SHARP

SYNAPPX™

SYNAPPX™ GO

PRODUCTIVITY WHEREVER YOU GO!

Administrator Setup and Configuration Guide

Table of Contents:

This page is intentionally left blank.

Synappx Go: Getting Started

Synappx Go Overview

Synappx Go is a mobile app that connects to Sharp multi-function printers (MFPs), shares content to Sharp displays, enables productive in-room meetings when used with Synappx Meeting and captures workspace locations with mobile check-in. Projects move with you throughout your workday, providing productivity wherever you go!

Synappx Go completes your scan, print, copy, share, meet and check-in tasks with the following features:

Easy Setup

- Follow the simple setup wizard—no training required!
- Create your own scan-to-cloud or email distribution lists right from your phone.
- Set default scan, print and copy settings to save time.
- No Login MFP mode enables scan to email and copy features with no license and limited set up

Scan

- Tap your phone to scan a file to yourself (via email), email distribution lists, and popular cloud storage services

Print

- Walk up to any enabled MFP to release print jobs and print from cloud storage.
- Enjoy convenience and privacy.

Copy

- Create contactless copy jobs from your mobile phone and save your favorite copy settings.

Unlock MFPs

- For MFPs that have been locked by PaperCut or Native Authentication, use Synappx Go mobile to unlock the MFP and access Synappx Go scan, copy and print related features.

Share

- Tap the NFC tag to display content on the Sharp display.
- Team members can also tap the NFC tag to retrieve content and collaborate.
- Remotely operate Microsoft Office files.
- Speed up collaboration with Synappx Go. Modified content is stored back in the original cloud location.

Meet (When Used with Synappx Meeting)

- Tap NFC tag, select a meeting from your mobile and automatically start web conference sessions on the display, connecting all necessary audio/video components.
- Create ad hoc meetings from your mobile for unscheduled collaborations
- Remotely operate web conference and cloud or attachment files from your smartphone.

- Close opened files, end and disconnect meeting with one click.

Check In

Health and safety are a key consideration for organizations. **Check In** helps track employee touch points in the workplace.

- Tap the Synappx Go NFC tag to check in to common work areas, such as break rooms and meeting rooms.
- Reports allow administrators to track touch points.

Guest Users Support

- Users from other companies can be licensed as guests and use Synappx Go MFP and display features.

System Requirements

Synappx Go Major Components	
1. Mobile Application (iOS and Android™) 2. NFC Tags 3. MFP and Display Agents	4. Admin Portal 5. Cloud System (Microsoft® Azure) 6. Embedded MFP Apps (for selected A4 models and PaperCut or Native Authentication integration with Synappx Go.

A stable internet connection is required.

Organizations must have a Microsoft® 365 or Google Workspace environment. Provider is designated after sign-up. If an organization uses both Microsoft 365 and Google Workspace, the administrator must choose one cloud service provider for Synappx to synchronize with the calendar (Synappx Meeting) and users (Meeting and Go).

Note: Support is available for environments that have on-premise Active Directory® synchronized using Google Cloud Directory Sync (GCDS) for user synchronization. GCDS is often used to synchronize the data in an organization's Google domain with Microsoft Active Directory or the Lightweight Directory Access Protocol (LDAP) server.

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

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

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

MFP Agent	Display Agent
• Microsoft Windows® 10 or greater or Windows Server 2016 or 2019, 32- or 64-bit • Microsoft .NET Framework 4.7.2 or higher • Minimum 4GB RAM • Minimum 75MB disk space (Requirements can vary based on the number of users and print jobs that the agent supports.) • Internet connectivity	• Display computer or Shuttle® PC with Windows 10 or greater, 32- or 64-bit • Microsoft .NET Framework 4.7.2 or higher • Minimum 4GB RAM • Minimum 10MB disk space • Microsoft 365 client applications (e.g. PowerPoint®, Word) and other apps (e.g. video viewer) for files that will be downloaded • Adobe® PDF reader for Google native files (view only) • Chrome™ browser for editing Google files and opening Microsoft 365 files in browser • Internet connectivity

Admin Portal
Browser-based: Google Chrome and Microsoft Edge (latest versions)

NFC Tags
• Sharp-provided or in select MFP models • See NFC Support chart

Users and Admins
• Supports 5,000 users • All users must: ○ Have Microsoft 365 or Google Workspace accounts ○ Be in Microsoft Azure Active Directory (AD) or Google Workspace Directory • Guest users can be added and licensed to access many Synappx Go features • First administrator to log in requires Azure AD or Google Workspace admin privileges

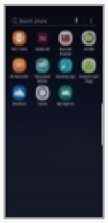
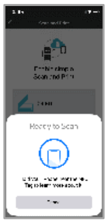
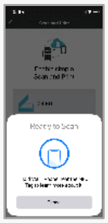
Supported Mobile Platform
Apple® iPhones®: NFC support, iOS 12 or later • 7/7+, 8/8+, X, XR, XS, XS Max, iPhone 11, 11 Pro, 11 Pro Max, and iPhone SE (Second Generation - 2020)
Android™ • 8 to 11, NFC support

Note: Companies have the option to integrate Synappx Go with PaperCut MF or Native Authentication. Reference the following Admin documents below for more details on system requirements, installation and configuration in those environments.

- PaperCut MFP with Synappx Go Installation and Configuration Guide
- Native Authentication with Synappx Go Installation and Configuration Guide

The free version of Synappx Go (No Login version) does not require agent install or NFC tags. The No Login version enables simple copy and scan to email functions by scanning a QR Code. To enable the No Login Synappx Go feature, install Synappx Go embedded applications on a Sharp MFP(s) to generate a QR code. Contact your authorized Sharp service technician to install the application and set up Sharp MFP(s). The full version of Synappx Go can be unlocked when a user license is assigned, the Synappx Go agent is installed and an NFC tag is mapped. Once the full version is unlocked, users will have an access to copy, scan to email, scan to cloud storage services, share to display, and more.

NFC Support

	Synappx Go Tag (MFP, Display, Check In)	**MFP Built-In Tag (Some Models)**
Android	**Background Access*, **** 	**Foreground Access***
iPhone XR, XS, XS, 11, SE (all versions)	**Background Access**** 	**Foreground Access** 
iPhone 7/7+, 8/8+, and X	**Foreground Access** 	**Foreground Access**

Background
When you tap the NFC tag, the phone brings you directly to the Synappx Go app (without having to open the app first). Some phones may display a notification. When you select the notification, the phone still brings you directly to the app.

Foreground
From the mobile screen, select the Synappx Go app. Then select the desired feature (e.g. Scan and Print).

Notes:
*If there are other apps that read NFC tags, you may be prompted to select Synappx Go each time you want to use the app, or if given the option, you can choose to make Synappx Go the default app for reading an NFC tag.
**NFC tag setup (admin task) is always a foreground operation.

MFP Support

Sharp MFPs running OSA® 4.0 or greater and supporting TLS 1.2 can be used with Synappx Go tags for scan, print release, and print cloud files. Later models have built-in NFC tags that can be used. However, MFP NFC configuration may be required if not already set up.

Teal model numbers can support the Synappx Go copy feature and optional integration with the rf IDEAS reader for PaperCut MF and Native Authentication use. The rf IDEAS integration requires installation of Synappx Go 1.0.0.emo file in the MFP on the models below.

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

[1] MX-PK13L Adobe® PostScript® 3™ Expansion Kit and MX-PU10L Direct Print Expansion Kit are required to print cloud files.
[2] Special firmware needed to enable TLS 1.2 support
[3] These models support the Synappx Go copy feature and optional rf IDEAS card reader integration (e.g. for PaperCut MF or Native Authentication) but require that the MX-AMX2L Application Communications Module (ACM) option be installed.
[4] These models can support the Synappx Go MFP No Login version after installation of the Synappx Go – No Login.emo application.

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

Printer Models	MX-C607P	MX-B427W
	MX-C507P	MXB427PW
	MX-C407P	MX-B467F
	MX-B707P	MX-B467P
	MX-B557P	

[1] For document scan and copy:

- **Hard Disk Drive** is recommended (standard on MX-B557F and MX-C507F) and required to create searchable PDF scans from Synappx Go.
- **Hard Disk Drive** is required to support job accounting log for native authentication.
- Install the **Synappx Go MFP app** (instructions here) for these models.
- To support the Synappx Go No Login version, install the Synappx Go – No Login.esf embedded app.
- For rf IDEAS reader and native MFP authentication integration with Synappx Go, install the Synappx Go with ID Card embedded applications. All three apps (Synappx-Go_2012a.fls, keyboardreader-2.4.11.fls and cardAuth_2012a.fls) should be installed.
- Sharp UD 3 is a recommended driver for print release.

[2] These models support the Synappx Go copy feature and optional rf IDEAS integration with PaperCut MF or Native Authentication but require that the MX-AMX2L Application Communications Module (ACM) option be installed.

Notes:

- If using built-in NFC tags, modify the following MFP web page settings:
  - **Network Connections** > **Easy Connections Setting**: Enable NFC tag
  - **Network Settings** > **Quick Settings** > **Wireless Settings:** Set **Connection Type** to either **Wireless (Infrastructure Mode)** or **Wired + Wireless (Access Point Mode)**
- There are no MFP web page network setting changes for external NFC tags.
- For information on early model compatibility, contact your reseller or Sharp representative.

Configure MFP Web Page for Copy

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

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

Display Support

Any interactive whiteboard or display with a Shuttle® PC or another PC system running Microsoft® Windows 10 or greater or Windows Server® 2016 or 2019 can be used with the Synappx Go display agent. System on Chip (SOC) models without a Shuttle PC are not supported at this time.

Synappx Go Setup and Configuration Overview

- If you are configuring the combined V3.0 Synappx Go and Synappx Meeting in room system, please see the separate **Synappx Collaboration Suite** guide.
- If you want to use only the limited MFP No Login (Free Copy and Scan version of Synappx Go, please see section of this document with set up instructions.

Note: The following are directions for installation and configuration of the standard, licensed Synappx Go system.

1. **Choose Provider**
    - Follow directions in your welcome email to select Microsoft 365 or Google Workspace as a cloud service provider.
    - Follow procedures in second welcome email specific to Microsoft 365 or Google Workspace.
        - Google Workspace: Configure Synappx support on the Google Workspace Admin page (requires Google Workspace admin privileges).
2. **Log in to the Admin Portal**
    - Use Microsoft 365 or Google Workspace credentials.
    - Grant Synappx Go app permissions for licensed users (one time only).
    - Microsoft 365: First administrator requires Azure admin privileges to log in.
3. **Configure and Download Agents**
    - MFP Agent:
        - Set SNMP IP discovery range to find MFPs automatically .
        - Download MFP agent software.
    - Display Agent:
        - Download display agent software.
4. **Install Agents**
    - MFP Agent:
        - Install MFP agent on PC/server.
        - Agent self-registers with Synappx Go cloud using X.509 certificates.
        - MFP discovery is automatically done for IP ranges.
        - MFP agent and discovered information is visible on the Admin Portal.
    - Display Agent:
        - Install display agent on PC/server.
        - Agent self-registers with Synappx Go cloud using X.509 certificates.
        - Display agent is visible on the Admin Portal.
    - System: Agent Updates, Admin Log, System Log, Check In Log (Optional).
5. **Add Workspaces**: Add or import Microsoft 365 or Google workspaces.
6. **Associate Devices to Workspaces**
    - Connect workspaces with MFPs and/or displays.
    - Configure display automatic input switch.
7. **Associate NFC Tags**: Use Synappx Go to associate NFC tags with devices and check-in.

8. **Add Users and Allocate Licenses**
   - Import Azure AD or Google users and assign licenses.
   - Newly licensed users receive emails with app download instructions.
   - Optionally, add guest users who can access Sharp hardward with your permission.
9. **Configure Print Release Driver**
   - Share configured print driver to users for the Synappx Go MFP agent.
10. **Windows Defender Firewall Post-Installation Configuration (Optional):** Open either or both inbound TC port(s) 9100 and 515 on the MFP agent server by creating rules on the machine's firewall (only necessary if print jobs are not getting to the MFP agent PC).
11. **Automatic Input Switch (Optional):** Configure displays to switch to the display agent input automatically when using Share and to return to default input at meeting end.

How It Works

Getting Started

Thanks for signing up for Synappx™. Get ready to experience productivity wherever you Go!

Here's what happens next:

The assigned administrator receives an email to choose Google Workspace or Microsoft 365 as a cloud service provider.

1. 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.
2. Log in to the Synappx Admin Portal and start adding users and workspaces.

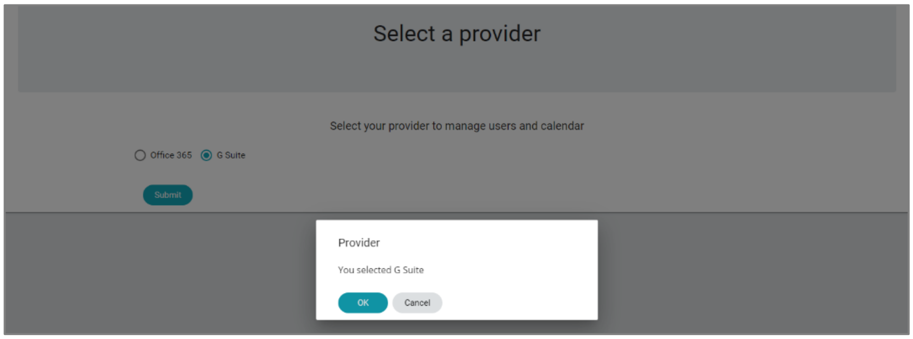
Choose Provider

Note: The assigned administrator for Microsoft 365 or Google Workspace must have administrator privileges for that service.

After a Synappx account is created for your organization, the assigned administrator will receive an email with a link to select either Microsoft 365 or Google Workspace as a cloud service provider. This provider defines how Synappx manages the users and calendar within the organization.

Here's how:

Select the link to choose your provider. The Synappx service validates the domain with the provider.



Select a provider

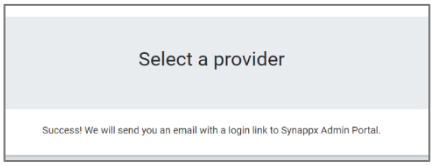
Select your provider to manage users and calendar

○ Office 365 ● G Suite

Provider

You selected G Suite

a. If validation fails, you will see an error message. Ensure you selected the correct provider.
b. When the domain is validated, you will receive another welcome email with instructions to log in to the Synappx Admin Portal. Select the link.



Select a provider

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

Synappx Admin Portal

After selecting a provider (Microsoft 365 or G Suite), the administrator will receive a second email with a link to the Synappx Admin Portal.

The Synappx Admin Portal is a browser-based platform designed for administrators to manage key components (e.g., licenses, workspaces, users) of Synappx Meeting and Synappx Go. Admins log in with the organization's Microsoft 365 or Google Workspace account. It is recommended to use the latest version of Google Chrome™ or Microsoft Edge.

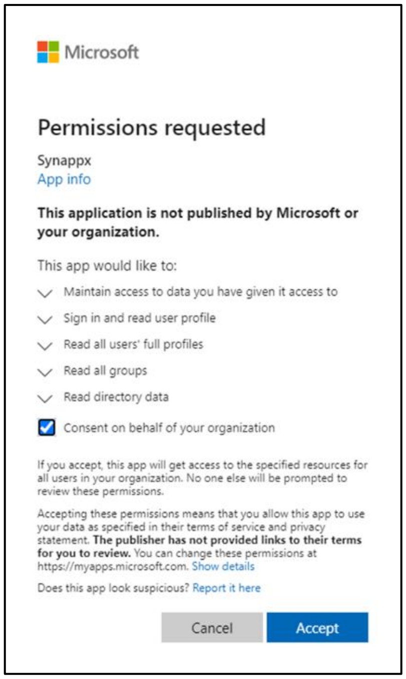
Admin Portal for Microsoft 365

After the admin selects a cloud service provider in the first Synappx email, a link to the Admin Portal will arrive in a second Synappx welcome email.
Select the link and log in with your Microsoft 365 credentials. At initial login, accept the permission request to allow Synappx apps to access selected Microsoft services on behalf of your organization.

Admin Portal for Google Workspace™

Before logging in to the Admin Portal, follow the steps described in the second welcome email to allow Synappx to communicate with your Google Workspace instance. This includes registering the Client ID and Application Programming Interface (API) scopes in the Google Workspace Admin Console. The steps from the email are in the procedure below.

1. Select Google Workspace as your cloud service provider in the initial welcome email.



Permissions requested

Synappx
App info

This application is not published by Microsoft or your organization.

This app would like to:

- Maintain access to data you have given it access to
- Sign in and read user profile
- Read all users' full profiles
- Read all groups
- Read directory data

☑ Consent on behalf of your organization

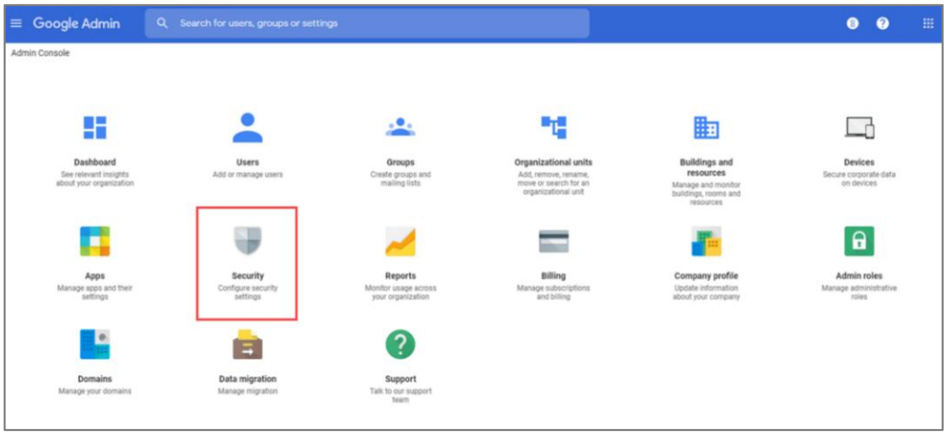
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

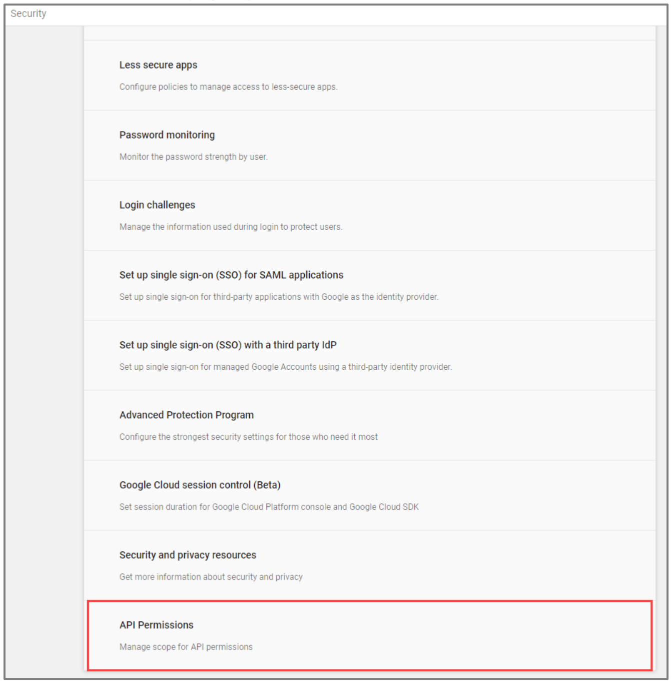
Does this app look suspicious? Report it here

2. Upon receiving the second welcome email, follow the instructions to set up your Google Workspace Admin Console to communicate with Synappx.

    a. In any web browser, go to admin.google.com.
    b. Select **Security**.


Google Admin
Search for users, groups or settings
Admin Console
Dashboard
See relevant insights about your organization
Users
Add or manage users
Groups
Create groups and mailing lists
Organizational units
Add, remove, rename, move or search for an organizational unit
Buildings and resources
Manage and monitor buildings, rooms and resources
Devices
Secure corporate data on devices
Apps
Manage apps and their settings
Security
Configure security settings
Reports
Monitor usage across your organization
Billing
Manage subscriptions and billing
Company profile
Update information about your company
Admin roles
Manage administrative roles
Domains
Manage your domains
Data migration
Manage migration
Support
Talk to our support team

    c. On the Security page, select **API Permissions**.


Security

Less secure apps

Configure policies to manage access to less-secure apps.

Password monitoring

Monitor the password strength by user.

Login challenges

Manage the information used during login to protect users.

Set up single sign-on (SSO) for SAML applications

Set up single sign-on for third-party applications with Google as the identity provider.

Set up single sign-on (SSO) with a third party IdP

Set up single sign-on for managed Google Accounts using a third-party identity provider.

Advanced Protection Program

Configure the strongest security settings for those who need it most

Google Cloud session control (Beta)

Set session duration for Google Cloud Platform console and Google Cloud SDK

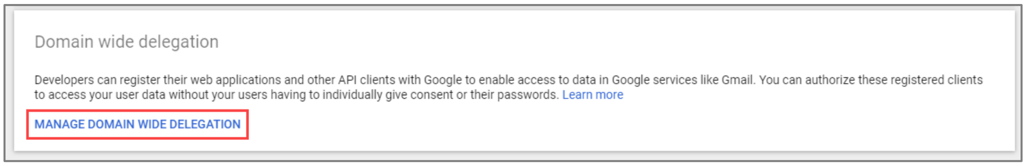
Security and privacy resources

Get more information about security and privacy

API Permissions

Manage scope for API permissions

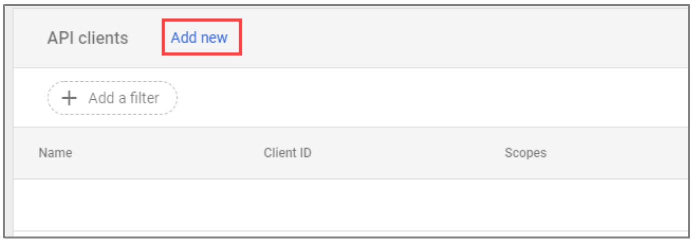
    d. Select **Manage Domain Wide Delegation**.


Domain wide delegation

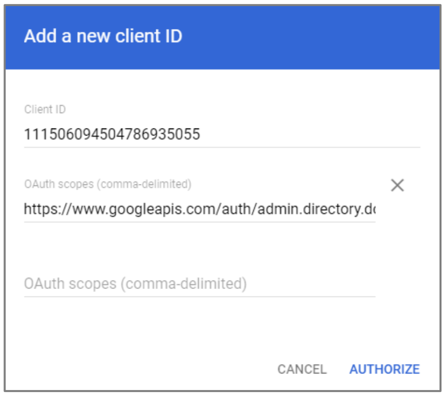
Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

MANAGE DOMAIN WIDE DELEGATION

e. Select **Add New**.



f. In the **Client Name** field, enter Sharp's ID number: **116382460935345417066**.



Client ID
111506094504786935055

OAuth scopes (comma-delimited)
https://www.googleapis.com/auth/admin.directory.d

OAuth scopes (comma-delimited)

Notes:

- Be sure to copy and paste these URLs. They require comma separation as shown. It may take up to 30 minutes for changes to activate in the G Suite account.
- If you are updating the system from V2.3 to V2.4 and later, an additional API scope is necessary to enable users to add attendees from the user directory. Add the following API scope: **https://www.googleapis.com/auth/directory.readonly**

g. Paste the Synappx API Scopes in to the **OAuth Scopes** field. Select **Authorize**.

https://www.googleapis.com/auth/admin.directory.domain.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/calendar.readonly,
https://www.googleapis.com/auth/calendar.events,
https://www.googleapis.com/auth/drive,
https://www.googleapis.com/auth/drive.file,
https://www.googleapis.com/auth/userinfo.profile,
https://www.googleapis.com/auth/directory.readonly

h. Open the second Synappx welcome email and select **Log in to your account** or go to https://synappxadminportal.sharpusa.com/ to log in to the Admin Portal.

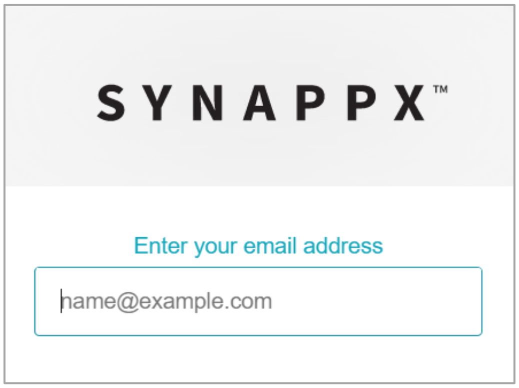
Synappx Go Setup and Configuration

Step 1: Log In (First Time) to Admin Portal

Notes:

- An email containing the Synappx Admin Portal URL will be sent to the assigned administrator when your organization signs up for Synappx. Google Workspace admins must complete the Admin Console setup before logging in to the Admin Portal. See Synappx Admin Portal for more information.
- The first administrator to log in must have admin privileges for Azure Active Directory or Google Workspace to authorize Synappx Go features for users. Subsequent administrators do not require Azure or Google Workspace admin access.
- If you are an existing Synappx customer (prior to v3.0) who previously opted into Microsoft permissions, ensure you or your users have already or now opt in to calendar access to enable use of the Synappx Collaboration Hub meeting features.

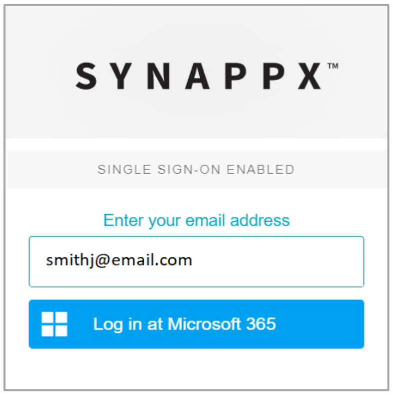
1. Use your Google Workspace or Microsoft 365 credentials to log in to the Synappx Admin Portal via the latest version of Google Chrome or Microsoft Edge. After typing your email in the Synappx log in page, select the **Log in to Microsoft 365** button if you are using Microsoft credentials and **Log in with Google Workspace** if you are using Google credentials.



SYNAPPX™

Enter your email address

name@example.com



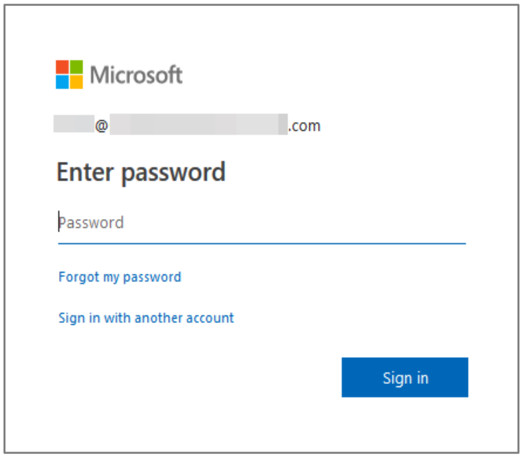
SYNAPPX™

SINGLE SIGN-ON ENABLED

Enter your email address

smithj@email.com

Log in at Microsoft 365



Microsoft

[redacted]@[redacted].com

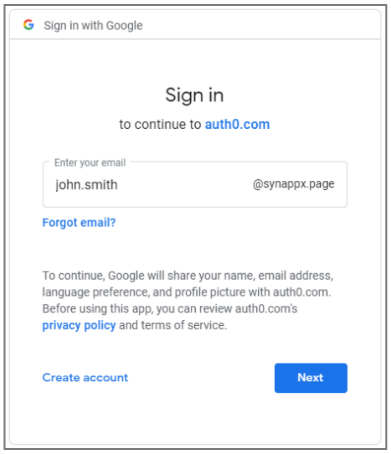
Enter password

Password

Forgot my password

Sign in with another account

Sign in



Sign in with Google

Sign in

to continue to auth0.com

Enter your email

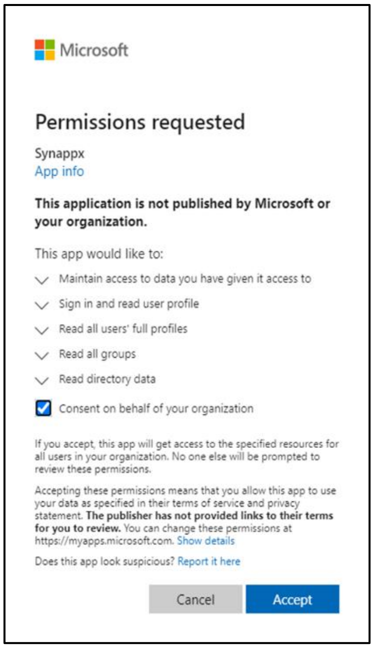
john.smith @synappx.page

Forgot email?

To continue, Google will share your name, email address, language preference, and profile picture with auth0.com. Before using this app, you can review auth0.com's privacy policy and terms of service.

Create account Next

2. **Microsoft 365: Check** the **Consent on behalf of your organization** box and select **Accept**.



Microsoft

Permissions requested

Synappx
App info

This application is not published by Microsoft or your organization.

This app would like to:

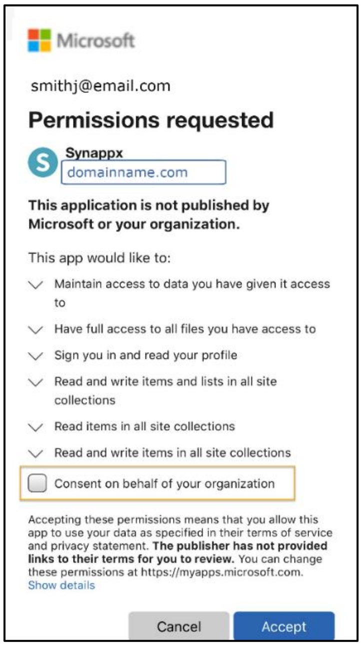
- Maintain access to data you have given it access to
- Sign in and read user profile
- Read all users' full profiles
- Read all groups
- Read directory data

☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here



Microsoft

smithj@email.com

Permissions requested

Synappx
domainname.com

This application is not published by Microsoft or your organization.

This app would like to:

- Maintain access to data you have given it access to
- Have full access to all files you have access to
- Sign you in and read your profile
- Read and write items and lists in all site collections
- Read items in all site collections
- Read and write items in all site collections

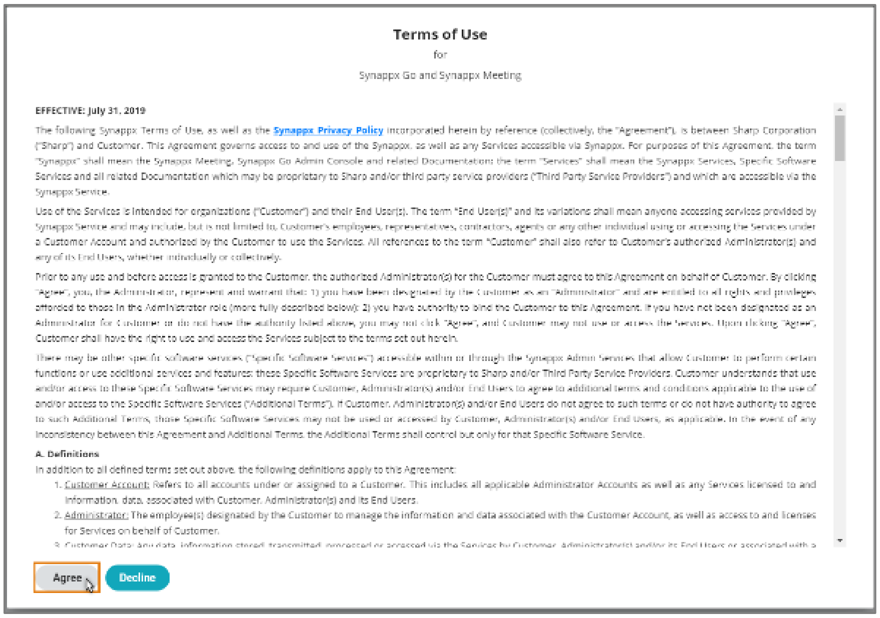
☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com.
Show details

Google Workspace: If login fails, go to the Google Workspace Admin Console and add the Synappx API scope.

Note: Agreement with the Terms of Use is only required with the initial Admin Portal login.

3. Review the **Terms of Use** (Synappx Privacy Policy) for Synappx Go users (and Synappx Meeting if also licensed). These Terms of Use are only granted to users for Synappx application use. Select **Agree** to continue.



Terms of Use

for

Synappx Go and Synappx Meeting

EFFECTIVE: July 31, 2019

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, as well as any Services accessible via Synappx. For purposes of this Agreement, the term "Synappx" shall mean the Synappx Meeting, Synappx Go Admin Console 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.

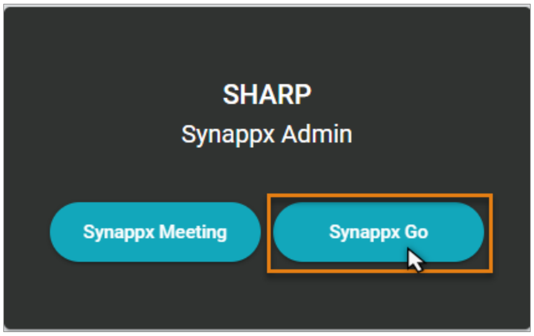
There may be other specific software services ("Specific Software Services") accessible within or through the Synappx Admin Services that allow Customer to perform certain functions or use additional services and features; these Specific Software Services are proprietary to Sharp and/or Third Party Service 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 Services ("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:

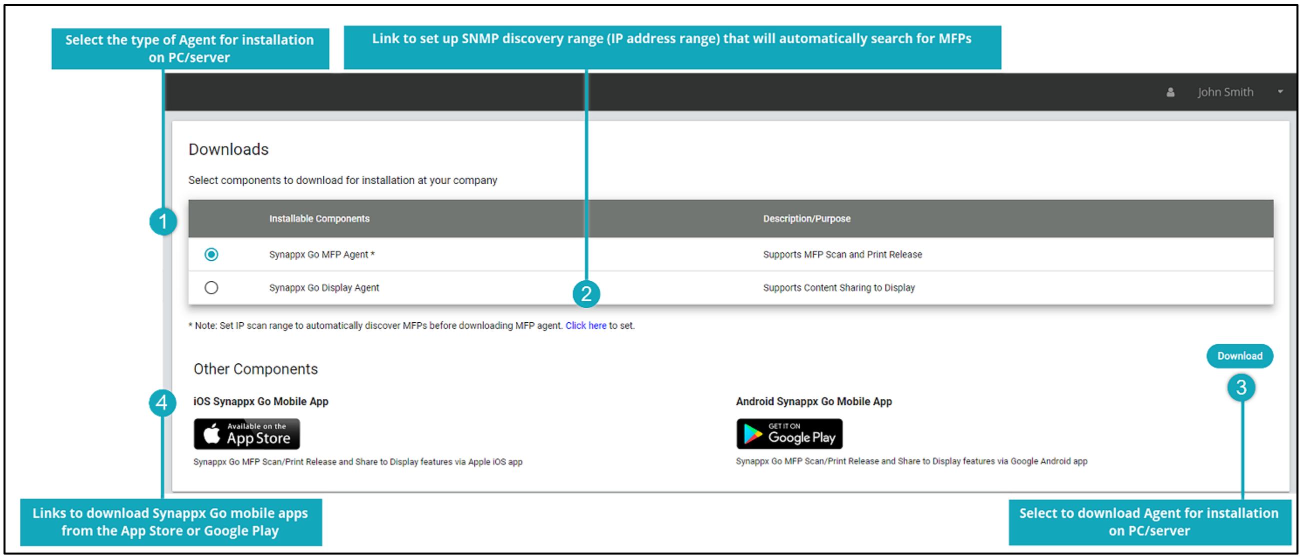
1. Customer Account: Refers to all accounts under or assigned to a Customer. This includes all applicable Administrator Accounts as well as any Services licensed to and information, data, associated with Customer, Administrator(s) and its End Users.
2. Administrator: The employee(s) designated by the Customer to manage the information and data associated with the Customer Account, as well as access to and licenses for Services on behalf of Customer.
3. Customer Data: Any data, information stored, transmitted, processed or accessed via the Services by Customer, Administrator(s) and/or its End Users or associated with a

4. If you have licensed Synappx Go and Synappx Meeting, both options will appear in the pop-up window. Select **Synappx Go**.



SHARP

Synappx Admin



Select the type of Agent for installation on PC/server

Link to set up SNMP discovery range (IP address range) that will automatically search for MFPs

Downloads

Select components to download for installation at your company

1

	Installable Components	Description/Purpose
●	Synappx Go MFP Agent *	Supports MFP Scan and Print Release
○	Synappx Go Display Agent	Supports Content Sharing to Display

2

* Note: Set IP scan range to automatically discover MFPs before downloading MFP agent. Click here to set.

3

Other Components

4

iOS Synappx Go Mobile App

Synappx Go MFP Scan/Print Release and Share to Display features via Apple iOS app

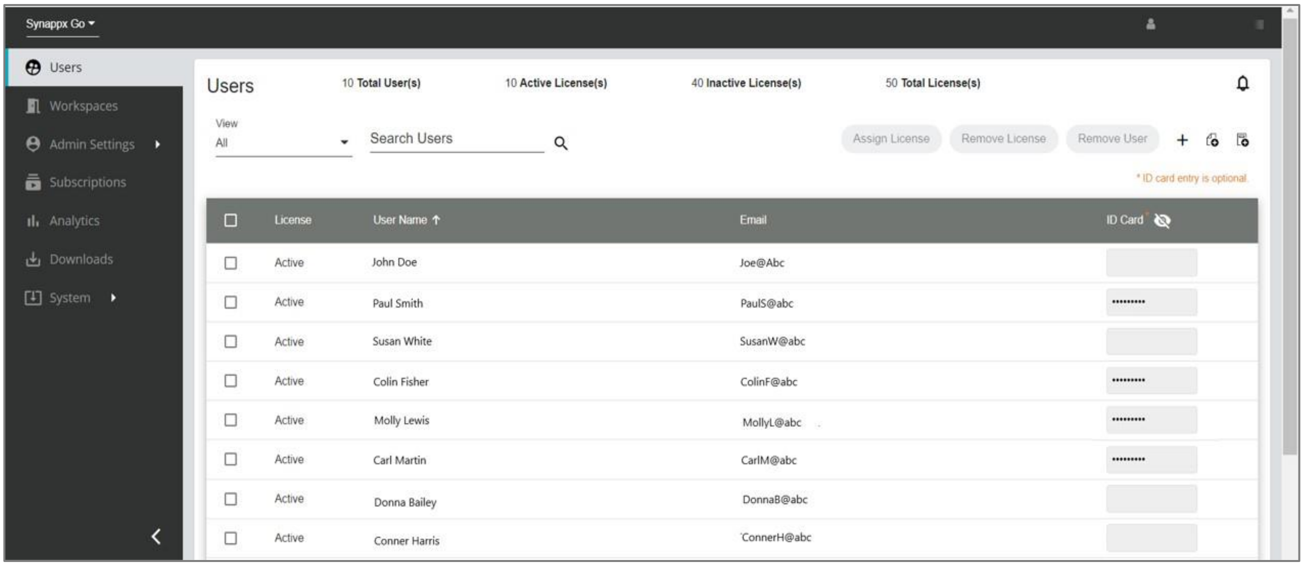
Android Synappx Go Mobile App

Synappx Go MFP Scan/Print Release and Share to Display features via Google Android app

Links to download Synappx Go mobile apps from the App Store or Google Play

Select to download Agent for installation on PC/server

The **Synappx Go Admin Portal** homepage will appear.



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

View: All

* ID card entry is optional

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

Step 2: Configure and Download Agents

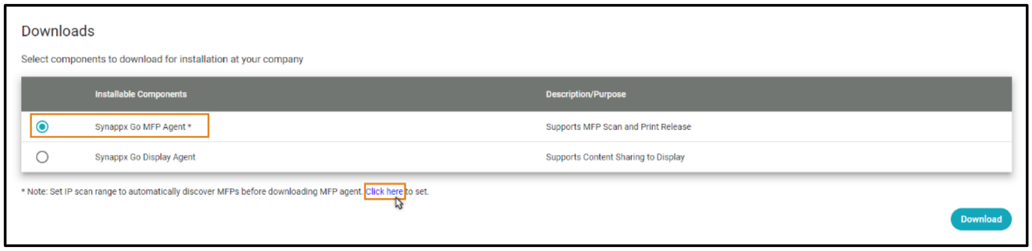
The **Downloads** page contains the MFP and display agent links. The MFP agent enables mobile scan, print and copy features. An internet protocol (IP) address range is necessary to collect information about Sharp MFPs. The display agent allows users to share content to enabled interactive or display boards; there is no action prior to downloading the display agent.

1. From the Synappx Go Admin Portal, select **Downloads**.

MFP Agent

Note: Be sure to allow pop-ups on your web browser (Google Chrome or Microsoft Edge) prior to downloading the agent.

1. Select **Synappx Go MFP Agent.** Then select the **Click here** link.



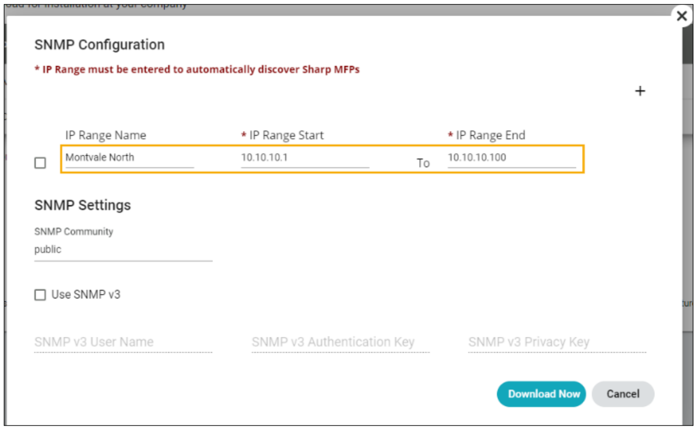
Downloads

Select components to download for installation at your company

	Installable Components	Description/Purpose
●	Synappx Go MFP Agent *	Supports MFP Scan and Print Release
○	Synappx Go Display Agent	Supports Content Sharing to Display

* Note: Set IP scan range to automatically discover MFPs before downloading MFP agent. Click here to set.

2. In the **SNMP Configuration window**, enter the **IP Range Name**. Then enter a start and end address. If this is the only IP Range, ensure the check box is selected and select **Download Now**. If this is not the only address range, select **(+)** to add another range (up to 15) and complete the same parameters. When all IP range names are entered, check all boxes and select **Download Now**.



SNMP Configuration

* IP Range must be entered to automatically discover Sharp MFPs

	IP Range Name	* IP Range Start		* IP Range End
□	Montvale North	10.10.10.1	To	10.10.10.100

SNMP Settings

SNMP Community: public

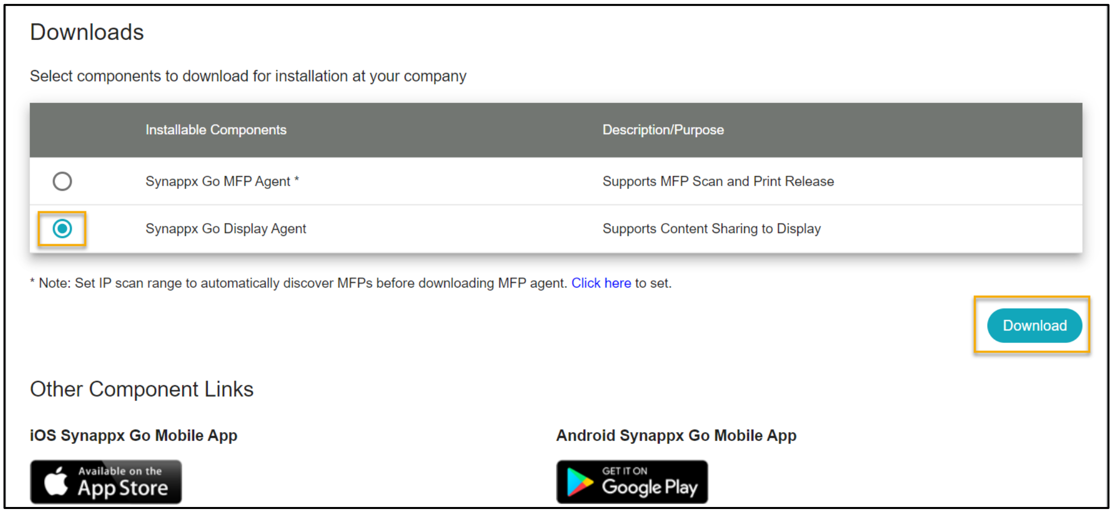
□ Use SNMP v3

Display Agent

Note: Be sure to allow pop-ups on your web browser (Google Chrome or Microsoft Edge) prior to downloading the agent.

1. Select **Synappx Go Display Agent**. There is no configuration prior to downloading.

2. Select **Download** to download the display agent software to the admin PC or target PC/server.



Downloads

Select components to download for installation at your company

	Installable Components	Description/Purpose
○	Synappx Go MFP Agent *	Supports MFP Scan and Print Release
●	Synappx Go Display Agent	Supports Content Sharing to Display

* Note: Set IP scan range to automatically discover MFPs before downloading MFP agent. Click here to set.

Other Component Links

iOS Synappx Go Mobile App

Android Synappx Go Mobile App

Information about the Synappx Go mobile app (iOS and Android devices supported) is also available on the Downloads page.

Step 3: Install Agents

MFP Agent

The Synappx Go MFP agent creates a secure connection to the Synappx Go cloud, discovers and maintains a list of MFPs, and manages scanning, printing, and copying in Synappx Go. A single MFP agent can manage anywhere from 50 to 100 MFPs in an organization, depending on the environment. Here is an overview of the MFP agent installation and configuration:

- MFP agent installation starts on the PC/server. Ensure the prerequisites are met.
  - .NET 4.7.2 is required. If not already installed, a prompt will appear to download it during the agent installation. Allow the download.
- MFP self-registers to the Synappx Go cloud using X.509 certificates.
- MFP discovery is automatically completed for the assigned IP address range(s).
- MFP agent and discovered MFPs are automatically visible on the Synappx Go Admin Portal.
- Although the Synappx Go agent application is code-signed to assure integrity and authenticity of the software, some anti-virus systems may require registration or configuration.

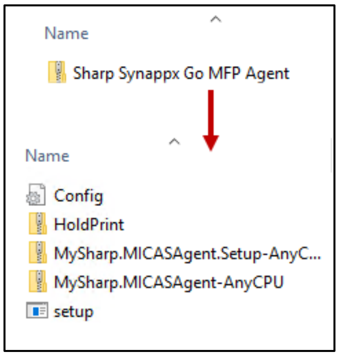
Notes:

- Prior to installing the agent, an administrator must set the Simple Network Management Protocol (SNMP) discovery range(s) and download the MFP agent from the Admin Portal.
- If MICAS℠ v4.8.1.121 or later is already installed, you can install the Synappx Go MFP agent on the same PC or server as long as MICAS is a minimum supported version and it has been registered. Synappx Go cannot coexist and operate on the same PC or server if MICAS is installed and registered after the Synappx Go agent is installed.
- Special characters in the PC name may prevent agent registration from completing. Avoid special characters in the PC name where agent is to be installed.
- If print jobs are not received by the MFP agent PC, it may be necessary to open either or both inbound Transmission Control Protocol (TCP) port(s) 9100 and 515 on the MFP agent server by creating rules on the machine's Windows firewall. See the Appendix for a description of the procedure that uses Windows 10 as an example.
  - From Version 2.0 agents onward, the inbound firewall will be opened automatically on the Synappx PC/server.
- The Synappx Go MFP agent runs background services to enable scan, print, and copy operations. Therefore, the agent PC or server must not be set for sleep mode since agents cannot operate on a computer in a sleep state.
- Synappx Go MFP agents use port 8080 for local communications. Ensure no other application on the agent PC/server is using port 8080.

Installing the MFP Agent

1. Copy the **Sharp Synappx Go MFP Agent.zip** file (downloaded in the previous step) and paste to a directory on the target PC or server.

2. Unzip the file in the PC/server location. The package will include the files shown below.



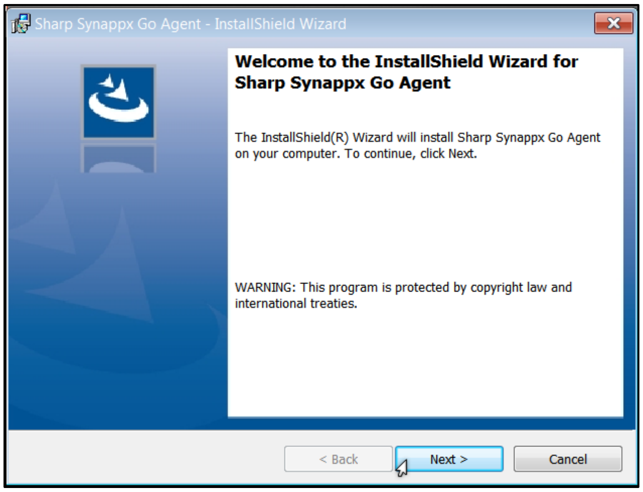
Name

Sharp Synappx Go MFP Agent

Name

Config
HoldPrint
MySharp.MICASAgent.Setup-AnyC...
MySharp.MICASAgent-AnyCPU
setup

3. Double-click **setup** (setup.exe) to execute the installation.
4. When the **InstallShield Wizard** pops up, select **Next.**



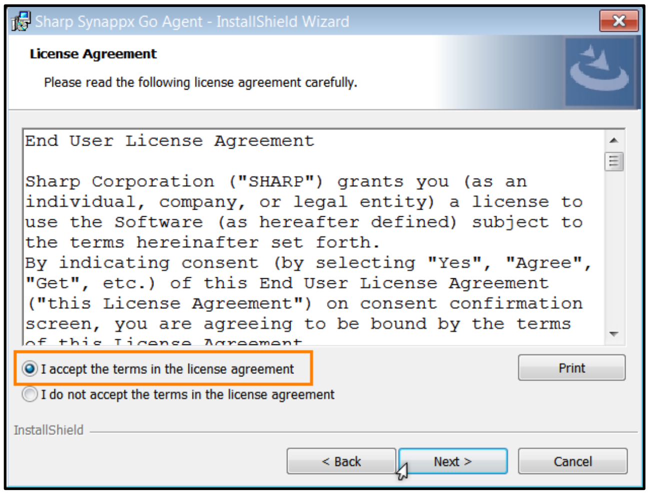
Sharp Synappx Go Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Sharp Synappx Go Agent

The InstallShield(R) Wizard will install Sharp Synappx Go Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. Read the **End User License Agreement (EULA)** and select **I accept the terms in the license agreement**. If desired, print a copy of the EULA. Then select **Next**.



Sharp Synappx Go Agent - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

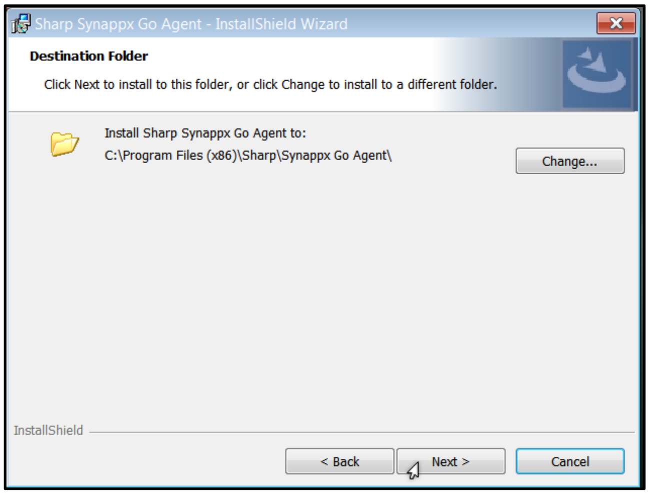
```
End User License Agreement

Sharp Corporation ("SHARP") grants you (as an
individual, company, or legal entity) a license to
use the Software (as hereafter defined) subject to
the terms hereinafter set forth.
By indicating consent (by selecting "Yes", "Agree",
"Get", etc.) of this End User License Agreement
("this License Agreement") on consent confirmation
screen, you are agreeing to be bound by the terms
of this License Agreement
```

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6. The **Destination Folder** screen will appear. This screen describes the default target directory for installation. In most instances, the default location is the preferred location. To override the default, select **Change** and select the desired folder. Then select **Next**. To use the default location, select **Next**.



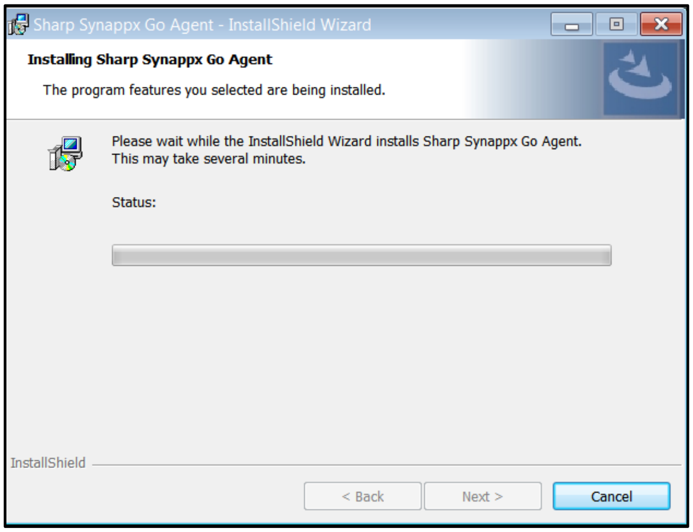
Sharp Synappx Go Agent - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Sharp Synappx Go Agent to:
C:\Program Files (x86)\Sharp\Synappx Go Agent\

7. The installation process will begin; it could take up to several minutes to complete. When the **InstallShield Wizard Completed** screen appears, select **Finish** to complete the installation.



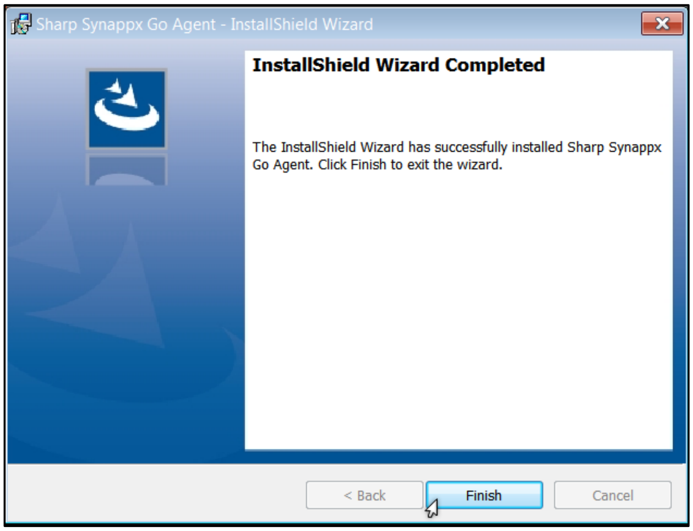
Sharp Synappx Go Agent - InstallShield Wizard

Installing Sharp Synappx Go Agent

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Sharp Synappx Go Agent. This may take several minutes.

Status:



Sharp Synappx Go Agent - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Sharp Synappx Go Agent. Click Finish to exit the wizard.

The Synappx Go MFP agent will automatically connect to the Synappx Go cloud (hosted on Microsoft Azure) and complete the agent provisioning, including use of X.509 certificates. Then, it will automatically discover all Sharp MFPs within the previously specified IP range. Synappx Go is now ready for assigning workspaces.

Display Agent

The Synappx Go display agent creates a secure connection to the Synappx Go cloud and manages document sharing to displays. A display agent must be installed on the PC of every display that will be used with Synappx Go. Here is an overview of the display agent installation and configuration:

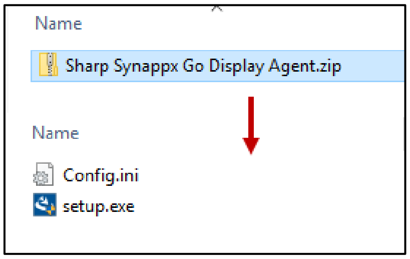
- The display agent installation starts on a PC (see steps below). Before installation, ensure the prerequisites are met.
    - .NET 4.7.2 is required. If not already installed, a prompt will appear to download it during the agent installation. Allow the download.
- The display agent cannot be loaded on the same PC or server as the MFP agent.
- The display device self-registers to the Synappx Go cloud using X.509 certificates.
- The display agent is automatically visible on the Synappx Go Admin Portal.

Notes:

- Prior to installing the agent, an administrator must download the display agent from the Admin Portal to a separate PC. For convenience, you can download the display agent from the Admin Portal once and copy the zip file to any other display computers that will be configured to support Synappx Go. Then, run the setup on each computer, and each will be configured and displayed automatically on the Admin Portal.
- Special characters in the PC name may prevent agent registration from completing. Avoid special characters in the PC name where agent is to be installed.

Installing the Display Agent: Step by Step

1. Copy the **Sharp Synappx Go Display Agent.zip** file to a directory on the target display PC or server and unzip it. The package will include the files shown below:



Name

Sharp Synappx Go Display Agent.zip

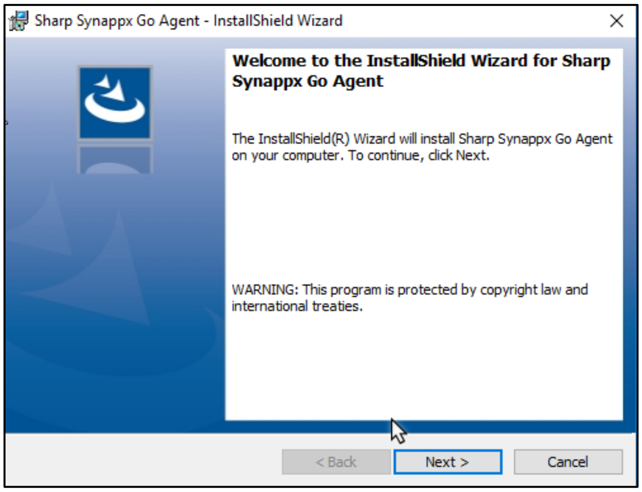
Name

Config.ini

setup.exe

2. Double click **setup.exe**.

3. When the **InstallShield Wizard** pops up, select **Next**.



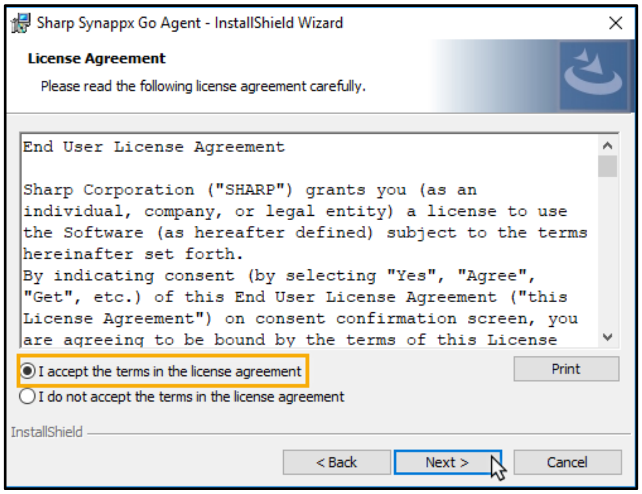
Sharp Synappx Go Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Sharp Synappx Go Agent

The InstallShield(R) Wizard will install Sharp Synappx Go Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. Read the End User License Agreement (EULA) and select **I accept the terms in the license agreement**. If desired, print a copy of the EULA. Then select **Next**.



Sharp Synappx Go Agent - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

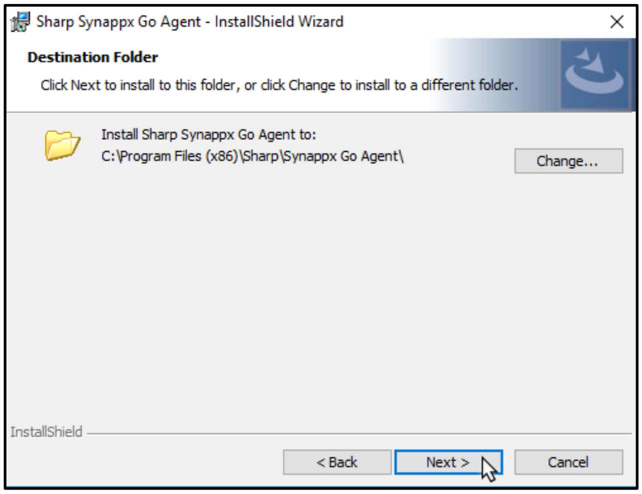
```
End User License Agreement

Sharp Corporation ("SHARP") grants you (as an
individual, company, or legal entity) a license to use
the Software (as hereafter defined) subject to the terms
hereinafter set forth.
By indicating consent (by selecting "Yes", "Agree",
"Get", etc.) of this End User License Agreement ("this
License Agreement") on consent confirmation screen, you
are agreeing to be bound by the terms of this License
```

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

5. The **Destination Folder** screen will appear. This screen describes the default target directory for installation. In most instances, the default location is the preferred



Sharp Synappx Go Agent - InstallShield Wizard

Destination Folder

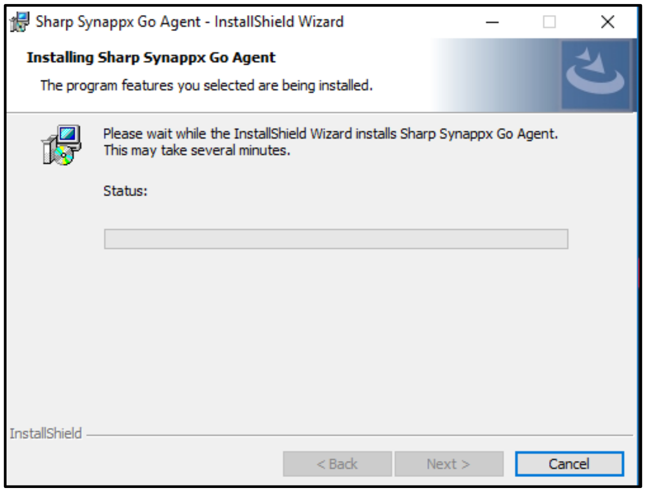
Click Next to install to this folder, or click Change to install to a different folder.

Install Sharp Synappx Go Agent to:
C:\Program Files (x86)\Sharp\Synappx Go Agent\

location. To override the default, select **Change** and select the desired folder. Then select **Next**. To use the default location, select **Next**.

6. The installation process will begin; it could take up to several minutes to com7. 7.
7. When the InstallShield Wizard Completed screen appears, select **Finish**.

The Synappx Go display agent will automatically connect to the Synappx Go cloud hosted on Microsoft Azure and complete the agent provisioning, including the use of X.509 certificates. The display is now ready to be assigned to a workspace on the Admin Portal.



Sharp Synappx Go Agent - InstallShield Wizard

Installing Sharp Synappx Go Agent

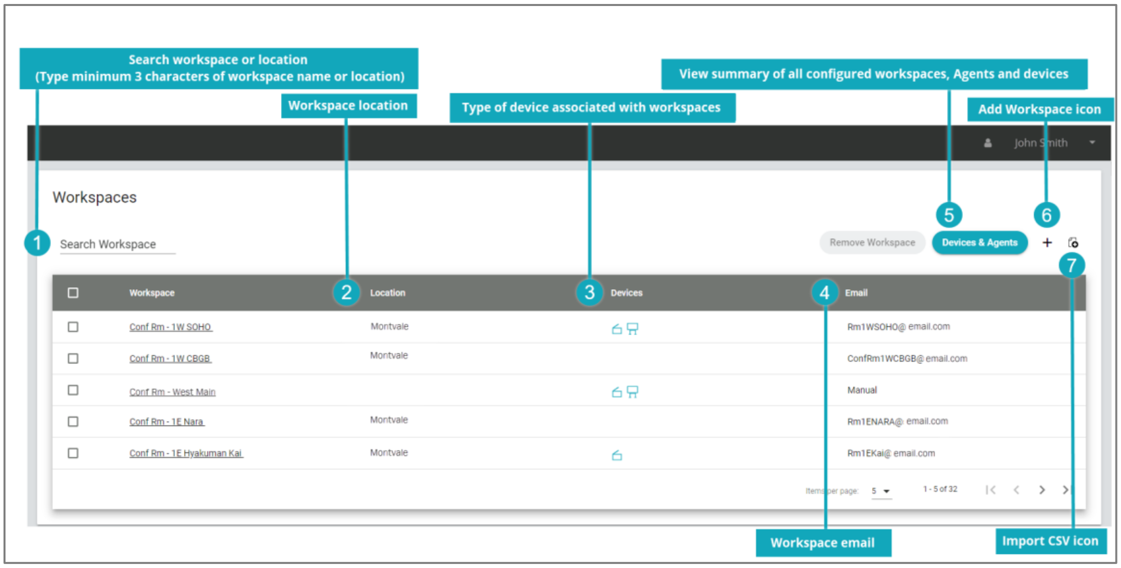
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Sharp Synappx Go Agent. This may take several minutes.

Status:

Step 4: Add Workspaces

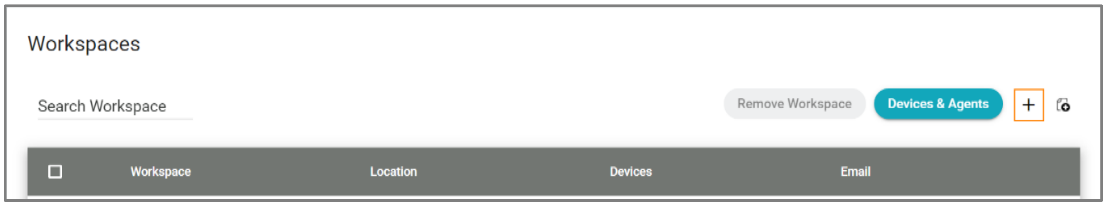
Workspaces can be meeting rooms, huddle rooms, individual offices, or common areas where MFPs or displays are located—wherever collaboration happens. Create or import workspaces from Microsoft 365 or Google Workspace on the Synappx Go Admin Portal **Workspaces** page.


Search workspace or location
(Type minimum 3 characters of workspace name or location)
Workspace location
Type of device associated with workspaces
View summary of all configured workspaces, Agents and devices
Add Workspace icon
John Smith
Workspaces
1
Search Workspace
Remove Workspace
5
Devices & Agents
6
+
7
2
3
4
Workspace email
Import CSV icon

□	Workspace	Location	Devices	Email
□	Conf Rm - 1W SOHO	Montvale	🖨 🖥	Rm1WSOHO@ email.com
□	Conf Rm - 1W CBGB	Montvale		ConfRm1WCBGB@ email.com
□	Conf Rm - West Main		🖨 🖥	Manual
□	Conf Rm - 1E Nara	Montvale		Rm1ENARA@ email.com
□	Conf Rm - 1E Hyakuman Kai	Montvale	🖨	Rm1EKai@ email.com

Items per page: 5 1 - 5 of 32

To add a workspace from your directory, select **(+)**.



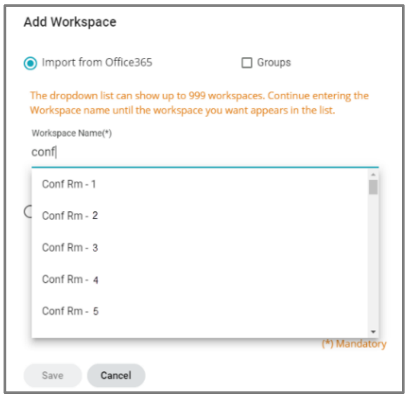
From the **Add Workspace** window, you can import workspaces from Microsoft 365 or Google Workspace or add workspaces manually.

Import Workspaces

Image shows Microsoft 365 as an example.

Note: Characters may be case sensitive.

1. Type a few characters in the **Workspace Name** box. Microsoft 365 or Google workspaces will appear. Select the workspace(s) to import. When finished, select **Save**.



Add Workspace

● Import from Office365 □ Groups

The dropdown list can show up to 999 workspaces. Continue entering the Workspace name until the workspace you want appears in the list.

Workspace Name(*)
conf

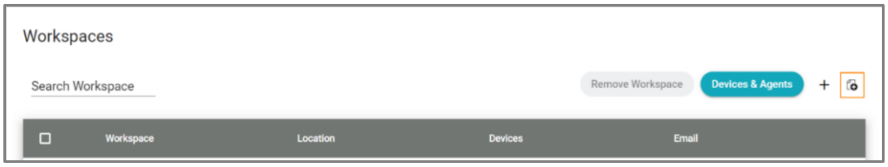
- Conf Rm - 1
- Conf Rm - 2
- Conf Rm - 3
- Conf Rm - 4
- Conf Rm - 5

(*) Mandatory

2. To add workspace groups, first check the **Groups** box. Then follow step 1.

Import Workspaces via CSV File

1. Select the **Import Multiple Workspaces** icon.

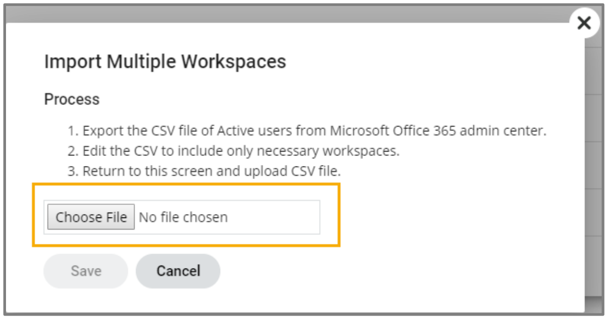


Workspaces

Search Workspace

□	Workspace	Location	Devices	Email

2. Follow the three-step process stated in the **Import of Multiple Workspaces** window. The CSV file has a maximum of 50 workspaces and 500KB.



Import Multiple Workspaces

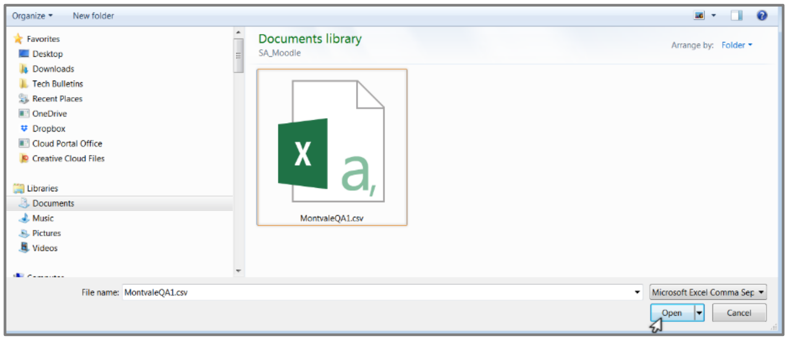
Process

1. Export the CSV file of Active users from Microsoft Office 365 admin center.
2. Edit the CSV to include only necessary workspaces.
3. Return to this screen and upload CSV file.

Choose File No file chosen

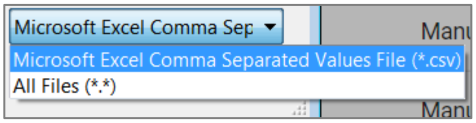
3. Select **Choose File**.

4. Choose your file and select **Open**. The selected .csv file must be a Microsoft Excel Comma Separated Values File.



File name: MontvaleQA1.csv

Microsoft Excel Comma Sep

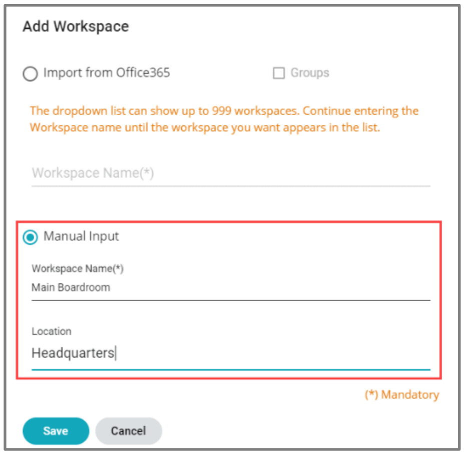

Microsoft Excel Comma Sep
Microsoft Excel Comma Separated Values File (*.csv)
All Files (*.*)
Manu
Manu

5. The file will attach in the **Import Multiple Workspaces** window. Select **Save**.

Manual Input

Image shows Microsoft 365 as an example.

1. Select **Manual Input**.



The dropdown list can show up to 999 workspaces. Continue entering the Workspace name until the workspace you want appears in the list.

● Manual Input

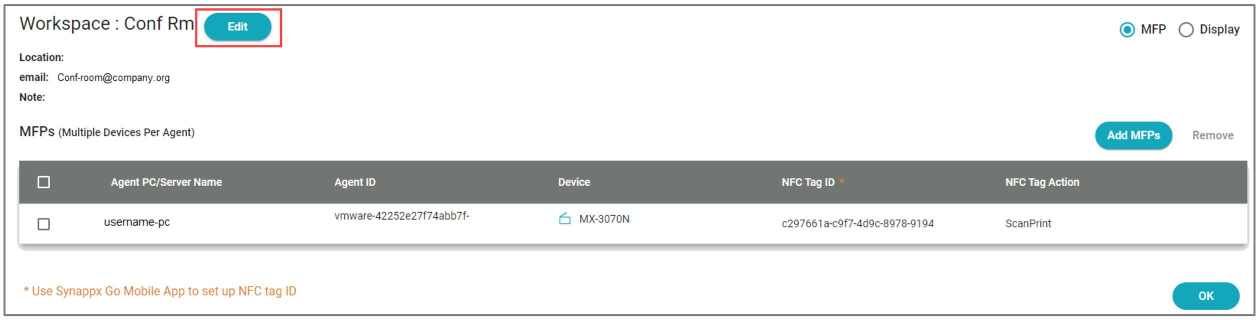
Workspace Name(*)
Main Boardroom

Location
Headquarters

2. Type the workspace name in the respective field. Type a location if desired.
3. Select **Save**.
4. Repeat to add more workspaces.

Edit Workspace Name (Optional)

1. Select the workspace.
2. Select **Edit**.



Workspace : Conf Rm Edit

● MFP ○ Display

Location:

email: Conf-room@company.org

Note:

MFPs (Multiple Devices Per Agent)

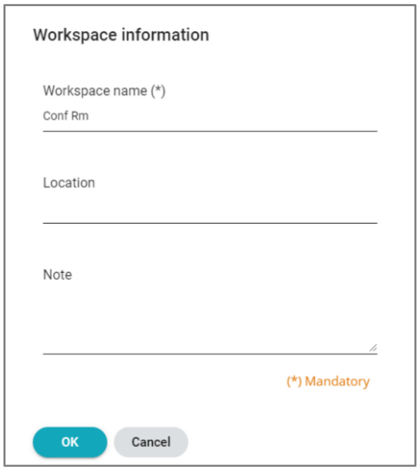
Add MFPs Remove

□	Agent PC/Server Name	Agent ID	Device	NFC Tag ID *	NFC Tag Action
□	username-pc	vmware-42252e27f74abb7f-	MX-3070N	c297661a-c9f7-4d9c-8978-9194	ScanPrint

* Use Synappx Go Mobile App to set up NFC tag ID

OK

3. The **Workspace information** box will pop up for editing.



Workspace information

Workspace name (*)
Conf Rm

Location

Note

(*) Mandatory

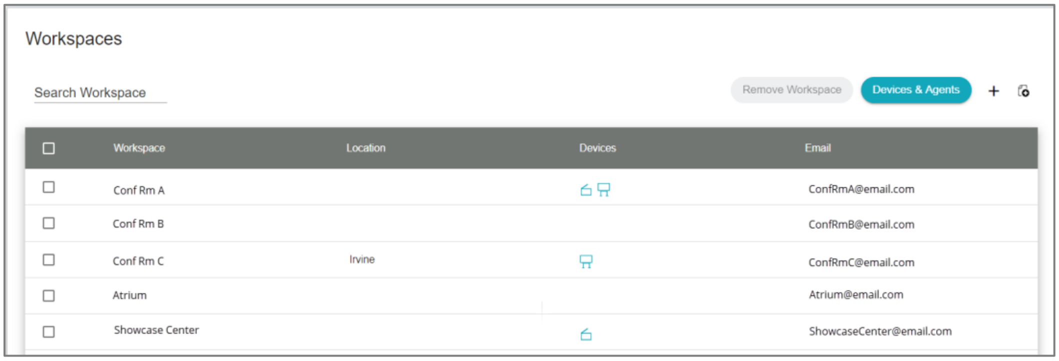
OK Cancel

4. Select **OK** when finished.

Step 5: Associate Devices to Workspaces

Associate MFPs to Workspaces

1. Start by selecting a workspace from the list**.**



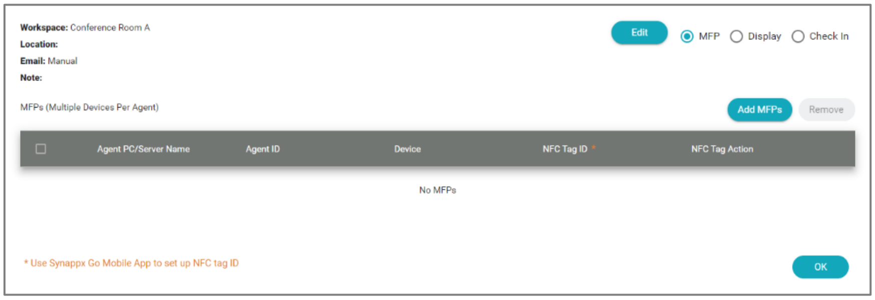
Workspaces

Search Workspace

Remove Workspace | Devices & Agents | +

□	Workspace	Location	Devices	Email
□	Conf Rm A		🖨 🖥	ConfRmA@email.com
□	Conf Rm B			ConfRmB@email.com
□	Conf Rm C	Irvine	🖥	ConfRmC@email.com
□	Atrium			Atrium@email.com
□	Showcase Center		🖨	ShowcaseCenter@email.com

2. The **Workspace Configuration** window will appear. Select **Add MFPs**.



Workspace: Conference Room A
Location:
Email: Manual
Note:

Edit ● MFP ○ Display ○ Check In

MFPs (Multiple Devices Per Agent)

Add MFPs | Remove

□	Agent PC/Server Name	Agent ID	Device	NFC Tag ID *	NFC Tag Action

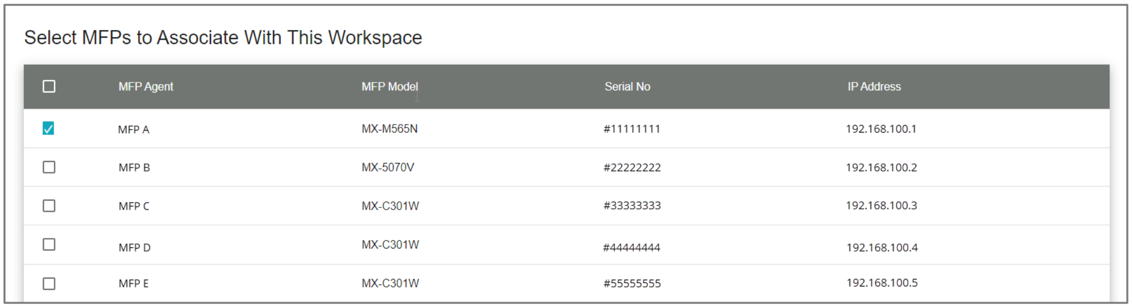
No MFPs

* Use Synappx Go Mobile App to set up NFC tag ID

OK

Note: An MFP can only be assigned to one workspace at a time (i.e., it will not show in the available MFP list after being assigned until removed from the other workspace). If a MFP is not discovered by a subsequent agent (with an overlapping IP address range), check to see if the MFP is already associated with another agent. This overlap information will also be found in the System Log. If necessary, you can delete the MFP from the first agent and rediscover it with the second agent.

3. Select the desired MFP model(s) to assign and select **OK.**



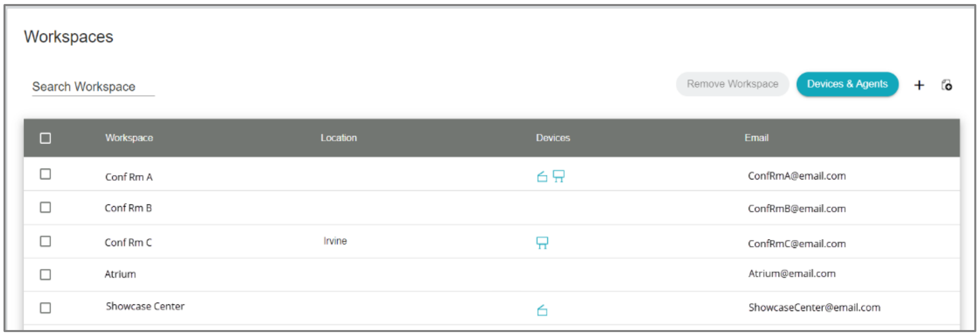
Select MFPs to Associate With This Workspace

□	MFP Agent	MFP Model	Serial No	IP Address
☑	MFP A	MX-M565N	#11111111	192.168.100.1
□	MFP B	MX-5070V	#22222222	192.168.100.2
□	MFP C	MX-C301W	#33333333	192.168.100.3
□	MFP D	MX-C301W	#44444444	192.168.100.4
□	MFP E	MX-C301W	#55555555	192.168.100.5

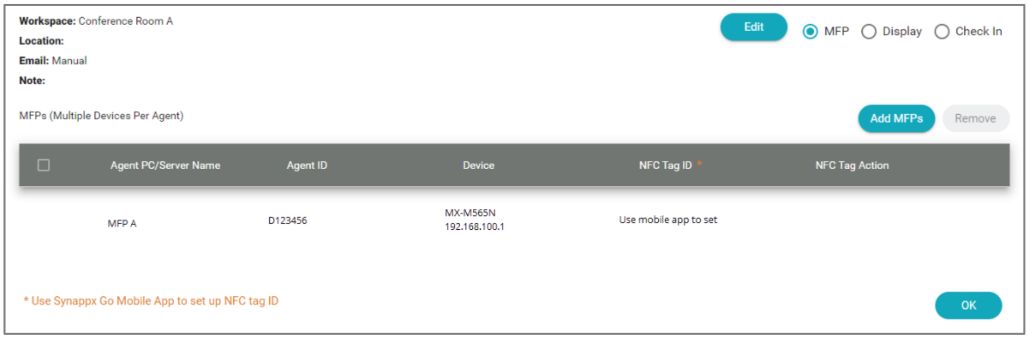
4. Your workspace will now list the associated MFP(s) under the **Device** column. A reminder to set up the NFC tag will appear. Select **OK**.

Associate Display to a Workspace

1. Start by selecting workspaces from the list**.**



□	Workspace	Location	Devices	Email
□	Conf Rm A		🖨 🖥	ConfRmA@email.com
□	Conf Rm B			ConfRmB@email.com
□	Conf Rm C	Irvine	🖥	ConfRmC@email.com
□	Atrium			Atrium@email.com
□	Showcase Center		🖨	ShowcaseCenter@email.com



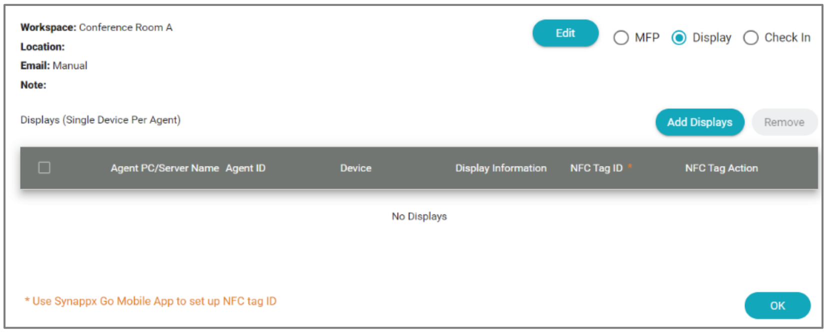
Workspace: Conference Room A
Location:
Email: Manual
Note:

MFPs (Multiple Devices Per Agent)

□	Agent PC/Server Name	Agent ID	Device	NFC Tag ID *	NFC Tag Action
	MFP A	D123456	MX-M565N 192.168.100.1	Use mobile app to set	

* Use Synappx Go Mobile App to set up NFC tag ID

2. The **Workspace Configuration** window will appear. Select **Add Displays**.



Workspace: Conference Room A
Location:
Email: Manual
Note:

Displays (Single Device Per Agent)

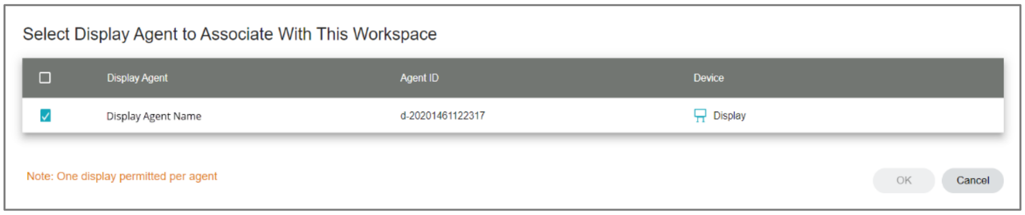
□	Agent PC/Server Name	Agent ID	Device	Display Information	NFC Tag ID *	NFC Tag Action

No Displays

* Use Synappx Go Mobile App to set up NFC tag ID

Note: A display can only be assigned to one workspace at a time (i.e., it will not show in the available display list after being assigned until removed from the other workspace).

3. Select the desired displays to assign and select **OK.**

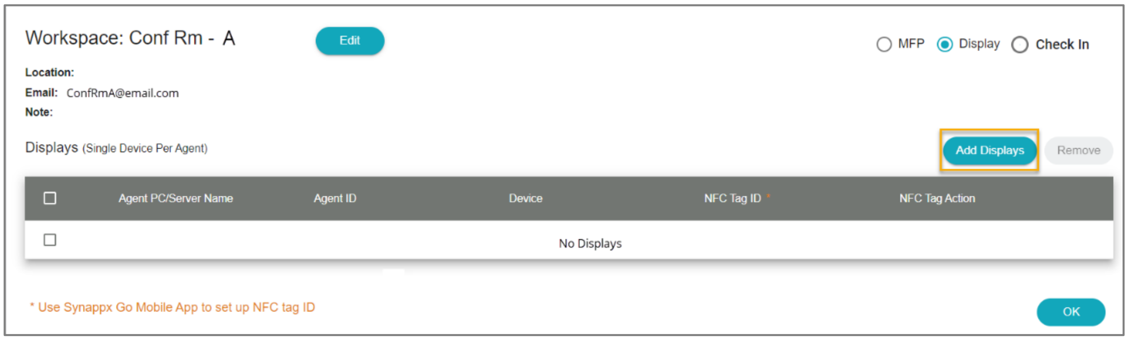


Select Display Agent to Associate With This Workspace

□	Display Agent	Agent ID	Device
☑	Display Agent Name	d-20201461122317	🖥 Display

Note: One display permitted per agent

4. Your workspace will now list the associated display agent under the **Device** column. A reminder to set up the NFC tag will appear. Select **OK**.



Workspace: Conf Rm - A

Location:
Email: ConfRmA@email.com
Note:

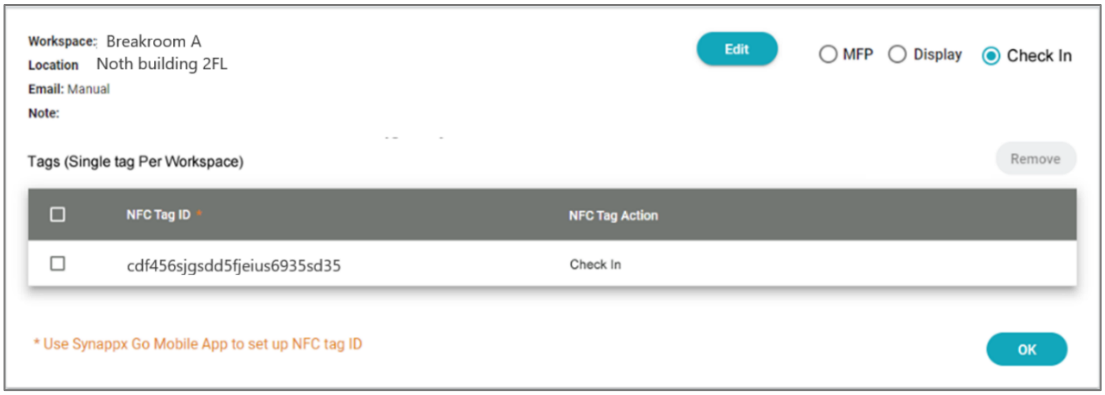
Displays (Single Device Per Agent)

□	Agent PC/Server Name	Agent ID	Device	NFC Tag ID *	NFC Tag Action
□			No Displays		

* Use Synappx Go Mobile App to set up NFC tag ID

Workspace Check In

An NFC tag can be configured for each workspace to capture check-ins. Users tap the tag to indicate their location. Selecting the **Check In** button on the workspace page displays the check-in tag information. See [Associate NFC Tags](#) for more information.



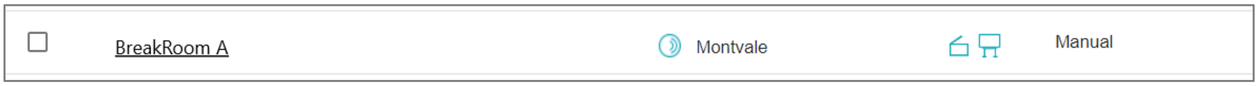
Workspace: Breakroom A
Location Noth building 2FL
Email: Manual
Note:

Tags (Single tag Per Workspace)

□	NFC Tag ID *	NFC Tag Action
□	cdf456sjgsdd5fjeius6935sd35	Check In

* Use Synappx Go Mobile App to set up NFC tag ID

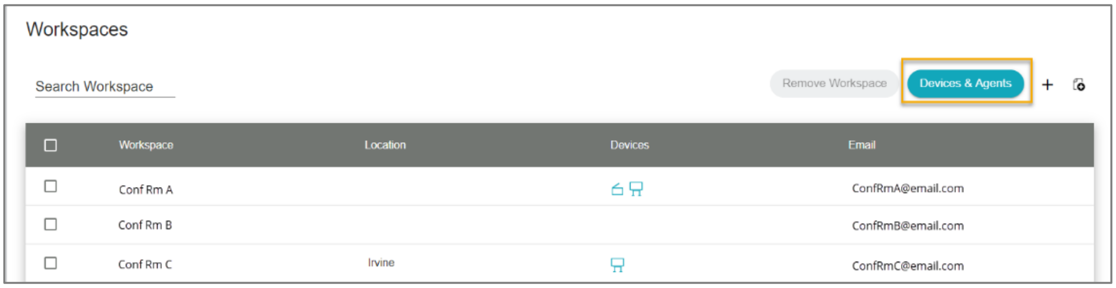
After a check-in tag is configured for a workspace, the check-in icon will display on the **Workspaces** page in the **Location** column.



□	BreakRoom A	Montvale	Manual

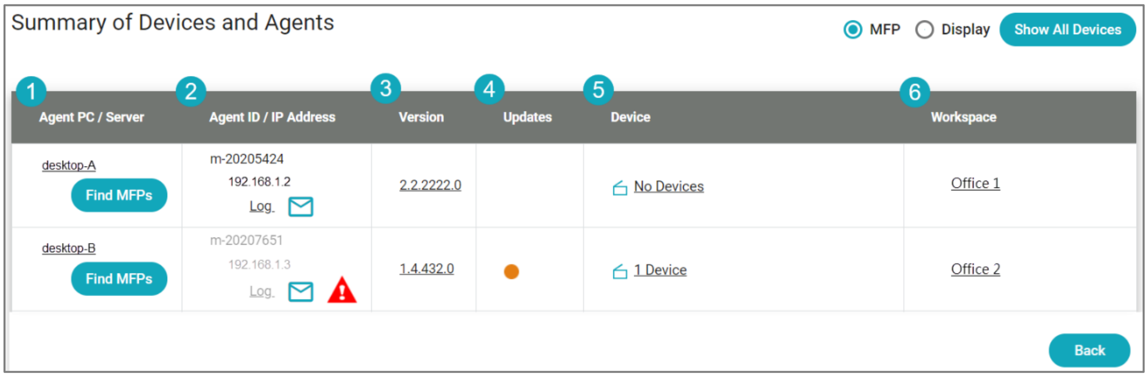
Summary of Devices and Agents—Management

From the **Workspaces** page, select **Devices & Agents** to access the **Summary of Devices and Agents** for ongoing agent management

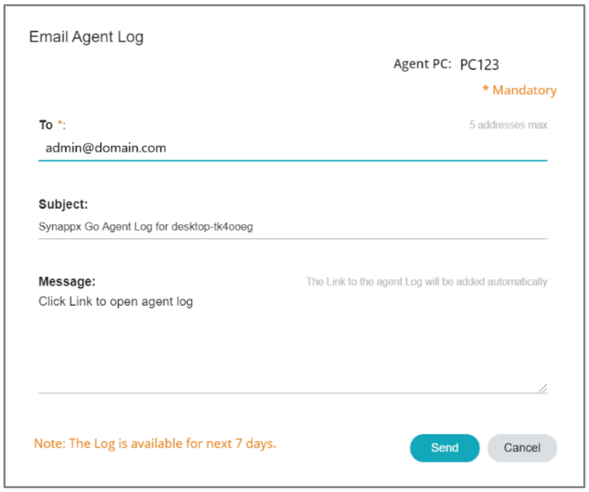


□	Workspace	Location	Devices	Email
□	Conf Rm A			ConfRmA@email.com
□	Conf Rm B			ConfRmB@email.com
□	Conf Rm C	Irvine		ConfRmC@email.com

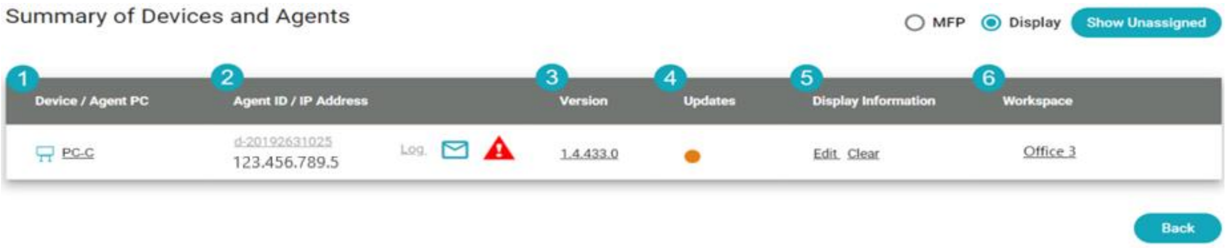
MFP Summary of Devices and Agents



1 Agent PC / Server	2 Agent ID / IP Address	3 Version	4 Updates	5 Device	6 Workspace
desktop-A Find MFPs	m-20205424 192.168.1.2 Log	2.2.2222.0		No Devices	Office 1
desktop-B Find MFPs	m-20207651 192.168.1.3 Log	1.4.432.0	●	1 Device	Office 2

MFP Summary of Devices and Agents		
1	**Agent PC/Server**	- Select the link to remove associated MFPs or the agent. ○ If removing the agent, uninstall it from the PC or server using the normal Windows uninstall procedure to complete removal and avoid reconnection. - Select **Find MFPs** to access **SNMP Configuration** and initiate MFP discovery.
2	**Agent ID/ IP Address**	- Select the **Log** link to view the system log for error or status messages - Each system log entry has an error code (e.g. C102) at the end of the message, which provides more detailed information on the log entry. Contact your Sharp service provider for details. - A gray agent ID indicates the agent has not been used for 14 days or longer. - A red triangle next to the agent ID indicates an agent error (e.g. agent is disconnected) that needs to be addressed. - Select the **envelope icon** ✉ to aquire the agent log files from the agent PC or server and email a link to the files to up to five email addresses. The log file will upload to the Synappx cloud and the link will be added to the email after selecting **Send**. The log link will remain active for seven days.  Email Agent Log Agent PC: PC123 * Mandatory To *: admin@domain.com 5 addresses max Subject: Synappx Go Agent Log for desktop-tk4ooeg Message: Click Link to open agent log The Link to the agent Log will be added automatically Note: The Log is available for next 7 days.
3	**Version**	Select the agent version number to go to **Agent Update** page.
4	**Updates**	- An orange dot indicates a recent agent version that requiring update. - A red dot indicates an outdated agent version requiring update.
5	**Device**	- Select the device view details. - Select **Show All Devices** to view all associated and unassigned MFPs.
6	**Workspace**	Select a workspace to view associated devices.

Display Summary of Devices and Agents

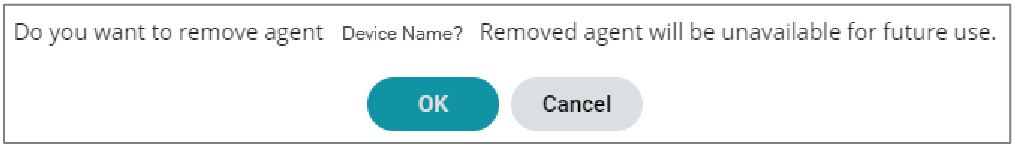


Summary of Devices and Agents

Device / Agent PC	Agent ID / IP Address		Version	Updates	Display Information	Workspace
PC-C	d-20192631025 123.456.789.5	Log	1.4.433.0	●	Edit Clear	Office 3

Remove Display Agent

1. Select the device/agent PC name. A dialog box will confirm agent removal.



Do you want to remove agent Device Name? Removed agent will be unavailable for future use.

2. Select **OK**. The **Summary of Devices and Agents** page will refresh and the agent will be removed.
3. Uninstall the display agent from the PC using the normal Windows uninstall procedure. This completes agent removal and avoids reconnection.

If an agent in the cloud is not removed during uninstallation, there may be more than one agent with that name and IP address in the Admin Portal. If this occurs, manually remove the uninstalled agent from the Admin Portal **Devices and Agents** page.

Display Information Settings (Required for Automatic Input Switching)

To support automatic input switching, each display must be configured on the Display Information page. This is not a required feature but can save users time before sharing files to displays (e.g. users may not know the display PC input or cannot find the remote) and to return the display to a default input. For more information, go to Appendix B: Synappx™ Go Automatic Input Switch.

Step 6: Associate NFC Tags

Once you have assigned MFPs or displays to a workspace, use the Synappx Go app to associate NFC tags with MFPs, displays, check-in locations, and assigned workspaces.

iOS

1. Download Synappx Go from the Apple® App store.

Download on the App Store

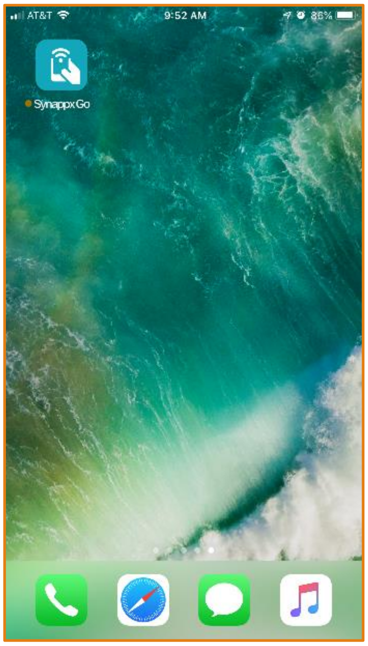
Android

1. Download Synappx Go from the Google Play™ store.

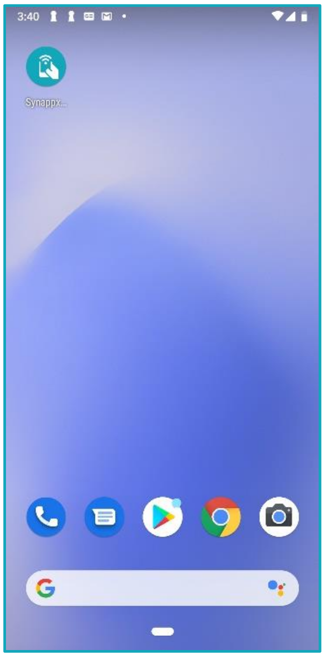
GET IT ON Google Play

Note: The sign-in information only needs to be entered the first time you sign in to the app unless you change your password, log out or do not use the app for 30 days.

2. Open the Synappx Go app. When prompted, enter your Microsoft 365 or Google Workspace credentials and accept the permissions request.

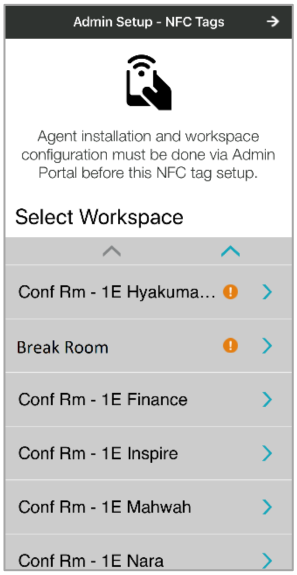


2. Open the Synappx Go app. When prompted, enter your Microsoft 365 or Google Workspace credentials and accept the permissions request.



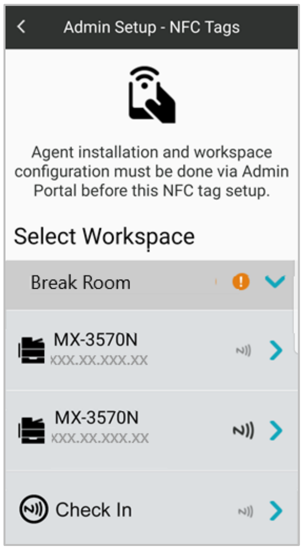
Note: When an MFP or display associated with a workspace needs to be set up, a ❗ will appear. You can sort by workspace name or by workspaces requiring NFC tag setup. Check-in can be configured for any workspace.

3. The **Select Workspace** screen will appear. All configured workspaces will display. Select a workspace.



Agent installation and workspace configuration must be done via Admin Portal before this NFC tag setup.

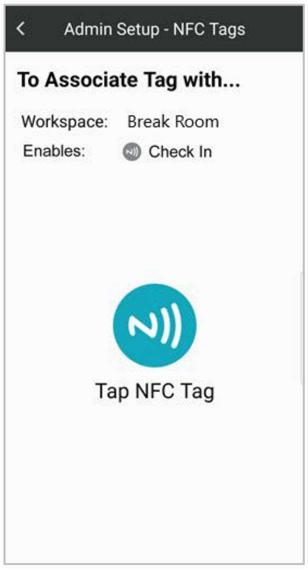
4. A list of devices and a check-in option will appear below the workspace. Select a device or select **Check In**.



Agent installation and workspace configuration must be done via Admin Portal before this NFC tag setup.

Note: A smaller light gray NFC image indicates the device does not yet have an associated NFC tag. A darker gray, larger icon indicates a tag has been associated.

5. Confirm the workspace and device information is correct. Then, tap a new NFC tag to associate the tag with the MFP, display, or check-in location.



Admin Setup - NFC Tags

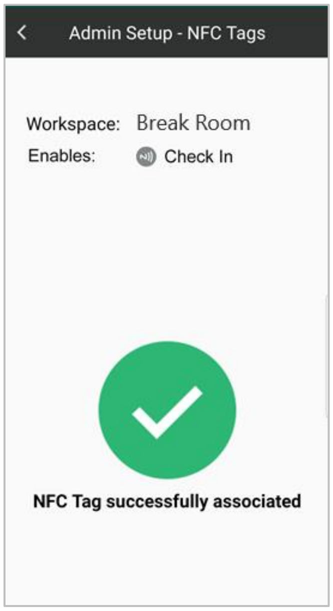
To Associate Tag with...

Workspace: Break Room

Enables: Check In

Tap NFC Tag

6. You will see a notification upon successfully associating the device or check-in tag. Repeat for all other devices and workspaces.



Admin Setup - NFC Tags

Workspace: Break Room

Enables: Check In

NFC Tag successfully associated

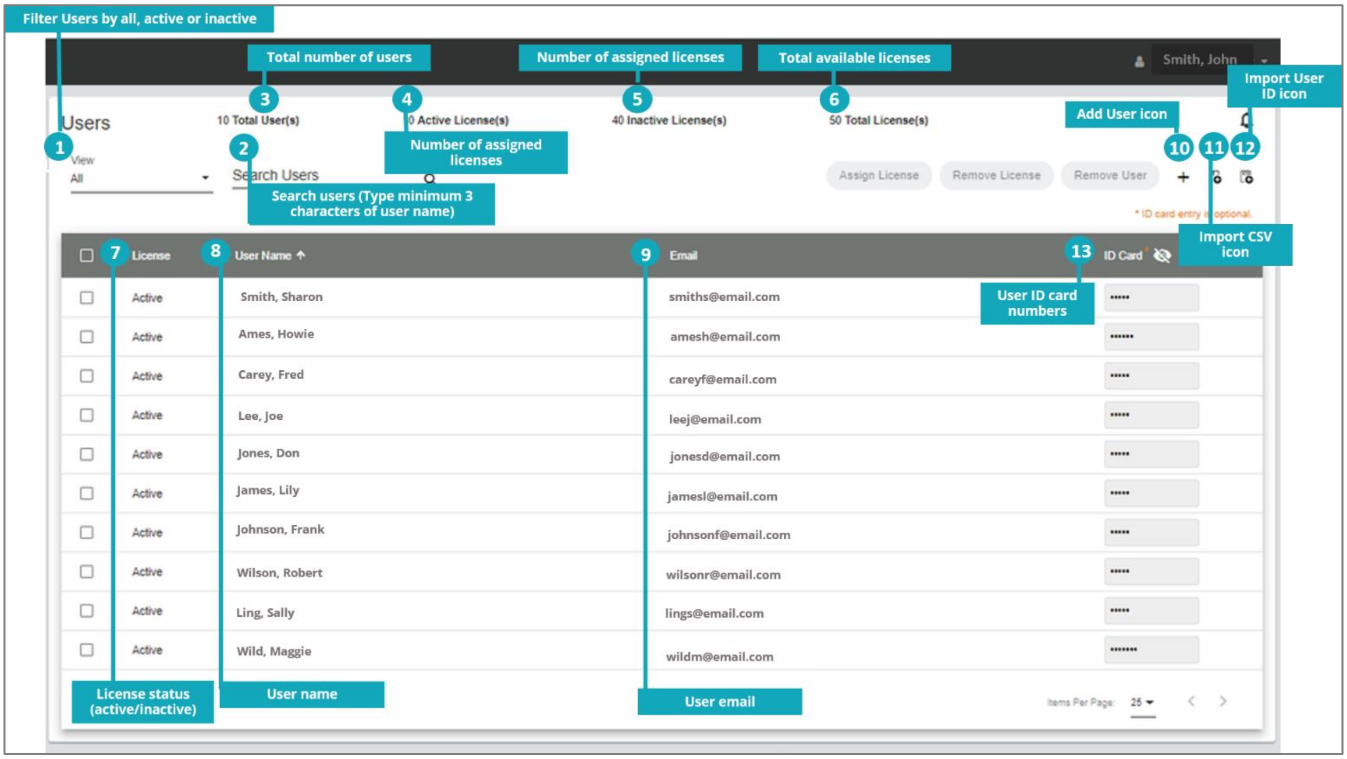
Notes:

- A black dot next to the workspace name on the app indicates a check-in tag has been configured.
- After configuration, the NFC tag ID for each configured device will automatically appear on the Synappx Go Admin Portal workspaces page.

NFC tag settings can be changed on the mobile app by going to **Settings** > **NFC Tag**.

Step 7: Add Users and Allocate Licenses

The Admin Portal users page allows you to manage the users in your organization who access Synappx Go features on the mobile application.



Smith, John

Users

10 Total User(s)   0 Active License(s)   40 Inactive License(s)   50 Total License(s)

View: All

Search Users

Assign License   Remove License   Remove User

* ID card entry is optional.

☐	License	User Name	Email	ID Card
☐	Active	Smith, Sharon	smiths@email.com	•••••
☐	Active	Ames, Howie	amesh@email.com	••••••
☐	Active	Carey, Fred	careyf@email.com	•••••
☐	Active	Lee, Joe	leej@email.com	•••••
☐	Active	Jones, Don	jonesd@email.com	•••••
☐	Active	James, Lily	jamesl@email.com	•••••
☐	Active	Johnson, Frank	johnsonf@email.com	•••••
☐	Active	Wilson, Robert	wilsonr@email.com	•••••
☐	Active	Ling, Sally	lings@email.com	•••••
☐	Active	Wild, Maggie	wildm@email.com	•••••••

Items Per Page: 25

Filter Users by all, active or inactive
Total number of users
Number of assigned licenses
Total available licenses
Import User ID icon
Add User icon
Number of assigned licenses
Search users (Type minimum 3 characters of user name)
Import CSV icon
User ID card numbers
License status (active/inactive)
User name
User email
1
2
3
4
5
6
7
8
9
10
11
12
13

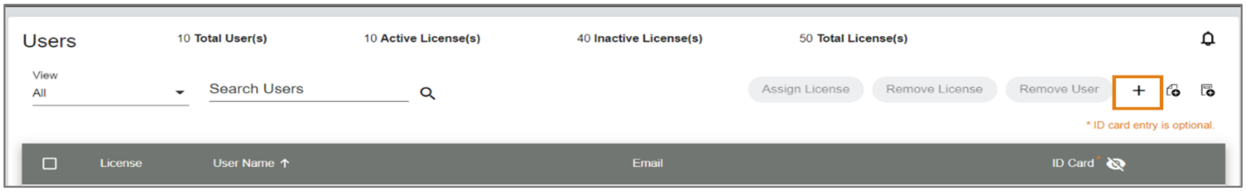
- Assign and remove licenses to and from users on this page.
- Guest users (who are frequently at your company) can also be invited to be Synappx guest users
- Add administrators from the **Admin Settings** page (optional during initial setup but recommended).
- Optional: Add user ID card numbers if MFPs are “locked” by PaperCut MF or Native Authentication

Synappx admins can add any user within Azure AD or Google Workspace (if the Google Workspace account permits). If there are multiple Synappx tenants within the same Azure AD, each domain can only be associated with one account at a time.

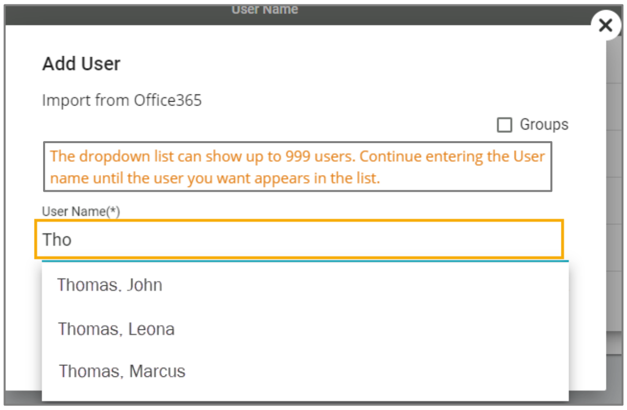
Add Users

Images show Microsoft 365 as an example.

1. Go to the **Users** page and select **(+)**.



2. Type a few characters in the **User Name** field. Microsoft 365 or Google Workspace users will populate. Select from the list shown. Then select **Save**.



The dropdown list can show up to 999 users. Continue entering the User name until the user you want appears in the list.

User Name(*)

Tho

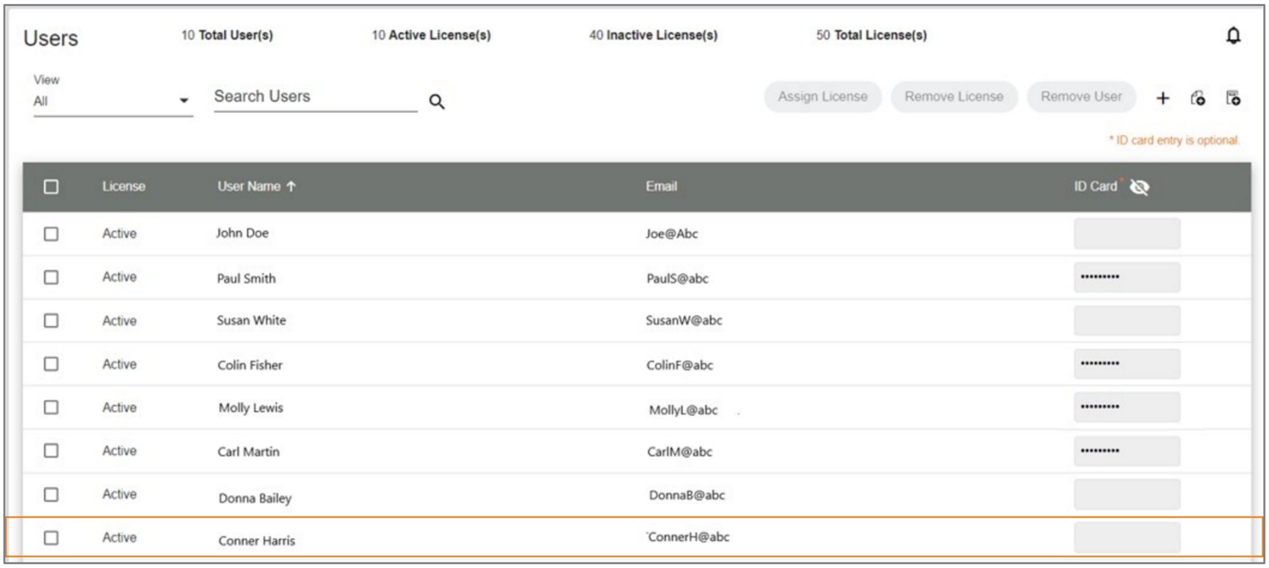
Thomas, John

Thomas, Leona

Thomas, Marcus

3. Groups of users may be added using the same procedure by first checking the **Groups** box. Repeat until all desired users are added. Users appear as inactive on the **Users** page

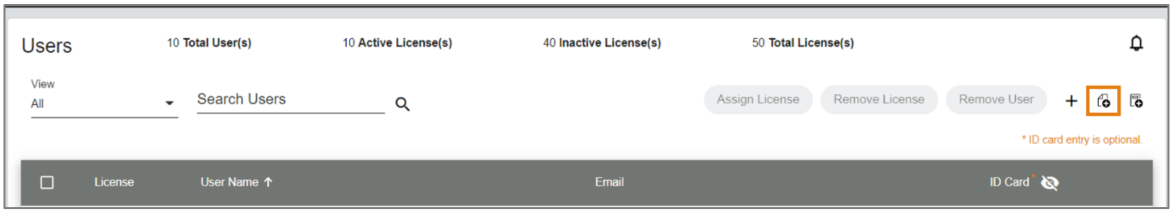
Images show Microsoft 365 as an example.



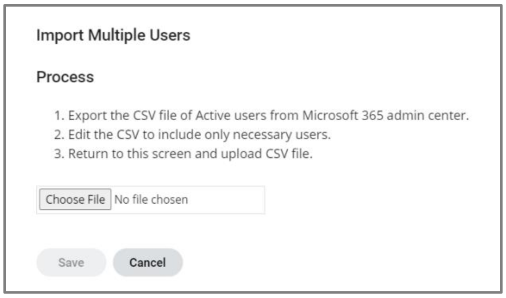
□	License	User Name ↑	Email	ID Card
□	Active	John Doe	Joe@Abc	
□	Active	Paul Smith	PaulS@abc	•••••••••
□	Active	Susan White	SusanW@abc	
□	Active	Colin Fisher	ColinF@abc	•••••••••
□	Active	Molly Lewis	MollyL@abc	•••••••••
□	Active	Carl Martin	CarlM@abc	•••••••••
□	Active	Donna Bailey	DonnaB@abc	
□	Active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

Import Users via CSV File

1. Select the **Add Multi-Users** icon.



2. The **Import of Multi-Users** window will appear. Follow the **Process** guidelines. The file has a maximum of 50 users and 500KB.

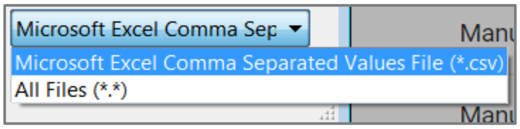


Import Multiple Users

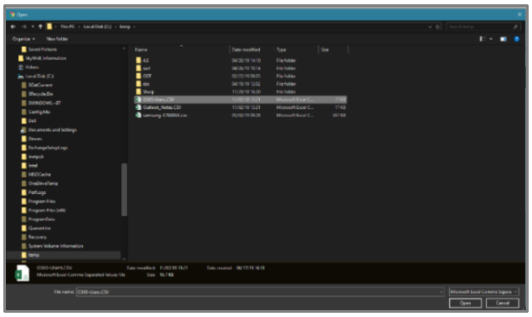
Process

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.

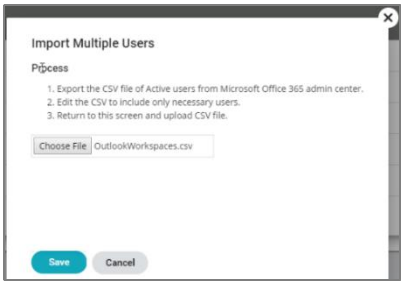
Note: The selected file must be a **Microsoft Excel Comma Separated Values File**.


Microsoft Excel Comma Sep
Microsoft Excel Comma Separated Values File (*.csv)
All Files (*.*)
Manu
Manu

3. Select **Choose File.** Choose the .csv file from the document library. Then select **Open**.



4. The uploaded file will appear in the **Process** pop-up window. Select **Save**. Users in the .csv file will be added to the **Users** list on the **Users** page.



Import Multiple Users

Process

1. Export the CSV file of Active users from Microsoft Office 365 admin center.
2. Edit the CSV to include only necessary users.
3. Return to this screen and upload CSV file.

Optional: Invite Guest Users

From this Users page, you can allow frequent guest users to use the Synappx Go mobile app and Synappx Meeting to access Sharp MFPs and display features. For example, a real estate broker can invite real estate agents who use their office (but have separate email domains) to use Synappx Go to easily share image or proposal files to a meeting room displays with co-workers or clients. The guest user can also scan, copy or print cloud files with their own personal settings from the mobile. Users can be a Synappx guest user for multiple companies but must be provided with a Synappx Go license in each company.

Note: The following table describes the Synappx Go features that different kinds of guest users can access. See the Synappx Go User Guide and the Synappx Meeting User Guide more details.

Synappx Go Guest User Support by Login Type			
Features	**Microsoft 365 Guest**[1]	**Google Workspace Guest**[1]	**Custom Synappx Account Guest**
MFP			
Scan	O	O	O
Copy	O	O	O
Print Cloud Files	O	O	O
Print Release	X	X	X
Locked MFPs	X	X	X
Share to Display			
Recently Modified, Search, Browse Files	O	O	O
Share Files to Download, View and Edit	O	O	O
Browser Based File Editing	O	O	X
Remote Control Downloaded Files	O	O	O
Meet			
Start Scheduled Meeting (If Invited)	O[2]	O[2]	X
End Scheduled Meeting (If Invited)	O[2]	O[2]	X
Meeting Control Page Access	O[2]	O[2]	X
Meeting Information Page	O[2]	O[2]	X
Create Ad Hoc Meeting	O[2,3]	O[2,3]	X
Check In	O	O	O

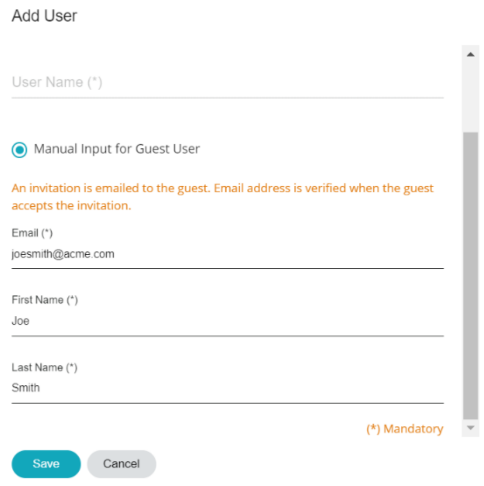
[1] Guest users who have existing Synappx Go logins to Microsoft 365 or Google Workspace may be requested to accept an additional calendar access permission to use Meet features.

[2] Workspaces on the Meet page will only reflect workspaces for (a) the first company that added you as a guest OR (b) your home Synappx company if you are also a regular licensed Synappx Go user.

[3] For ad hoc meetings, as a guest, you can select a workspace to start a meeting in your home company (if you have a home Synappx license) or a workspace in the first company that added you as a guest; however, the workplace in the guest company will not be checked or booked on the calendar.

To invite a guest user:

1. Select the **+** icon.
2. At the bottom of the Add Users page, enter the guest email address, first name and last name. Press **Save.**



Add User

User Name (*)

● Manual Input for Guest User

An invitation is emailed to the guest. Email address is verified when the guest accepts the invitation.

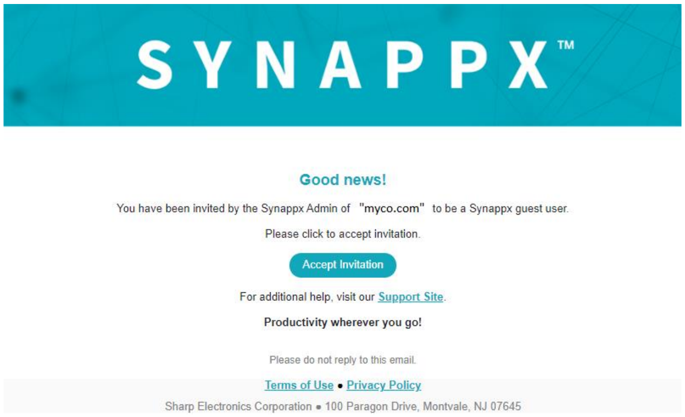
Email (*)
joesmith@acme.com

First Name (*)
Joe

Last Name (*)
Smith

(*) Mandatory

3. An email (example below) is sent to the guest notifying them that your company has invited them to be a Synappx Guest. See [Synappx Go User Guide]() for details on their acceptance process.



Good news!

You have been invited by the Synappx Admin of "myco.com" to be a Synappx guest user.

Please click to accept invitation.

For additional help, visit our Support Site.

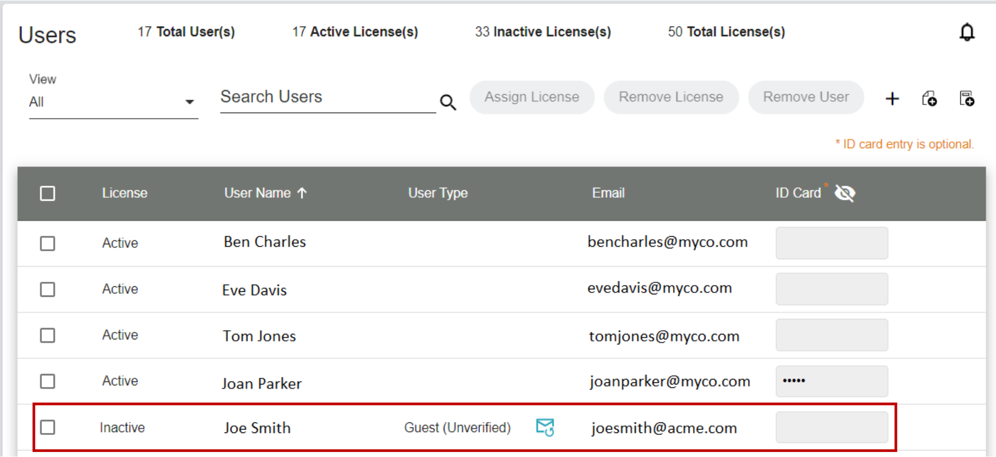
Productivity wherever you go!

Please do not reply to this email.

Terms of Use • Privacy Policy

Sharp Electronics Corporation • 100 Paragon Drive, Montvale, NJ 07645

4. The guest name is shown on the Admin Portal Users page as a **Guest (Unverified)** until the guest accepts and selects their log in provider (Microsoft 365 user, Google Workspace user or create a new Synappx custom account with their emal).

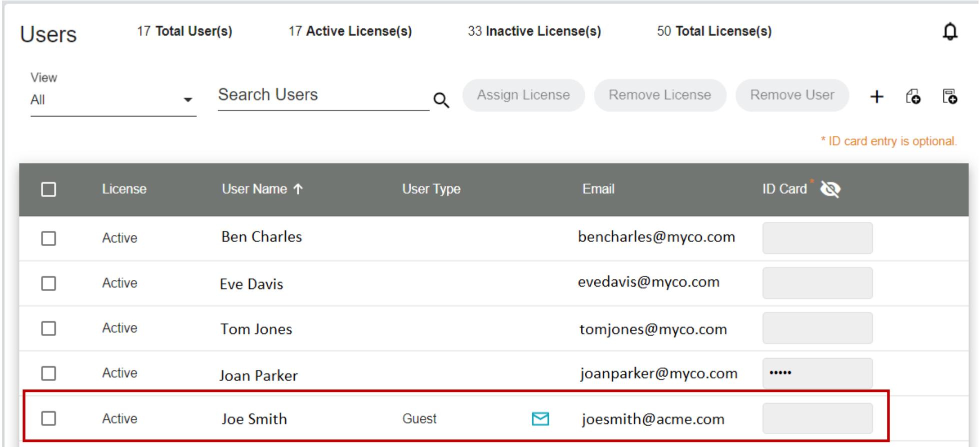


17 Total User(s) 17 Active License(s) 33 Inactive License(s) 50 Total License(s)

* ID card entry is optional.

□	License	User Name ↑	User Type	Email	ID Card *
□	Active	Ben Charles		bencharles@myco.com	
□	Active	Eve Davis		evedavis@myco.com	
□	Active	Tom Jones		tomjones@myco.com	
□	Active	Joan Parker		joanparker@myco.com	•••••
□	Inactive	Joe Smith	Guest (Unverified)	joesmith@acme.com	

5. If the guest accepts the invitation and log in provider to use to log into the Synappx apps, the Admin Portal will show them as **Guest**. You can resend an email if the guest didn't receive it by selecting the envelope. Assign a license for the guest (see section below) and the guest will receive an email with details on how to download and access the Synappx Go app.



17 Total User(s) 17 Active License(s) 33 Inactive License(s) 50 Total License(s)

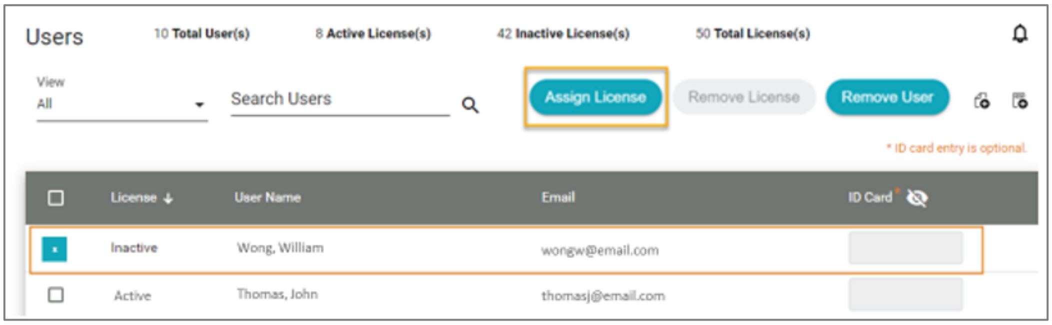
* ID card entry is optional.

□	License	User Name ↑	User Type	Email	ID Card *
□	Active	Ben Charles		bencharles@myco.com	
□	Active	Eve Davis		evedavis@myco.com	
□	Active	Tom Jones		tomjones@myco.com	
□	Active	Joan Parker		joanparker@myco.com	•••••
□	Active	Joe Smith	Guest	joesmith@acme.com	

Note:

- If you invite Google Workspace users to be Synappx guests in your company, the guest user will need to have their company admin add required Synappx scopes in order for that guest user to be able to use Synappx features. See Google scope details in this document for more details.

Assign Licenses



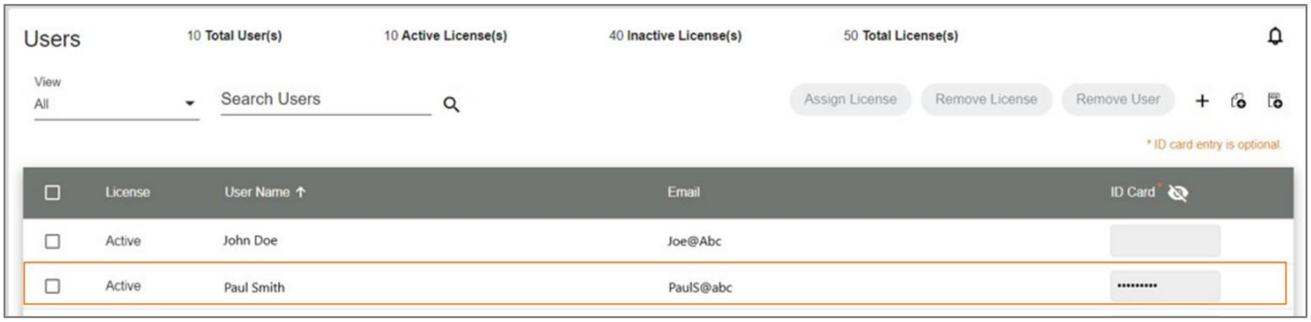
10 Total User(s) 8 Active License(s) 42 Inactive License(s) 50 Total License(s)

* ID card entry is optional.

□	License ↓	User Name	Email	ID Card *
☒	Inactive	Wong, William	wongw@email.com	
□	Active	Thomas, John	thomasj@email.com	

From the **Users** page, check the box(es) of the user(s) to license and select **Assign License.**

License status will change to **Active**. Newly licensed users will receive automatic notification emails with instructions to download and set up the Synappx Go mobile app. Print release driver instructions need to be provided to licensed users (see Step 9: Configure Print Release Driver and Share with users).



View: All

□	License	User Name ↑	Email	ID Card *
□	Active	John Doe	Joe@Abc	
□	Active	Paul Smith	PaulS@abc	•••••••••

Optional: Manual Entry or Import User ID Card Numbers

Note: Only applicable to companies configuring Synappx Go for use with PaperCut MF or Native Authentication. Do not enter user ID card numbers if Sharp MFP are not locked.

Integration with either of these systems requires entry of supported user ID card numbers in one of three ways:

- Manual entry, editing or deletion of card IDs on this Users page.
- Import of user ID card numbers associated with supported Users.
- Synappx Go mobile entry of card numbers by each user.

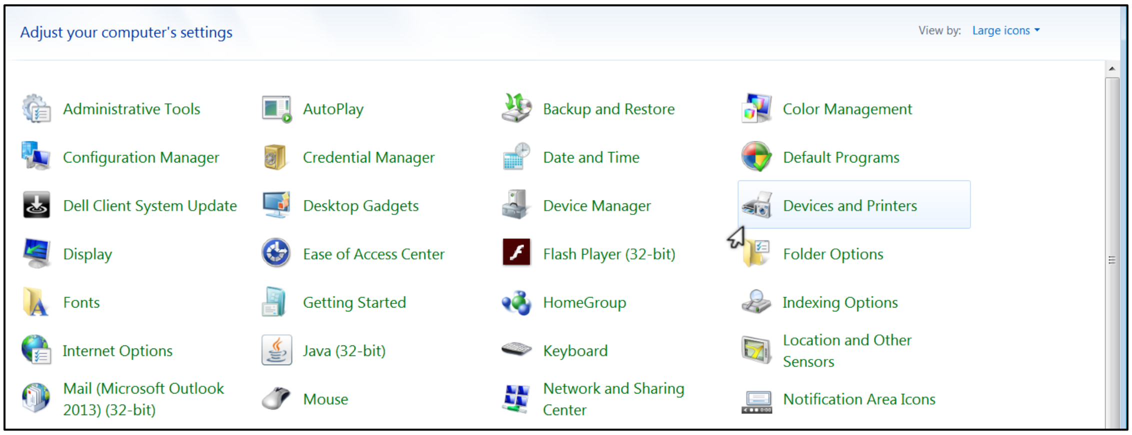
For more details on card ID entry or import, see the separate Synappx Go Integration with PaperCut Admin Guide or Synappx Go Integration with Native Authentication Admin Guide.

Step 8: Configure Print Release Driver

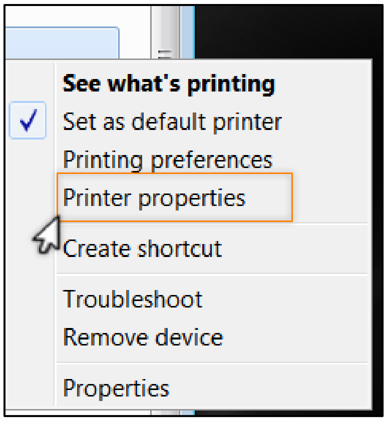
To enable print release on the Synappx Go app, the network administrator or user must configure a print driver.

Follow the steps below to install the Sharp universal print driver (or the respective MFP driver) on your network PC. The Sharp UD3 is the recommended driver for print release.

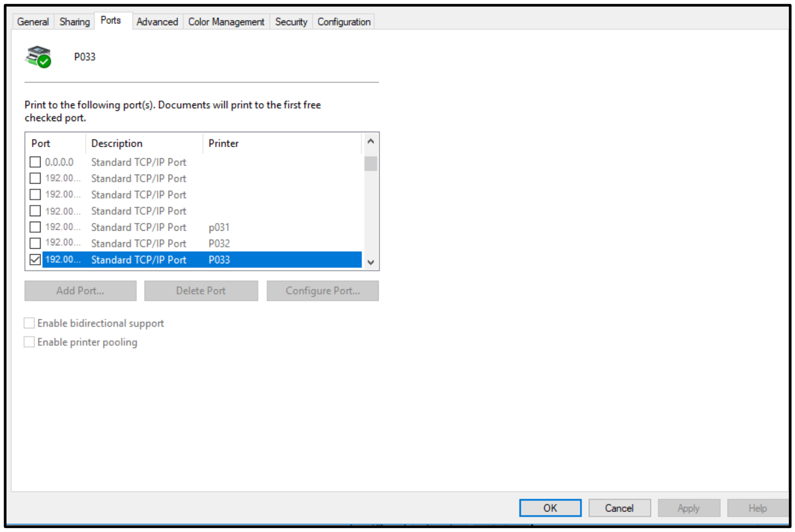
1. Navigate to the **Control Panel** and select **Devices and Printers**.



2. Right click on the printer driver. Select **Printer Properties**.



3. Select the **Ports** tab. Then select **Configure Port**.



P033

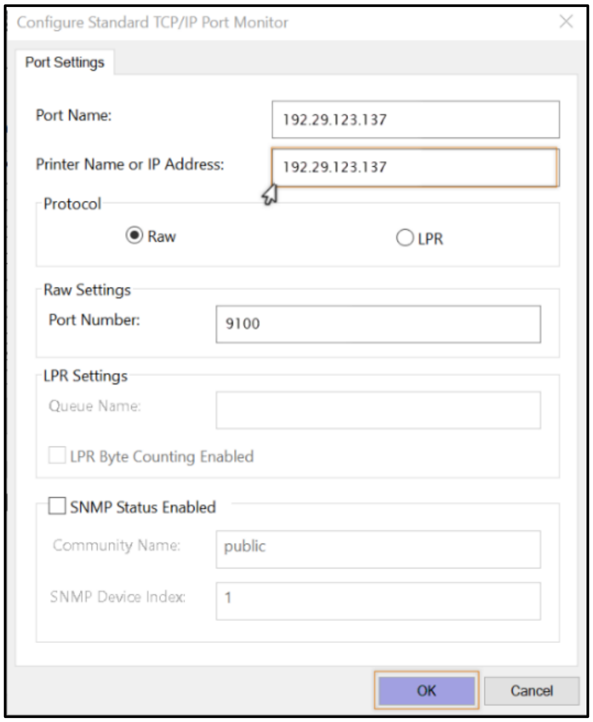
Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ 0.0.0.0	Standard TCP/IP Port	
□ 192.00...	Standard TCP/IP Port	
□ 192.00...	Standard TCP/IP Port	
□ 192.00...	Standard TCP/IP Port	
□ 192.00...	Standard TCP/IP Port	p031
□ 192.00...	Standard TCP/IP Port	P032
☑ 192.00...	Standard TCP/IP Port	P033

□ Enable bidirectional support

□ Enable printer pooling

4. Delete the current entry in the **Printer Name or IP Address** field and enter the address of the MFP agent. Both RAW (TCP port 9100) and Line Printer Remote (LPR) (TCP port 515) printing are supported. Ensure the PC firewall is configured to allow TCP traffic on the selected port. Then select **OK**.



Port Name: 192.29.123.137

Printer Name or IP Address: 192.29.123.137

Protocol

● Raw ○ LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name:

□ LPR Byte Counting Enabled

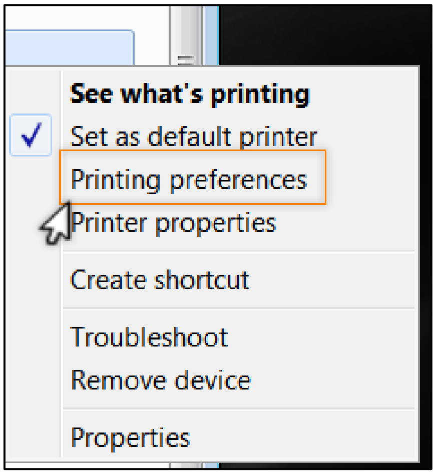
□ SNMP Status Enabled

Community Name: public

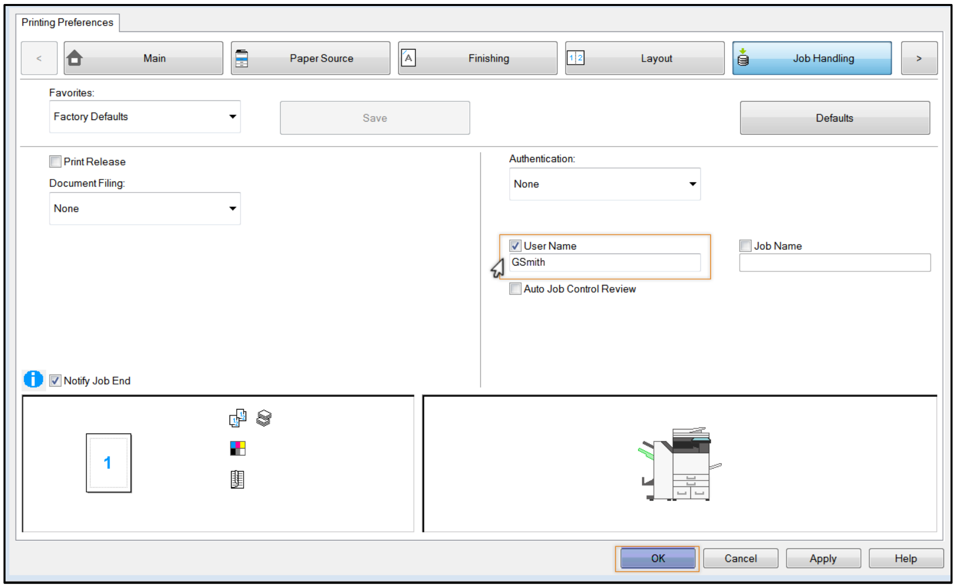
SNMP Device Index: 1

Note: If the username can be determined automatically, proceed to step 7. If the username is not the same as the network credentials or if print jobs do not appear in a user's print queue when using Synappx Go, follow steps 5 and 6.

5. If the username is not the same as the network credentials, right click the selected MFP print driver and select **Printer Preferences**.



6. Select the **Job Handling** tab. Check the **User Name** box and enter the user email -prefix (e.g. GSmith). Select **OK** to save the setting for this driver.



Favorites: Factory Defaults

☐ Print Release

Document Filing: None

Authentication: None

☑ User Name
GSmith

☐ Job Name

☐ Auto Job Control Review

☑ Notify Job End

7. Through your normal driver distribution process, provide the configured Synappx Go print release driver to licensed users. Users will use the driver in normal print operations for Synappx Go print release jobs.

Note: If Synappx Go print jobs do not get to the MFP agent PC, see Appendix A: Windows Defender Firewall Post-Installation Configuration. **Licensed Synappx Go is now ready to use!**

Admin Settings (Optional)

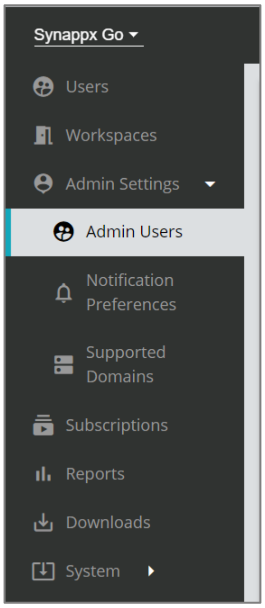
Administrator Management

Admin users are administrators for the Synappx Admin Portal. Administrators manage key components such as workspaces, users, devices and licenses. Administrators can also add and remove other administrators to and from the system. Additional admins do not require Azure administrator privileges. However, they need to be a member of the organization's Microsoft 365 or Google Workspace environment.

Here is a list of features for full and support administrators.

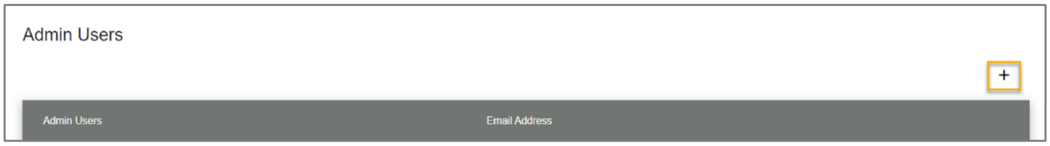
Service	Page	Functions	Admin	Support Admin
Synappx Admin Portal (Common)	Workspaces	View workspace list	Yes	Yes
		Add workspace (manual)	Yes	No
		Add workspace (import from Office 365/ Google Workspace)	Yes	No
		Add workspaces with Group	Yes	No
		Add workspace (import CSV)	Yes	No
		Remove workspace	Yes	No
		Edit workspace	Yes	No
	Admin User	View admin user list	Yes	No
		Add/remove admin user	Yes	No
		Edit admin role	Yes	No
	Domains	View supported domains list	Yes	Yes
		Refresh domain list	Yes	No
		Edit supported domain alias list	Yes	No
	Subscription	View subscription list	Yes	Yes
	Report	View report	Yes	No
		Export report	Yes	No
	System Log	View and export log	Yes	Yes
	Admin Log	View and export log	Yes	Yes
Synappx Meeting	Workspaces	Register/remove device in workspace	Yes	No
		View workspace details	Yes	Yes
		Assign/remove license	Yes	No
Synappx Go	User	View user list	Yes	Yes
		Add user (import from Office 365/Google Workspace)	Yes	Yes
		Add users with Group	Yes	Yes
		Add user (import CSV)	Yes	No
		Assign/remove license	Yes	Yes
		Remove user	Yes	No
	Workspace	Add MFP	Yes	No
		Add display	Yes	No
	Devices and Agents	View workspace details	Yes	Yes
		Edit settings, re-discover, etc.	Yes	No
	Notifications	View pages	Yes	Yes
		Edit notification email settings	Yes	No
	Downloads	Download MFP agent	Yes	No
		Download display agent	Yes	No
	Agent Update	Update agent	Yes	No
		Update policy	Yes	No

Add Administrators (Recommended)

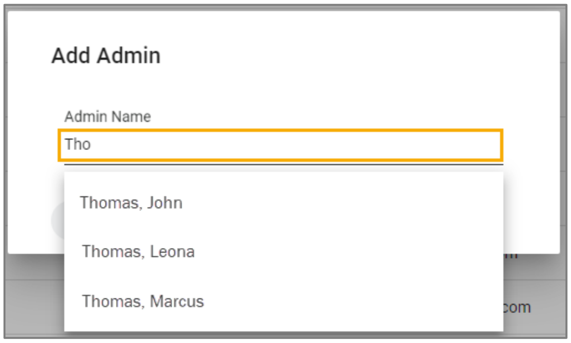


Full administrators can perform all functions on the Admin Portal after the primary admin accepts the initial permissions.

1. Go to **Admin Settings** on the Admin Portal. On the **Admin Users** page, select **(+)**.



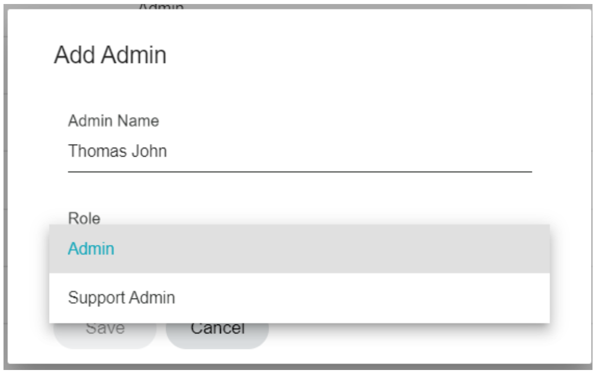
2. Type a few characters of the admin's name in the **Admin Name** field. Names from your organization will appear. Select names from the list.



Add Admin

Admin Name: Tho

3. Under **Role**, select **Admin** for full administrative rights or **Support Admin** for limited capabilities. Admin is the default. See Administrator Management for more information. The role can be edited later by selecting the admin name.



Add Admin

Admin Name: Thomas John

Role: Admin

4. Select **Save**. The new administrator will appear on the **Admin Users** list.

Notification Preferences

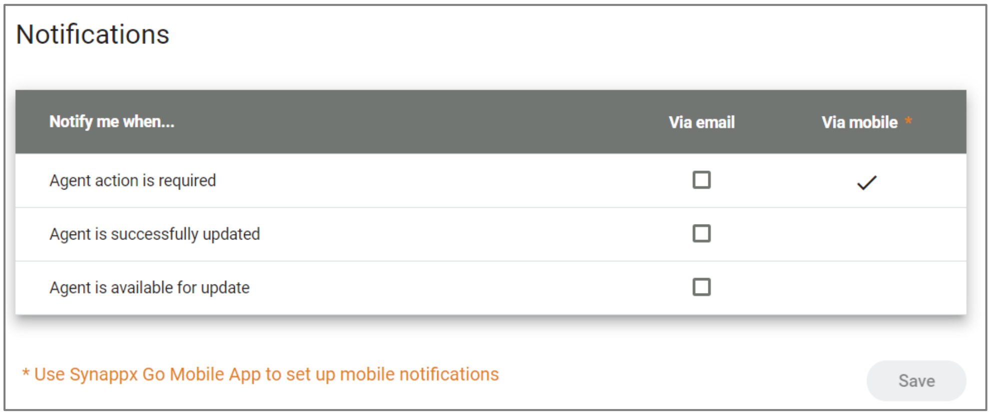
Administrators can set preferences to receive notification emails or mobile push notifications. Admins set their own email notifications; individual selections will not impact other admins. The default is no notifications.

There are three notification options:

- **Agent Service Action Required:** Notifies admin of agent error that requires action.
- **Agent Successfully Updated:** Notifies admin when agent update is successful.
- **Agent Available for Update:** Notifies admin of available agent update.

To set email notifications:

1. Individual admins log in to the Admin Portal.
2. Select **Notification Preferences** in the **Admin Settings** tab.
3. Check the box(es) to enable notifications.



Notifications

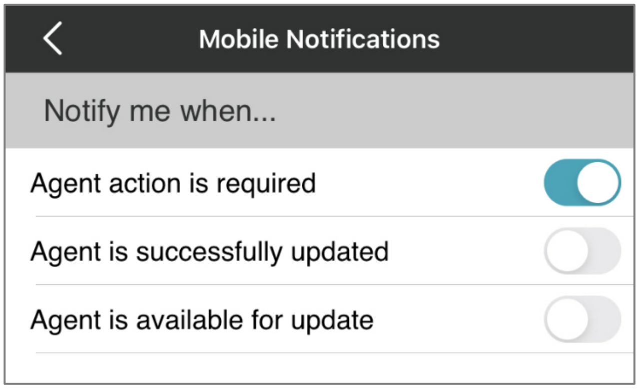
Notify me when...	Via email	Via mobile *
Agent action is required	□	✓
Agent is successfully updated	□	
Agent is available for update	□	

* Use Synappx Go Mobile App to set up mobile notifications

Use the Synappx Go Mobile App to set up mobile notifications. Selected notifications are shown on the Notifications page but cannot be edited.

To set mobile notifications:

1. Open the Synappx Go app.
2. Open the menu. ☰
3. Select **Settings** > **Mobile Notifications**.
4. Tap the toggle to enable mobile notifications. A teal toggle enables notifications.



Mobile Notifications

Notify me when...

Agent action is required ●

Agent is successfully updated ○

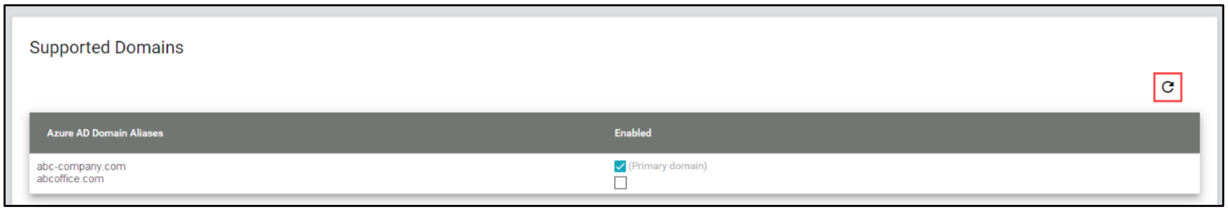
Agent is available for update ○

Supported Domains

The **Supported Domains** page automatically collects domain aliases from Azure Active Directory or Google Workspace. The default setting is to enable all domains.

> **Note**: If an admin disables a domain that is already selected, then the associated users and workspaces will also be disabled.

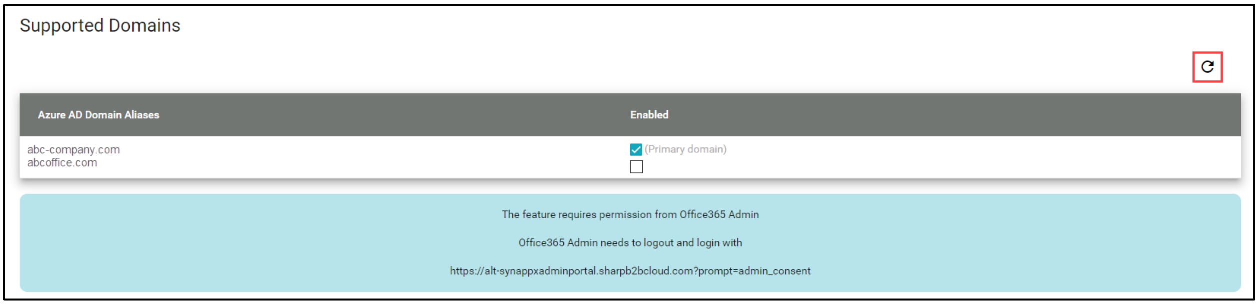
Admins can choose which domain aliases to enable or disable by checking and unchecking the boxes; these settings apply to Synappx Go and Synappx Meeting. Primary domains cannot be unselected. Select the refresh icon ↻ to view new domain aliases added to Azure AD or Google Workspace.



Supported Domains

Azure AD Domain Aliases	Enabled
abc-company.com	☑ (Primary domain)
abcoffice.com	□

Microsoft 365 customers who licensed Synappx Go or Meeting before Version 1.3 may see a blue box with a link to opt in to the directory.read.all permission to retrieve domains.



Supported Domains

Azure AD Domain Aliases	Enabled
abc-company.com	☑ (Primary domain)
abcoffice.com	□

The feature requires permission from Office365 Admin

Office365 Admin needs to logout and login with

https://alt-synappxadminportal.sharpb2bcloud.com?prompt=admin_consent

System Options: Agent Updates and Logs

The Admin Portal **System** page has four options: **Agent Updates, Admin Log**, **System Log,** and **Check In Log**.

Logs

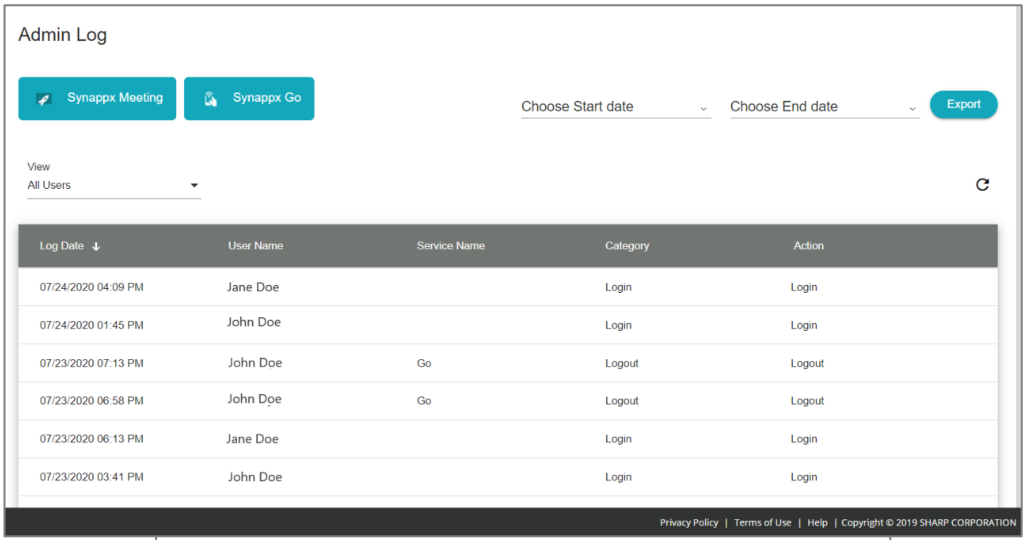
The Synappx Admin Portal provides event data to assist with identifying and resolving issues.

Admin Log

Since multiple administrators can configure and manage the system, the admin log provides a record of administrator actions on the Admin Portal. For selected Actions, hover over the text to see more details.

If both Synappx Go and Synappx Meeting are licensed, system logs for both services are available on this page.

1. To filter log events, select the button to select and deselect services. (Teal buttons are selected, and white buttons are deselected.)
2. To export all logs, enter a start and end date and select **Export.** A CSV file will download automatically.
3. Select **OK**.

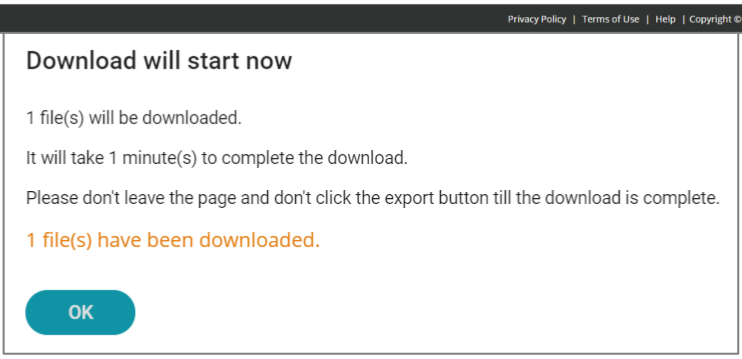

Admin Log

Synappx Meeting
Synappx Go
Choose Start date
Choose End date
Export

View
All Users

Log Date ↓	User Name	Service Name	Category	Action
07/24/2020 04:09 PM	Jane Doe		Login	Login
07/24/2020 01:45 PM	John Doe		Login	Login
07/23/2020 07:13 PM	John Doe	Go	Logout	Logout
07/23/2020 06:58 PM	John Doe	Go	Logout	Logout
07/23/2020 06:13 PM	Jane Doe		Login	Login
07/23/2020 03:41 PM	John Doe		Login	Login

Privacy Policy | Terms of Use | Help | Copyright © 2019 SHARP CORPORATION


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.

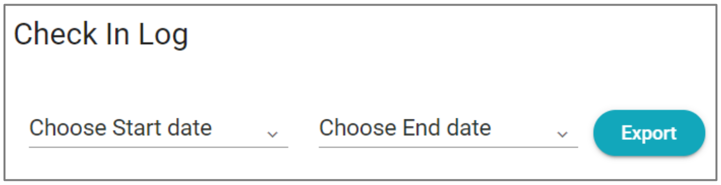
1 file(s) have been downloaded.

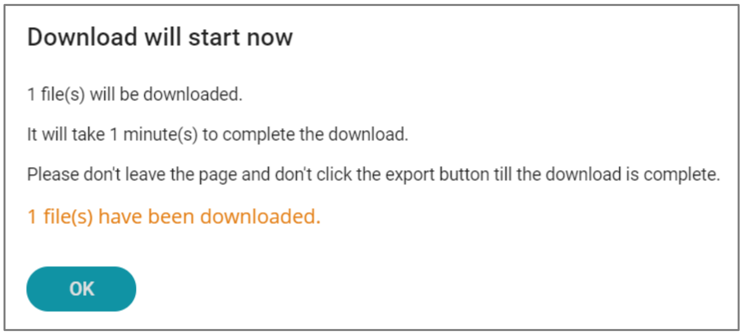
Check In Log

Check-in logs help admins track employees’ touch points in the workplace.

Note: Synappx Go tags must be configured to capture user check-in events (see Step 5: Associate NFC Tags).

1. Enter a start and end date and select **Export.** A CSV file will download automatically.
2. Select **OK**.




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.

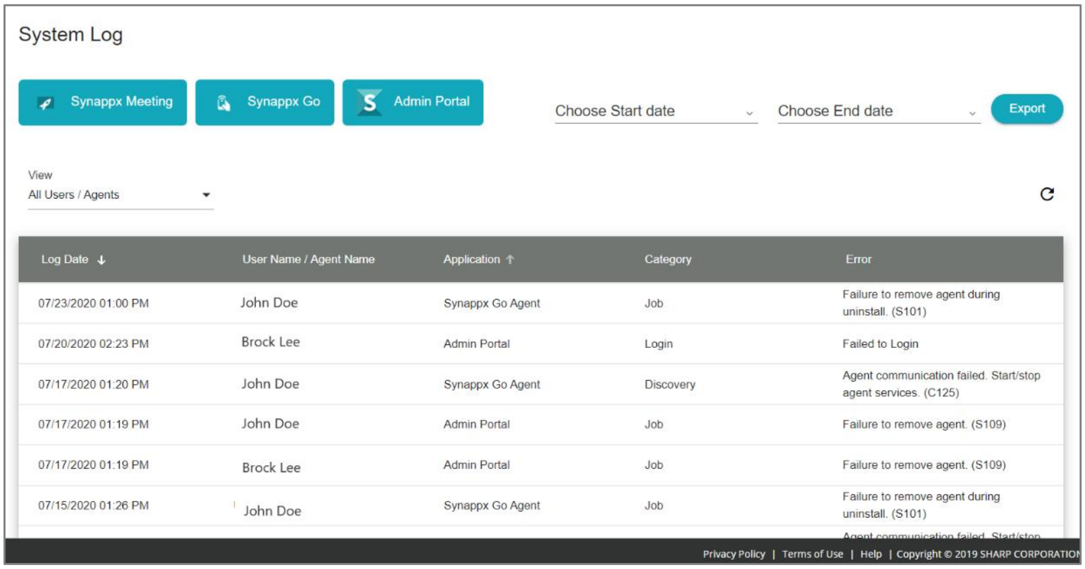
The CSV file contains information on users who have tapped check-in, MFP or display NFC tags. Log data includes user name, user ID (email address), date and time, workspace location, action and MFP or display agent IP address (if applicable).

System Log

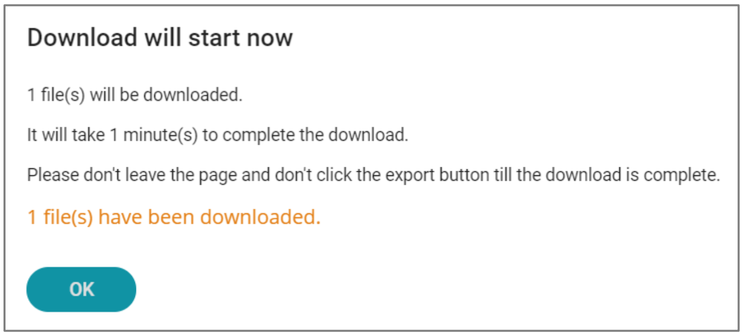
If an MFP or display agent is unable to complete configuration with the Synappx cloud or if subsequent agent or mobile error conditions occur, information on those events can be found in the system log. Some errors have additional details that can be viewed by hovering over the error text. Logs for successfully installed and configured individual agents can also be found by selecting the **Log** link for each agent (see **Summary of Devices and Agents**).

If both Synappx Go and Synappx Meeting are licensed, system logs for both services are available on this page.

1. To filter system log events, select the button to select and deselect services. (Teal buttons are selected, and white buttons are deselected.)
2. To export all system logs, enter a start and end date and select **Export.** A CSV file will download automatically.
3. Select **OK**.



Log Date ↓	User Name / Agent Name	Application ↑	Category	Error
07/23/2020 01:00 PM	John Doe	Synappx Go Agent	Job	Failure to remove agent during uninstall. (S101)
07/20/2020 02:23 PM	Brock Lee	Admin Portal	Login	Failed to Login
07/17/2020 01:20 PM	John Doe	Synappx Go Agent	Discovery	Agent communication failed. Start/stop agent services. (C125)
07/17/2020 01:19 PM	John Doe	Admin Portal	Job	Failure to remove agent. (S109)
07/17/2020 01:19 PM	Brock Lee	Admin Portal	Job	Failure to remove agent. (S109)
07/15/2020 01:26 PM	John Doe	Synappx Go Agent	Job	Failure to remove agent during uninstall. (S101)
				Agent communication failed. Start/stop



Download will start now

1 file(s) will be downloaded.

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

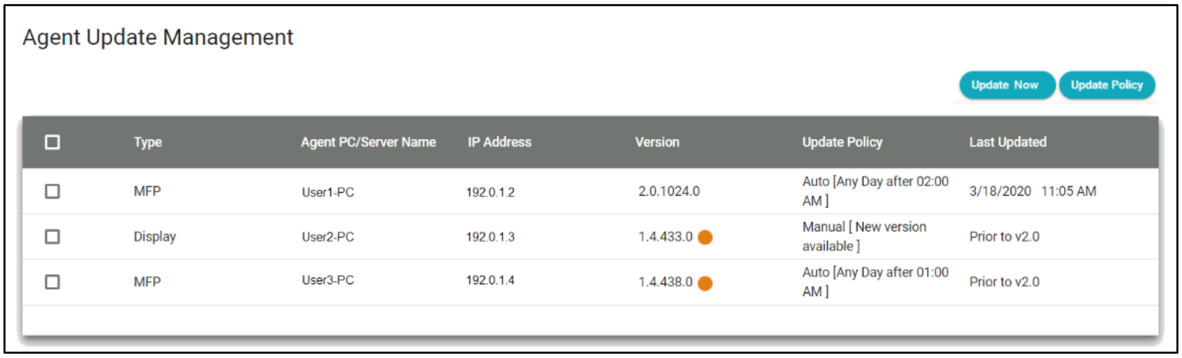
Please don't leave the page and don't click the export button till the download is complete.

1 file(s) have been downloaded.

Each Synappx Go system log entry on this page and on the individual agent log pages have an error code (e.g. C102) at the end of the message. This provides more detailed information on the log entry. Contact your Sharp service provider for details. Note: If a MFP was discovered and associated with a previous agent, it cannot also be discovered by a different agent. This error will be shown in the System Log page (underlined text) and can be removed from the first agent (if desired) so the MFP can be rediscovered and added to a different agent.

Update Agents

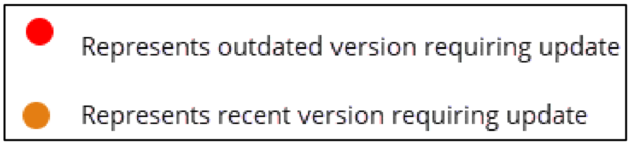
Agent Updates displays an overview of all agent version numbers, including new versions available or recommended for installation and the option to set an update policy.



Agent Update Management

□	Type	Agent PC/Server Name	IP Address	Version	Update Policy	Last Updated
□	MFP	User1-PC	192.0.1.2	2.0.1024.0	Auto [Any Day after 02:00 AM]	3/18/2020 11:05 AM
□	Display	User2-PC	192.0.1.3	1.4.433.0 🟠	Manual [New version available]	Prior to v2.0
□	MFP	User3-PC	192.0.1.4	1.4.438.0 🟠	Auto [Any Day after 01:00 AM]	Prior to v2.0

Synappx Go MFP agents with versions 1.3.323 and later and display agents with version 1.3.322.0 and later update automatically by default. The **Version** column shows the version number of each agent. Colored circles represent older versions that require updates.



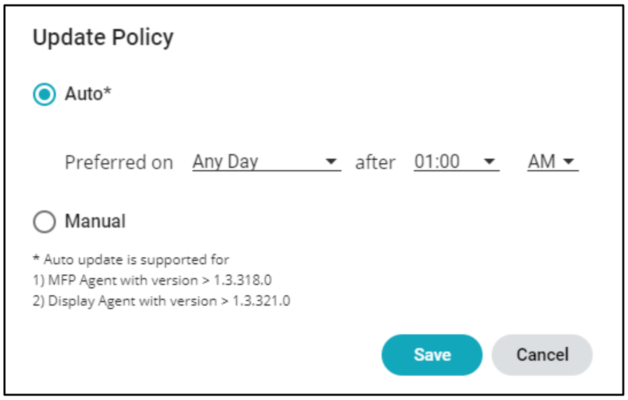
🔴 Represents outdated version requiring update

🟠 Represents recent version requiring update

The **Last Updated** column shows the day and time of the last successful update. If an agent was updated before version 2.0, the entry for that agent shows **Prior to v2.0**.

Update Policy

Admins have options to customize the agent update policy by selecting an agent and the **Update Policy** button.



Update Policy

● Auto*

Preferred on Any Day after 01:00 AM

○ Manual

* Auto update is supported for
1) MFP Agent with version > 1.3.318.0
2) Display Agent with version > 1.3.321.0

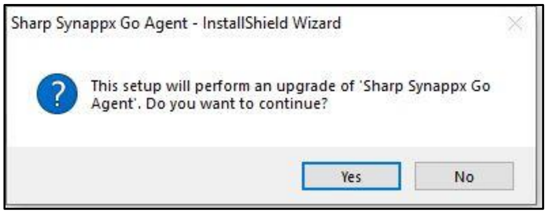
- Set a preferred day and time for automatic updates (Default is any day after 1:00 A.M.)
- Select **Manual** to disable automatic updates

Note:

- If agent PC/server is asleep during the auto update time, the system will check for updates after the Synappx services are restarted. Recommend to set the auto update schedule for a time when the agent PC is likely to be available for auto update.

Manually Update Agents Released before Version 1.3

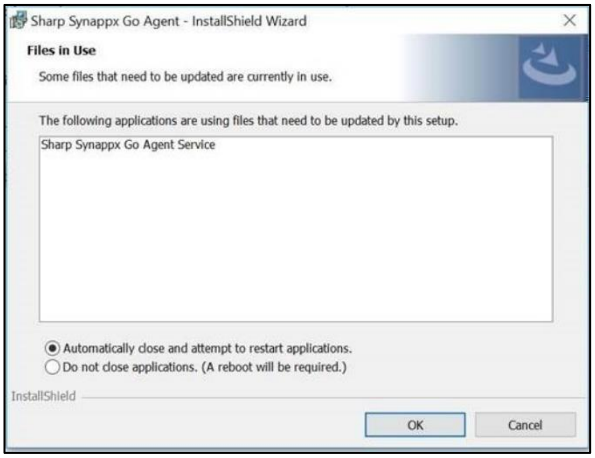
1. From the **Downloads** page, download the agent again.
2. A pop-up box will display a prompt to upgrade the agent. Select **Yes**.



Sharp Synappx Go Agent - InstallShield Wizard

This setup will perform an upgrade of 'Sharp Synappx Go Agent'. Do you want to continue?

3. Follow the **InstallShield Wizard** instructions.
4. If the Synappx service is running, a window will prompt the admin to stop the service to continue the upgrade installation. Select **Automatically close and attempt to restart applications**. Then select **OK**.



Sharp Synappx Go Agent - InstallShield Wizard

Files in Use

Some files that need to be updated are currently in use.

The following applications are using files that need to be updated by this setup.

Sharp Synappx Go Agent Service

● Automatically close and attempt to restart applications.

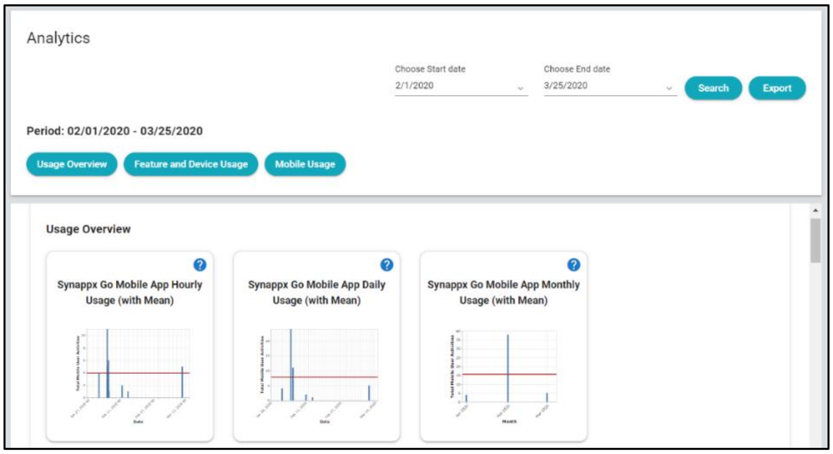
○ Do not close applications. (A reboot will be required.)

5. Repeat this procedure for both agents if applicable.

Analytics

Overview

Reports provide visualized data to help administrators understand Synappx Go usage patterns. Administrators can select start and end dates to view analytics within specific time periods.



Analytics

Choose Start date: 2/1/2020

Choose End date: 3/25/2020

Period: 02/01/2020 - 03/25/2020

Usage Overview

Search
Export
Usage Overview
Feature and Device Usage
Mobile Usage
Synappx Go Mobile App Hourly Usage (with Mean)
Synappx Go Mobile App Daily Usage (with Mean)
Synappx Go Mobile App Monthly Usage (with Mean)

Reports can be downloaded as CSV file(s) by selecting the time period from the start date and end date drop-down windows and selecting **Export**.

Available Data, Feature and Device Usage

Mobile App Usage (with Mean)
These three bar charts show mobile app usage by user activity (i.e., scan, print release, share to display) per hour, day, or month with mean.

Usage by User: Top 10
The stacked bar chart shows MFP usage (i.e., scan to me, scan to email, scan to cloud, print release) by username during the selected time period.

Usage by Device: Top 10
The stacked bar chart shows MFP usage (i.e., scan to me, scan to email, scan to cloud, print release) by MFP during the selected time period.

Display Content Downloaded by Cloud Storage
The pie chart organizes downloaded content by cloud storage provider.

Display Content Types Downloaded: Top 10
The pie chart organizes downloaded content by file type (e.g. PDF, TIFF).

Usage by Workspace: Top 10
The horizontal bar chart shows feature usage by workspace.

MFP Usage by Job Type
The pie chart displays overall scan and print release proportions during the selected time period.

MFP Usage by Scan Job Type
The pie chart shows the scan destination (me, email, cloud storage) proportions during the selected time period.

MFP Scan File Size by Destination
The scatter chart displays the file size by scan destination during the selected time period. It displays the scan file size mean and standard deviation.

MFP Job Usage by MFP: Top 10
The Sankey diagram shows the flow of scan and print jobs by MFP during the selected time period.

MFP Usage by Hours: Top 10
The heat map visualizes individual MFP usage over hours of the day during the selected time period.

MFP Scan to Cloud Usage by Storage Sites
The pie chart shows providers used to scan to cloud storage.

MFP Scan File Size by Type
The scatter chart displays file size and mean by scan job destination.

Display Usage by Hours: Top 10
The heat map visualizes individual display agent usage over hours of the day during the selected time period.

Mobile Usage by User and Date: Top 10
The area chart shows the overall mobile app usage by username and date during the selected time period.

Mobile App Usage Frequency by User: Top 10
The stacked bar chart shows the mobile app feature (e.g., scan, print, share, NFC setup) usage by user during the selected time period.

Mobile App Daily Usage by Operating System
The stacked bar chart displays mobile user activities by mobile operating system (iOS and Android) during the selected time period.

Check In Actions by Workspace
The stacked bar chart shows check-in actions by workspace, including check-in NFC tag actions and MFP or display feature use.

Synappx Go No Login (Free Scan to email and Copy)

As an alternative to the fully featured, licensed Synappx Go application, you have an option for users to access **Synappx Go No Login** (free copy and scan to email).

The free version of Synappx Go does not require agent install or NFC tags. It enables simple copy and scan to email functions by scanning a QR Code.

The full version of Synappx Go can be unlocked when a user license is assigned, the Synappx Go agent is installed and an NFC tag is mapped. Once the full version is unlocked, users will have an access to copy, scan to email, scan to cloud storage services, share to display, and more.

Both the licensed and free Synappx Go are available from the same Synappx Go mobile app downloaded from the Apple App Store or Google Play site.

System Configuration

Before using the Synappx Go No Login version, you need to configure the Sharp workgroup (A3) and workgroup desktop (A4) MFPs by installing an embedded app in each MFP users will access. Go to the MFP application section in the Synappx Support Site for more information about the applications. For compatible MFPs, see the list of supported Sharp A3 Workgroup MFPs.

Here are the installation steps for each MFP type:

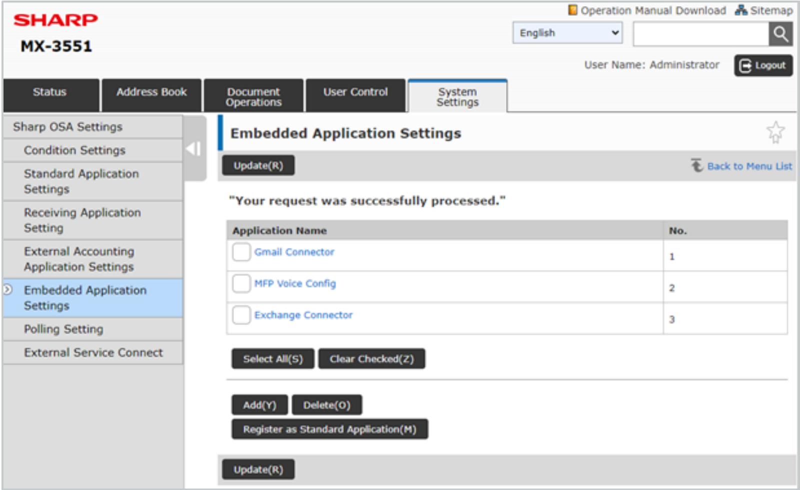
Sharp Wrokgroup A3 MFP and Select A4 Model Setup

To install and configure each MFP to support Synappx Go No Login use:

1. Download **Synappx Go - No Login.emo** from the Application Portal or contact your authoried Sharp service provider to receive the application

2. Open browser and access **http://<IP Address of SHARP MFP>** and log in as administrator.

3. Navigate to **System Settings >> Sharp OSA Settings >> Embedded Application Settings.** Click on **Add(Y).**

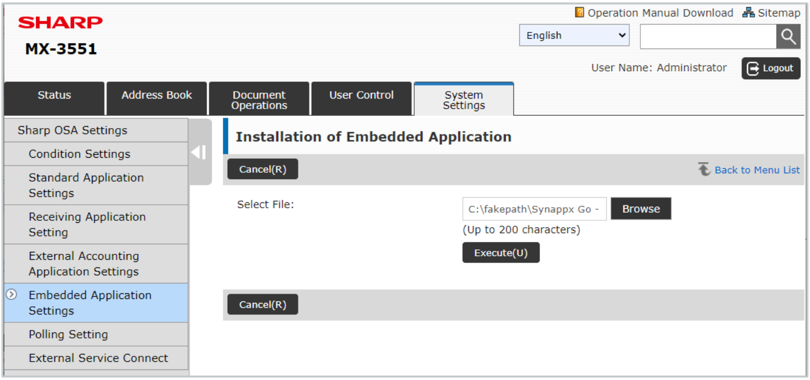


Embedded Application Settings

"Your request was successfully processed."

Application Name	No.
□ Gmail Connector	1
□ MFP Voice Config	2
□ Exchange Connector	3

4. Browse and select ‘Synappx Go - No Login.emo’ file. Click on **Execute(U).**

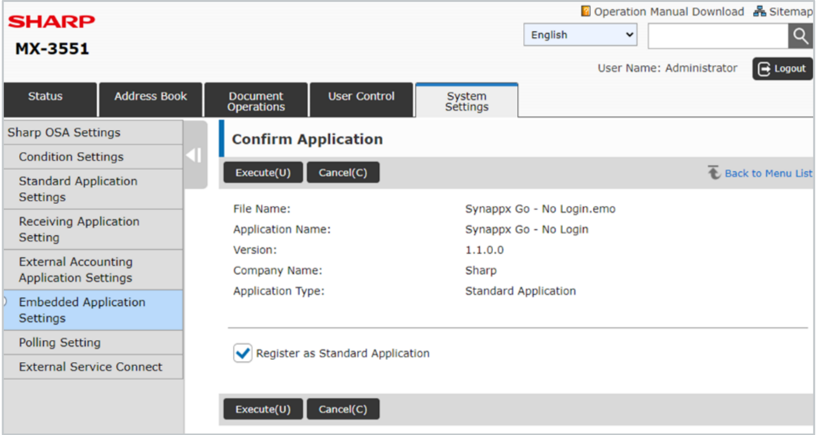


Installation of Embedded Application

Select File: C:\fakepath\Synappx Go -

(Up to 200 characters)

5. Ensure that **Register as Standard Application checkbox is selected.** Click on **Execute(U).**

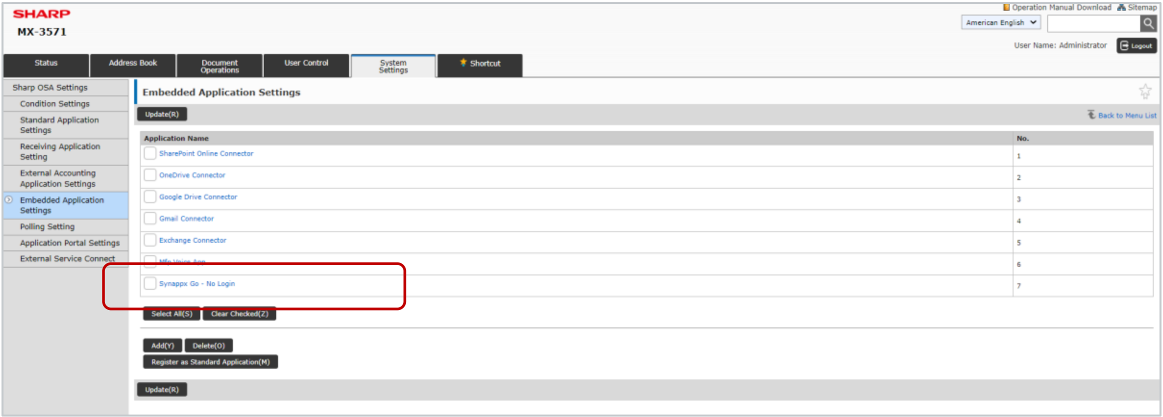


Confirm Application

File Name:	Synappx Go - No Login.emo
Application Name:	Synappx Go - No Login
Version:	1.1.0.0
Company Name:	Sharp
Application Type:	Standard Application

☑ Register as Standard Application

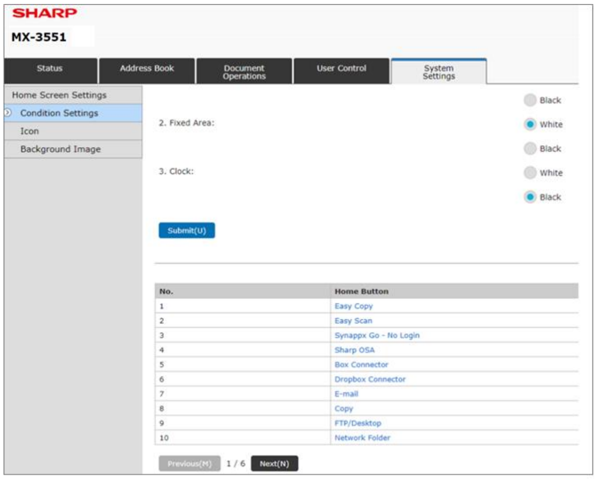
6. Ensure that app registered successfully.



Embedded Application Settings

Application Name	No.
□ SharePoint Online Connector	1
□ OneDrive Connector	2
□ Google Drive Connector	3
□ Gmail Connector	4
□ Exchange Connector	5
□ Mfp Voice App	6
□ Synappx Go - No Login	7

7. Navigate to **System Settings >> Home Screen Settings >> Condition Settings.** Go to **Home Button** table and select the home screen app you want to replace with Synappx Go No Login. Click that app name.



	○ Black
2. Fixed Area:	● White
	○ Black
3. Clock:	○ White
	● Black

No.	Home Button
1	Easy Copy
2	Easy Scan
3	Synappx Go - No Login
4	Sharp OSA
5	Box Connector
6	Dropbox Connector
7	E-mail
8	Copy
9	FTP/Desktop
10	Network Folder

8. Go to **Sharp OSA** section and select **Application.** Use the dropdown next to Application to select the **Synappx Go No Login** app. Press **Submit** at the bottom of the page.

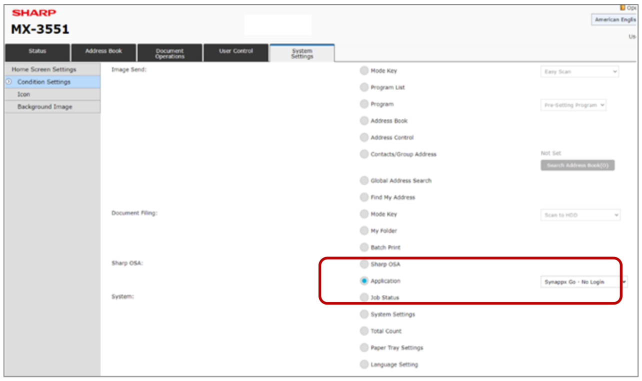
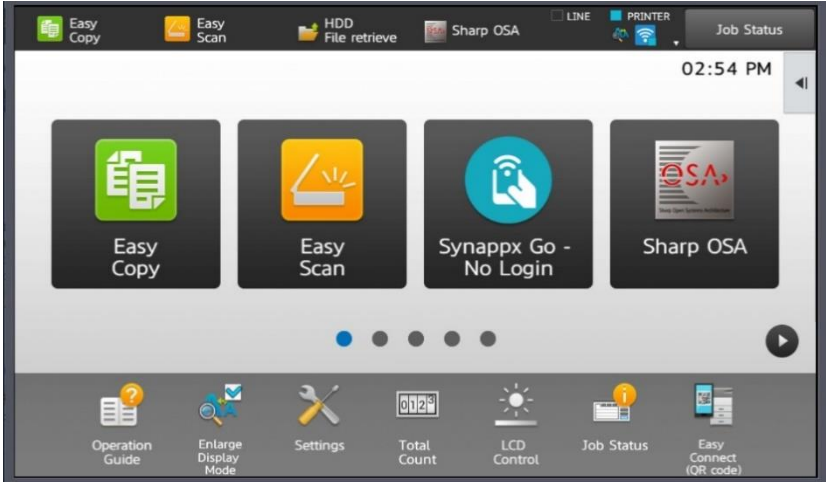
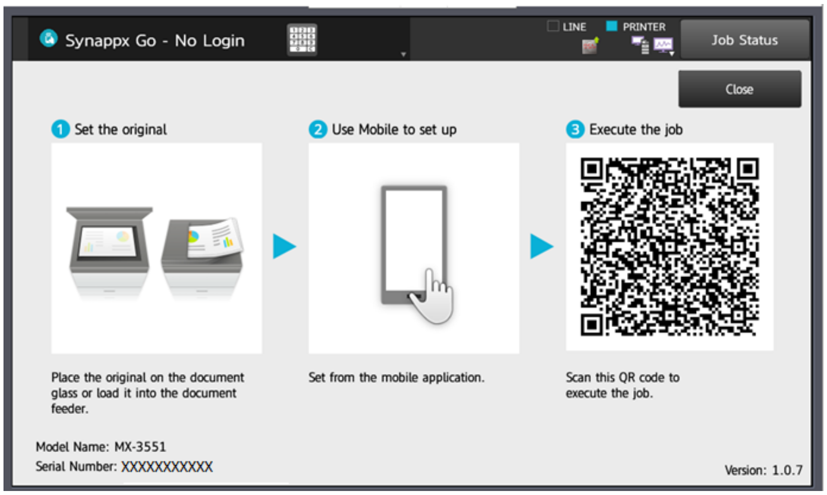


Image Send:	○ Mode Key	Easy Scan
	○ Program List	
	○ Program	Pre-Setting Program
	○ Address Book	
	○ Address Control	
	○ Contacts/Group Address	Not Set
	○ Global Address Search	
	○ Find My Address	
Document Filing:	○ Mode Key	Scan to HDD
	○ My Folder	
	○ Batch Print	
Sharp OSA:	○ Sharp OSA	
	● Application	Synappx Go - No Login
System:	○ Job Status	
	○ System Settings	
	○ Total Count	
	○ Paper Tray Settings	
	○ Language Setting	

9. View MFP home screen to confirm front panel is show showing the **Synappx Go – No Login** button.



10. **Press the Synappx button** and content with a QR code is displayed on the MFP. This is the QR code that should be scanned to use the Synappx Go - No Login Go features.



Place the original on the document glass or load it into the document feeder.

Set from the mobile application.

Scan this QR code to execute the job.

Model Name: MX-3551
Serial Number: XXXXXXXXXXX

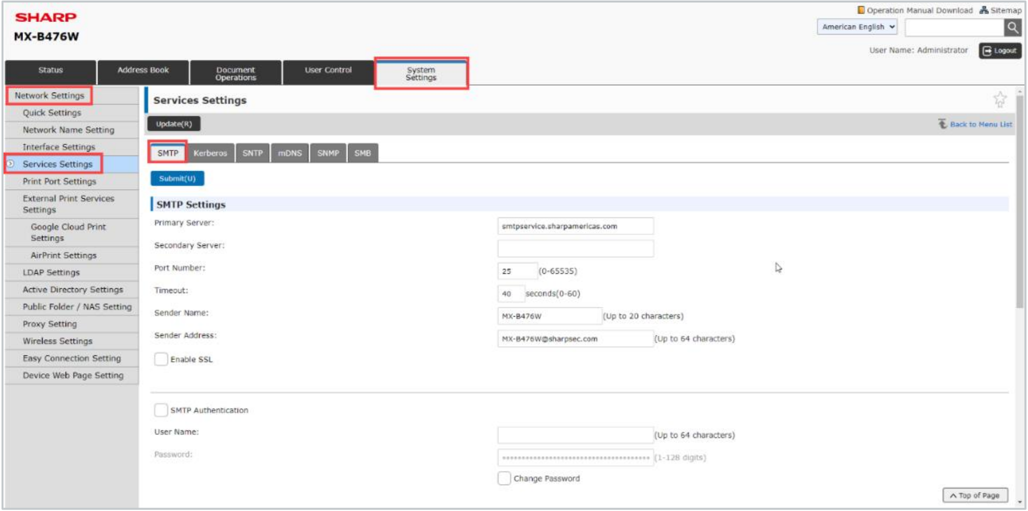
Version: 1.0.7

Notes:

- In the future, selected MFPs will be configurable to allow the QR code to be shown on the MFP home screen.
- If you are installing a new version of the embedded app, uninstall the previous version

Configure E-mail Settings on Sharp Workgroup A3 and Select A4 MFPs

1. From browser, navigate to http://<MFP_IP_ADDRESS> e.g., http://172.29.123.45
2. Select **System Settings > Network Settings > Services Settings > SMTP**.
3. Ensure appropriate E-mail SMTP fields are configured for your environment.



Services Settings

SMTP Settings

Primary Server: smtpservice.sharpamericas.com

Secondary Server:

Port Number: 25 (0-65535)

Timeout: 40 seconds(0-60)

Sender Name: MX-B476W (Up to 20 characters)

Sender Address: MX-B476W@sharpsec.com (Up to 64 characters)

□ Enable SSL

□ SMTP Authentication

User Name: (Up to 64 characters)

Password: ••••••••••••••••••••••••••••••••••••••• (1-128 digits)

□ Change Password

Configure Email Setting for Office 365 SMTP Server

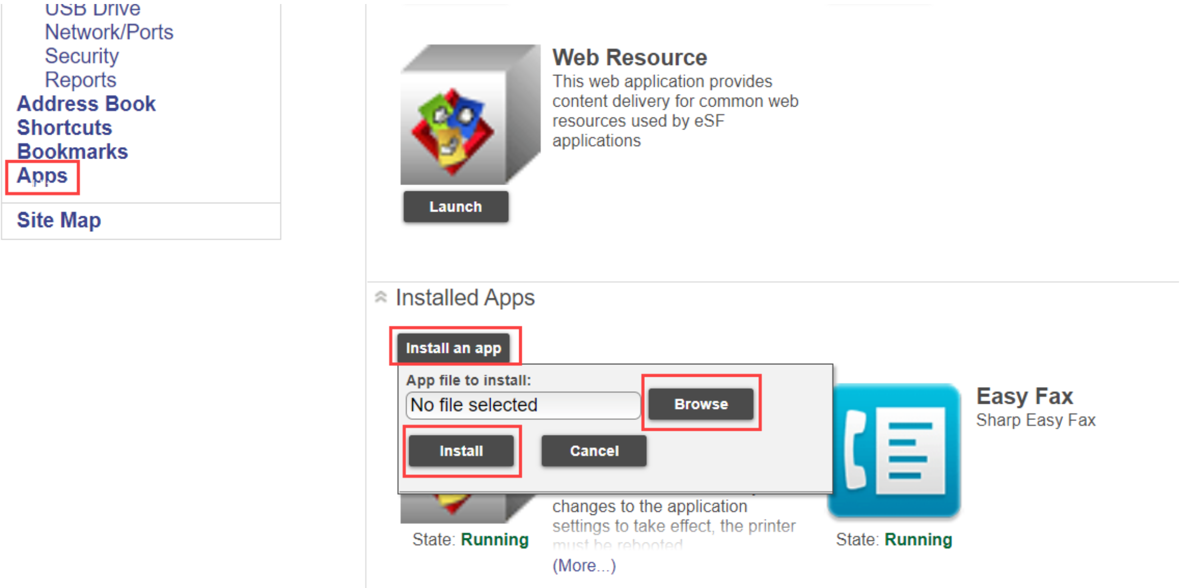
In the page shown above, when configuring for an Office 365 SMTP server, set the values as follows:

a. Primary Server: smtp.office365.com
b. Port Number: 587
c. Sender Name: <Office 365 username of account enable for Authenticated SMTP>
d. Sender Address: <Office 365 email address of account enabled for Authenticated SMTP>
e. Enable SSL: Check box
f. SMTP Authentication: Check box
g. User Name: <Office 365 email address of account enabled for Authenticated SMTP>
h. User Password: <account password>

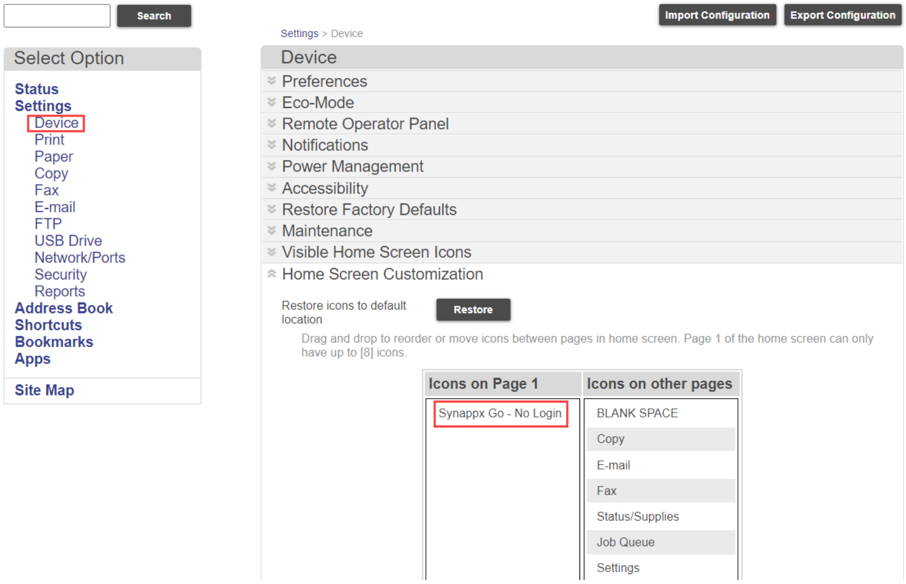
Sharp Workgroup Desktop A4 MFP Model Setup (MX-Cx07, MX-C357F, MX-B427, MX-B467, MX-Bxx7 Series)

See the list of supported Sharp A4 MFPs. To install and configure each A4 MFP to support Synappx Go No Login use:

1. Download the **Synappx Go-No Login.fls** from the Sharp app download site
2. From browser, navigate to http://<MFP_IP_ADDRESS> e.g., http://172.29.134.45
3. From the left side menu, select **Apps.**
4. Expand **Installed Apps** section, select **Install an app.**
5. Select **Browse**, navigate to the Synappx Go – No Login.fls file), select **Open**.
6. Select **Install.**



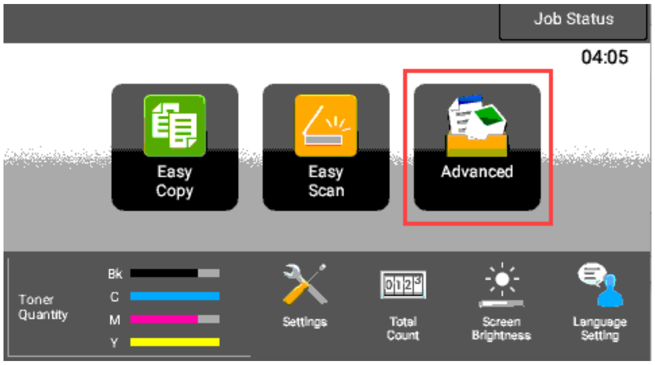
7. From the MFP embedded web page, Select **Device** in **Settings** section.
8. Expand **Home Screen Customization** section.
9. Drag **Synappx Go – No Login** from **Icons on other pages** column to **Icons on Page 1** column.
10. Select **Save.**



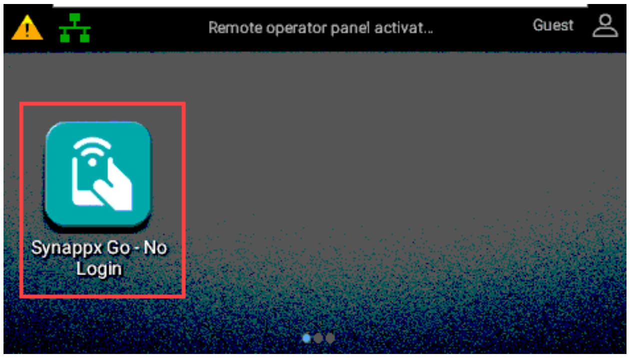
Drag and drop to reorder or move icons between pages in home screen. Page 1 of the home screen can only have up to [8] icons.

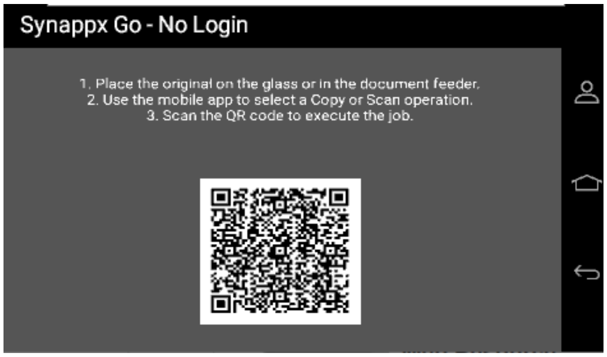
Icons on Page 1	Icons on other pages
Synappx Go - No Login	BLANK SPACE
	Copy
	E-mail
	Fax
	Status/Supplies
	Job Queue
	Settings

11. To launch the application, from the MFP home screen select **Advanced**.



12. Select **Synappx Go – No Login** application icon and the QR code will be shown for the Synappx Go user to capture from the mobile app to start scan to email and copy.




Synappx Go - No Login

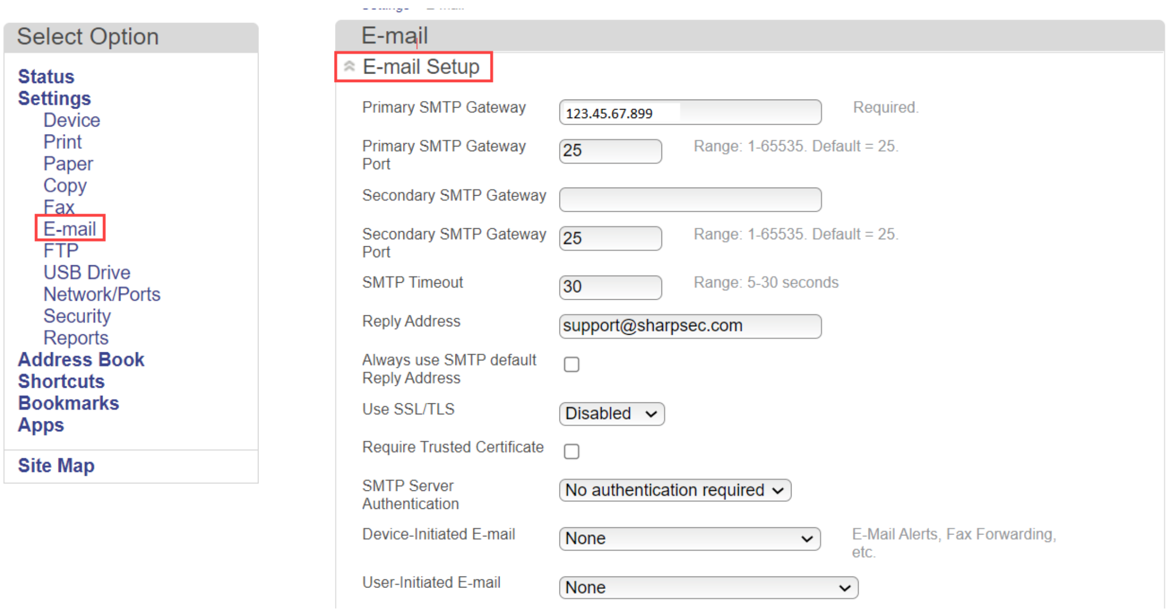
1. Place the original on the glass or in the document feeder.
2. Use the mobile app to select a Copy or Scan operation.
3. Scan the QR code to execute the job.

- Note: If you are installing a new version of the embedded app, uninstall the previous version

Configure Scan E-mail Settings

To send scan emails from the A4 model, configure the MFP SMTP settings.

1. From browser, navigate to http://<MFP_IP_ADDRESS> e.g., http://172.29.134.45.
2. From the left side menu, select **E-mail** under **Settings** section.
3. Expand **E-mail Setup** section.
4. Ensure appropriate E-mail SMTP fields are configured for your environment.



E-mail

E-mail Setup

Primary SMTP Gateway	123.45.67.899	Required.
Primary SMTP Gateway Port	25	Range: 1-65535. Default = 25.
Secondary SMTP Gateway		
Secondary SMTP Gateway Port	25	Range: 1-65535. Default = 25.
SMTP Timeout	30	Range: 5-30 seconds
Reply Address	support@sharpsec.com	
Always use SMTP default Reply Address	□	
Use SSL/TLS	Disabled	
Require Trusted Certificate	□	
SMTP Server Authentication	No authentication required	
Device-Initiated E-mail	None	E-Mail Alerts, Fax Forwarding, etc.
User-Initiated E-mail	None	

Configure Scan Email Sending Use with Office 365 SMTP Server

If using Office 365 as the SMTP server:

1. To enable account for SMTP, login to **admin.microsoft.com.**
2. Select **Users > Active Users**, then select user account that will be used for SMTP authentication.
3. On the right-hand side pane, select **Mail** tab.
4. Under **Email apps** section, select **Manage email apps.**
5. Select **Authenticated SMTP** and **Save changes.**
6. Browse to device embedded web pages.
7. From the left side menu, select **E-mail** under **Settings** section.
8. Expand **E-mail Setup** section.
9. Set the values as follows:
    a. Primary SMTP Gateway: smtp.office365.com
    b. Primary SMTP Gateway Port: 587
    c. Reply address: <Office 365 email address of account enabled for Authenticated SMTP>
    d. Use SSL/TLS: Required
    e. SMTP Server Authentication: Login / Plain
    f. User-Initiated E-mail: Use Device SMTP Credentials
    g. Device Userid: <Office 365 email address of account enabled for Authenticated SMTP>
    h. Device Password: <account password>

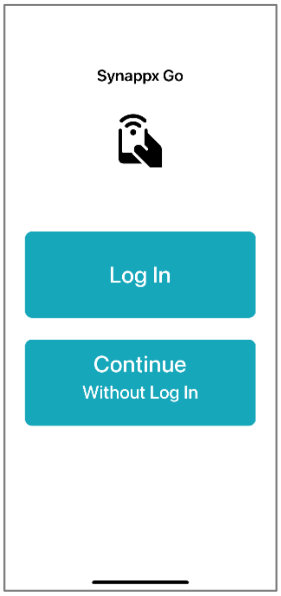
No Login User Experience

As an alternative to the more fully featured, licensed Synappx Go application, users have an option to use the **Continue Without Login** (unlicensed) version with more limited MFP features—scan to email and copy. Both the licensed and No login (free copy and scan to email) Synappx Go are available from the same Synappx Go mobile app downloaded from the Apple App Store or Google Play site.

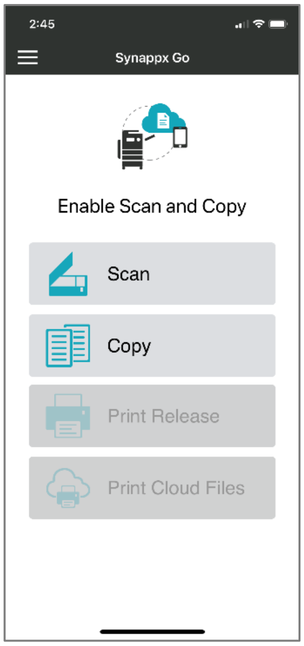
Before using the Continue Without Login (unlicensed) version of Synappx Go, ensure the Sharp MFP you will use has been configured to support this feature. You should be able to select the Synappx Go – No Login icon from the MFP. See details below for more information.

To use the Synappx Go No Login version:

1. Download the Synappx Go iOS or Android app from the Apple or Google app stores.
2. Select **Continue Without Log In**.



3. Agree to the End User License Agreement.
4. The Home screen is displayed on your mobile.



Scan Features

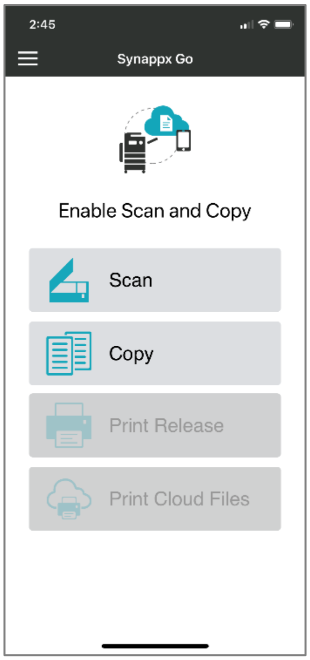
With this No Login scan feature, you can:

- Scan to Me (scans to your email)
- Scan to Email addresses
- Scan to Favorites (pre-set email groups)

For time savings, you can optionally set up the following before using Scan.

Scan to Me set up:

1. Select **Scan**.


2:45

Synappx Go

Enable Scan and Copy

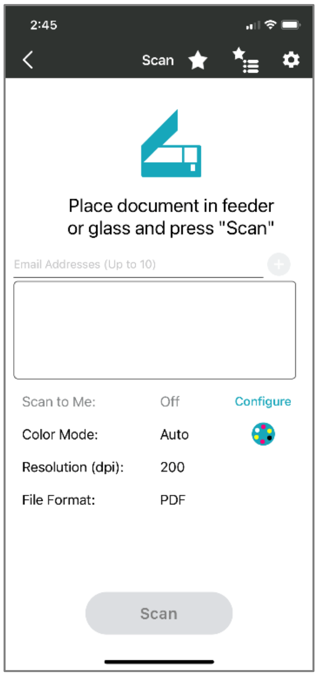
Scan

Copy

Print Release

Print Cloud Files

2. Select **Configure** next to Scan to Me and enter your email address. To later change or remove this, select Edit.


2:45

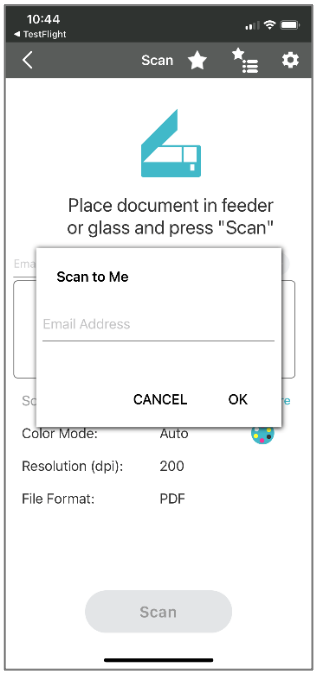
Scan

Place document in feeder or glass and press "Scan"

Email Addresses (Up to 10)

Scan to Me:	Off	Configure
Color Mode:	Auto	
Resolution (dpi):	200	
File Format:	PDF	

Scan


10:44

◂ TestFlight

Scan

Place document in feeder or glass and press "Scan"

Scan to Me

Email Address

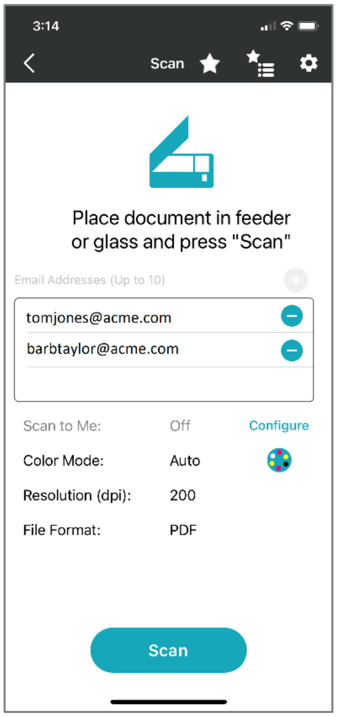
CANCEL OK

Color Mode:	Auto
Resolution (dpi):	200
File Format:	PDF

Scan

Scan to Favorites set up:

1. Select **Scan** from home page.
2. **Enter each email address and press +**. Repeat as needed to add up to ten email addresses.



Place document in feeder or glass and press "Scan"

Email Addresses (Up to 10)

tomjones@acme.com

barbtaylor@acme.com

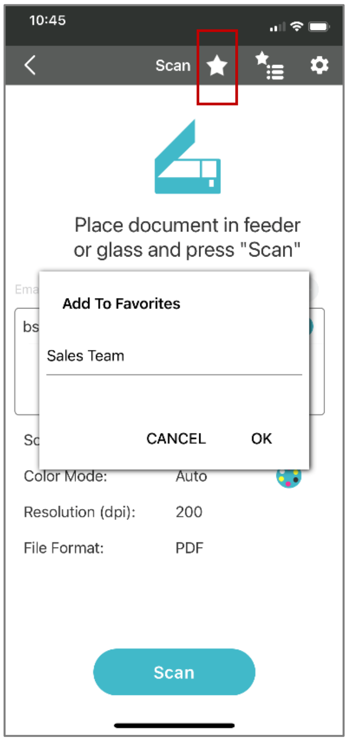
Scan to Me: Off Configure

Color Mode: Auto

Resolution (dpi): 200

File Format: PDF

3. Select the **Star** ★ icon at the top of the page. Enter a favorite email group name and press **OK**. The favorite list will be selectable each time you scan. You can add up to five favorites.



Place document in feeder or glass and press "Scan"

Add To Favorites

Sales Team

CANCEL OK

Color Mode: Auto

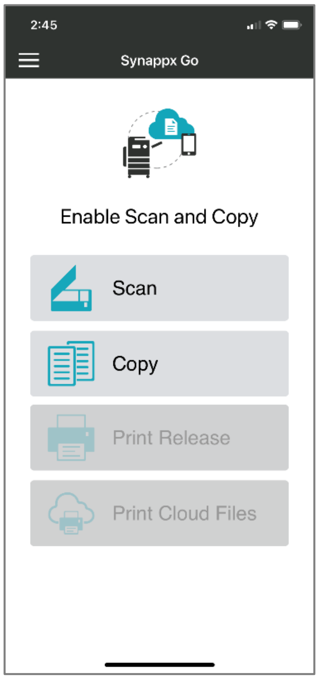
Resolution (dpi): 200

File Format: PDF

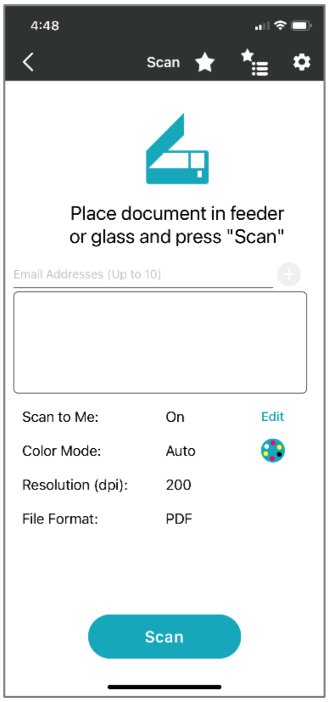
Scan Use

1. Place the document to scan in the MFP feeder or place a single page on the glass.

2. Select **Scan**.



3. Select a scan destination (one of the following options).
    a. For Scan to Me (if configured), select **Off** to turn **On**.


4:48
Scan
Place document in feeder or glass and press "Scan"
Email Addresses (Up to 10)
Edit
Scan

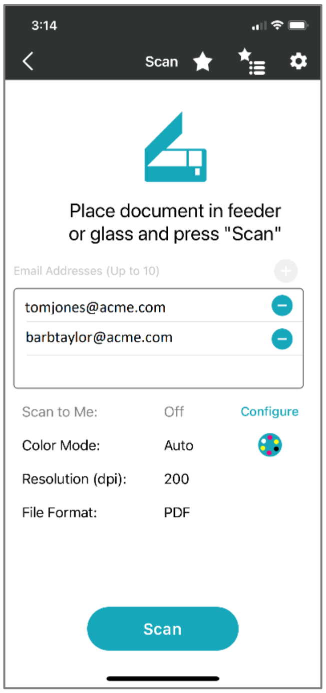
Scan to Me: On

Color Mode: Auto

Resolution (dpi): 200

File Format: PDF

    b. For ad hoc Scan to Email, **enter each email and press +** to add to list. If you have provided access to your mobile contacts, names matching your typing will be shown as you type. Note: If Scan to Me is turned On, turn Off to scan to other addresses or favorite



Place document in feeder or glass and press "Scan"

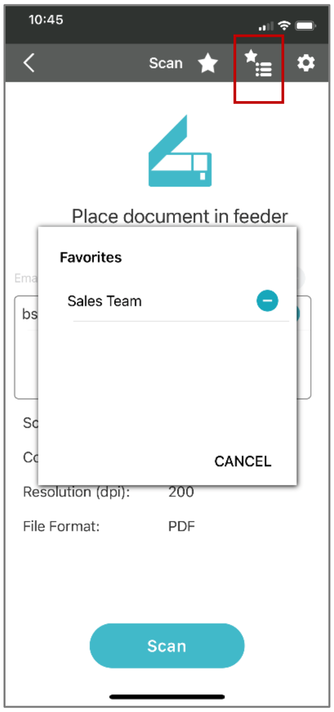
Email Addresses (Up to 10)

tomjones@acme.com

barbtaylor@acme.com

Scan to Me:	Off	Configure
Color Mode:	Auto	
Resolution (dpi):	200	
File Format:	PDF	

c. For pre-defined Favorites, select the **Favorites icon** at the top of the page and select the **Favorite** email list to use.

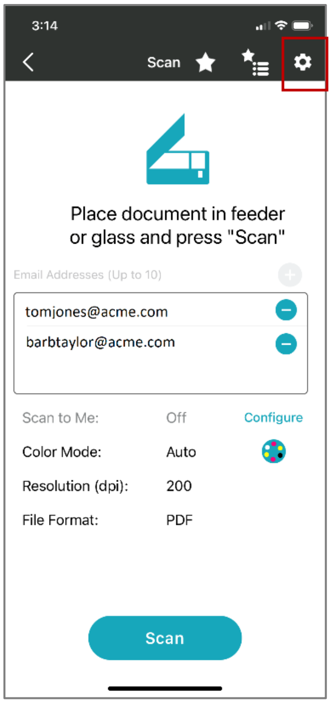


Favorites

Sales Team

Resolution (dpi):	200
File Format:	PDF

4. Check the scan settings and, if desired, touch the default scan settings to select another option. Optionally, you can also select the gear icon ⚙ in the upper right corner to view and change any of the supported scan settings. Note: Some settings are only available in the full licensed version.



3:14

Scan

Place document in feeder or glass and press "Scan"

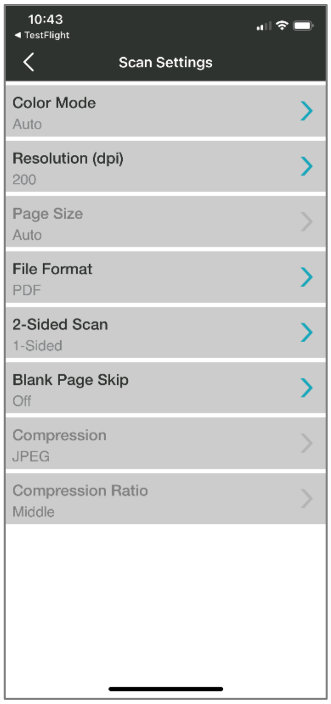
Email Addresses (Up to 10)

tomjones@acme.com

barbtaylor@acme.com

Scan to Me:	Off	Configure
Color Mode:	Auto	
Resolution (dpi):	200	
File Format:	PDF	

Scan



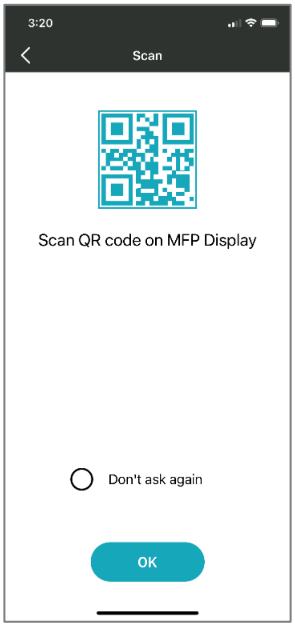
10:43

◂ TestFlight

Scan Settings

Color Mode	Auto
Resolution (dpi)	200
Page Size	Auto
File Format	PDF
2-Sided Scan	1-Sided
Blank Page Skip	Off
Compression	JPEG
Compression Ratio	Middle

5. Select **Scan**.
6. You are prompted to scan the Synappx QR code on the MFP front panel. Press **OK** on that page and your camera will automatically open (note: the first time, you will be asked to allow the Synappx Go app to access your camera).



3:20

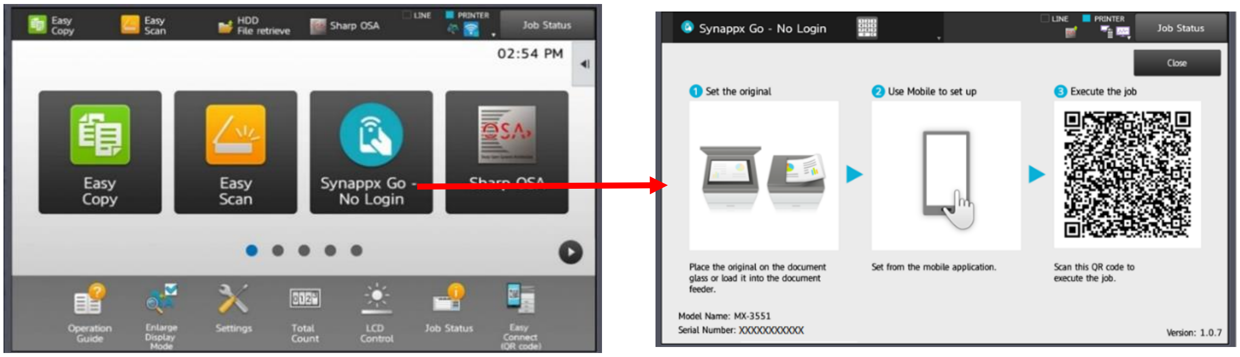
Scan

Scan QR code on MFP Display

○ Don't ask again

OK

7. Point your phone at the Synappx QR code. Depending on the MFP model, you may have to select the **Synappx Go – No Login** button or **Advanced** button, then **Synappx Go – No Log in** button on the front panel before the QR code is displayed.   Note: In the future, some models will be configurable so QR codes can be shown on the MFP home screen (with no touch required).



1 Set the original

2 Use Mobile to set up

3 Execute the job

Place the original on the document glass or load it into the document feeder.

Set from the mobile application.

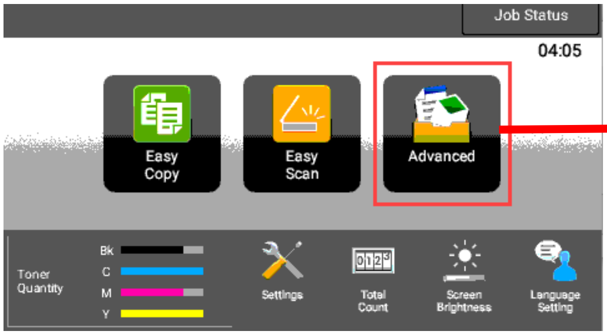
Scan this QR code to execute the job.

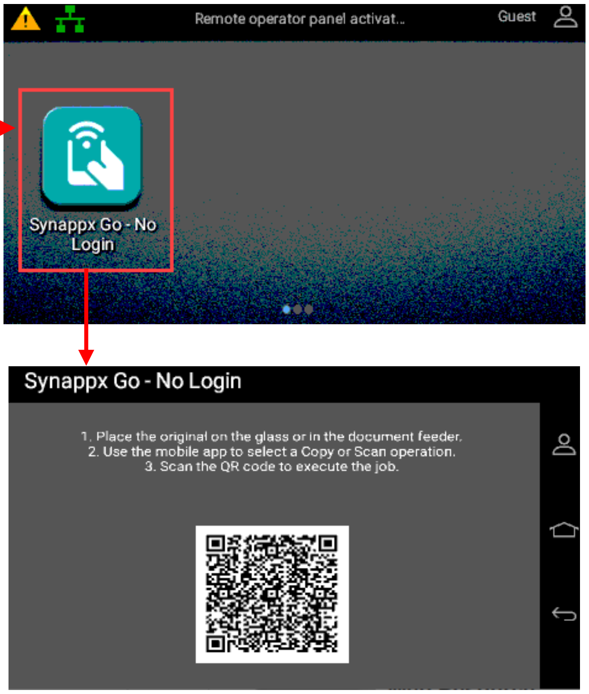
Model Name: MX-3551

Serial Number: XXXXXXXXXXX

Version: 1.0.7

On Supported Sharp A3 Models



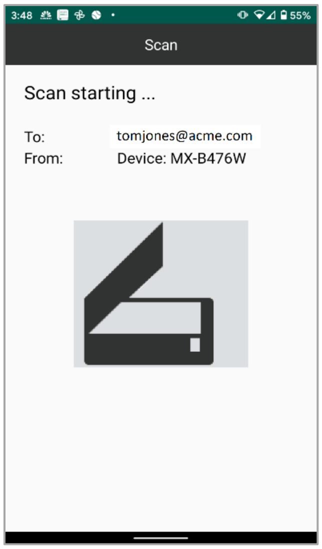


Synappx Go - No Login

1. Place the original on the glass or in the document feeder.
2. Use the mobile app to select a Copy or Scan operation.
3. Scan the QR code to execute the job.

On Supported Sharp A4 Models

8. When the mobile camera captures the Synappx QR code image, MFP scanning starts and you will see a scan success screen on your mobile. The MFP front panel will also show the status. Email with scan attached is sent from the MFP. The app returns to the home page. Note: You need to scan the QR code again is you want to scan another job.



Scan starting ...

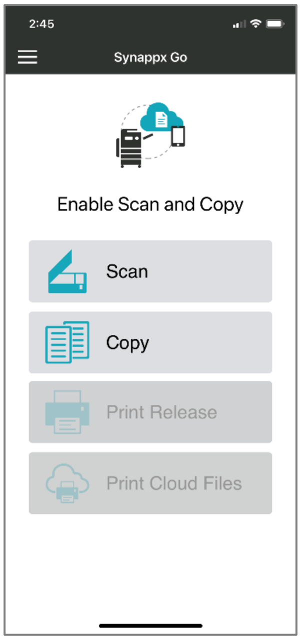
To: tomjones@acme.com
From: Device: MX-B476W

Copy Features

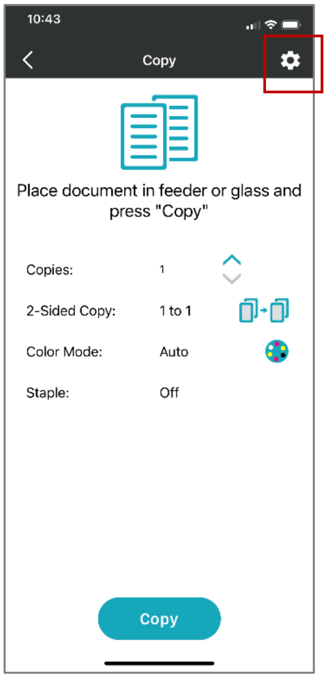
There is no pre-defined set up for the Copy feature.

Copy Use

1. Place the document to copy in the MFP feeder or place a single page on the glass.
2. Select **Copy**.



3. Check the copy settings and, if desired, touch the default copy settings to select another option. Optionally, you can also select the gear icon ⚙ in the upper right corner to view and change any of the supported copy settings. Note: Some settings are only available in the full licensed version.



10:43

Copy

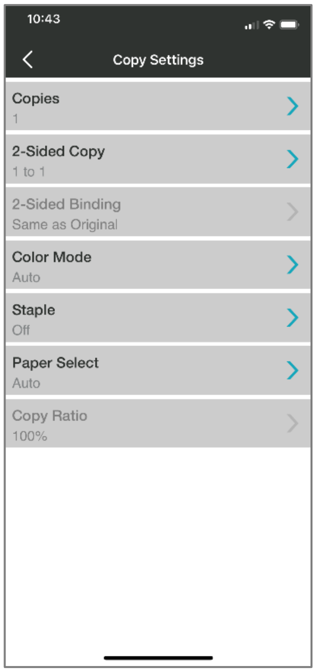
Place document in feeder or glass and press "Copy"

Copies: 1

2-Sided Copy: 1 to 1

Color Mode: Auto

Staple: Off



10:43

Copy Settings

Copies
1

2-Sided Copy
1 to 1

2-Sided Binding
Same as Original

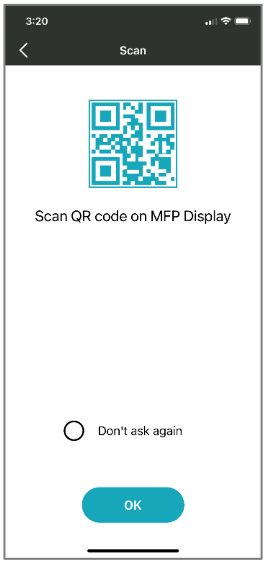
Color Mode
Auto

Staple
Off

Paper Select
Auto

Copy Ratio
100%

4. Select **Copy**.
5. You are prompted to scan the Synappx QR code on the MFP front panel. Press **OK** on that page and your camera will automatically open (note: the first time, you will be asked to allow the Synappx Go app to access your camera).



3:20

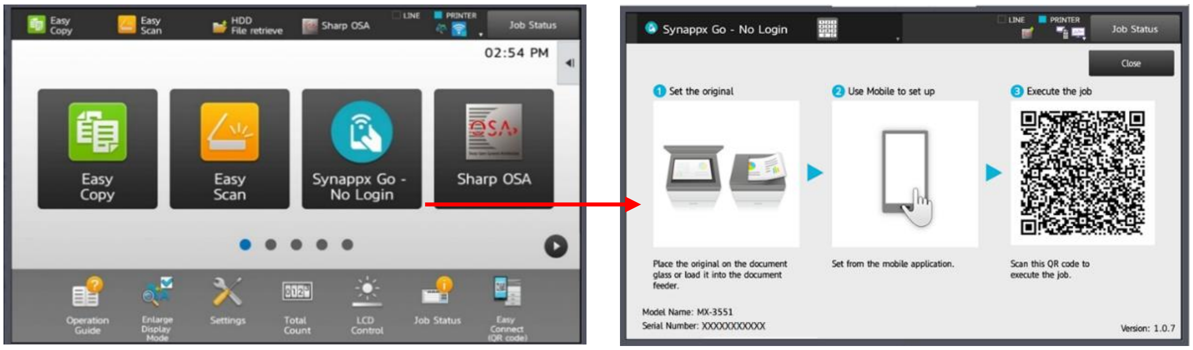
Scan

Scan QR code on MFP Display

○ Don't ask again

6.

7. Point your phone at the MFP Synappx QR code. Depending on the MFP model, you may have to select the **Synappx Go – No Login** button or **Advanced** button, then **Synappx Go – No Login** button on the front panel before the QR code is displayed. Note: In the future, some models will be configurable so QR codes can be shown on the MFP home screen (with no touch required).



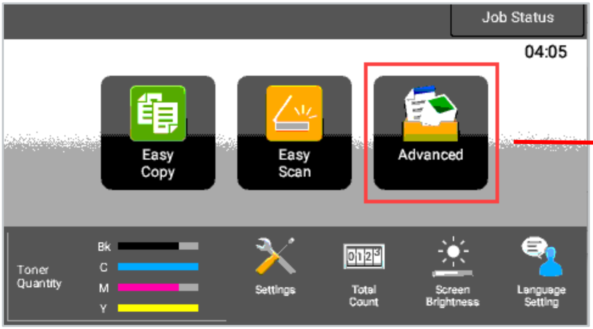
1 Set the original — Place the original on the document glass or load it into the document feeder.

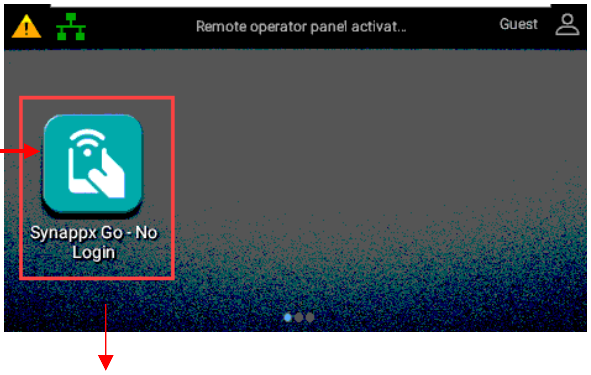
2 Use Mobile to set up — Set from the mobile application.

3 Execute the job — Scan this QR code to execute the job.

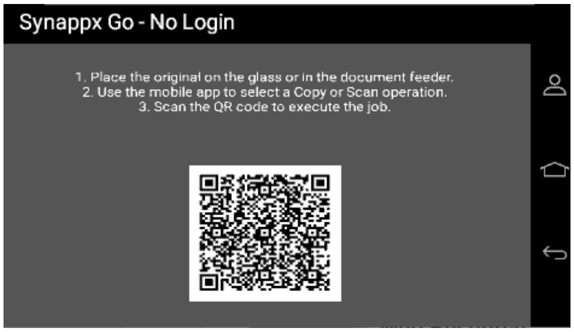
Model Name: MX-3551
Serial Number: XXXXXXXXXXX
Version: 1.0.7

On Supported Sharp A3 Models



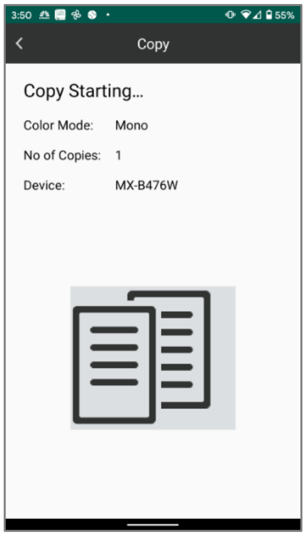


On Supported Sharp A4 Models


Synappx Go - No Login

1. Place the original on the glass or in the document feeder.
2. Use the mobile app to select a Copy or Scan operation.
3. Scan the QR code to execute the job.

8. When the mobile camera captures the QR code image, MFP will start to copy and you will see the success screen. The app returns to the home page. Note: You need to scan the QR code again is you want to copy another document.



Copy

Copy Starting...

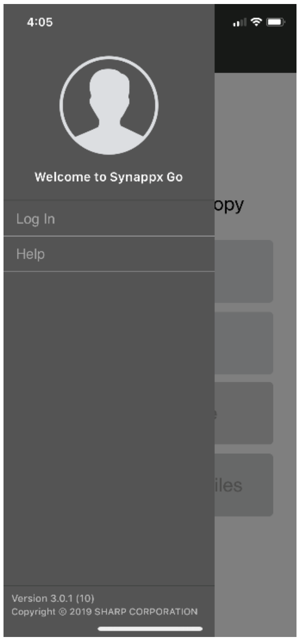
Color Mode: Mono

No of Copies: 1

Device: MX-B476W

Upgrading to Licensed Synappx Go App

You can easily upgrade from the unlicensed version to the more featured, licensed Synappx Go app once you have a license and your Admin has completed the full Synappx Go system configuration. After that Admin set-up, simply go to **Settings** (upper left corner) and select **Log In.**



You will be prompted to enter your normal user log in credentials. Once confirmed, you will have access to full Synappx Go features. See sections above for details.

Appendix A: Windows Defender Firewall Configuration

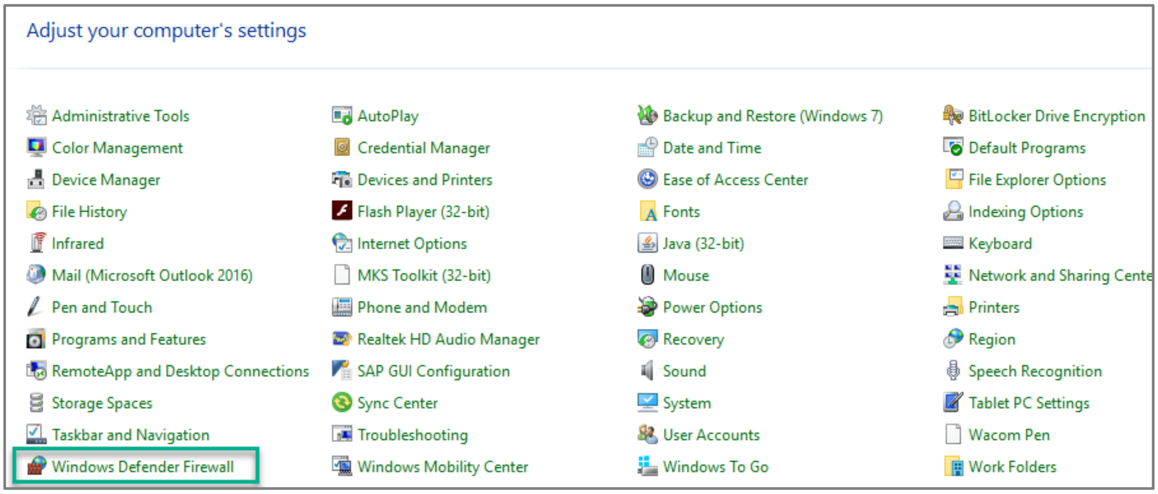
Background

If print jobs are not received by the MFP agent PC, it may be necessary to open either or both inbound port(s) 9100 and 515 on the MFP agent server by creating rules on the machine's Windows firewall.

Note: From version 2.0, the agent automatically opens the inbound port as part of the installation.

The following procedure uses Windows 10 as an example if manual port opening is required.

1. Launch the **Windows Defender Control Panel**. Then launch the **Windows Firewall** applet.



Adjust your computer's settings

Administrative Tools
Color Management
Device Manager
File History
Infrared
Mail (Microsoft Outlook 2016)
Pen and Touch
Programs and Features
RemoteApp and Desktop Connections
Storage Spaces
Taskbar and Navigation
Windows Defender Firewall

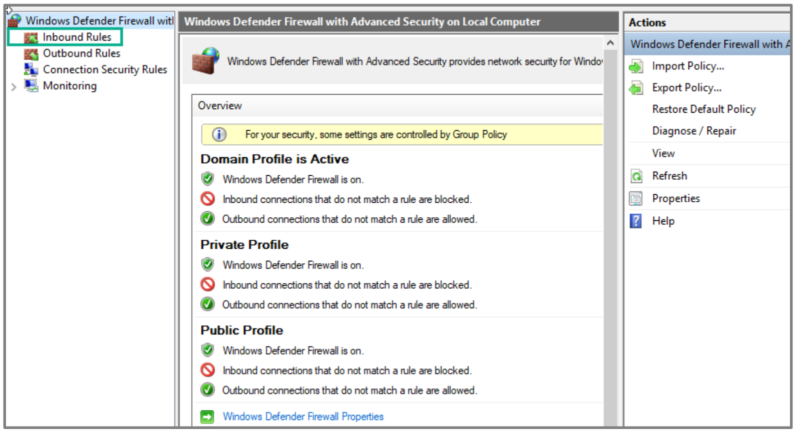
AutoPlay
Credential Manager
Devices and Printers
Flash Player (32-bit)
Internet Options
MKS Toolkit (32-bit)
Phone and Modem
Realtek HD Audio Manager
SAP GUI Configuration
Sync Center
Troubleshooting
Windows Mobility Center

Backup and Restore (Windows 7)
Date and Time
Ease of Access Center
Fonts
Java (32-bit)
Mouse
Power Options
Recovery
Sound
System
User Accounts
Windows To Go

BitLocker Drive Encryption
Default Programs
File Explorer Options
Indexing Options
Keyboard
Network and Sharing Cente
Printers
Region
Speech Recognition
Tablet PC Settings
Wacom Pen
Work Folders

2. The main **Windows Defender Firewall** interface is shown below. Select **Advanced Settings**.

3. The **Advanced Security** window will pop up. Select **Inbound Rules**. The goal is to allow inbound TCP traffic to the MFP agent on either or both ports 9100 and 515. This allows print jobs to be sent securely and held at the MFP agent until they are released for printing by the Synappx Go mobile app.



Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

For your security, some settings are controlled by Group Policy

Domain Profile is Active

Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile

Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Public Profile

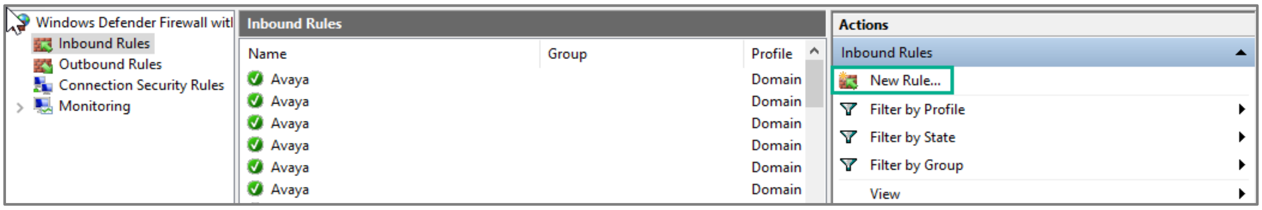
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

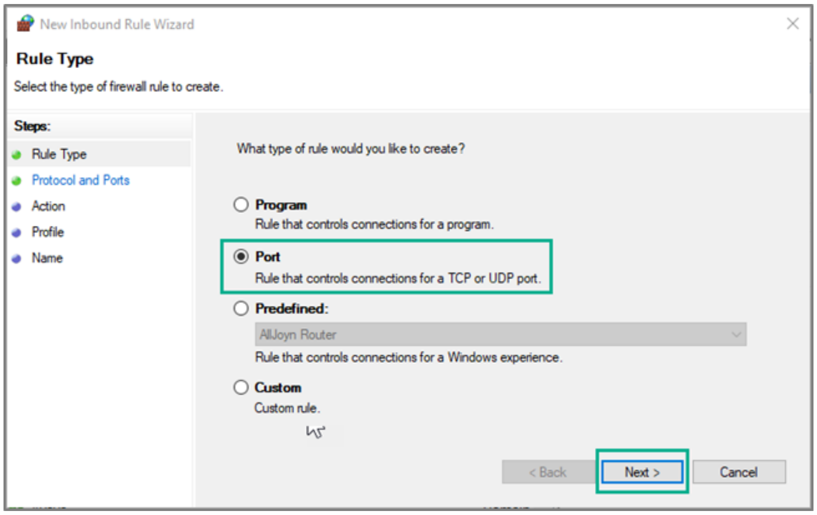
Actions

Windows Defender Firewall with A
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

4. Select the **New Rule** option on the **Actions** pane at the far right.



5. The **Rule Type** window will pop open. Select the **Port** rule type. Then select **Next.**


New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

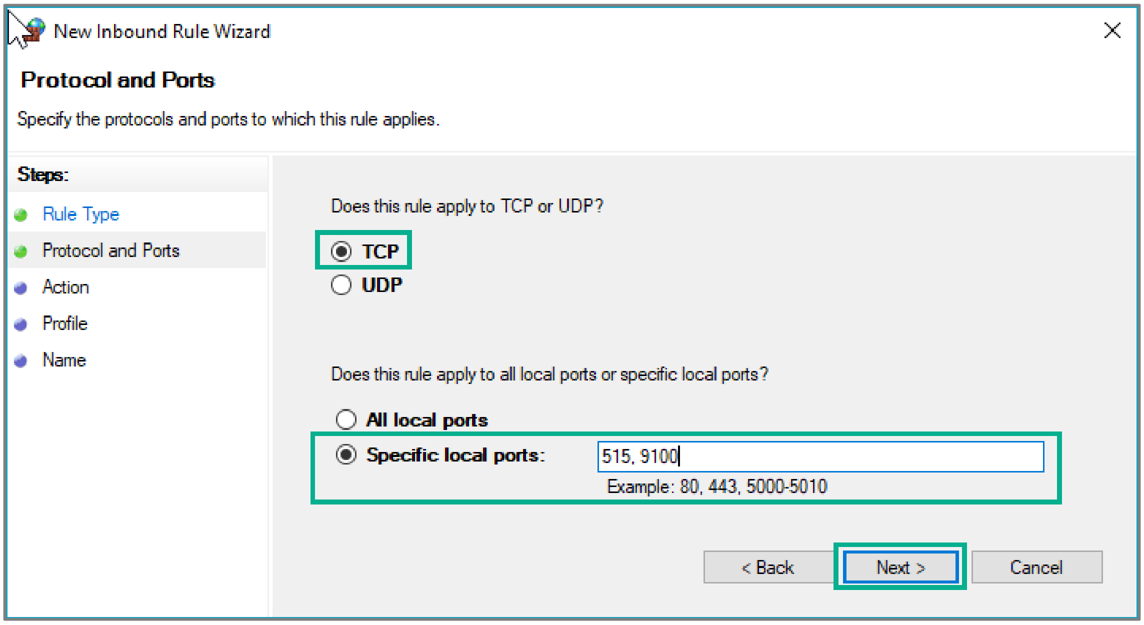
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

< Back | Next > | Cancel

6. On the Protocol and Ports window, select the **TCP** option and then select the **Specific local ports** option. In the adjacent field, enter the port(s) you wish to open for traffic.


New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

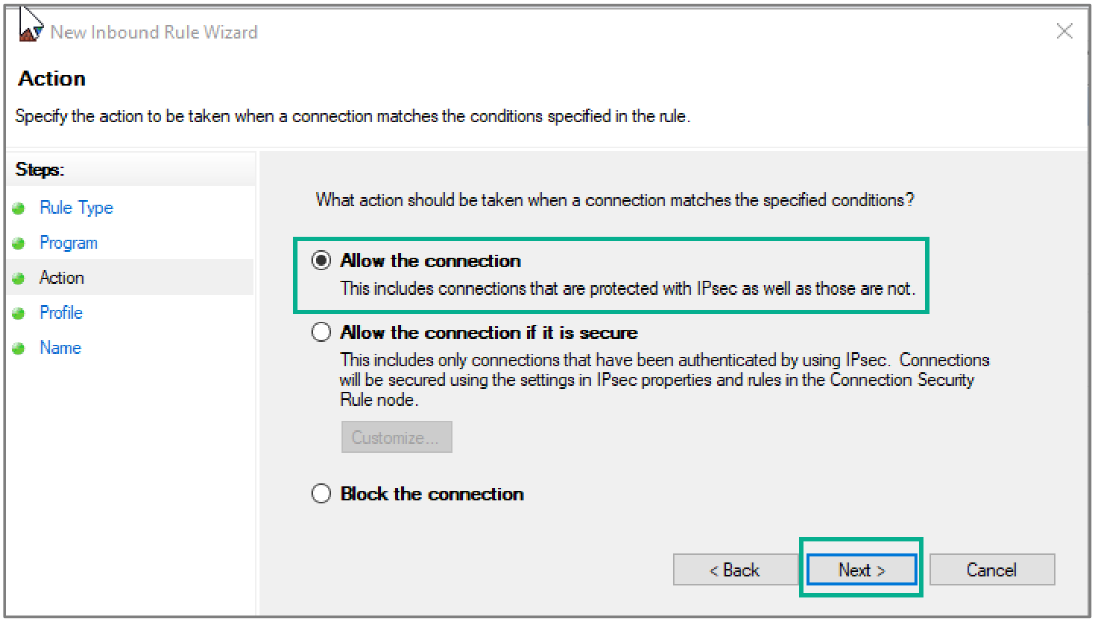
Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 515, 9100
Example: 80, 443, 5000-5010

< Back | Next > | Cancel

You can select 9100 (RAW), 515 (LPR) or both. The example below uses both ports. Select **Next** when finished.

7. Select **Allow the connection** and then select **Next.**



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

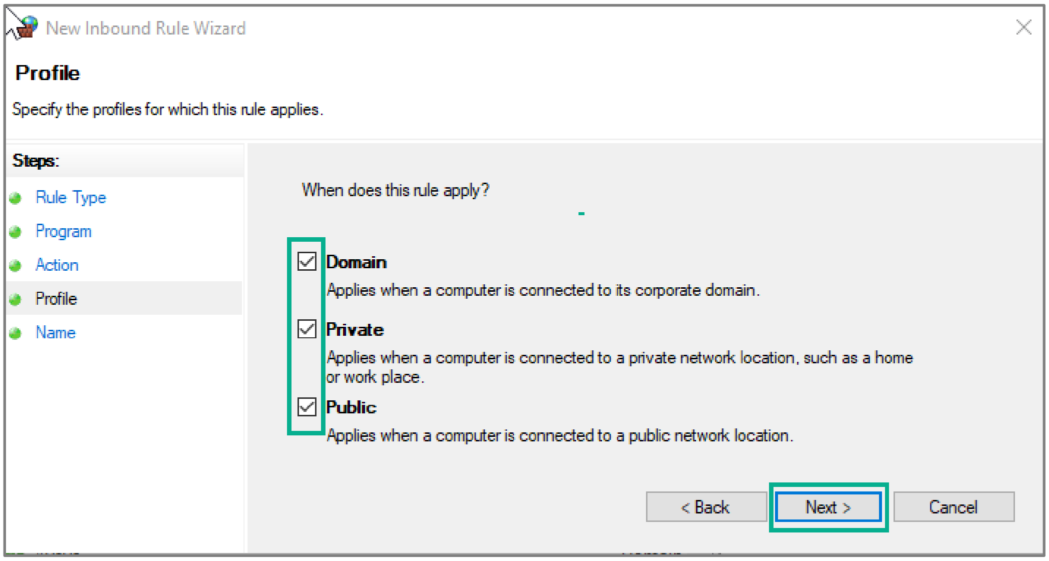
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

8. In the **Profile** window, select one or more of the available options. In most cases, selecting **Domain** should suffice. Then click **Next**.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

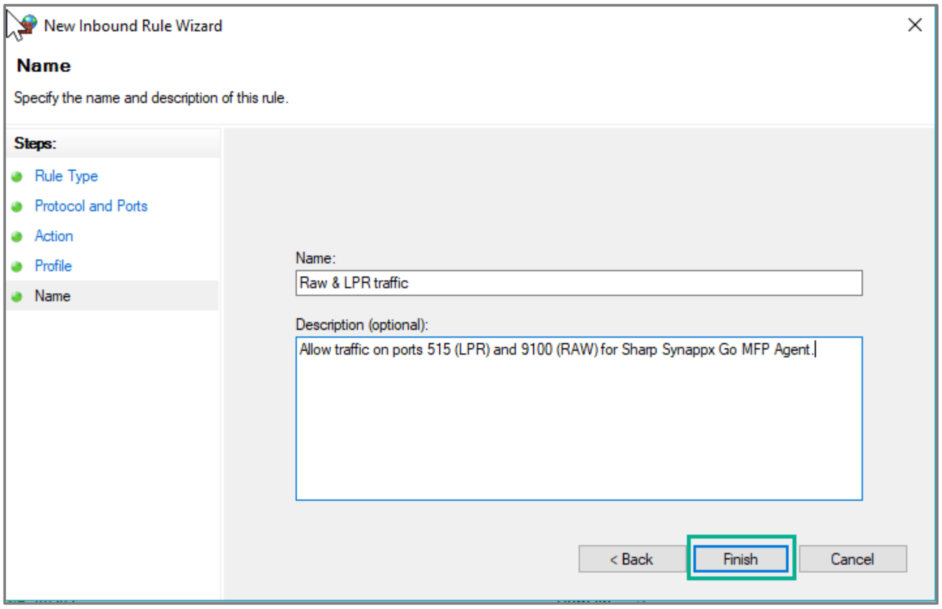
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

9. Give the rule a convenient **Name** and **Description** and then click **Finish**.



New Inbound Rule Wizard

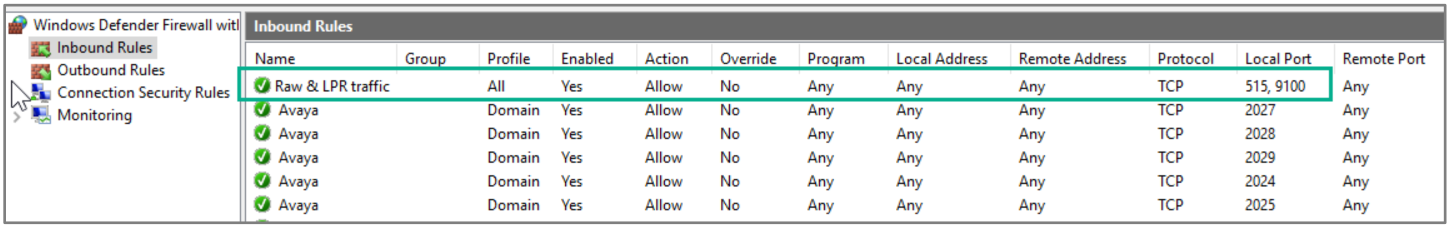
Name

Specify the name and description of this rule.

Name:
Raw & LPR traffic

Description (optional):
Allow traffic on ports 515 (LPR) and 9100 (RAW) for Sharp Synappx Go MFP Agent.

10. The rule is enabled by default, as shown below. You may now close the **Windows Defender Firewall** applet.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
✓ Raw & LPR traffic		All	Yes	Allow	No	Any	Any	Any	TCP	515, 9100	Any
✓ Avaya		Domain	Yes	Allow	No	Any	Any	Any	TCP	2027	Any
✓ Avaya		Domain	Yes	Allow	No	Any	Any	Any	TCP	2028	Any
✓ Avaya		Domain	Yes	Allow	No	Any	Any	Any	TCP	2029	Any
✓ Avaya		Domain	Yes	Allow	No	Any	Any	Any	TCP	2024	Any
✓ Avaya		Domain	Yes	Allow	No	Any	Any	Any	TCP	2025	Any

Appendix B: Synappx Go Automatic Input Switch

Synappx Go automatic input switching helps users quickly access Go-enabled Sharp interactive whiteboard (IWB) displays. Once boards are configured, users do not need to manually change the display input to share content or use the Meet feaatures. In many cases, users do not know the correct input for the display PC or may not be able to find the remote. Setting the default input from this page can also automatically return the display to it's default condition after collaboration including after completion of meetings through use of the Synappx Go Meet feature. This time-saving auto input feature also minimizes contact with display equipment.

Overview

1. Configure supported IWBs for Telnet over LAN or RS-232C auto-input switching
2. Configure Admin Portal display settings, including the auto-input port for display PCs
3. Configure default input for display PCs
4. Automatic input switch usage

Preconditions for Go Auto-Input Switch Configuration

- Administrator has administrative permission to make changes to supported display devices
- Go display agents V2.2 or later are installed, updated, and associated to workspaces (Admin Portal)
    - NFC tag association with the display can be completed after display information page setup but must be done before users access Synappx Go
- Users have Go version 2.2 (or later)
- Users who use the Synappx Go and Meeting combined Meet features must update the Go agent version 3.0

Note: If Go agent displays are not configured for auto-input switching (default), users must change the display manually if not on the correct input. If agent displays are not configured with a default input, users would manually switch the input (if different than the PC input) after collaboration.

Step 1: Configure Interactive Whiteboards

Note: See the display manual for details on your specific model.

There are two options for configuring auto-input switching on supported Sharp displays. Telnet over LAN is recommended because it does not require a physical cable. If your display does not support telnet, use RS-232C, which is available across all display models.

Supported IWB Models and Input options

LAN Telnet Supported	Inputs											Power Controls	
Model	HDMI 1	HDMI 2	HDMI 3	Display 1	Display 2	DSUB	DSUB 1	DSUB 2	Wireless	Application	Option	Power ON	Power OFF
PN-L401C/ PN-L501C	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	N/A	N/A	OK	OK
PN-L651H	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	OK	N/A	OK	OK
PN-L751H/ PN-L851H	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	OK	N/A	OK	OK

RS-232 Supported		Inputs											Power Controls	
Model	Display Gender	HDMI 1	HDMI 2	HDMI 3	Display 1	Display 2	DSUB	DSUB 1	DSUB 2	Wireless	Application	Option	Power ON	Power OFF
PNL-C751H	Male (#1)	OK	OK	OK	N/A	N/A	OK	N/A	N/A	N/A	OK	N/A	OK	OK
PN-C861H	Female (#1, 2)	OK	OK	OK	N/A	N/A	OK	N/A	N/A	N/A	OK	N/A	OK	OK
PN-CE701H	Female (#1, 2)	OK	OK	OK	N/A	N/A	N/A	OK	OK	OK	OK	N/A	OK	OK
PN-L401C/ PN-L501C	Male (#1)	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	N/A	N/A	OK	OK
PN-L651H	Female (#1, 2)	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	OK	N/A	OK	OK
PN-L751H/ PN-L851H	Female (#1, 2)	OK	OK	N/A	OK	N/A	OK	N/A	N/A	OK	OK	N/A	OK	OK

#1 Male to USB cable: StarTech.com ICUSB232SM3 USB to Serial Adapter - Prolific PL-2303 - 3 ft / 1m - DB9 (9-pin) - USB to RS232 Adapter Cable - USB Serial

#2 Gender changer: StarTech.com GC9SF Slimline DB9 Serial Gender Changer - F/F

General Display Configuration Notes

- The Go display agent and display must be on a network where they can communicate directly.
- In power save mode, the monitor may not wake up as LAN is turned off (default setting).
- For models PN-L651H and PNL-C751H, the input switch command is not accepted for up to a minute after power on. The switching command will not work on initial power-on because the switch command is sent after power-on.
- It is not recommended to use the Crestron® control interface and Go auto-input switch at the same time. Since both options can change inputs dynamically, the results may not be as expected.
- On some models, Consumer Electronics Control (CEC) can be enabled for automatic switching when a device is connected to the display. This may cause unexpected results as the display will switch away from the original view. In that case, disable the CEC feature for auto-switch use.

If you encounter display configuration issues, go to Troubleshooting Tips and/or check with your display integrator for configuration support.

Telnet over LAN

Notes

- Most models require a user and password for access to remote commands.
- Multiple telnet sessions at once are not supported. There is a setting for logging off a current session that defaults to five minutes.

Check your display operation manual for **Controlling the Monitor with a Computer (LAN)**. On most models, the settings are accessible from the menu on the remote or application screen.

1. Ensure the display is configured with a static IP Address.
2. Go to **Settings** > **Communication** or **Setup Ethernet (LAN)** (applicable to most models).
   Most models require either LAN or RS-232C as a selection in the display menu.
3. Ensure the telnet server is set to **On** and create a user and password (this can be different from the admin user on the board).
4. For displays supporting **Application mode**: Go to the display board and select **Application Input** on the screen.
5. Open the **Settings/Setup** menu.
6. Configure settings to use a Telnet server:
   - Telnet Server .... When using Telnet Server function, set to ON
   - Username ....Set an account name when connecting to this display
   - Password...............................Set a password when connecting to this display

Make note of the display IP address, port number (default is 10008), username and password (if set), and the input port to be configured for use with the display PC. This information is necessary when completing the display information setup on the Synappx Go Admin Portal.

RS-232C

Notes

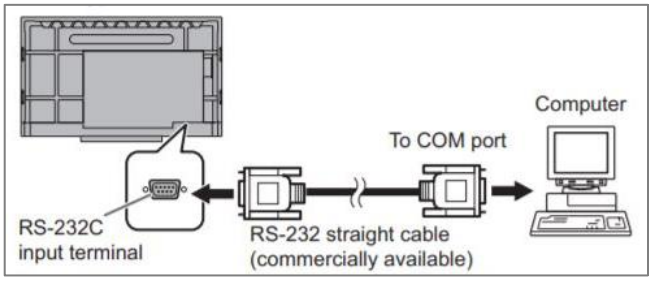
- RS-232 cable gender varies on models. Do not use a null modem cable. Auto-input switching will not work with a null model cable.
- Note all relevant display settings before completing the auto-input switch configuration on the Synappx Go Admin Portal.

1. Read the display operation manual for **Controlling the Monitor with a Computer (RS-232C).**

Note: Computers without serial ports may require USB-to-serial converters to allow compatibility with RS-232 serial devices. Before obtaining a USB connector, note the RS-232C (9-

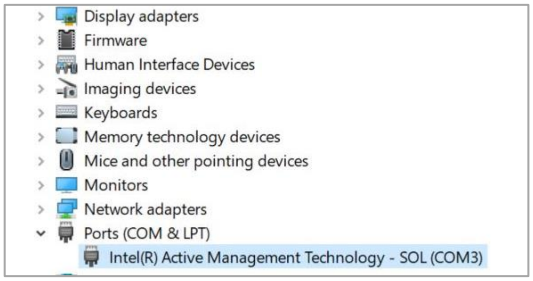
pin) connector on your display (connector gender varies). Note the cable recommendations in the Supported IWB Models and Input Options table.

2. Ensure all RS-232 cables are connected securely to the display board, ideally using the provided screws.



Note: There may be more than one COM port on the agent PC.

3. In Windows®, go to **Device Manager** to confirm the port that the agent PC is using to communicate with the Display (e.g. COM3, COM5).



4. On some models, the RS-232C settings are accessible from the menu on the remote or display application screen. Go to **Settings > Communication** or **Setup Ethernet (LAN)**. Switch to **RS-232C**.
5. For displays supporting **Application** mode, select the **Application** input. Open the **Settings/Setup** menu on the display.
6. Note the baud rate on your display. Some displays have a fixed baud rate (e.g. 9600) while others allow it to be configured. The settings in the Admin Portal must match the display settings for com port and baud rate.

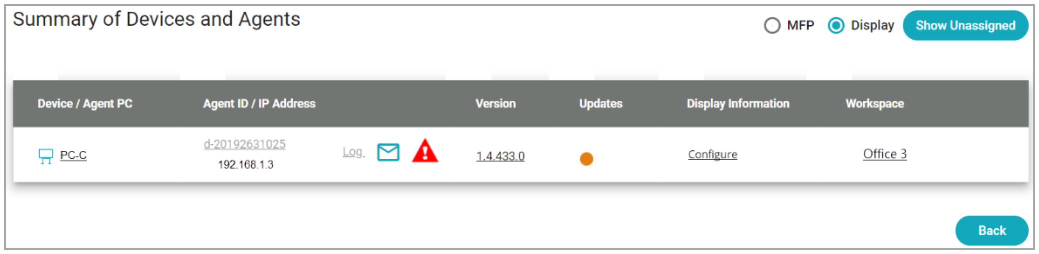
Step 2: Configuring the Admin Portal

Notes:

- Display information setup is only required for Go users to leverage auto-input switching or default input.
- Display agents must already be installed and configured with Synappx Go workspaces before configuring displays for auto-input switch on the admin portal.

1. Log in to the Synappx Admin Portal with your Microsoft® 365 or Google Workspace™ credentials.
2. If both Synappx Go and Meeting are licensed, choose **Synappx Go**.
3. Go to **Workspaces**.

4. Select **Devices & Agents**.
5. Select the **Display** radio button. The **Summary of Devices and Agents** display page will show all configured display agents.



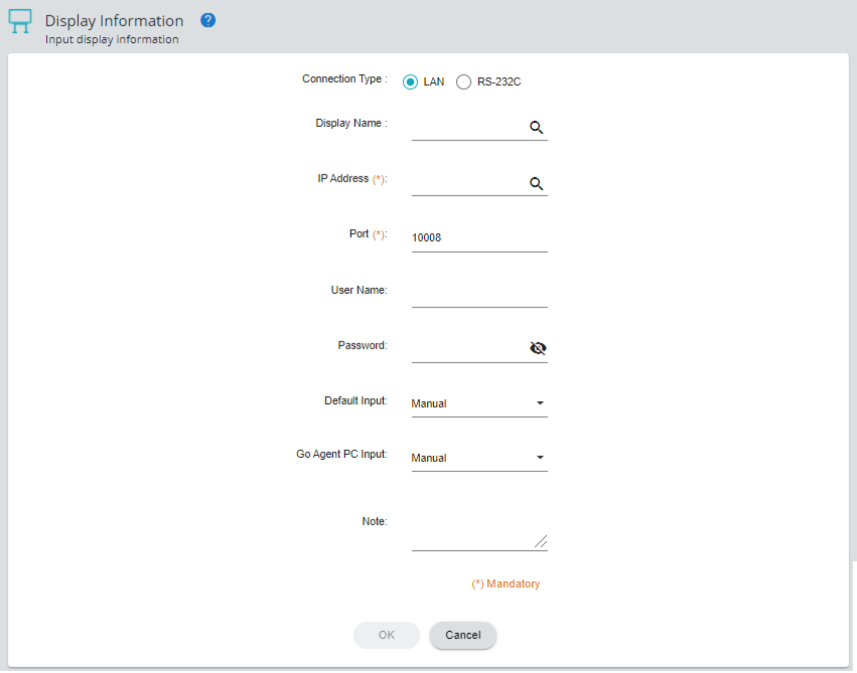
Summary of Devices and Agents

○ MFP ● Display **Show Unassigned**

Device / Agent PC	Agent ID / IP Address		Version	Updates	Display Information	Workspace
PC-C	d-20192631025 192.168.1.3	Log.	1.4.433.0	●	Configure	Office 3

Back

6. To set up auto-input switching information for each display, select **Configure** in the **Display Information** column. A dialog box will open.
7. Be sure to choose the connection type: **Telnet LAN** or **RS-232C**. Enter the relevant information for the display including **Go Agent PC Input** (for auto switching when Synappx Go is used) and **Default Input** (to return display input to default after collaboration).
8. Select **OK** to save the settings. Auto-input switching and Default Input are now available for Go users.



Display Information

Input display information

Connection Type : ● LAN ○ RS-232C

Display Name :

IP Address (*):

Port (*): 10008

User Name:

Password:

Default Input: Manual

Go Agent PC Input: Manual

Note:

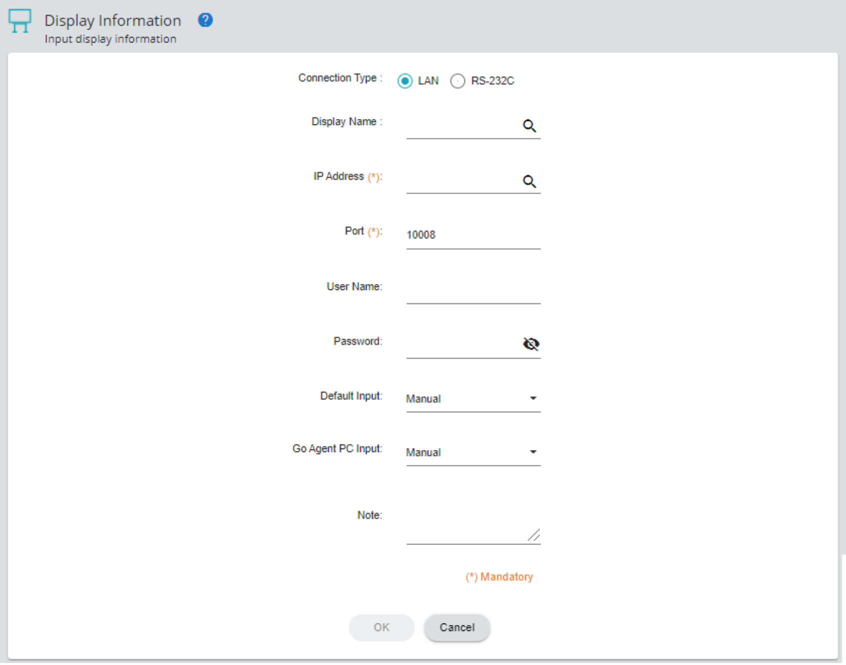
(*) Mandatory

OK Cancel

LAN Configuration

1. **Display Name** (optional): Enter an alias for the workplace display or use the display search feature.
2. **IP Address** (required): Enter the display IP address or use the display search feature.
3. **Port** (required): The default is 10008.
4. **User Name** (optional): This field is only required if the display is configured with a username and password.
5. **Password** (optional): This field is only required if the display is configured with a username and password.

6. **Default Input** (optional): This field is only required if a default display input is desired. The default setting is Manual (no return to default input). Select the arrow to choose the desired default display input (e.g. HDMI 2). At the end of the collaboration, the user can automatically restore the display to the default input via Go mobile.
7. **Go Agent PC Input** (required): The default setting is **Manual** (auto-input switch not configured). Select the arrow to choose the display PC input (e.g. HDMI 1) where the Synappx Go agent is installed. When a user taps the display NFC tag, the display will switch to the selected input automatically.
8. **Note** (optional): Add applicable notes.



Display Information
Input display information

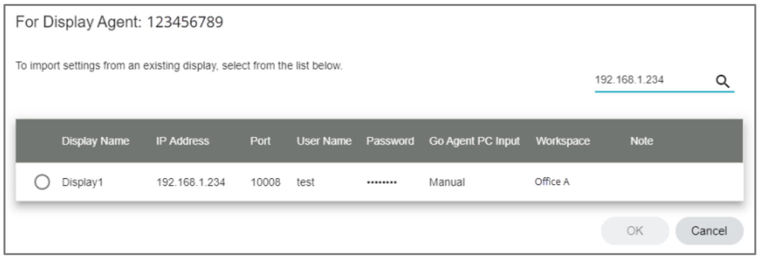
Connection Type : ● LAN ○ RS-232C
Display Name :
IP Address (*):
Port (*): 10008
User Name:
Password:
Default Input: Manual
Go Agent PC Input: Manual
Note:

(*) Mandatory

Display Search

The **Display Name** or **IP Address** search icon 🔍 can be used to look up information on an existing display and leverage those display settings (avoids re-entry if display is already configured).

1. Type a display name or IP address up to the second dot or more (e.g. 172.29.) and select the search icon 🔍 to see a list of devices matching the display name or IP address fields.
2. Select a display from the list. Select **OK** to auto-populate the information into the **Display Information** box. Information can be edited after populating.
3. Select **OK** to save the display settings.



For Display Agent: 123456789

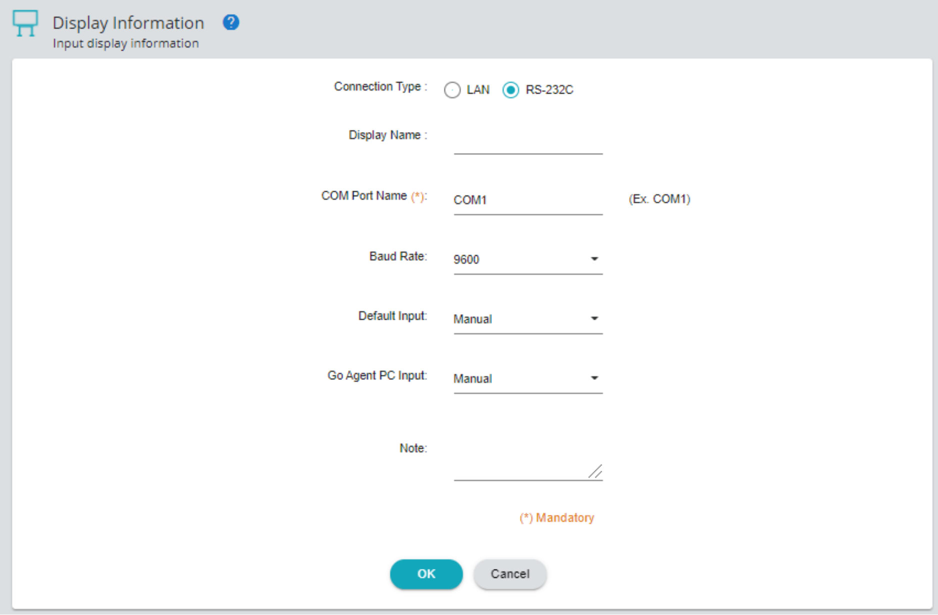
To import settings from an existing display, select from the list below.

192.168.1.234

	Display Name	IP Address	Port	User Name	Password	Go Agent PC Input	Workspace	Note
○	Display1	192.168.1.234	10008	test	••••••••	Manual	Office A	

RS-232C Configuration

1. **Display Name** (optional): Enter an alias for the workplace display.
2. **COM Port Name** (required): Enter the display COM port name. The default is **COM1**.
3. **Baud Rate** (optional): The default is 9600. Select the arrow to choose the value that matches the display baud rate.
4. **Default Input** (optional): This field is only required if a default display input is desired. The default setting is Manual (no return to default input). Select the arrow to choose the desired default display input (e.g. HDMI 2). At the end of the collaboration, the user can automatically restore the display to the default input via Go mobile.
5. **Go Agent PC Input** (required): The default setting is **Manual** (auto-input switch not configured). Select the arrow to choose the display PC input (e.g. HDMI 1) where the Synappx Go agent is installed. When a user taps the display NFC tag, the display will switch to the selected input automatically.
6. **Note** (optional): Add applicable notes.



Display Information

Input display information

Connection Type : ○ LAN ● RS-232C

Display Name :

COM Port Name (*): COM1 (Ex. COM1)

Baud Rate: 9600

Default Input: Manual

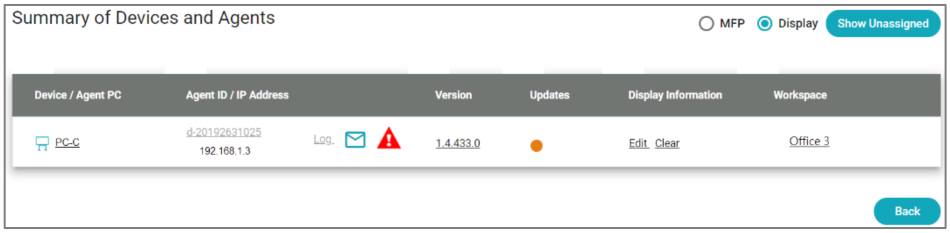
Go Agent PC Input: Manual

Note:

(*) Mandatory

Editing or Clearing Display Information

After configuring display information, the choices in the **Display Information** column change to **Edit** and **Clear**. Select **Edit** to review or change any of the settings.

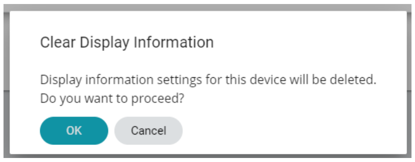


Summary of Devices and Agents

○ MFP ● Display

Device / Agent PC	Agent ID / IP Address		Version	Updates	Display Information	Workspace
PC-C	d-20192631025 192.168.1.3	Log	1.4.433.0	●	Edit Clear	Office 3

Select **Clear** to remove the display information settings associated with the display agent. A dialog box will appear to confirm information deletion. Select **OK** to clear all display information.

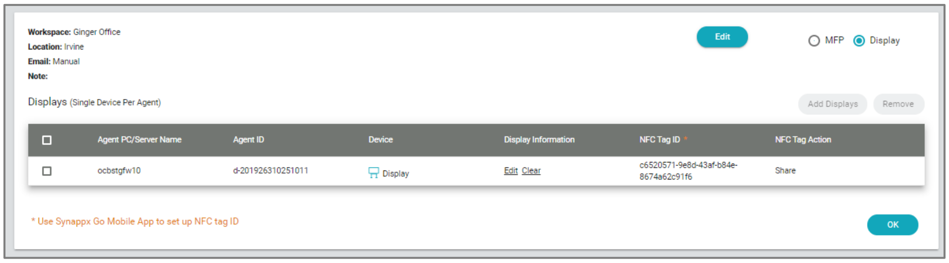


Clear Display Information

Display information settings for this device will be deleted. Do you want to proceed?

The **Display Information** column option will change back to **Configure** once information is removed.

Display information can also be configured, edited, or cleared from the **Workspace Display** page.



Workspace: Ginger Office
Location: Irvine
Email: Manual
Note:

Displays (Single Device Per Agent)

□	Agent PC/Server Name	Agent ID	Device	Display Information	NFC Tag ID *	NFC Tag Action
□	ocbstgfw10	d-201926310251011	Display	Edit Clear	c6520571-9e8d-43af-b84e-8674a62c91f6	Share

* Use Synappx Go Mobile App to set up NFC tag ID

Automatic Input Switch Usage

Once display and Admin Portal configuration are complete, the feature is ready for Go users.

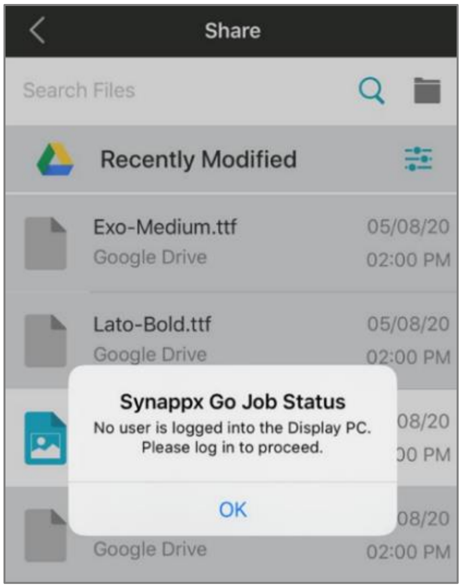
Auto input switching is supported in the following environments:

- Display and Display PC are powered on, PC and display are not sleeping:
    - Display PC is already logged in (no user login is required to access display PC)
    - Display PC is not already logged in, requires user to log in to gain PC/network access (user will be prompted after auto-input switch)
- Display is powered on but is in sleep mode
    - If the display is in power save or sleep mode, touch the display or use the remote or power button, then tap the NFC tag.
- Display PC is powered on but is in sleep mode
    - If the display PC is in sleep mode, touch the keyboard, then tap the NFC tag.

The NFC tap initiates auto-input switching if the display is not already on the defined Go agent PC input. Both tap first and tap last (i.e., foreground and background operation) are supported.

For background operation (tap first), auto-switching is enabled and multiple files can be shared. However, if someone changes to another input, the user will have to tap the NFC tag again to auto-switch back to the correct input to share additional files.

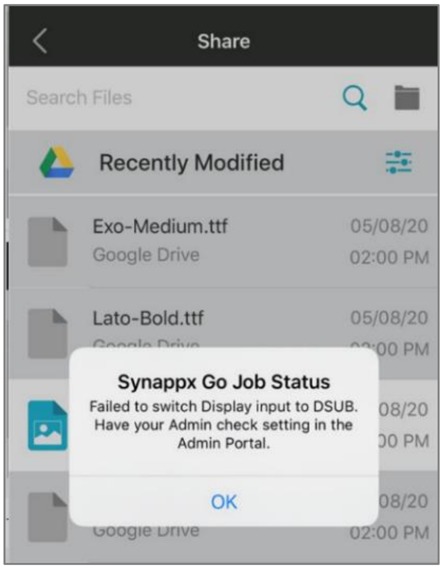
If the display PC is not logged in, a message will appear prompting the user to log in with their Microsoft or Google Workspace credentials. Go files can then be shared to display by that user and other Go mobile users.



Synappx Go Job Status

No user is logged into the Display PC. Please log in to proceed.

If an error occurs, the user must switch the input manually and contact the administrator.



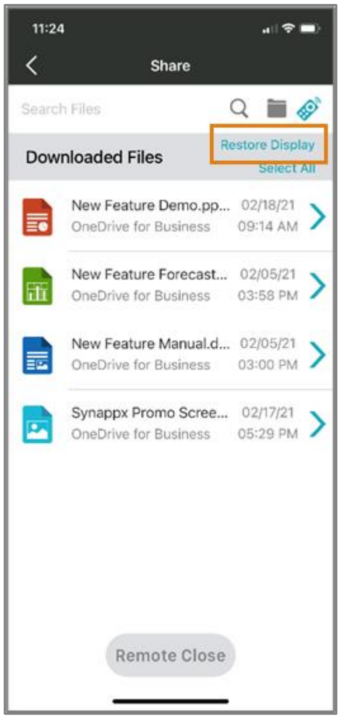
Synappx Go Job Status

Failed to switch Display input to DSUB. Have your Admin check setting in the Admin Portal.

Return to Default Input Usage

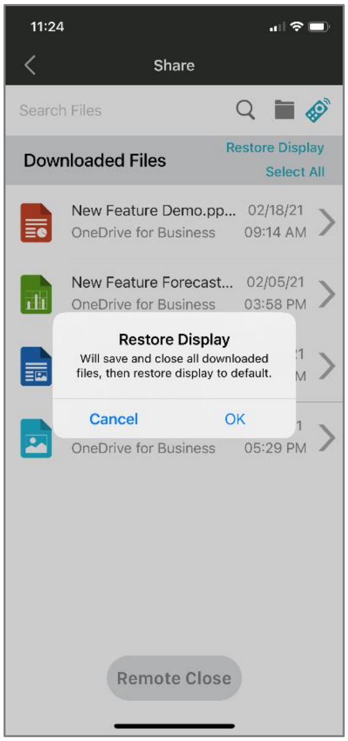
Once display and Admin Portal configurations are complete, the return to default input feature is ready for Go users. See the Synappx Go User Guide for more details.

1. After files are downloaded via Go Share operations (for viewing or remote operations), at the end of the Share collaboration, the Synappx Go user can select **Restore Display**.


11:24
Share
Search Files
Downloaded Files
Restore Display
Select All
New Feature Demo.pp... 02/18/21
OneDrive for Business 09:14 AM
New Feature Forecast... 02/05/21
OneDrive for Business 03:58 PM
New Feature Manual.d... 02/05/21
OneDrive for Business 03:00 PM
Synappx Promo Scree... 02/17/21
OneDrive for Business 05:29 PM
Remote Close

2. A message will confirm that all downloaded files will be saved and the display input will be returned to default.

   Note: If default display has not been set, user will receive an error message and request to have default input set. User can stilluse normal remote close operations to close and save downloadable files.


Restore Display
Will save and close all downloaded files, then restore display to default.
11:24
Share
Search Files
Downloaded Files
Restore Display
Select All
New Feature Demo.pp... 02/18/21
OneDrive for Business 09:14 AM
New Feature Forecast... 02/05/21
OneDrive for Business 03:58 PM
Cancel
OK
OneDrive for Business 05:29 PM
Remote Close

Note: The V3.0 combined Synappx Go and Synappx Meeting experience benefits from configuration of the the automatic return to default input feature and is strongly recommended.

Troubleshooting Tips

1. Verify the Synappx Admin Portal settings on the display match the display setup.
2. Ensure the display agent is online and communicating with the Synappx Admin Portal.

Telnet over LAN

1. Ensure the display board has a static IP address.
2. Follow the manual instructions for the display to enable telnet commands (the agent uses telnet commands to switch the input).
3. Verify that the display agent can communicate directly with the display board using ping or a similar tool. The agent PC should be able to ping the display board.
4. Try to open a telnet session from the agent PC using the username and password. (Windows 10 has telnet installed, but it may need to be enabled). Be sure to use the correct port to connect. Port 10008 is the default on Sharp monitors, but it is not the default telnet port.

RS-232C

1. Connect the display agent PC to the board with the proper serial connector securely fastened.
2. Follow the board manual instructions to enable RS-232C commands.
3. Verify the communication port used on the agent PC.
4. Ensure the serial connector or cable is correct. The cable must be a straight through cable, not a null modem or crossover cable. Avoid cables with chipsets. There are adapters available to change the gender of the serial connection. Ensure the adapter itself is not a null modem adapter (sometimes called a crossover).
5. Verify the baud rate. The Admin Portal must match the board's configured rate or the inputs will not switch.

This page is intentionally left blank.

SYNAPPX™

For more information, visit the Synappx support site.

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

entities in the United States and other countries. wePresent® and MirrorOp® are registered trademarks or trademarks of Barco Inc. ZOOM is a trademark of Zoom Video Communications, Inc. All other trademarks are the property of their respective holders.