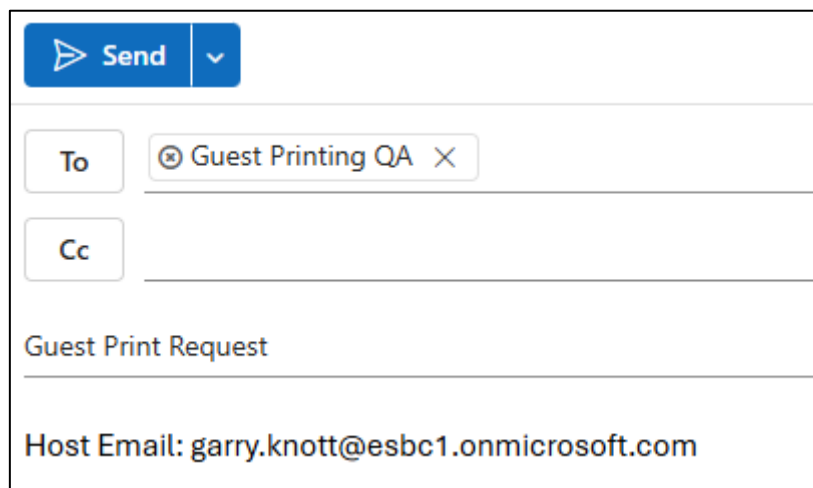
For Guests to Print

Step 1: Request Access

Guests who want to have access to printing must send an email with the following conditions:

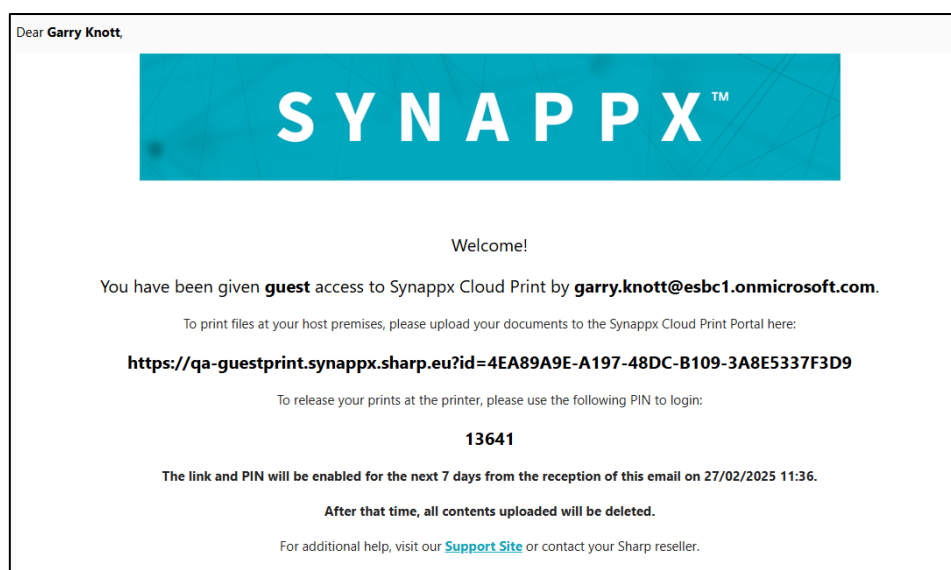
- Email recipient is the dedicated email listed in Guest Print settings
- Email Subject must be "Guest Print Request"
- Email Body text is Host Email: [\[any valid customer tenant email\]](#)

Example:



The screenshot shows an email client interface. At the top is a blue 'Send' button with a right-pointing arrow and a dropdown arrow. Below it are the 'To' and 'Cc' fields. The 'To' field contains 'Guest Printing QA' with a close button (X) on the right. The 'Cc' field is empty. The subject line is 'Guest Print Request'. The body of the email contains the text 'Host Email: garry.knott@esbc1.onmicrosoft.com'.

The email contains a unique link to upload documents for printing, details of session expiry and a PIN to release the prints on site. If the email is not correctly formatted, it will be rejected by the system and the guest will not receive a reply.



Step 2: Sending Files to be printed

The guest must use the link included in the “Welcome” email to access the SCP upload page

First the Guest will receive a Terms & Conditions page, they must click [Agree]

Terms & Conditions of Use - for Synappx™

EFFECTIVE: 25/04/2023

The following Synappx™ Terms of Use, as well as the [Synappx Privacy Policy](#) incorporated herein by reference (collectively, the “Agreement”), is between Sharp Corporation (“Sharp”) and Customer. This Agreement governs access to and use of the Synappx Go, Synappx Admin Portal and related Documentation; the term “Services” shall mean the Synappx Services, Specific Software Services and all related Documentation which may be proprietary to Sharp and/or third party service providers (“Third Party Service Providers”) and which are accessible via the Synappx Service.

Use of the Services is intended for organizations (“Customer”) and their End User(s). The term “End User(s)” and its variations shall mean anyone accessing services provided by Synappx Service and may include, but is not limited to, Customer’s employees, representatives, contractors, agents or any other individual using or accessing the Services under a Customer Account and authorized by the Customer to use the Services. All references to the term “Customer” shall also refer to Customer’s authorized Administrator(s) and any of its End Users, whether individually or collectively.

Prior to any use and before access is granted to the Customer, the authorized Administrator(s) for the Customer must agree to this Agreement on behalf of Customer. By clicking “Agree”, you, the Administrator, represent and warrant that: 1) you have been designated by the Customer as an “Administrator” and are entitled to all rights and privileges afforded to those in the Administrator role (more fully described below); 2) you have authority to bind the Customer to this Agreement. If you have not been designated as an Administrator for Customer or do not have the authority listed above, you may not click “Agree”, and Customer may not use or access the Services. Upon clicking “Agree”, Customer shall have the right to use and access the Services subject to the terms set out herein.

There may be other specific software services (“Specific Software Services”) accessible within or through the Synappx Admin Services that allow Customer to perform certain functions or use additional services and features; these Specific Software Services are proprietary to Sharp and/or Third Party Service Providers. Customer understands that use and/or access to these Specific Software Services may require Customer, Administrator(s) and/or End Users to agree to additional terms and conditions applicable to the use of and/or access to the Specific Software Service (“Additional Terms”). If Customer, Administrator(s) and/or End Users do not agree to such terms or do not have authority to agree to such Additional Terms, those Specific Software Services may not be used or accessed by Customer, Administrator(s) and/or End Users, as applicable. In the event of any inconsistency between this Agreement and Additional Terms, the Additional Terms shall control but only for that Specific Software Service.

A. Definitions

In addition to all defined terms set out above, the following definitions apply to this Agreement:

1. **Customer Account:** Refers to all accounts under or assigned to a Customer. This includes all applicable Administrator Accounts as well as any Services licensed to and information, data associated with Customer, Administrator(s) and its End Users.

Agree

Decline

Then click on [Getting Started] – this will auto direct after 10 seconds

SYNAPPX™

Welcome to Synappx Cloud Print

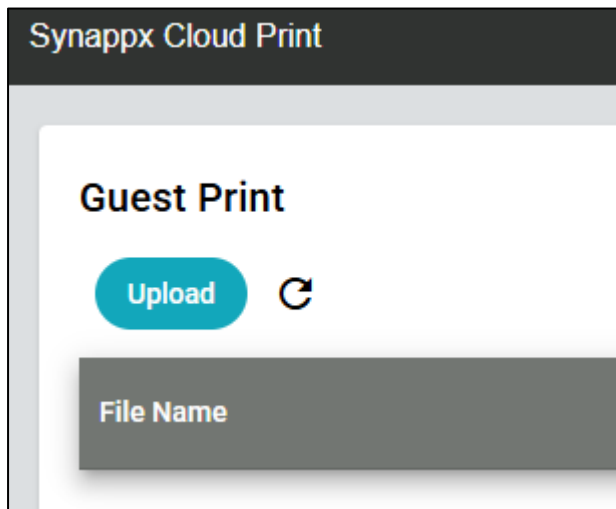
Your section ID: 4EA89A9E-A197-48DC-B109-3A8E5337F3D9

You will be redirected in 2 seconds...

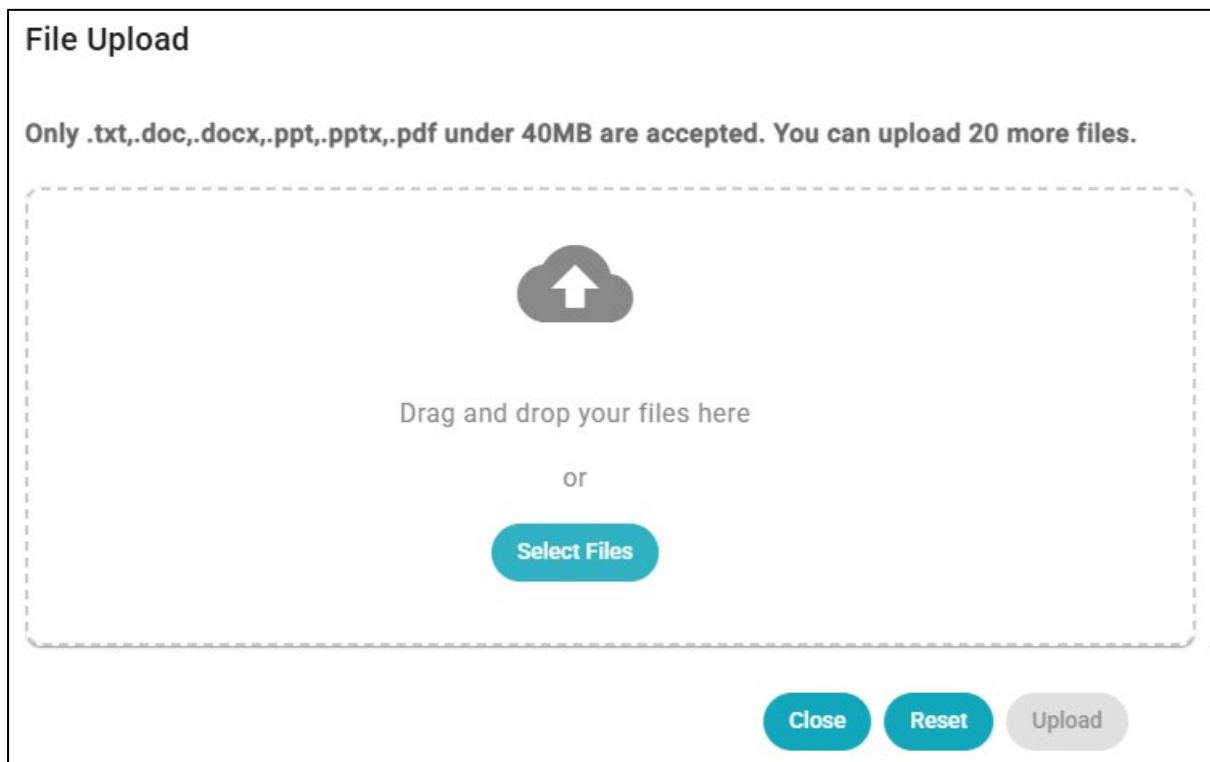
Click the button below to enter the guest printing files upload if not redirected automatically

Getting Started

The guest is then able to upload files. Click [Upload]



Files can be dragged into the [Upload] area or selected via the [Select Files] button



The guest user can upload up to 20 files, each up to a maximum file size of 40MB and of the following file types: [.txt](#), [.doc](#), [.docx](#), [.ppt](#), [.pptx](#), [.pdf](#)

In this example, three files have been selected for printing, these are shown before uploading

File Upload

Only .txt,.doc,.docx,.ppt,.pptx,.pdf under 40MB are accepted. You can upload 20 more files.



Drag and drop your files here

or

Select Files

Files to be uploaded:

- PDF_Test_Sheet.pdf (0.016 MB)
- PowerPoint_Test_Sheet.pptx (0.033 MB)
- Word_Test_Print.docx (0.013 MB)

CloseResetUpload

Now click [Upload]

Guest Print	
<button>Upload</button>	
File Name	Action
PDF_Test_Sheet.pdf	
PowerPoint_Test_Sheet.pptx	
Word_Test_Print.docx	

The guest can now see the uploaded files and is able to delete them if required

Step 3: Printing Files

Go to the Synappx Cloud Print enabled MFP

Enter the 5-digit PIN code that was provided in the Guest Print welcome email

SYNAPPX™

04:03 PM
31/06/2025



Login with Your Mobile Device

3FV928

OR



Swipe your Card to Login

OR



Login with Email

1

2

3

4

5

6

7

8

9

ⓧ

0

ⓧ

Login

SHARP

Click [Login] and you will be logged in as your email username, from where you are able to view and print your uploaded files

Print jobs can be printed with additional print options, but you cannot delete print jobs via the MFP

SYNAPPX™

Queue

04:03 PM
31/06/2025





Queue

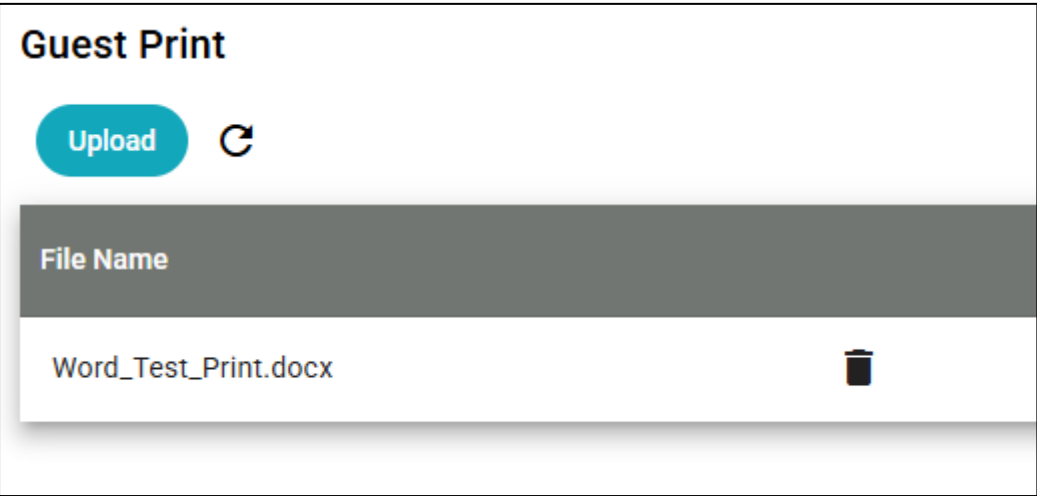
Sync

☐	Name	Submitted	Finishing	Copies
☐	Invoice_April2025.pdf 13 Pages	2 mins ago	  	 1 
☐	Roadmap_product.xlsx 2 Pages	53 mins ago	  	 1 
☐	Lease_Agreement.docx 8 Pages	1 hour ago	  	 1 
☐	Marketing Proposal.pdf 7 Page	2 days ago	  	 1 
☐	Team Meeting Notes.docx 3 Pages	1 month ago	  	 1 

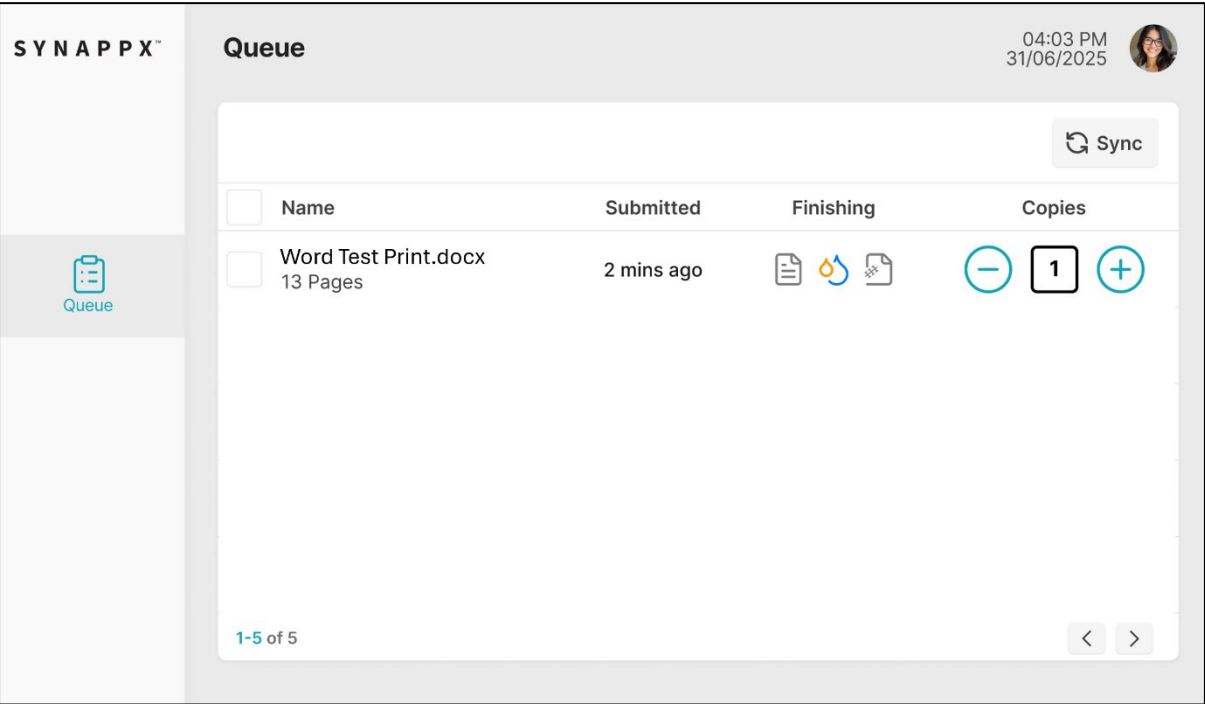
1-5 of 5

In the example below, the PDF and PowerPoint test prints were deleted from the Guest Print Upload page



The MFP screen reflects the changes



If not deleted manually, print jobs will be automatically deleted after the selected session time set by the administrator of 7, 14 or 21 days

Guest Print Security Information

With the Synappx Cloud Print Guest Print feature, a temporary private storage area is created for your guest. Your guest is only allowed to upload printable documents like PDF, Word, PowerPoint, etc (see Guest Print requirements), and are not allowed to download from this storage area. All files in the guest storage area are only able to be sent to the Sharp multifunctional printer.

As an extra level of security, Sharp offers a Bitdefender license option for our multifunctional printers which scans documents in real time to detect malware or malicious code. Please ask your Sharp sales representative about the Security Kit

Additional security is provided by controlling session expiry, after which files are deleted automatically. This is controlled by the customer through the Synappx Cloud Print Administrator Portal (see Guest Print configuration).

When implementing Guest Print it is recommended to follow usual best security practices for the dedicated email account.

Recommendations:

Email Gateway & Firewall Protection

- **Deploy a Dedicated Email Security Gateway:**
Use a solution that sits between the internet and your email server. It can inspect incoming traffic, filter out suspicious emails, and block IPs known for malicious activity.
- **Network-Level DDoS Protection:**
Utilise firewalls and intrusion prevention systems that can detect and mitigate volumetric attacks before they reach your email infrastructure.

Rate Limiting & Throttling

- **Configure Rate Limits:**
Set limits on the number of incoming connections or emails accepted per IP address or sender within a given time frame.
 - **For Exchange/Outlook:** Adjust settings in your Receive Connectors to limit the number of messages per connection.
- **Throttling Policies:**
Implement policies that slow down email processing if a sudden spike in traffic is detected, preventing system overload.

Connection Filtering & Reputation Management

- **IP Reputation Services:**
Integrate tools that assess the reputation of sending IP addresses. Block or challenge emails from sources with a poor reputation.

- **Blacklisting:**
Automatically block IP addresses or domains that are known for sending excessive or malicious emails.

Cloud-Based DDoS Mitigation

- **Leverage Cloud Services:**
Many cloud providers offer DDoS protection that can help absorb and mitigate large-scale email floods.
- **Load Balancing:**
Distribute incoming email traffic across multiple servers to prevent any single server from being overwhelmed.

Please also refer to documentation from Microsoft:

Limiting application permissions to specific Exchange Online mailboxes

<https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access>

Addendum D – 3rd Party Printer Support

Introduction

3rd Party Printer Support extends the scope of devices that can be managed by Synappx Cloud Print for the following functions:

- Discovery
- Licensing
- Printing
- Accounting

Printing via 3rd Party Printer Support uses Internet Printing Protocol, (IPP), creating a base for future development leveraging modern printing standards

Note: 3rd Party Printer Support does not include an 'embedded' application on the device and does not support 'print release' or the mobile app

How it works

The 3rd party printer is discovered and activated via the Admin Portal

The Synappx PC Client is configured to allow 3rd Party Printing, the target printer is available is available in a drop-down list

A new print driver is installed on the client PC that uses the most compatible print driver, (Microsoft IPP Class Driver), which sends print jobs to the local Synappx PC Client on port 57200

The print job received by the Synappx PC Client is sent directly to the selected 3rd party printer and will print immediately

The Admin Portal will record the printed job

Pre-Requisites

3rd Party Printers must support SNMP v1.0 or later and IPP Printing

Microsoft Windows 10 or 11 fully updated

Printer discovery and activation

The following steps are required for printer discovery and activation:

- Ensure that the PC-client is up and running and you are logged in to it as an administrator
- Discover the printer using MFP discovery feature available on the Devices page of the Admin Portal

3rd Party Printers will show as [Others]

Devices

Activate device(s)

Deactivate device(s)

☐	Device	Type ↓	IP Address	Status
☐	Aficio MP C305 Aficio MP C305	OTHERS	192.168.15.192	
☐	BRN001BA9B8D696 MFC-8950DW	OTHERS	192.168.5.91	
☐	Develop C3350i Develop C3350i	OTHERS	192.168.0.42	
☐	ET0021B749E16F CX410de	OTHERS	192.168.15.104	

- Verify that the printer you require is listed on the Devices page

☐	BRN001BA9B8D696 MFC-8950DW	OTHERS	192.168.5.91		10/07/2025 10:35:26		
--------------------------	-------------------------------	--------	--------------	--	---------------------	--	--

Once the printer is listed, (as shown above), select it using the check box and [activate it](#)

Once activated the “activation key” will show as green

Printer Driver Installation for 3rd Party Printer

The following steps are required to setup an IPP printer driver

Step 1: Add a printer

From [Devices and Printers] click on [Add a printer]

Wait a few seconds — then click [The printer that I want isn't listed]

Select [Add a local printer or network printer with manual settings]

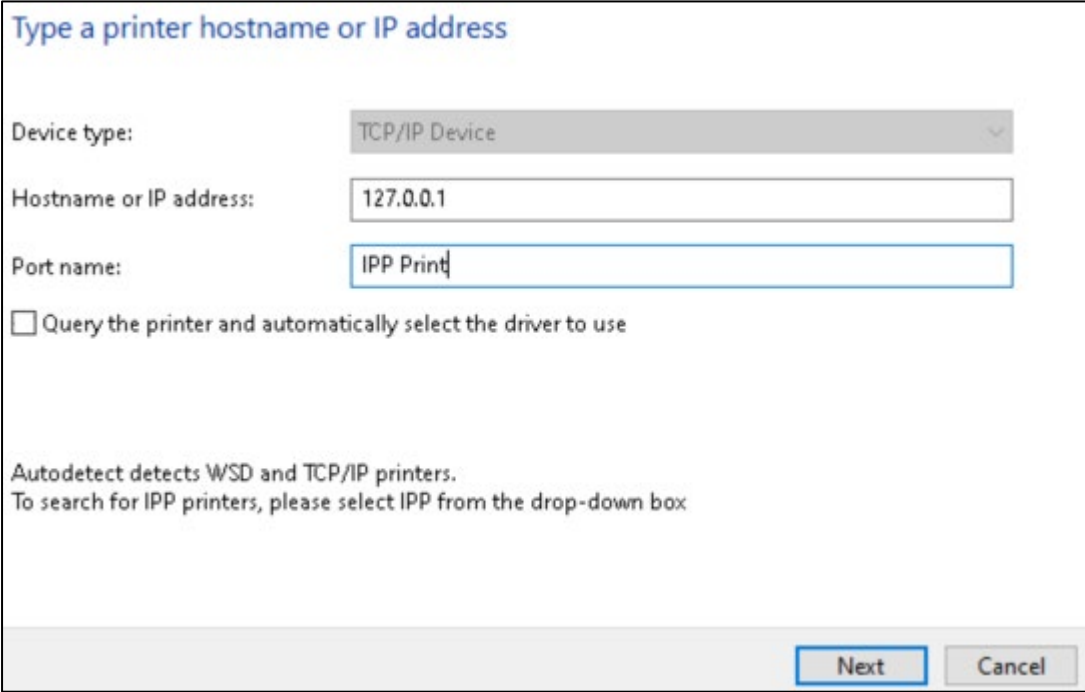
Click [Next]

From [Choose a Printer Port] select [Create a New Port] – Select [Standard TCP/IP Port]

In [Hostname or IP Address] type 127.0.0.1

In [Port Name] you can use anything suitable, in this example we have used [IPP Print]

Untick [Query the printer and automatically select the driver to use]



Type a printer hostname or IP address

Device type: TCP/IP Device

Hostname or IP address: 127.0.0.1

Port name: IPP Print

☐ Query the printer and automatically select the driver to use

Autodetect detects WSD and TCP/IP printers.
To search for IPP printers, please select IPP from the drop-down box

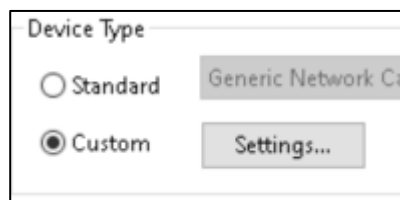
Next Cancel

Click [Next]

The setup will take a short while detecting the TCP/IP Port

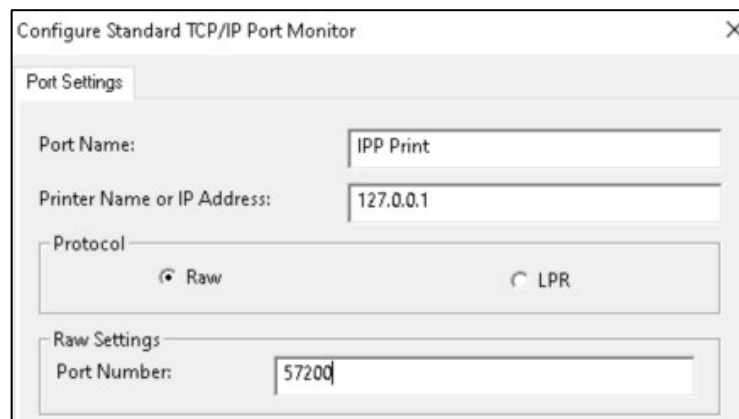
When prompted for “Additional Information Required”

Select [Custom] and then click [Settings]



Protocol = Raw

Port Number = 57200

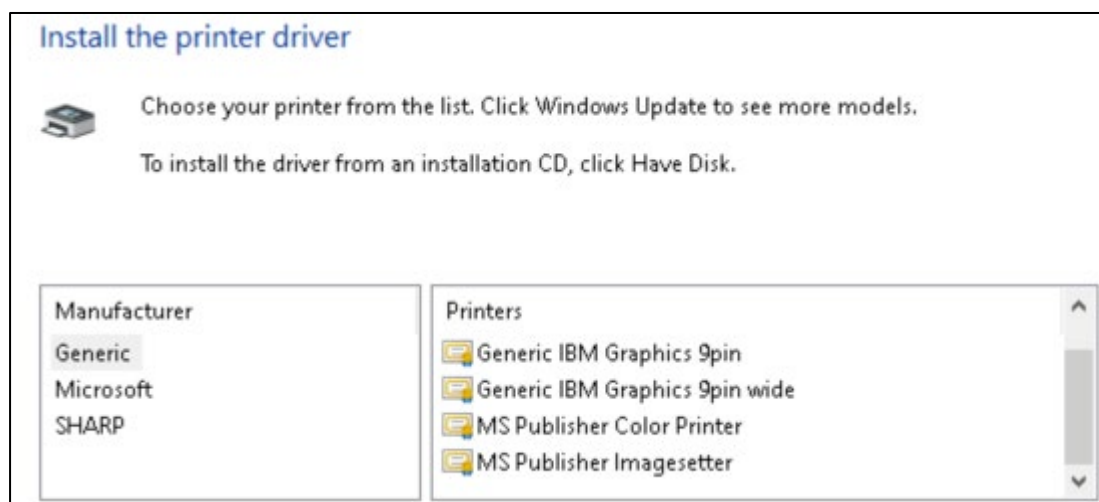


Click [Next] and [Next] again until you see the [Install Printer Drivers] page

For Printer Driver

Manufacturer - select [Generic]

Printers - select [Generic / MS Publisher Imagesetter]



Click [Next]

Name the Printer Driver – as an example “SCP Virtual IPP Printer”

Click [Next]

For sharing select [Not Shared]

Click Finish

You will now have installed the IPP Printer Driver

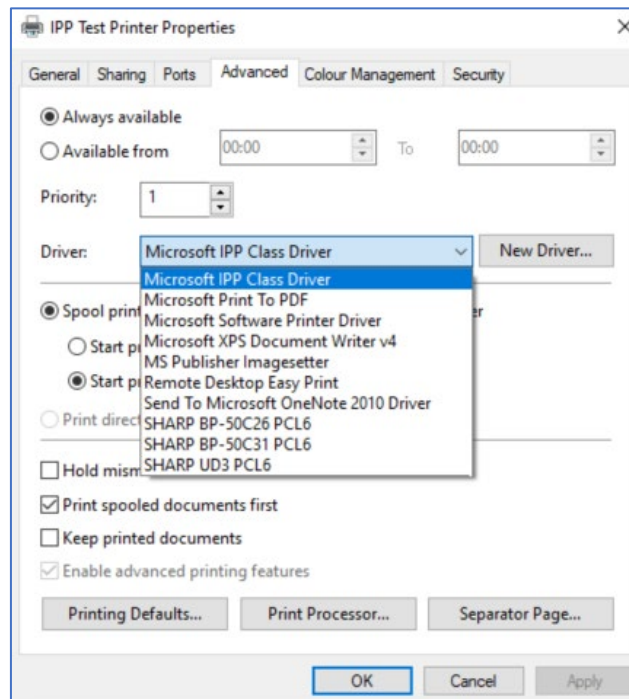


If the driver you installed is [MS Publisher Imagesetter], please continue with the next steps

Right click the new printer driver and select [Properties]

From the [Properties] tab, select [Advanced]

In the [Driver] dropdown menu – select “Microsoft IPP Class Driver”



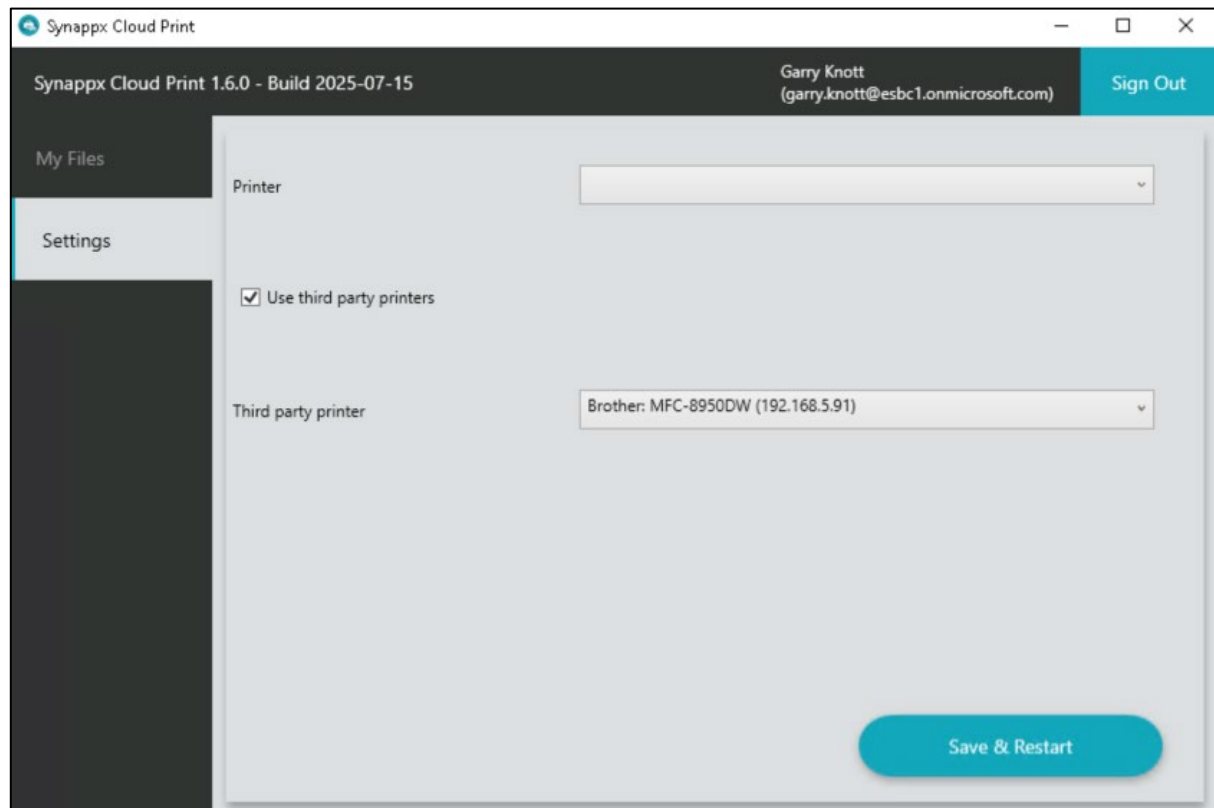
You are now ready to setup the PC Client to print to the 3rd Party Printer

PC Client

Open the PC Client and go to the [Settings] page

Tick the box named [Use 3rd party printers]

From the dropdown [Third party printer] select the device that you discovered and activated



Click [Save & Restart]

The PC Client will restart, and you are ready to print to your 3rd party printer by printing to the driver you installed earlier, (SCP Virtual IPP Printer).

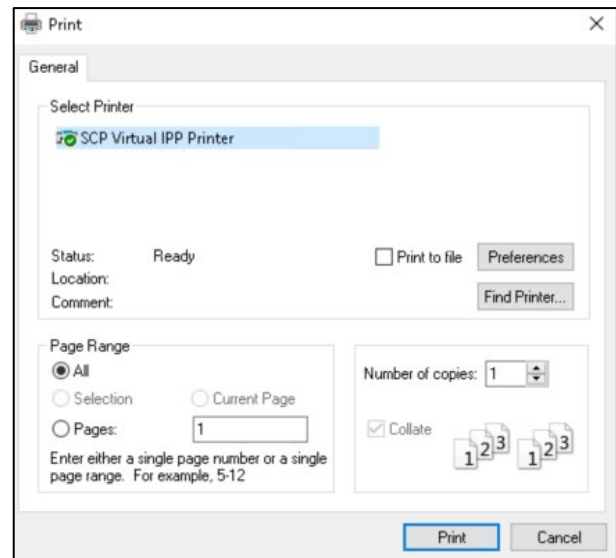
To print to the 3rd Party Printer

From your application select to print

Select the IPP Printer you setup earlier

Select [Print]

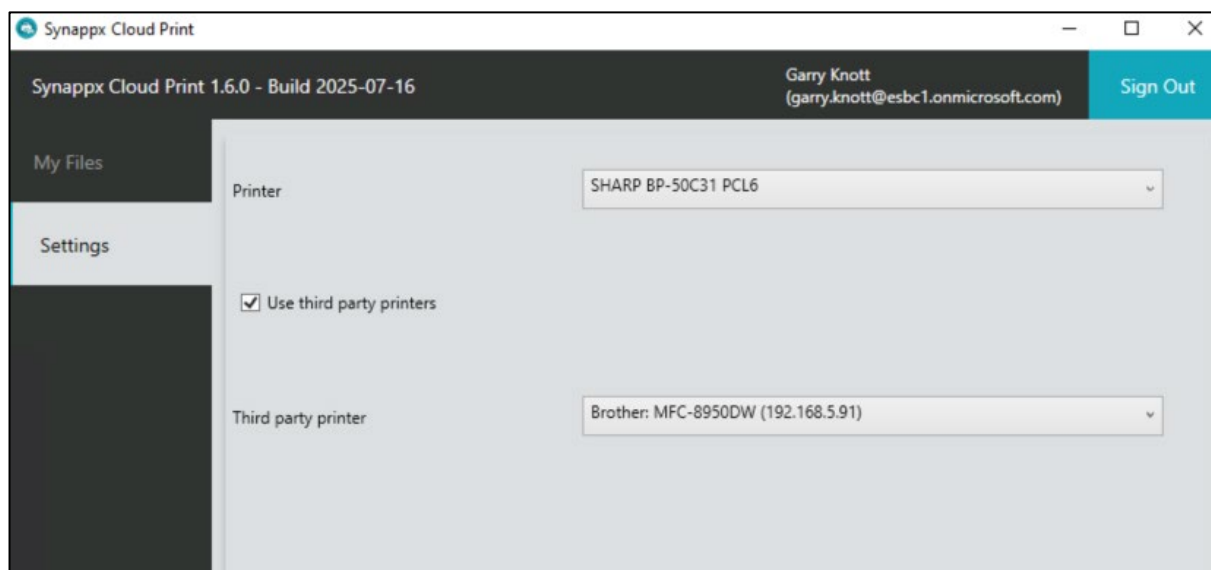
The print job will now be sent to the 3rd party printer via Synappx Cloud Print PC Client



Once printed, the print job will be displayed under [History] in the Admin Portal

Date/Time ↓	User	Job Name	Model	Type	Status
15/07/2025 09:58:56	Garry Knott	print-1752569966029	MFC-8950DW	PRINT	SUBMITTED
15/07/2025 09:48:16	Garry Knott	print-1752569326856	MFC-8950DW	PRINT	SUBMITTED

Please note, you are still able to have your regular Synappx Cloud Print driver available for printing held print jobs to your group 1 and group 2 devices.



Adding Non-compliant Group 1 and Group 2 Sharp Devices as 3rd Party Printers

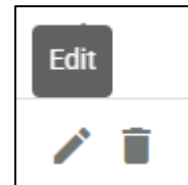
Sharp devices that are not supported by via Group 1 or Group 2 type devices can also be added by Synappx Cloud Print to be used as 3rd Party Printers

Any Sharp device that needs to be added must support SNMP v1.0 or later and IPP Printing

The Sharp device must be discovered and activated in the Admin Portal

In the Admin Portal – [Devices] – select the device you wish to print to

Click the pencil [Edit] icon



Under [Details] you need to make two changes

- Change [Device Type] to [Others]
- Add the device MAC Address

Click [Save]

Details	Options
The following section contains all relevant details for this device.	
Device Type OTHERS	IP Address 192.168.15.146
Device Alias ET788C77514BC7	
UUID SN701941040LG7MMNSHARP MX-B427W	
Machine ID 701941040LG7M	
MAC Address 78:8C:77:51:4B:C7	
Model MX-B427W	

Once done the device will become available in the dropdown menu for 3rd party printers

☒ Use third party printers

Third party printer

Brother: MFC-8950DW (192.168.5.91)

Brother: MFC-8950DW (192.168.5.91)

-: Develop C3350i (192.168.0.42)

MX-B427W (192.168.15.146)

Hewlett Packard: Color LaserJet MFP M477fdn (192.168.5.90)

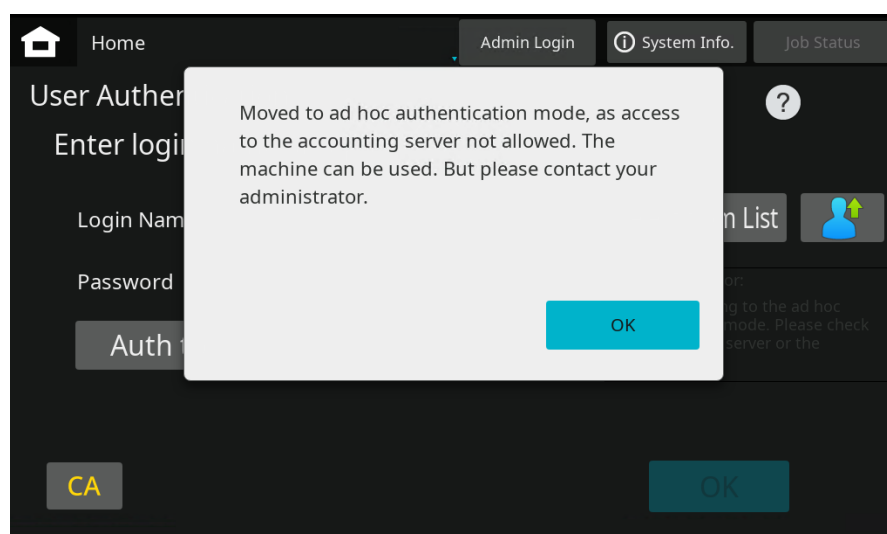
Addendum E – Red Firmware Upgrade

The Radio Equipment Directive, (RED), means that from August 1st 2025 all new devices and any firmware upgrades within the European Union will apply much tighter security. This complies with RED in that any device with radio, (WIFI), potential is designed and manufactured to avoid interference with other devices and to protect users and networks.

Some of the updated [default settings] may cause OSA Applications to fail until those settings are updated.

Potential Issue 1

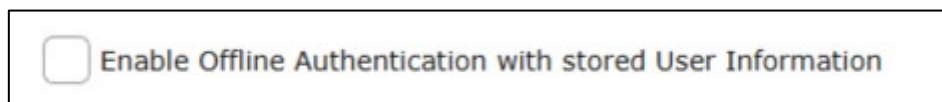
The device has moved into Ad Hoc Authentication Mode



This is caused by the setting:

[System Settings] – [Authentication Settings] – [Default Settings] – [[Enable Offline Authentication with stored User Information](#)]

This setting is enabled by default, please disable it by unchecking the tickbox

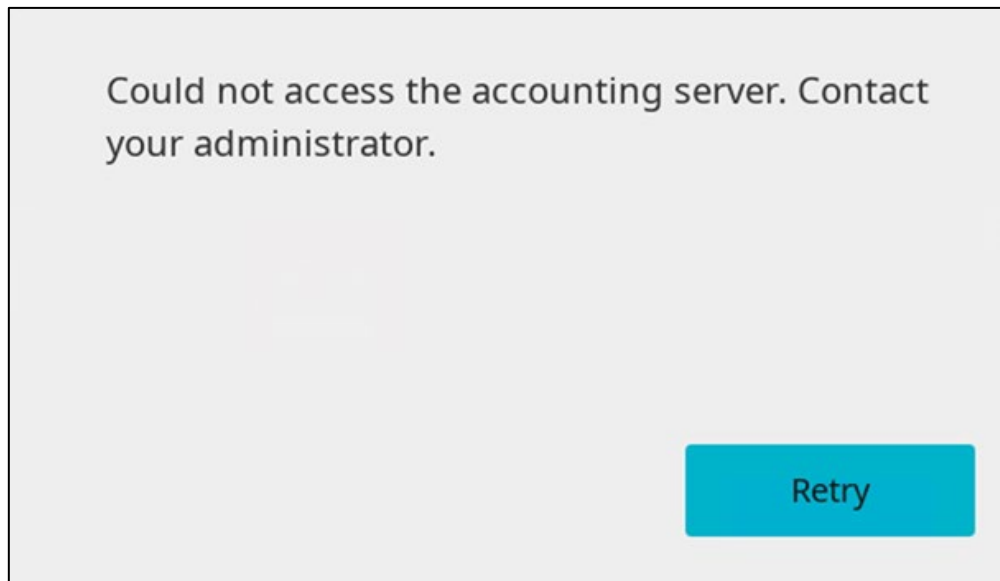


****Please be aware that the setting [Enable Offline Authentication] is only available when [User Authentication] is enabled****

Reboot the device

Potential Issue 2

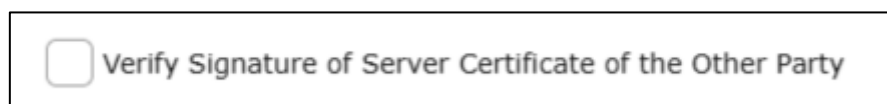
Once rebooted, you may see the following screen:



This is caused by the following setting:

[System Settings] – [Security Settings] – [SSL/TLS Settings] – [[Verify Signature of Server Certificate of the Other Party](#)]

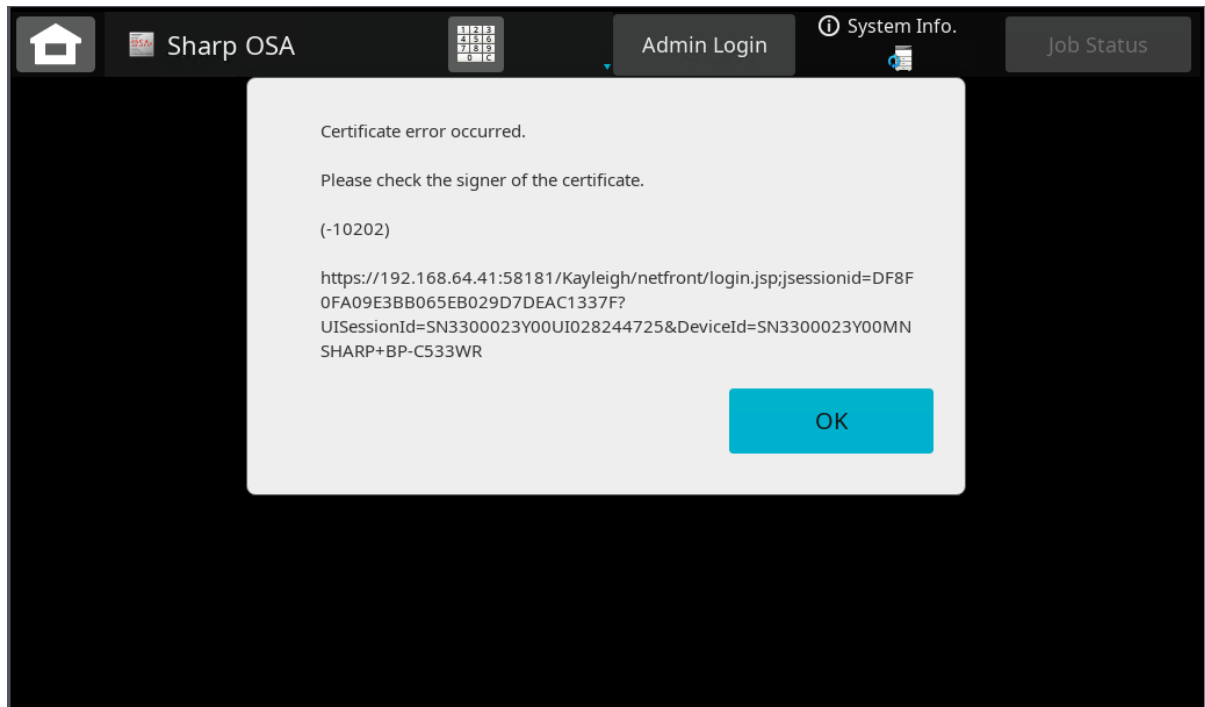
This setting is enabled by default, please disable it by unchecking the tickbox



Reboot the device

Potential Issue 3

A Certificate error occurred. This could be caused when a card reader is attached and set to - [Use IC Card for Authentication]



Disable the following setting:

[System Settings] – [Authentication Settings] – “Cache Authentication Information for External Service Connect”

Disable this setting and reboot the device

☐ Cache Authentication Information for External Service Connect
--

Potential Issue 4

You cannot print a held job from Synappx Cloud Print

This is caused by the following setting:

[System Settings] – [Security Settings] – [Port Control] – [[Raw Print](#)]

This setting is disabled by default, set it to Enable

Raw Print:	Enable ▼	Port Number:	9100	(0-65535)
------------	---	--------------	-----------------------------------	-----------

Pull printing will now work as expected



Potential Issue 5

Any Synappx Cloud Print page shows as a blank page on the device

If any Standard OSA Application is displaying a blank screen when called, then the following settings need to be changed

[System Settings] – [Security Settings] – [Port Control] – [[Sharp OSA \(Extended Platform\)](#)]

Depending on the Application, you may need to change HTTP or HTTPS to Enable

Sharp OSA(Extended Platform):				
HTTP:	Enable ▼	Port Number:	10080	(0-65535)
HTTPS:	Enable ▼	Port Number:	10443	(0-65535)

Standard Applications will now display as expected

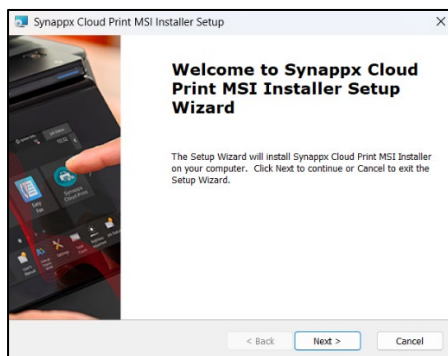
It is also advisable to upgrade to the latest version of RED firmware as soon as it becomes available

Addendum F – PC Client deployment using MSI file

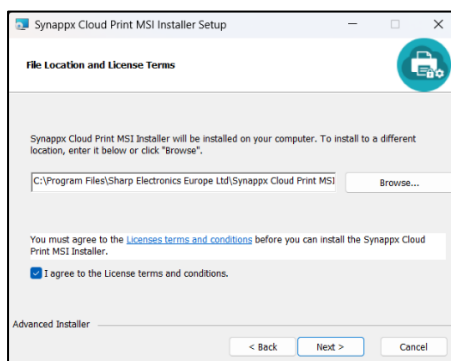
The PC Client can be deployed to client PC's using the application MSI file. The installation takes care of PC Client installation, driver installation and Windows configuration in one step.

The MSI can be installed manually or deployed using Group Policy or other bulk deployment methods including Microsoft Intune.

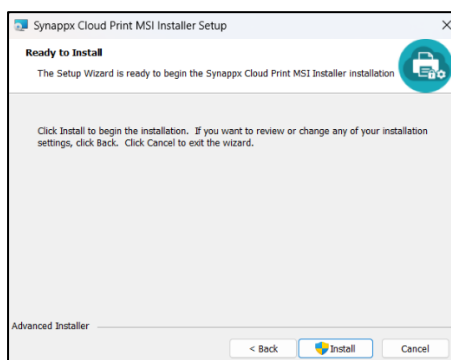
Start the MSI installer



Accept the terms and conditions



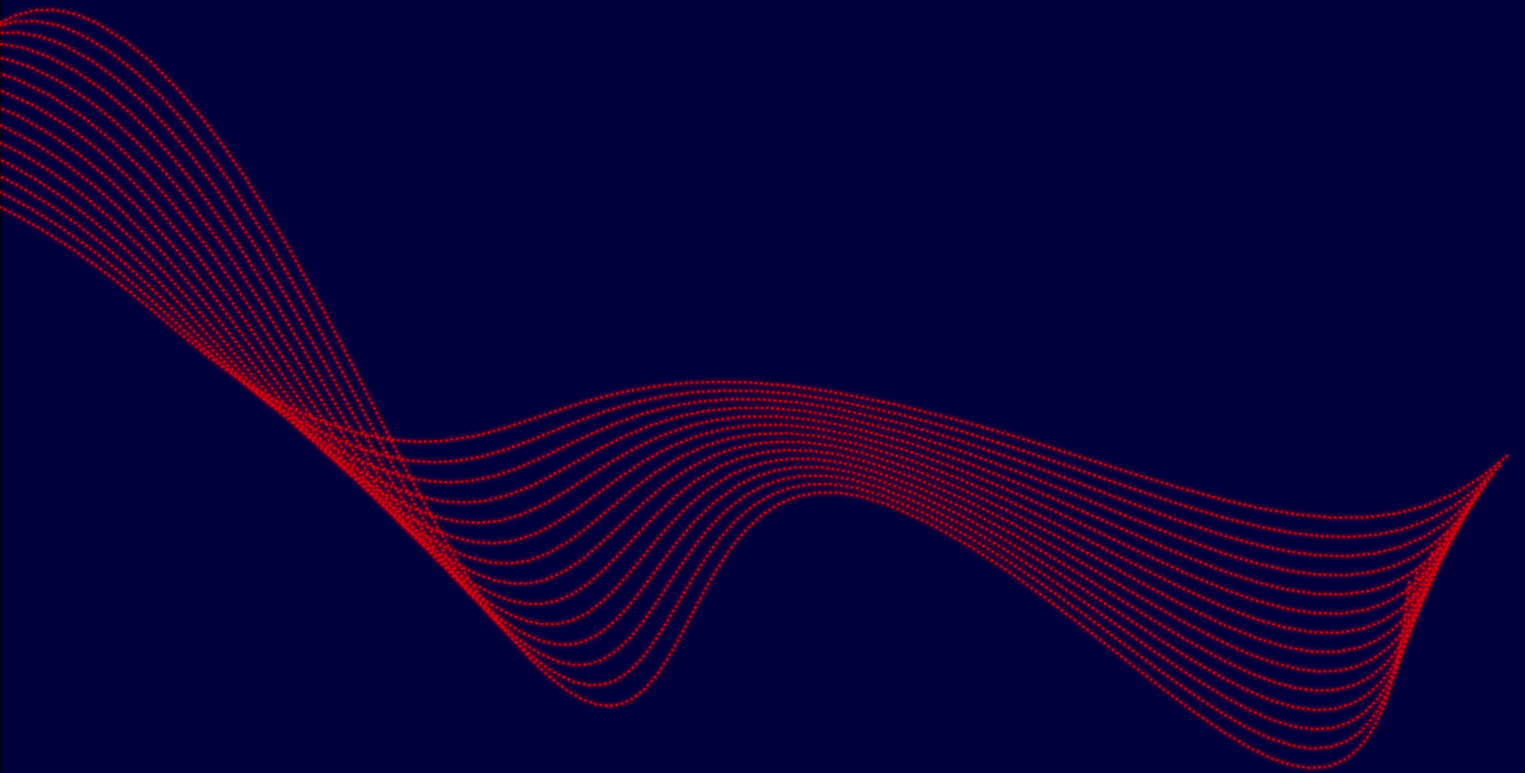
Click 'install'



Note:

The package will install a 'standard' UDL3 printer driver, compatible with both Intel and ARM processors

To deploy a customised driver, copy the driver file to c:\drivers on each users PC. This can be done manually or using Group Policy or bulk deployment tools.



sharp.eu

SHARP