

SHARP®

SYNAPPX™



SYNAPPX™ GO

PRODUCTIVITY WHEREVER YOU GO!

**ADMINISTRATOR SETUP
AND CONFIGURATION GUIDE**

Contents

- Synappx Go: Getting Started 4
 - Synappx Go Overview..... 4
- System Requirements 5
 - NFC Support..... 7
 - MFP Support 8
 - Display Support 9
- Synappx Go Setup and Configuration Overview 10
- How It Works..... 11
 - How to Get Started..... 11
 - Step 1: Choose Provider 11
- Synappx Admin Portal..... 12
 - Admin Portal for Microsoft 365..... 12
 - Admin Portal for Google Workspace™ 13
- Synappx Go Setup and Configuration..... 15
 - Step 2: Log In (First Time) to Admin Portal 15
 - Step 3: Configure and Download Agents 18
 - Step 4: Install Agents..... 20
 - System: Agent Updates, Admin Log, System Log, Check In Log (Optional during Setup).26
 - Step 5: Add Workspaces..... 31
 - Step 6: Associate Devices to Workspaces 36
 - Summary of Devices and Agents—Management..... 39
 - Step 7: Associate NFC Tags 43
 - Step 8: Add Users and Allocate Licenses 46
 - Step 9: Configure Print Release Driver and Share with Users 50
- Admin Settings (Optional)..... 53
- Analytics 57
- Appendix A: Windows Defender Firewall Configuration 59
- Appendix B: Synappx™ Go Automatic Input Switch..... 63
 - Overview..... 63
 - Automatic Input Switch Usage 71
 - Troubleshooting Tips 72

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, 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, and check-in tasks with the following features:

Easy Setup

- Follow the simple setup wizard—no training required!
- Create your own scan to email distribution lists right from your phone.
- Set default scan, print, and copy settings to save time.

Scan

- Tap your phone to scan a file to
 - Yourself (via email)
 - Email distribution lists
 - 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.

Share

- Tap the NFC tag to display content on the Sharp display.
- Team members can also tap 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.

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.

System Requirements

Synappx Go Major Components	
1. Mobile Application (iOS and Android™)	4. Admin Portal
2. NFC Tags	5. Cloud System (Microsoft® Azure)
3. MFP and Display Agents	

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




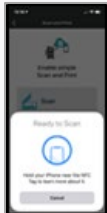



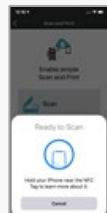
*This package offers only the web or mobile version of Microsoft Office applications. Synappx Go requires Office applications to be installed on the display PC for full functionality. Otherwise, the file will open in the web browser.

Users and Admins
<ul style="list-style-type: none"> • Supports 5,000 users • All users must: <ul style="list-style-type: none"> ○ Have Microsoft 365 or Google Workspace accounts ○ Be in Microsoft Azure Active Directory (AD) or Google Workspace Directory • First administrator to log in requires Azure AD or Google Workspace admin privileges

Supported Mobile Platform
Apple® iPhones®: NFC support, iOS 12 or later <ul style="list-style-type: none"> • 7/7+, 8/8+, X, XR, XS, XS Max, iPhone 11, 11 Pro, 11 Pro Max, and iPhone SE (Second Generation - 2020)
Android™ <ul style="list-style-type: none"> • 8 to 11, NFC support

MFP Agent	Display Agent
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	
<ul style="list-style-type: none"> • Sharp-provided or in select MFP models • See NFC Support chart 	

NFC Support

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

Background

When you tap the NFC tag, the phone brings you directly to the Synappx Go app (without needing 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.

Copy is supported on models with OSA 5.5.

Teal model numbers have OSA 5.5 and can support the Synappx Go copy feature.

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

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

²Special firmware needed to enable TLS 1.2 support

³These models support the Synappx Go copy feature but require that the MX-AMX2L Application Communications Module (ACM) option be installed.

A4 Models	MX-B376W	MX-C557F¹	Printer Models	MX-C607P	MX-B427W
	MX-B476W	MX-C507F¹		MX-C507P	MX-B427PW
	MX-C303W²	MX-C407F¹		MX-C407P	MX-B467F
	MX-C304W	MX-C357F¹		MX-B707P	MX-B467P
	MX-B355W	MX-B707F¹		MX-B557P	
	MX-B455W	MX-B557F¹			

¹For 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.
- [Install the Synappx Go MFP app \(instructions here\)](#).
- Sharp UD 3 is a recommended driver for print release.

²These models support the Synappx Go copy feature 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.
 - 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

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
9. **Configure Print Release Driver**
 - Share configured print driver to users for the Synappx Go MFP agent

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)

Automatic Input Switch: Configure displays to switch to the display agent input automatically when using Share

How It Works

How to Get Started

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

Here's what happens next.



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



2. 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.



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

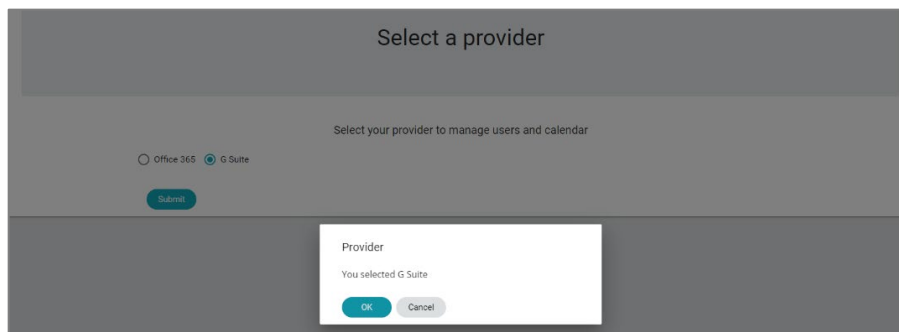
Step 1: Choose Provider

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

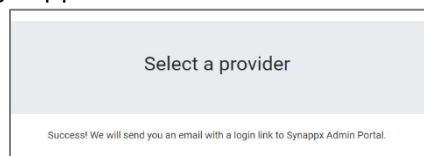
After a Synappx account is created for your organization, the assigned administrator will receive an email with a link to select either Microsoft 365 or Google Workspace as a cloud service provider. This provider defines how Synappx manages the users and calendar within the organization.

Here's how:

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



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



Synappx Admin Portal

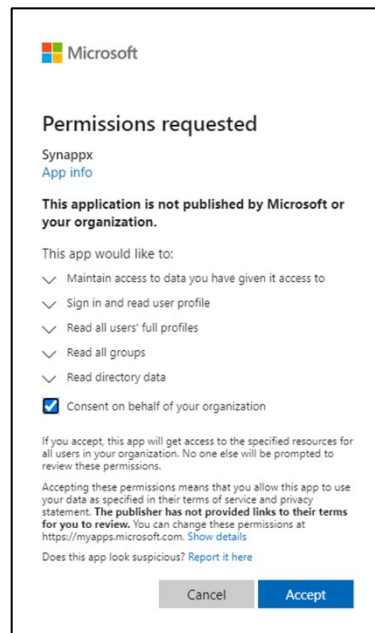
After selecting a provider (Microsoft 365 or G Suite), the administrator will receive a second email with a link to the [Synappx Admin Portal](#).

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.

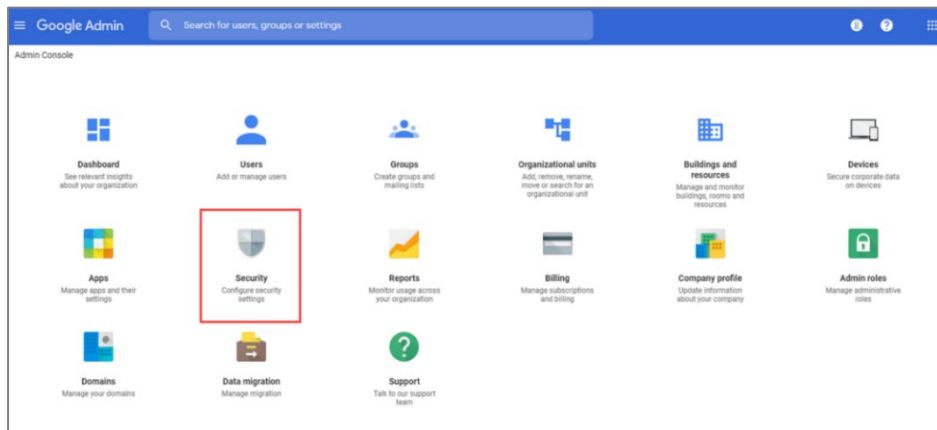
Select the link and log in with your Microsoft 365 credentials. At initial login, accept the permission request to allow Synappx apps to access selected Microsoft services on behalf of your organization.



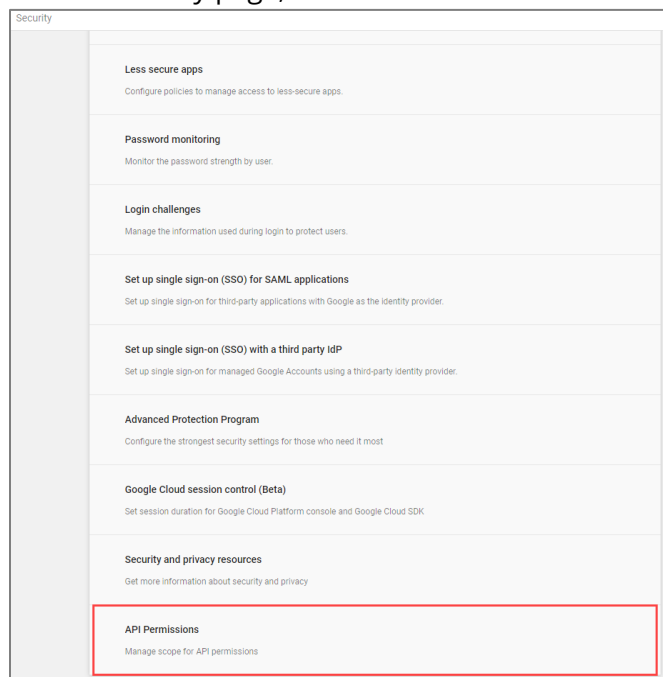
Admin Portal for Google Workspace™

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.

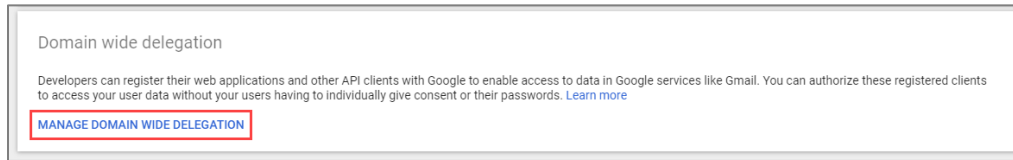
1. Select Google Workspace as your cloud service provider in the initial welcome email.
2. Upon receiving the second welcome email, follow the instructions to set up your Google Workspace Admin Console to communicate with Synappx.
 - a. In any web browser, go to admin.google.com.
 - b. Select **Security**.



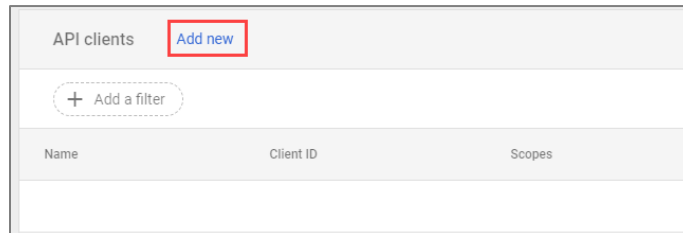
- c. On the Security page, select **API Permissions**.



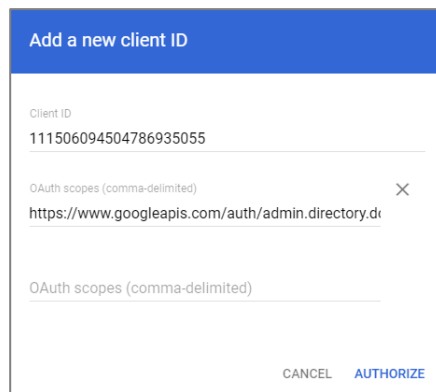
d. Select **Manage Domain Wide Delegation**.



e. Select **Add New**.



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



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

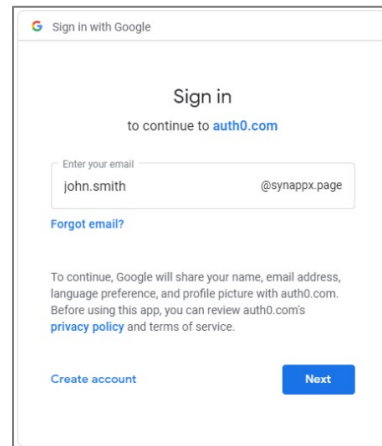
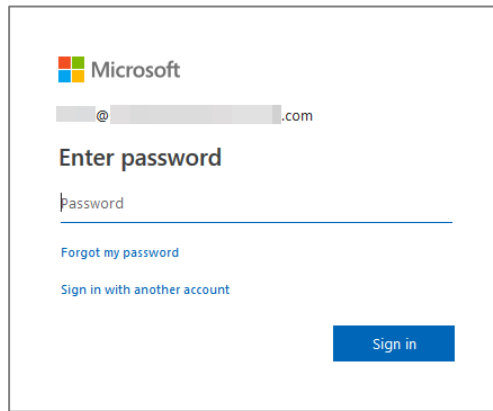
h. Open the second Synappx welcome email and select **Log in to your account** or go to <https://synappxadminportal.sharppusa.com/> to log in to the Admin Portal.

Synappx Go Setup and Configuration

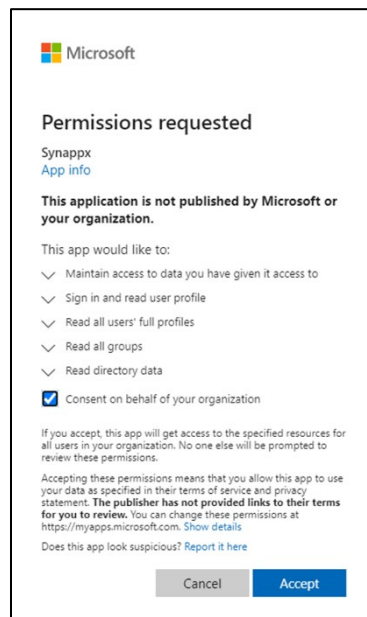
Step 2: Log In (First Time) to Admin Portal

Notes:

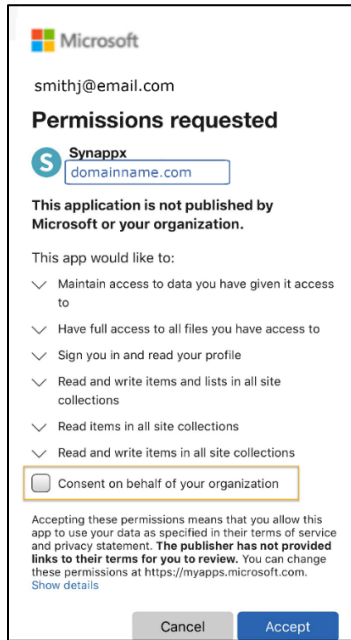
- An email containing the Synappx Admin Portal URL will be sent to the assigned administrator when your organization signs up for Synappx. Google Workspace admins must complete the Admin Console setup before logging in to the Admin Portal. See [Synappx Admin Portal](#) for more information.
 - The first 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.
1. Use your Google Workspace or Microsoft 365 credentials to log in to the [Synappx Admin Portal](#) on the latest version of Google Chrome or Microsoft Edge.



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

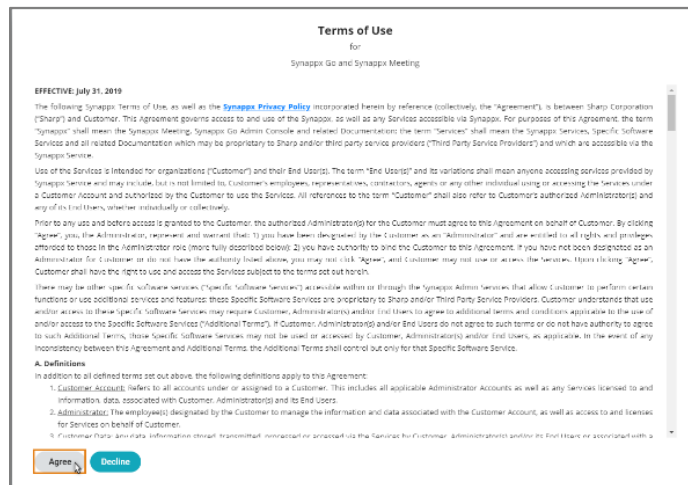


- **Google Workspace:** If login fails, go to the Google Workspace Admin Console and add the [Synappx API scope](#).

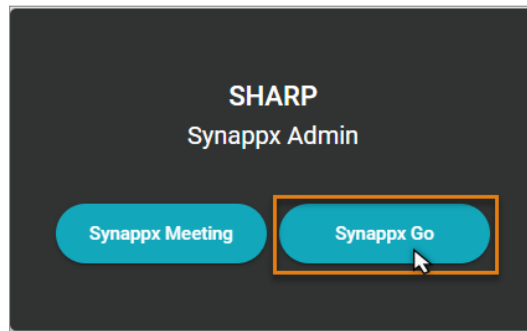


Note: Agreement with the Terms of Use is only required with the initial Admin Portal login.

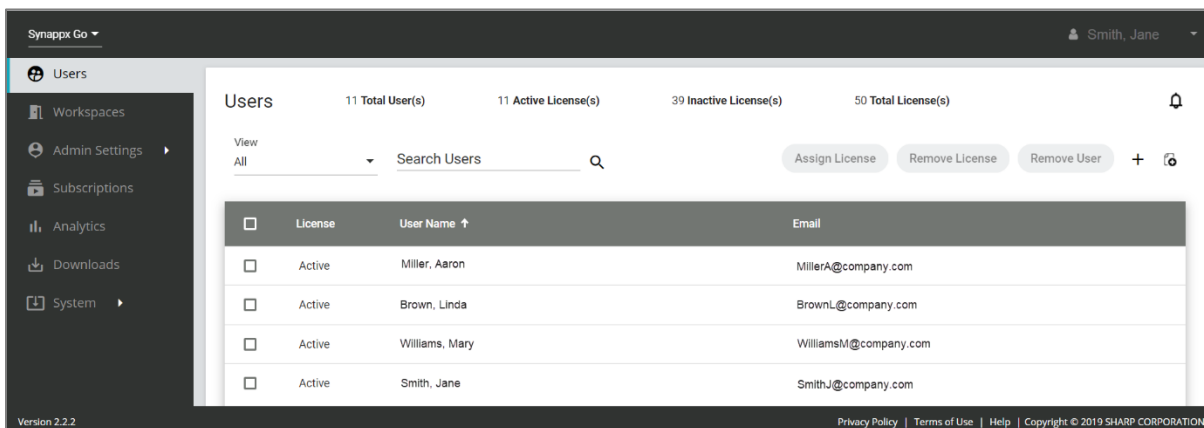
3. Review the **Terms of Use** (Synappx Privacy Policy) for Synappx Go users (and Synappx Meeting if also licensed). These Terms of Use are only granted to users for Synappx application use. Select **Agree** to continue.



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



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



Step 3: 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**.

The screenshot shows the 'Downloads' page in the Synappx Go Admin Portal. The page title is 'Downloads' and it includes the instruction 'Select components to download for installation at your company'. There are two main sections: 'Installable Components' and 'Other Components'. The 'Installable Components' section contains a table with two rows:

Installable Components	Description/Purpose
<input checked="" type="radio"/> Synappx Go MFP Agent *	Supports MFP Scan and Print Release
<input type="radio"/> Synappx Go Display Agent	Supports Content Sharing to Display

Below the table is a note: '* Note: Set IP scan range to automatically discover MFPs before downloading MFP agent. [Click here to set.](#)'

The 'Other Components' section includes links for 'iOS Synappx Go Mobile App' (Available on the App Store) and 'Android Synappx Go Mobile App' (GET IT ON Google Play). A 'Download' button is located at the bottom right of the page.

Numbered callouts and annotations are present:

- 1: Points to the 'Synappx Go MFP Agent' radio button.
- 2: Points to the 'Synappx Go Display Agent' radio button.
- 3: Points to the 'Download' button.
- 4: Points to the 'iOS Synappx Go Mobile App' link.

Annotations at the top of the page:

- 'Select the type of Agent for installation on PC/server' points to the radio buttons.
- 'Link to set up SNMP discovery range (IP address range) that will automatically search for MFPs' points to the note below the table.

Annotations at the bottom of the page:

- 'Links to download Synappx Go mobile apps from the App Store or Google Play' points to the mobile app links.
- 'Select to download Agent for installation on PC/server' points to the 'Download' button.

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.

This is a close-up screenshot of the 'Downloads' page. It shows the 'Installable Components' table with the 'Synappx Go MFP Agent' radio button selected. The 'Click here' link in the note below the table is highlighted with a red box and a mouse cursor. A 'Download' button is visible at the bottom right.

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**.

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.

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

Step 4: Install Agents

MFP Agent

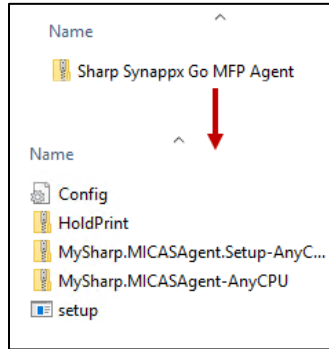
The Synappx Go MFP agent creates a secure connection to the Synappx Go cloud, discovers and maintains a list of MFPs, and manages scanning, printing, and copying in Synappx Go. A single MFP agent can manage anywhere from 50 to 100 MFPs in an organization, depending on the environment. Here is an overview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

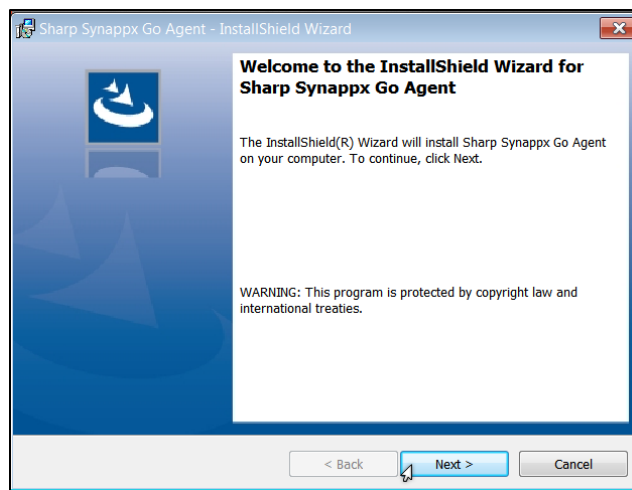
Notes:

- 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 MICASSM 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.
 - 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.
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.

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



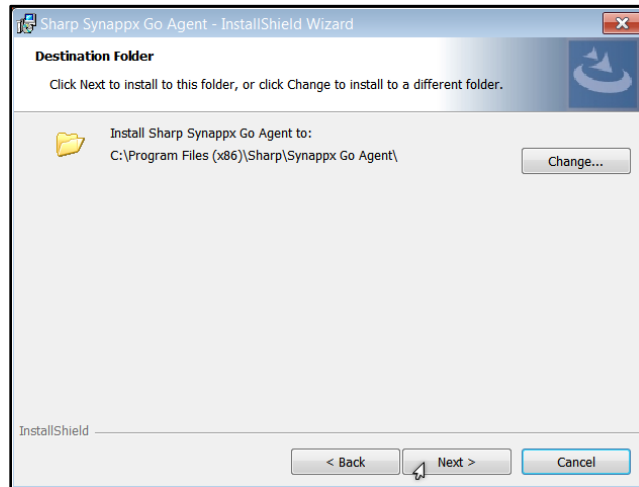
- Double-click **setup** (setup.exe) to execute the installation.
- When the **InstallShield Wizard** pops up, select **Next**.



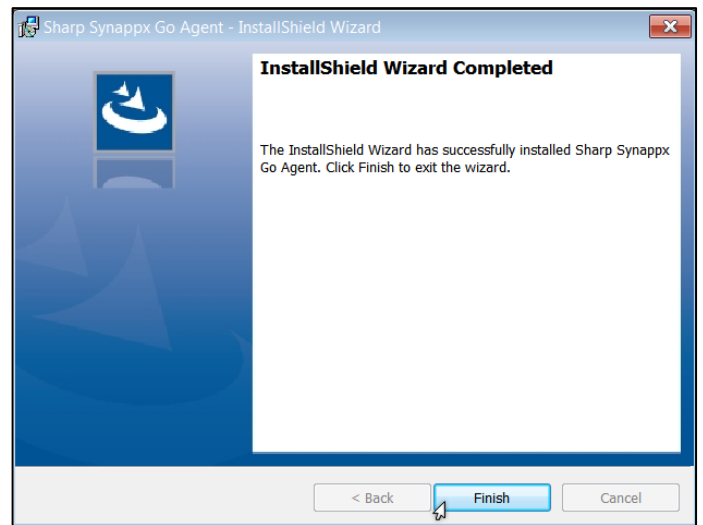
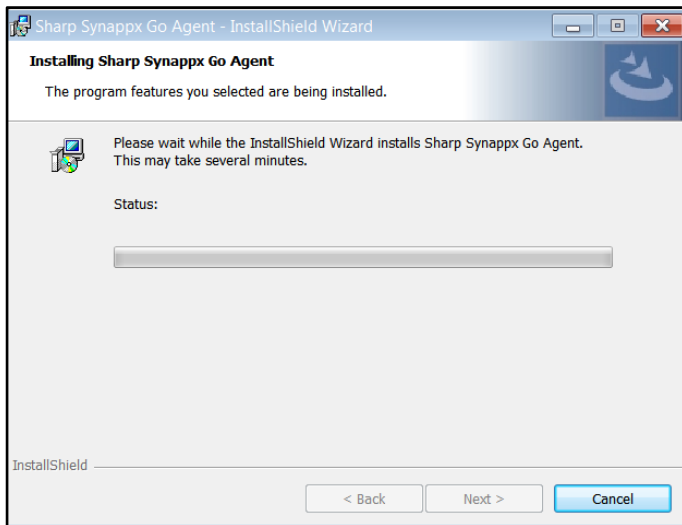
- Read the **End User License Agreement (EULA)** and select **I accept the terms in the license agreement**. If desired, print a copy of the EULA. Then select **Next**.



- 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**.



- 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.



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

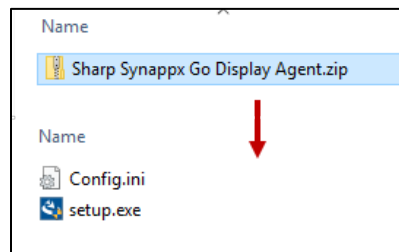
The Synappx Go display agent creates a secure connection to the Synappx Go cloud and manages document sharing to displays. A display agent must be installed on the PC of every display that will be used with Synappx Go. Here is an overview of the display agent installation and configuration:

- 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.

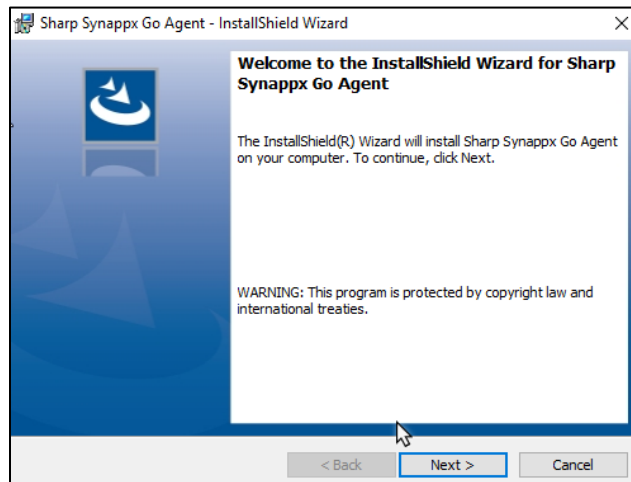
Notes:

- 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.

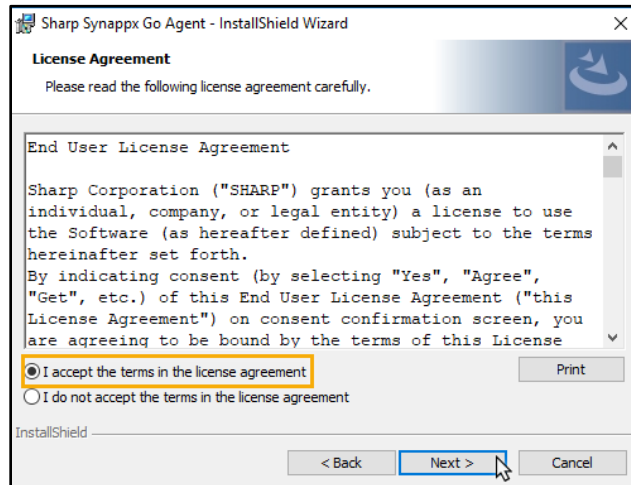
1. Copy the **Sharp Synappx Go Display Agent.zip** file to a directory on the target display PC or server and unzip it. The package will include the files shown below:



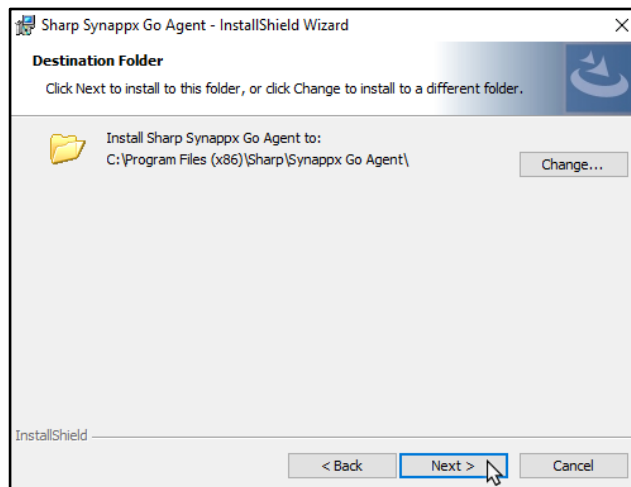
2. Double click **setup.exe**.
3. When the **InstallShield Wizard** pops up, select **Next**.



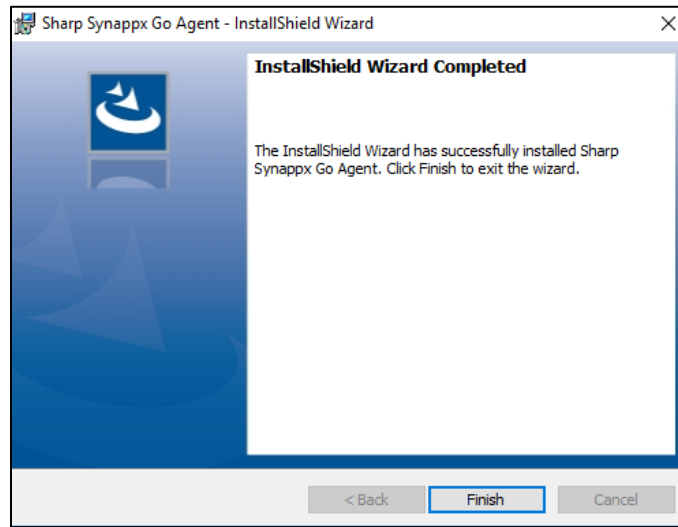
4. Read the End User License Agreement (EULA) and select **I accept the terms in the license agreement**. If desired, print a copy of the EULA. Then select **Next**.



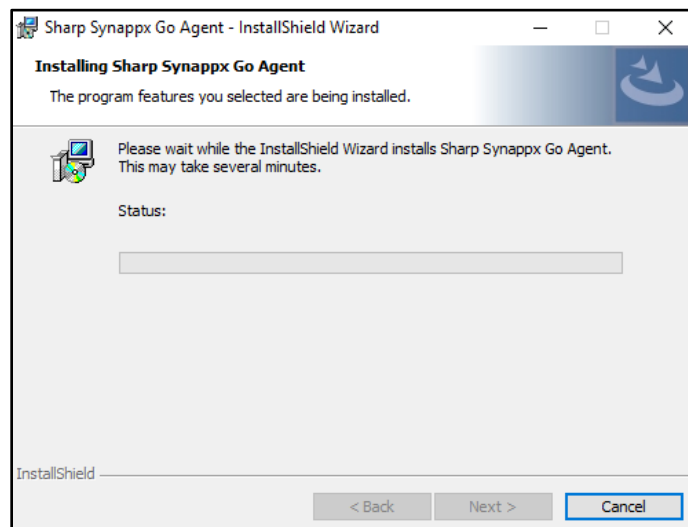
5. The **Destination Folder** screen will appear. This screen describes the default target directory for installation. In most instances, the default location is the preferred location. To override the default, select **Change** and select the desired folder. Then select **Next**. To use the default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



- The installation process will begin; it could take up to several minutes to complete. 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.

System: Agent Updates, Admin Log, System Log, Check In Log (Optional during Setup)

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

Logs

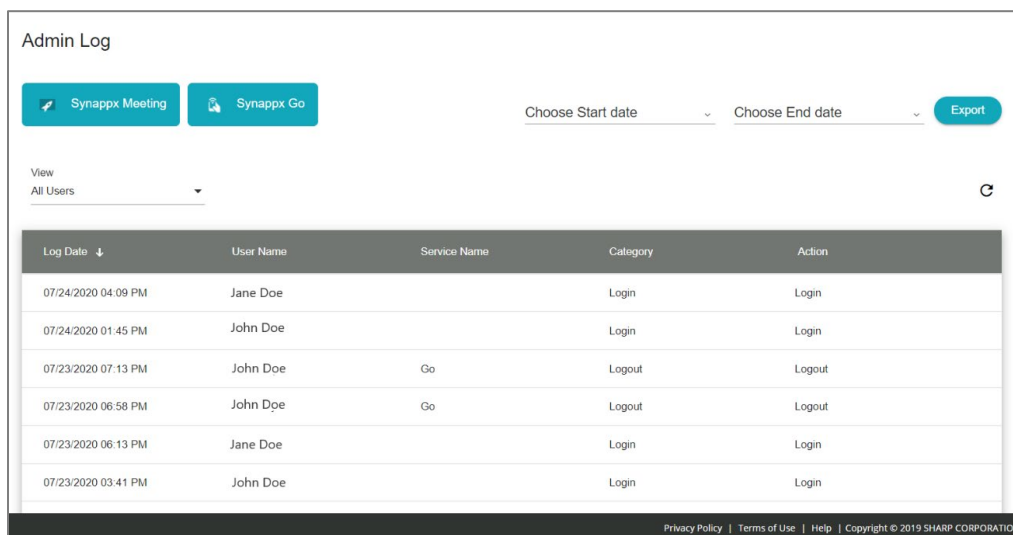
The Synappx Admin Portal provides event data to assist with identifying and resolving issues.

Admin Log

Since multiple administrators can configure and manage the system, the admin log provides a record of administrator actions on the Admin Portal.

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

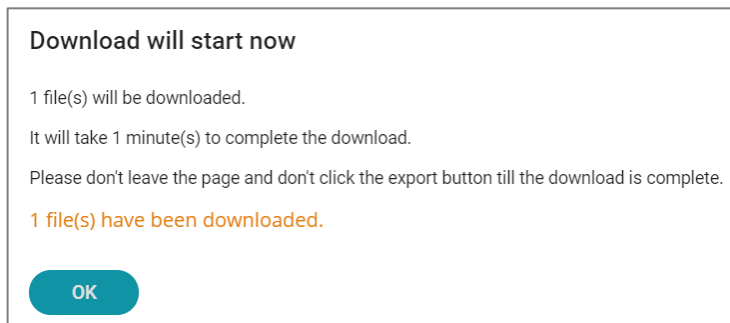
1. To filter log events, select the button to select and deselect services. (Teal buttons are selected, and white buttons are deselected.)
2. To export all logs, enter a start and end date and select **Export**. A CSV file will download automatically.
3. Select **OK**.



The screenshot shows the 'Admin Log' interface. At the top, there are two teal buttons for 'Synappx Meeting' and 'Synappx Go'. To the right, there are two date pickers labeled 'Choose Start date' and 'Choose End date', followed by a teal 'Export' button. Below this is a 'View' dropdown menu set to 'All Users' and a refresh icon. The main part of the interface is a table with the following data:

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

At the bottom right of the interface, there is a footer with links for 'Privacy Policy', 'Terms of Use', 'Help', and '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.

OK

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**.

Check In Log

Choose Start date Choose End date

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.

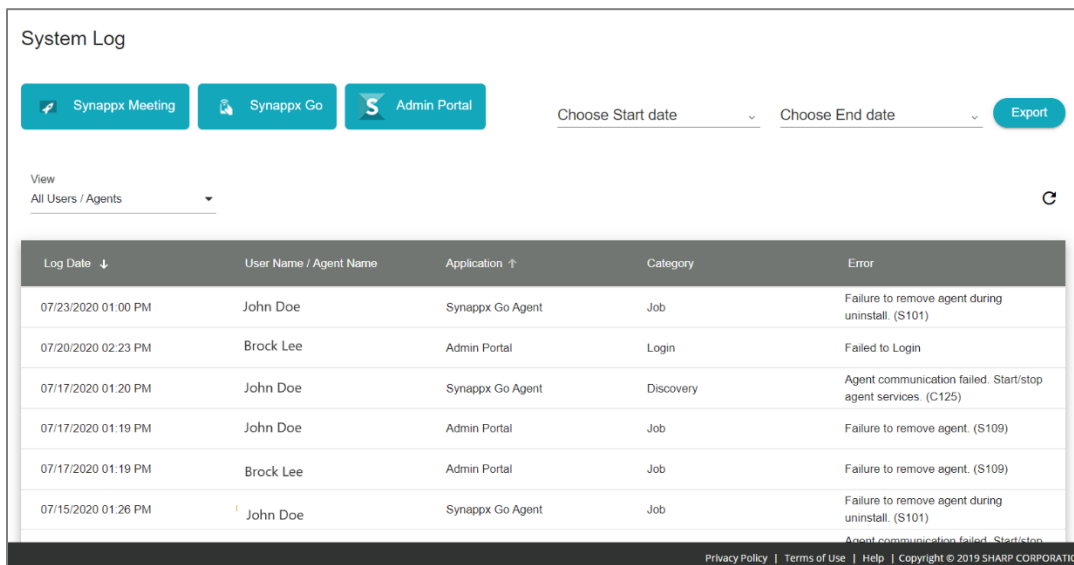
The CSV file contains information on users who have tapped check-in, MFP, or display NFC tags. Log data includes user name, user ID (email address), date and time, workspace location, action, and MFP or display agent IP address (if applicable).

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. 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](#)).

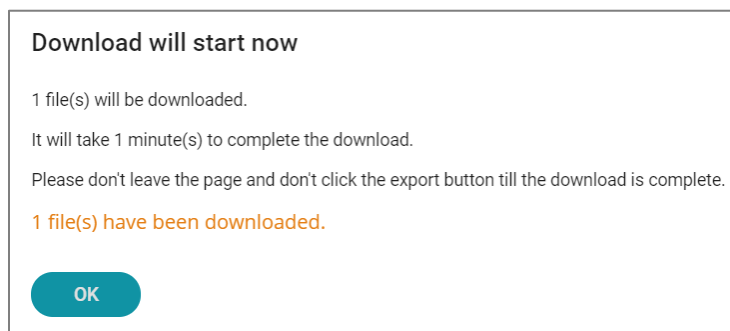
If both Synappx Go and Synappx Meeting are licensed, system logs for both services are available on this page.

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**.



The screenshot shows the 'System Log' interface. At the top, there are three teal buttons: 'Synappx Meeting', 'Synappx Go', and 'Admin Portal'. To the right of these buttons are two dropdown menus for 'Choose Start date' and 'Choose End date', and an 'Export' button. Below the buttons is a 'View' dropdown menu set to 'All Users / Agents'. The main part of the interface is a table with the following columns: 'Log Date', 'User Name / Agent Name', 'Application', 'Category', and 'Error'. The table contains several rows of log entries. At the bottom right of the interface, there is a footer with links for 'Privacy Policy', 'Terms of Use', 'Help', and 'Copyright © 2019 SHARP CORPORATION'.

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)

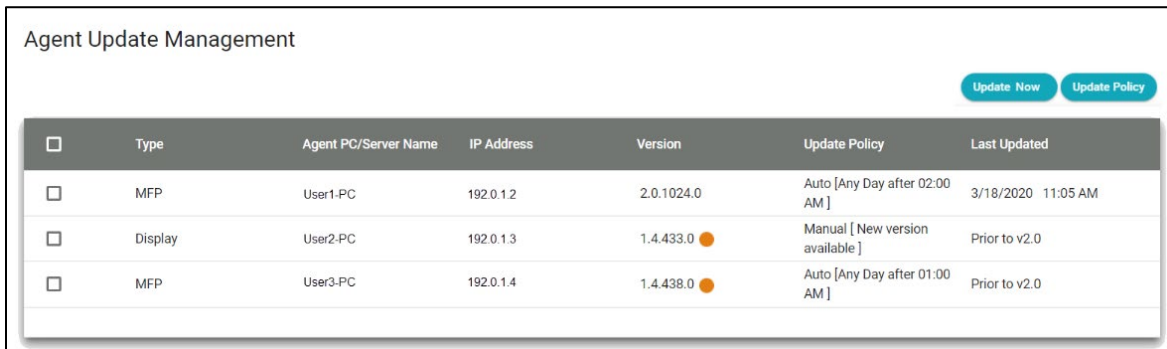


The screenshot shows a dialog box titled 'Download will start now'. The text inside the dialog box reads: '1 file(s) will be downloaded. It will take 1 minute(s) to complete the download. Please don't leave the page and don't click the export button till the download is complete.' Below this text, it says '1 file(s) have been downloaded.' and there is an 'OK' button.

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.

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.

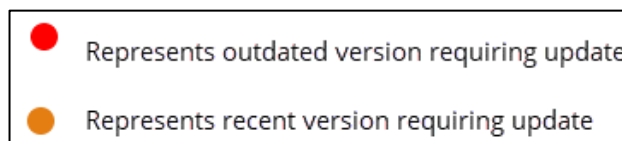


Agent Update Management

[Update Now](#) [Update Policy](#)

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

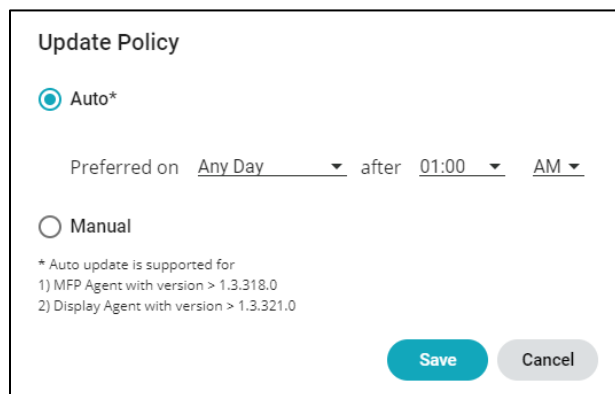
Synappx Go MFP agents with versions 1.3.323 and later and display agents with version 1.3.322.0 and later update automatically by default. The **Version** column shows the version number of each agent. Colored circles represent older versions that require updates.



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

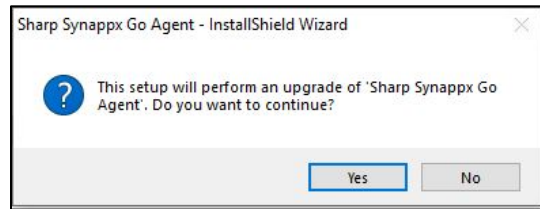
* Auto update is supported for
1) MFP Agent with version > 1.3.318.0
2) Display Agent with version > 1.3.321.0

[Save](#) [Cancel](#)

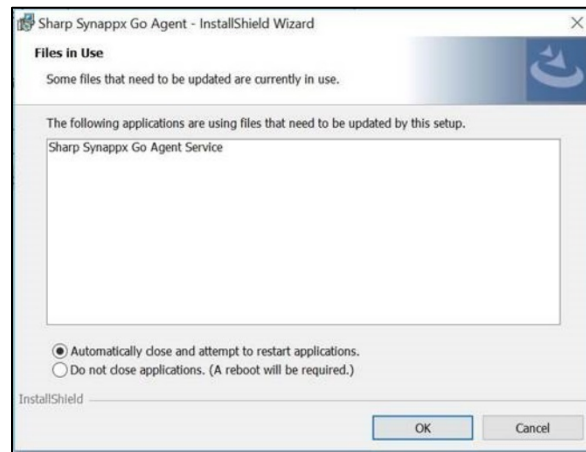
- Set a preferred day and time for automatic updates (Default is any day after 1:00 A.M.)
- Select **Manual** to disable automatic updates

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**.



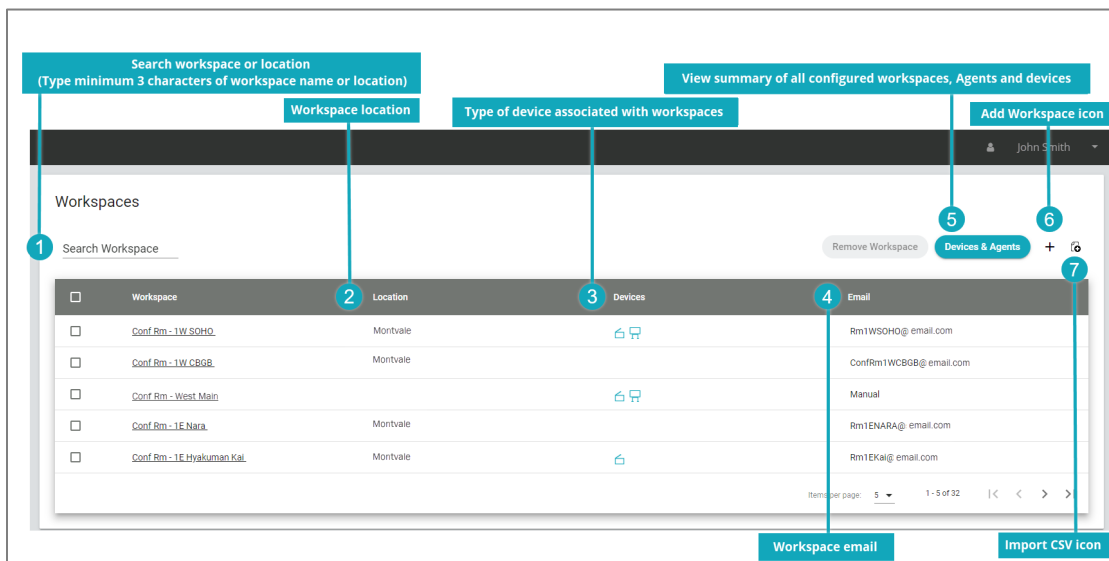
3. Follow the **InstallShield Wizard** instructions.
4. If the Synappx service is running, a window will prompt the admin to stop the service to continue the upgrade installation. Select **Automatically close and attempt to restart applications**. Then select **OK**.



5. Repeat this procedure for both agents if applicable.

Step 5: 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.



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



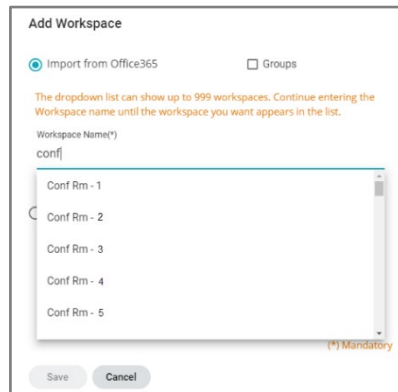
From the **Add Workspace** window, you can import workspaces from Microsoft 365 or Google Workspace or add workspaces manually.

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**.



The screenshot shows a dialog box titled "Add Workspace". At the top, there are two radio buttons: "Import from Office365" (which is selected) and "Groups". Below this, there is a text box labeled "Workspace Name(*)" containing the text "conf". A dropdown menu is open below the text box, displaying a list of workspace names: "Conf Rm - 1", "Conf Rm - 2", "Conf Rm - 3", "Conf Rm - 4", and "Conf Rm - 5". At the bottom of the dialog, there are "Save" and "Cancel" buttons. A red asterisk and the word "Mandatory" are located at the bottom right of the dialog box.

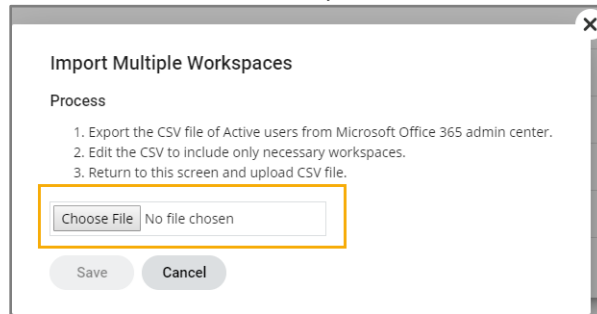
2. To add workspace groups, first check the **Groups** box. Then follow step 1.

Import Workspaces via CSV File

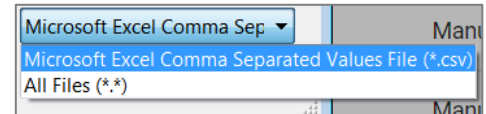
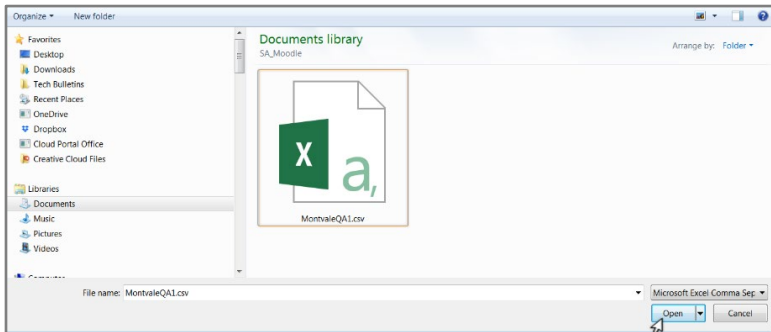
1. Select the **Import Multiple Workspaces** icon.



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.



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

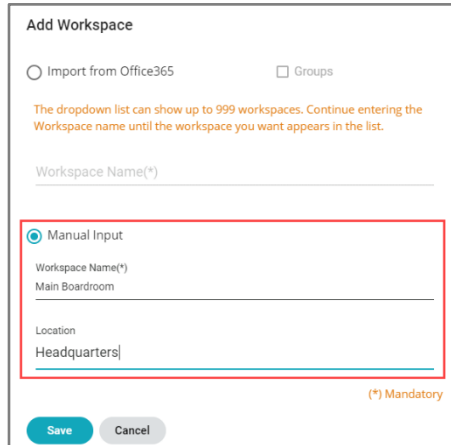


5. The file will attach in the **Import Multiple Workspaces** window. Select **Save**.

Manual Input

Image shows Microsoft 365 as an example.

1. Select **Manual Input**.



The screenshot shows a dialog box titled "Add Workspace". At the top, there are two radio buttons: "Import from Office365" (which is selected) and "Groups". Below these is a note: "The dropdown list can show up to 999 workspaces. Continue entering the Workspace name until the workspace you want appears in the list." There is a text input field labeled "Workspace Name(*)" which is currently empty. Below this, the "Manual Input" section is highlighted with a red box. It contains a radio button that is selected, followed by a text input field labeled "Workspace Name(*)" containing the text "Main Boardroom", and another text input field labeled "Location" containing the text "Headquarters|". At the bottom right of the dialog, there is a note "(*) Mandatory". At the bottom left, there are two buttons: "Save" and "Cancel".

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

<input type="checkbox"/>	Agent PC/Server Name	Agent ID	Device	NFC Tag ID *	NFC Tag Action
<input type="checkbox"/>	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

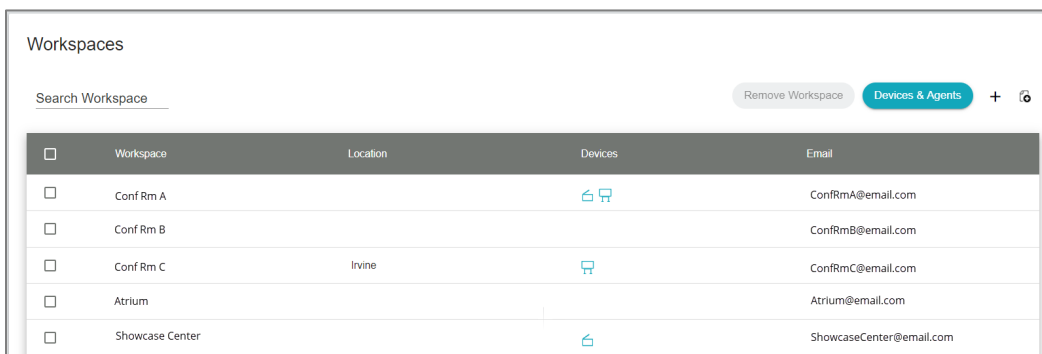
OK Cancel

4. Select **OK** when finished.

Step 6: Associate Devices to Workspaces

Associate MFPs to Workspaces

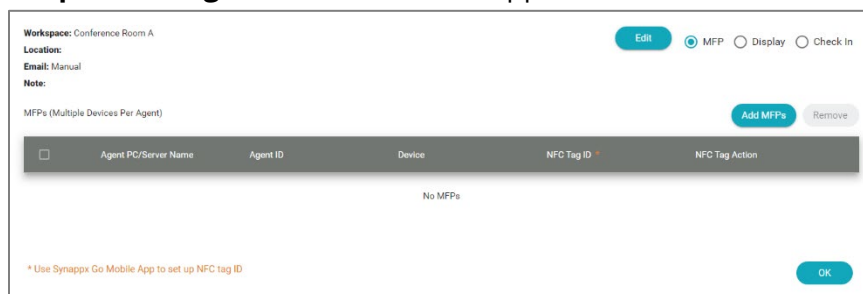
1. Start by selecting a workspace from the list.



The screenshot shows a 'Workspaces' management page. At the top, there is a search bar labeled 'Search Workspace' and two buttons: 'Remove Workspace' and 'Devices & Agents'. Below this is a table with the following columns: Workspace, Location, Devices, and Email. The table contains five rows of workspace information.

<input type="checkbox"/>	Workspace	Location	Devices	Email
<input type="checkbox"/>	Conf Rm A			ConfRmA@email.com
<input type="checkbox"/>	Conf Rm B			ConfRmB@email.com
<input type="checkbox"/>	Conf Rm C	Irvine		ConfRmC@email.com
<input type="checkbox"/>	Atrium			Atrium@email.com
<input type="checkbox"/>	Showcase Center			ShowcaseCenter@email.com

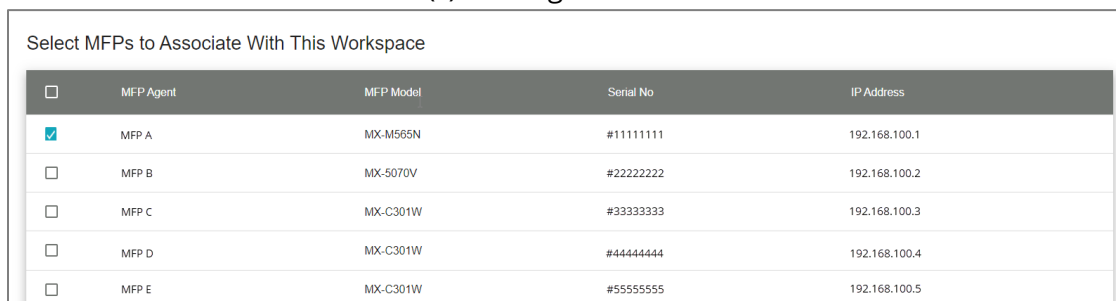
2. The **Workspace Configuration** window will appear. Select **Add MFPs**.



The screenshot shows the 'Workspace Configuration' window for 'Conference Room A'. It includes an 'Edit' button and radio buttons for 'MFP', 'Display', and 'Check In'. Below this, there are fields for 'Location', 'Email: Manual', and 'Note'. A section titled 'MFPs (Multiple Devices Per Agent)' contains an 'Add MFPs' button and a 'Remove' button. Below this is a table with columns: Agent PC/Server Name, Agent ID, Device, NFC Tag ID, and NFC Tag Action. The table currently shows 'No MFPs'. At the bottom, there is a note: '* Use Synappx Go Mobile App to set up NFC tag ID' and an 'OK' button.

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).

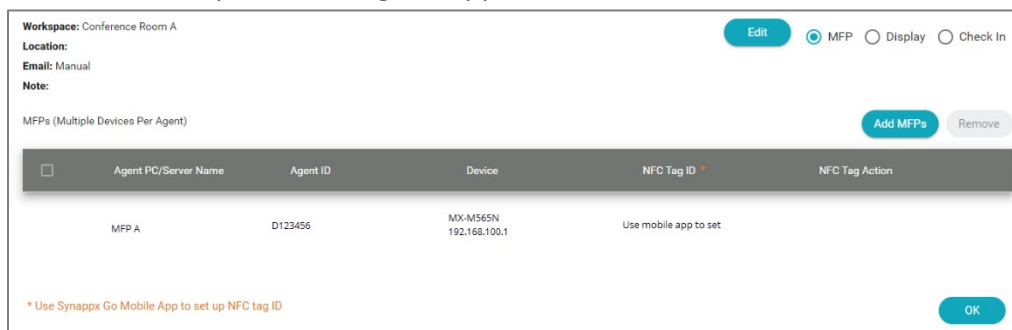
3. Select the desired MFP model(s) to assign and select **OK**.



The screenshot shows a dialog titled 'Select MFPs to Associate With This Workspace'. It contains a table with the following columns: MFP Agent, MFP Model, Serial No, and IP Address. The first row, 'MFP A', is selected with a checked checkbox.

<input type="checkbox"/>	MFP Agent	MFP Model	Serial No	IP Address
<input checked="" type="checkbox"/>	MFP A	MX-M565N	#11111111	192.168.100.1
<input type="checkbox"/>	MFP B	MX-5070V	#22222222	192.168.100.2
<input type="checkbox"/>	MFP C	MX-C301W	#33333333	192.168.100.3
<input type="checkbox"/>	MFP D	MX-C301W	#44444444	192.168.100.4
<input type="checkbox"/>	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**.



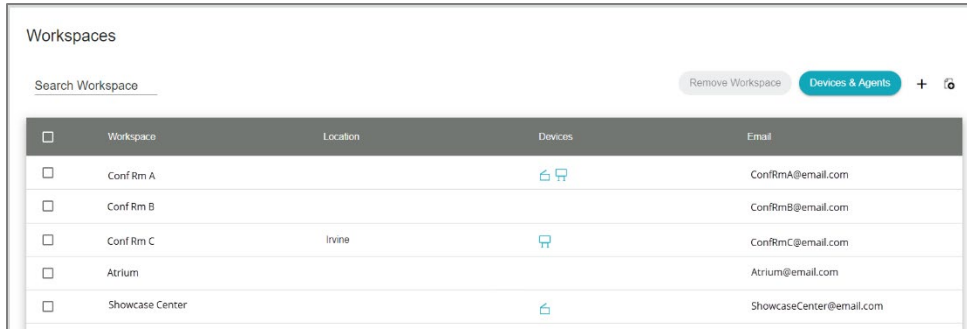
The screenshot shows the 'Workspace Configuration' window for 'Conference Room A' after an MFP has been assigned. The 'MFPs (Multiple Devices Per Agent)' section now contains one entry in the table:

<input type="checkbox"/>	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

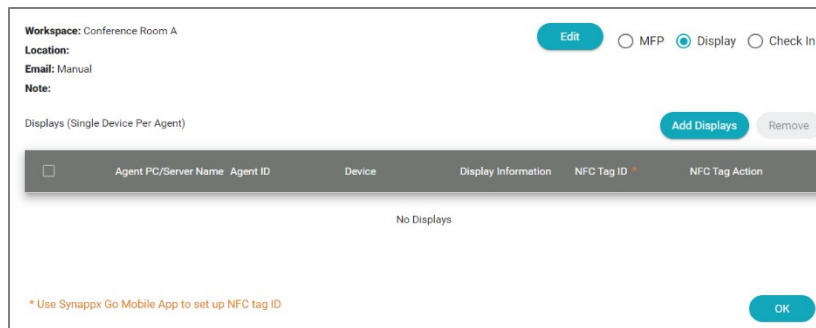
At the bottom, there is a note: '* Use Synappx Go Mobile App to set up NFC tag ID' and an 'OK' button.

Associate Display to a Workspace

1. Start by selecting workspaces from the list.

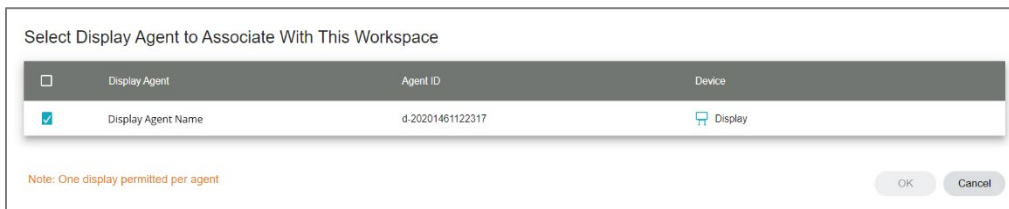


2. The **Workspace Configuration** window will appear. Select **Add Displays**.

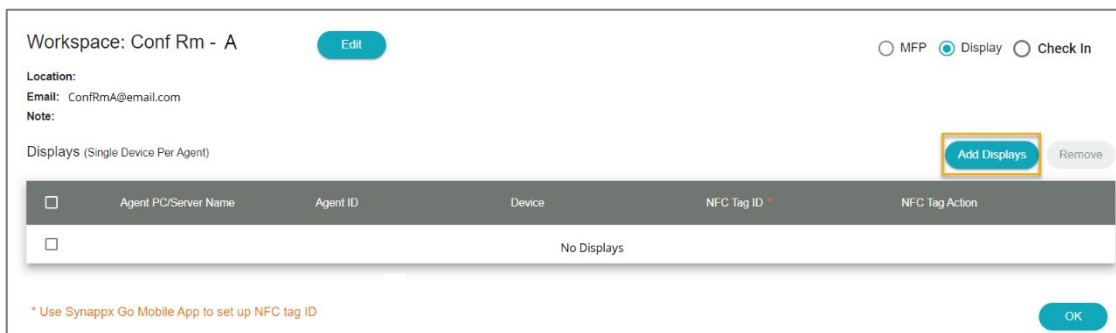


Note: A display can only be assigned to one workspace at a time (i.e., it will not show in the available display list after being assigned until removed from the other workspace).

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



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 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)

<input type="checkbox"/>	NFC Tag ID	NFC Tag Action
<input type="checkbox"/>	cdf456sjgsdd5fjeius6935sd35	Check In

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

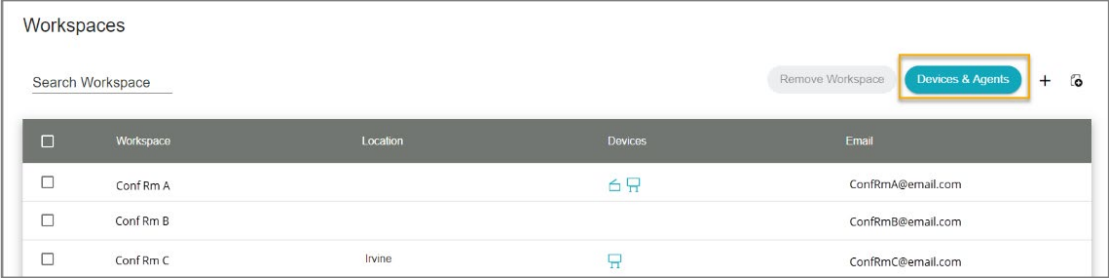
Buttons: Edit, MFP, Display, Check In, Remove, OK

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

<input type="checkbox"/>	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**.




MFP Summary of Devices and Agents

Summary of Devices and Agents					
<input checked="" type="radio"/> MFP <input type="radio"/> Display Show All Devices					
1	2	3	4	5	6
Agent PC / Server	Agent ID / IP Address	Version	Updates	Device	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

[Back](#)

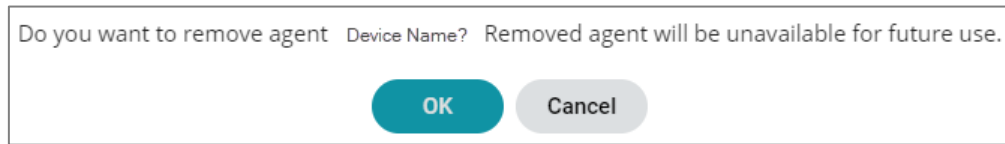
MFP Summary of Devices and Agents	
1	Agent PC/Server <ul style="list-style-type: none"> Select the link to remove associated MFPs or the agent. <ul style="list-style-type: none"> If removing the agent, uninstall it from the PC or server using the normal Windows uninstall procedure to complete removal and avoid reconnection. Select Find MFPs to access SNMP Configuration and initiate MFP discovery.
2	Agent ID/ IP Address <ul style="list-style-type: none"> 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 acquire 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. <div data-bbox="938 1081 1518 1564" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Email Agent Log Agent PC: PC123</p> <p style="text-align: right;">* Mandatory</p> <p>To *: 5 addresses max</p> <p>admin@domain.com</p> <hr/> <p>Subject:</p> <p>Synappx Go Agent Log for desktop-lk40oeg</p> <hr/> <p>Message: The Link to the agent Log will be added automatically</p> <p>Click Link to open agent log</p> <hr/> <p>Note: The Log is available for next 7 days. Send Cancel</p> </div>
3	Version Select the agent version number to go to Agent Update page.
4	Updates <ul style="list-style-type: none"> An orange dot indicates a recent agent version that requiring update. A red dot indicates an outdated agent version requiring update.
5	Device <ul style="list-style-type: none"> 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

Display Summary of Devices and Agents		
1	Device/ Agent PC	<ul style="list-style-type: none"> Select the link to remove the display agent.
2	Agent ID/ IP Address	<ul style="list-style-type: none"> 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 acquire 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. <div data-bbox="950 926 1528 1402" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Email Agent Log Agent PC: PC123</p> <p style="text-align: right;">* Mandatory</p> <p>To *: 5 addresses max</p> <p>admin@domain.com</p> <hr/> <p>Subject:</p> <p>Synappx Go Agent Log for desktop-1k400eg</p> <hr/> <p>Message: The Link to the agent Log will be added automatically</p> <p>Click Link to open agent log</p> <hr/> <p>Note: The Log is available for next 7 days. Send Cancel</p> </div>
3	Version	Select the agent version number to go to Agent Update page.
4	Updates	<ul style="list-style-type: none"> An orange dot indicates a recent agent version that requiring update. A red dot indicates an outdated agent version requiring update.
5	Display Information	<ul style="list-style-type: none"> Select Configure to set up and manage display automatic input switching. Edit and Clear are shown after configuration. Select Show Unassigned to view display agents not associated with workspaces.
6	Workspace	<ul style="list-style-type: none"> Select a workspace to view associated devices.

Remove Display Agent

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



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). For more information, go to [Appendix B: Synappx™ Go Automatic Input Switch](#).

Step 7: 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.



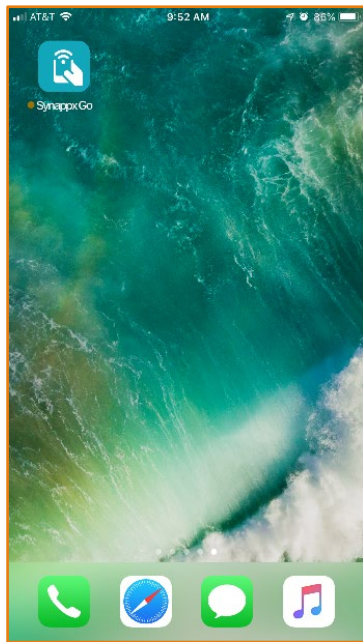
Android

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

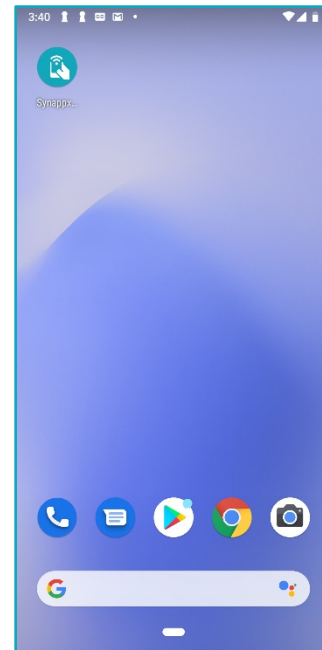



Note: The sign-in information only needs to be entered the first time you sign in to the app unless you change your password, log out or do not use the app for 30 days.

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

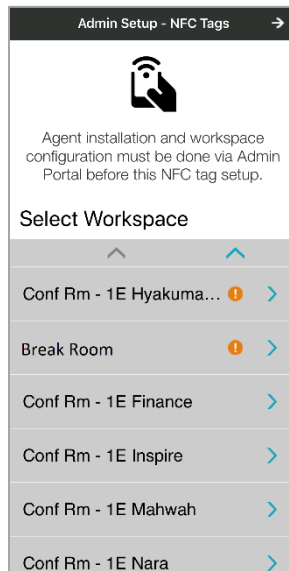


2. Open the Synappx Go app. When prompted, enter your Microsoft 365 or Google Workspace credentials and accept the permissions request.

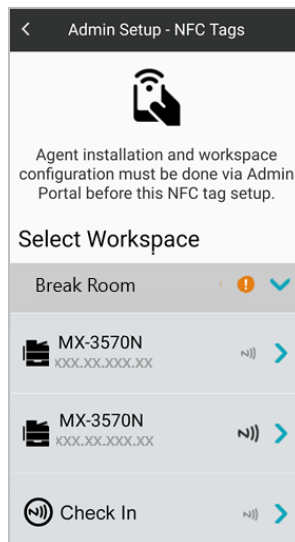


Note: When an MFP or display associated with a workspace needs to be set up, a  will appear. You can sort by workspace name or by workspaces requiring NFC tag setup. Check-in can be configured for any workspace.

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

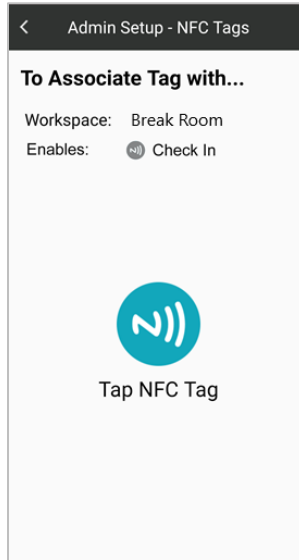


4. A list of devices and a check-in option will appear below the workspace. Select a device or select **Check In**.

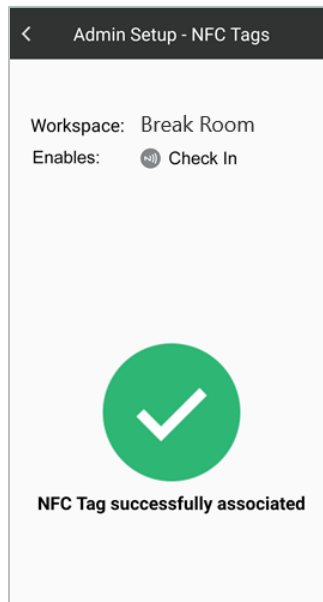


Note: A smaller light gray NFC image indicates the device does not yet have an associated NFC tag. A darker gray, larger icon indicates a tag has been associated.

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.



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



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 8: 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.

The screenshot shows the 'Users' management page in the Admin Portal. It features a search bar, filter options, and summary statistics for users and licenses. A table lists individual users with their license status, names, and email addresses. Callouts 1-11 point to specific UI elements, and labels at the bottom describe the data in the table.

License	User Name	Email
Active	Ames, Howie	amesh@email.com
Active	Withall, Sharon	withall@email.com
Active	Carey, Don	careyd@email.com
Active	Ling, Yolanda	lingy@email.com
Active	McCarin, Brock	mcannb@email.com

- Assign and remove licenses to and from users on this page.
- Add administrators from the **Admin Settings** page (optional during initial setup but recommended).

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.

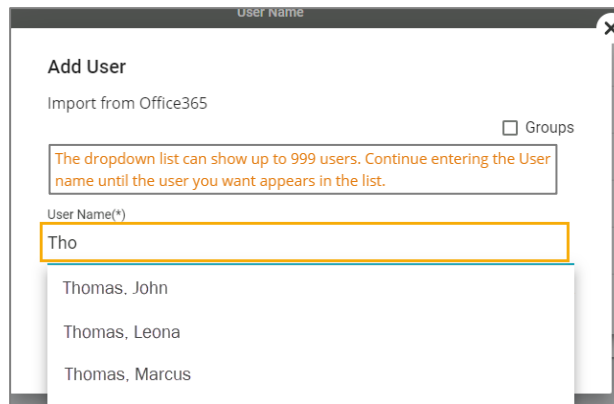
Add Users

Images show Microsoft 365 as an example.

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

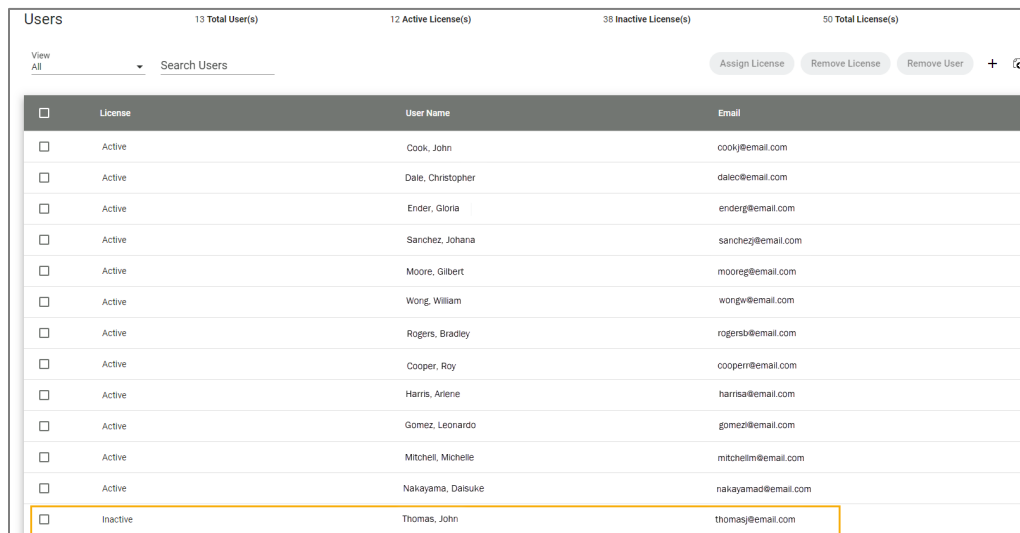


2. Type a few characters in the **User Name** field. Microsoft 365 or Google Workspace users will populate. Select from the list shown. Then select **Save**.



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.



The screenshot shows the 'Users' page with a table of users. The table has columns for 'License', 'User Name', and 'Email'. The newly added user 'Thomas, John' is highlighted with a yellow border and is listed as 'Inactive'.

License	User Name	Email
<input type="checkbox"/>	Cook, John	cookj@email.com
<input type="checkbox"/>	Dale, Christopher	dalec@email.com
<input type="checkbox"/>	Ender, Gloria	enderg@email.com
<input type="checkbox"/>	Sanchez, Johana	sanchezj@email.com
<input type="checkbox"/>	Moore, Gilbert	mooreg@email.com
<input type="checkbox"/>	Wong, William	wongw@email.com
<input type="checkbox"/>	Rogers, Bradley	rogersb@email.com
<input type="checkbox"/>	Cooper, Roy	cooperf@email.com
<input type="checkbox"/>	Harris, Arlene	harrisr@email.com
<input type="checkbox"/>	Gomez, Leonardo	gomezl@email.com
<input type="checkbox"/>	Mitchell, Michelle	mtchellm@email.com
<input type="checkbox"/>	Nakayama, Daisuke	nakayamad@email.com
<input type="checkbox"/>	Thomas, John	thomasj@email.com

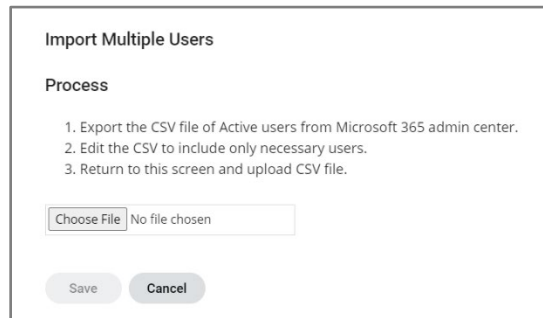
Import Users via CSV File

Images show Microsoft 365 as an example.

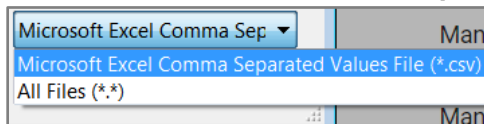
1. Select the **Add Multi-Users** icon.



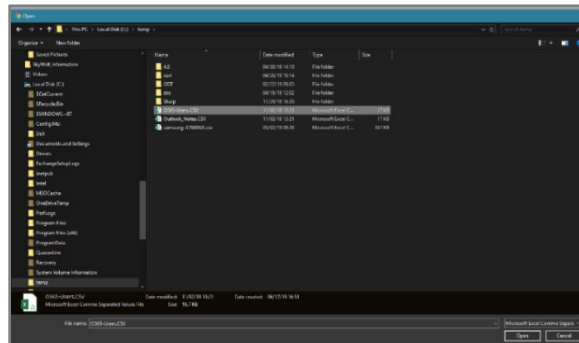
2. The **Import of Multi-Users** window will appear. Follow the **Process** guidelines. The file has a maximum of 50 users and 500KB.



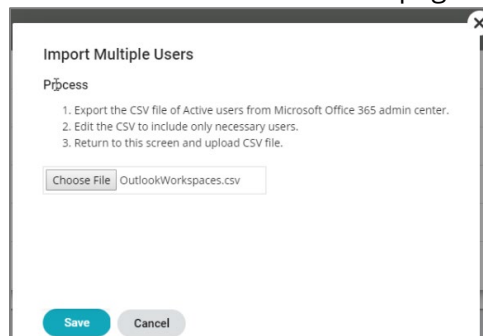
Note: The selected file must be a **Microsoft Excel Comma Separated Values File**.



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.



Assign Licenses

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

The screenshot shows the 'Users' page with the following statistics: 11 Total User(s), 9 Active License(s), 41 Inactive License(s), and 50 Total License(s). The 'View' dropdown is set to 'All'. A search bar is present. The 'Assign License' button is highlighted with a yellow box. The 'Remove License' and 'Remove User' buttons are also visible. The table below shows the user list:

<input type="checkbox"/>	License	User Name ↓	Email
<input type="checkbox"/>	Active	Wong, William	wongw@email.com
<input checked="" type="checkbox"/>	Inactive	Thomas, John	thomasj@email.com

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](#)).

The screenshot shows the 'Users' page with updated statistics: 11 Total User(s), 11 Active License(s), 39 Inactive License(s), and 50 Total License(s). The 'View' dropdown is set to 'All'. The search bar is present. The 'Assign License' button is now disabled. The 'Remove License' and 'Remove User' buttons are also visible. The table below shows the user list:

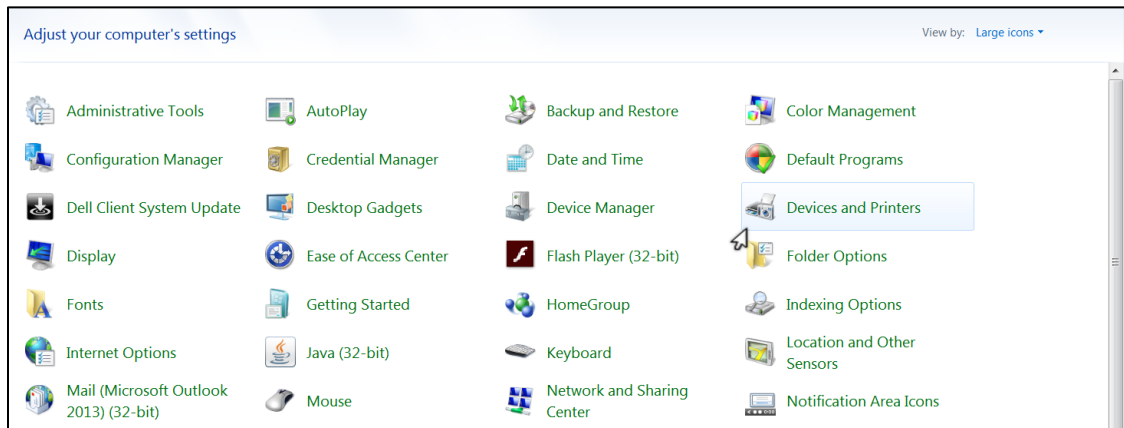
<input type="checkbox"/>	License	User Name ↓	Email
<input type="checkbox"/>	Active	Wong, William	wongw@email.com
<input type="checkbox"/>	Active	Thomas, John	thomasj@email.com

Step 9: Configure Print Release Driver and Share with Users

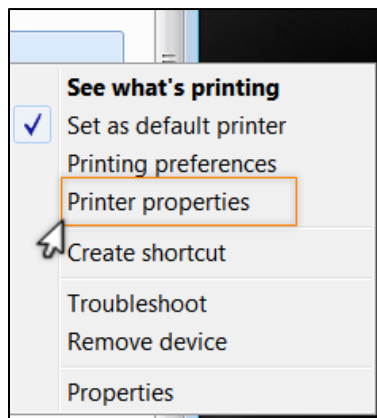
To enable print release on the Synappx Go app, the network administrator or user must configure a print driver.

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.

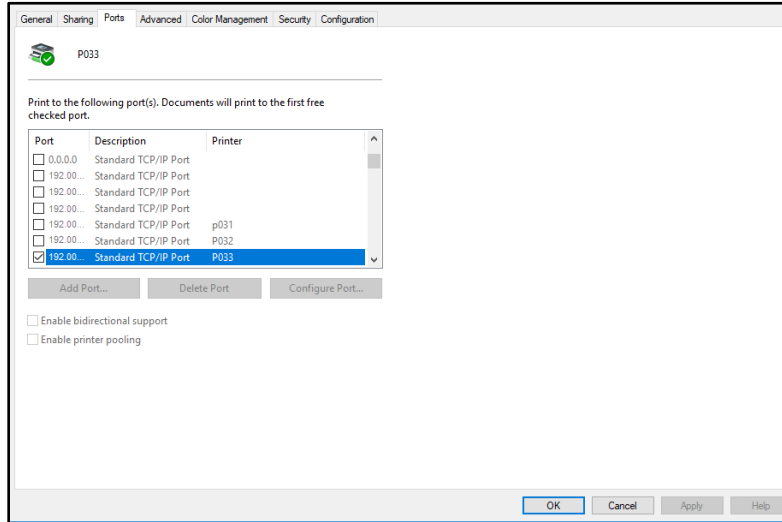
1. Navigate to the **Control Panel** and select **Devices and Printers**.



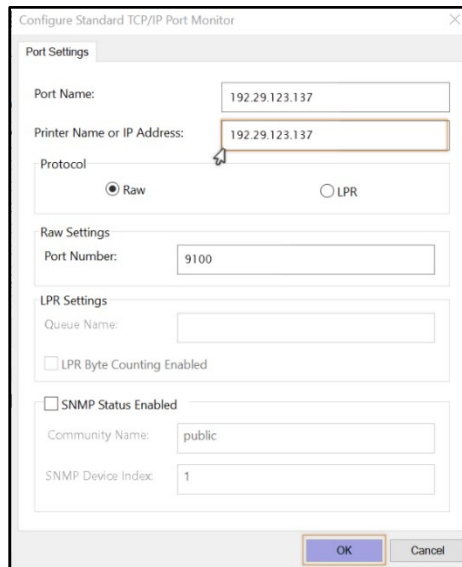
2. Right click on the printer driver. Select **Printer Properties**.



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

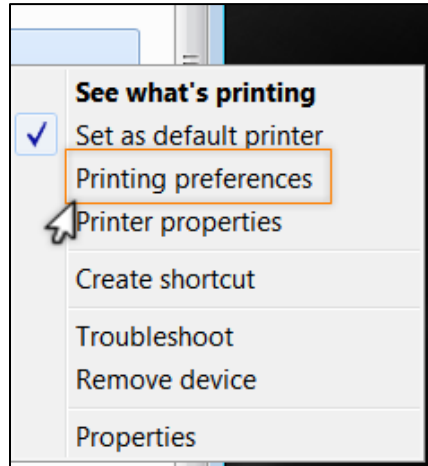


4. Delete the current entry in the **Printer Name or IP Address** field and enter the address of the MFP agent. Both RAW (TCP port 9100) and Line Printer Remote (LPR) (TCP port 515) printing are supported. Ensure the PC firewall is configured to allow TCP traffic on the selected port. Then select **OK**.

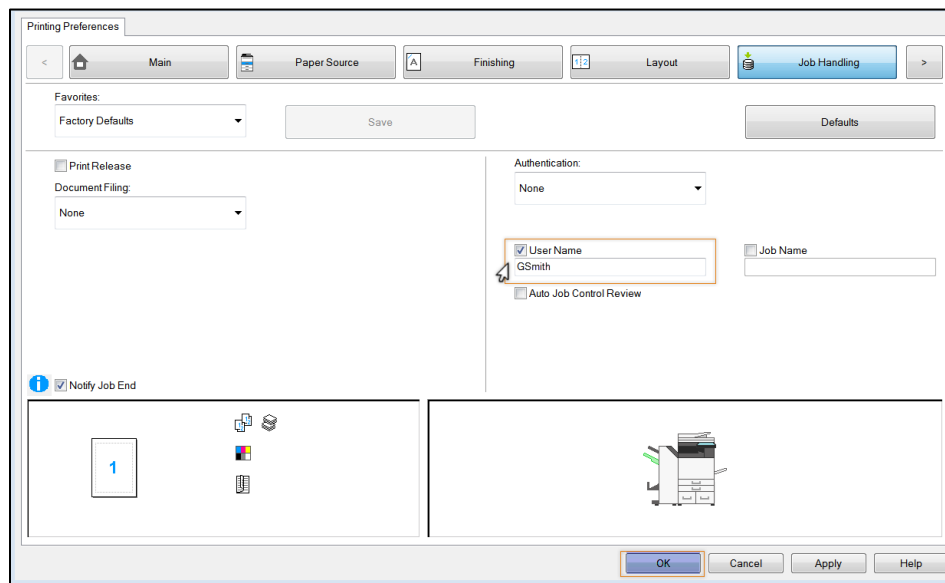


Note: If the username can be determined automatically, proceed to step 7. If the username is not the same as the network credentials or if print jobs do not appear in a user's print queue when using Synappx Go, follow steps 5 and 6.

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.



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](#).

Synappx Go is now ready to use!

Admin Settings (Optional)

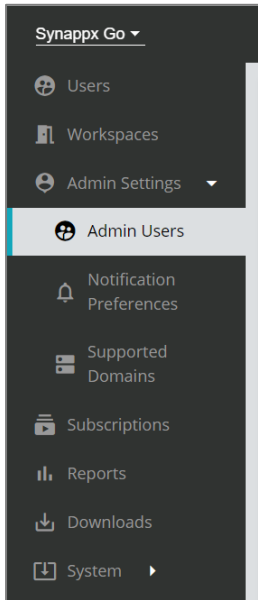
Administrator Management

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.

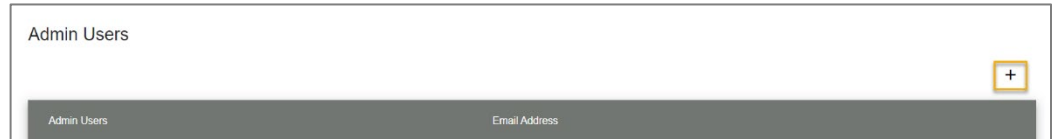
Service	Page	Functions	Admin	Support Admin
Synappx Admin Portal (Common)	Workspaces	View workspace list	Yes	Yes
		Add workspace (manual)	Yes	No
		Add workspace (import from Office 365/ Google Workspace)	Yes	No
		Add workspaces with Group	Yes	No
		Add workspace (import CSV)	Yes	No
		Remove workspace	Yes	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)

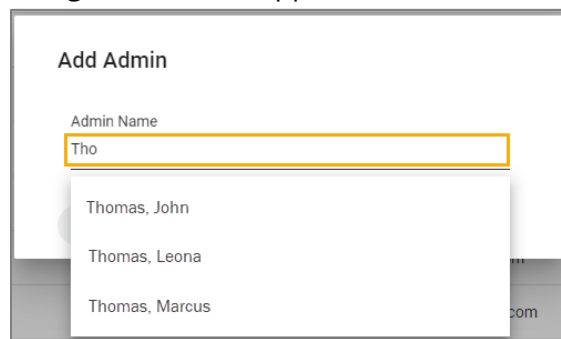


Full administrators can perform all functions on the Admin Portal after the primary admin accepts the initial permissions.

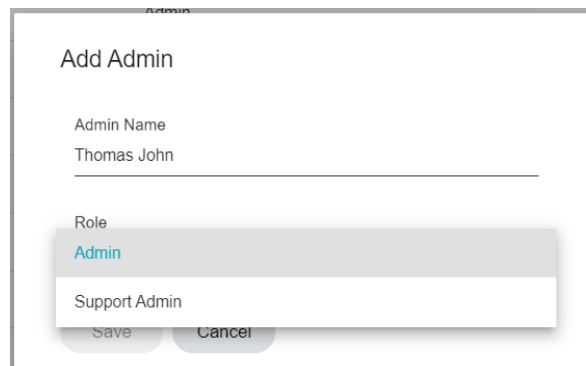
1. Go to **Admin Settings** on the Admin Portal. On the **Admin Users** page, select **(+)**.



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.



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.



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.

Notify me when...	Via email	Via mobile *
Agent action is required	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Agent is successfully updated	<input type="checkbox"/>	<input type="checkbox"/>
Agent is available for update	<input type="checkbox"/>	<input type="checkbox"/>

* Use Synappx Go Mobile App to set up mobile notifications

Save

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

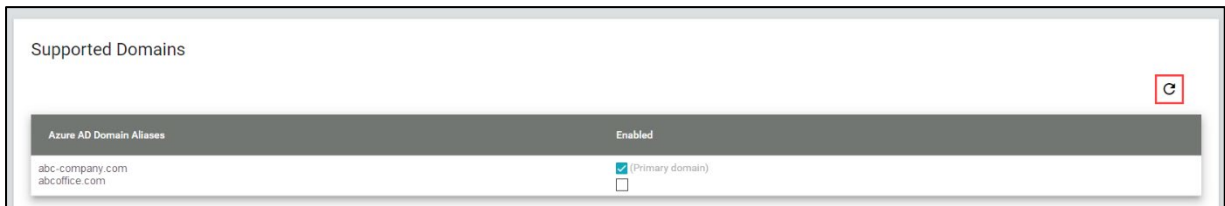
Agent is available for update

Supported Domains

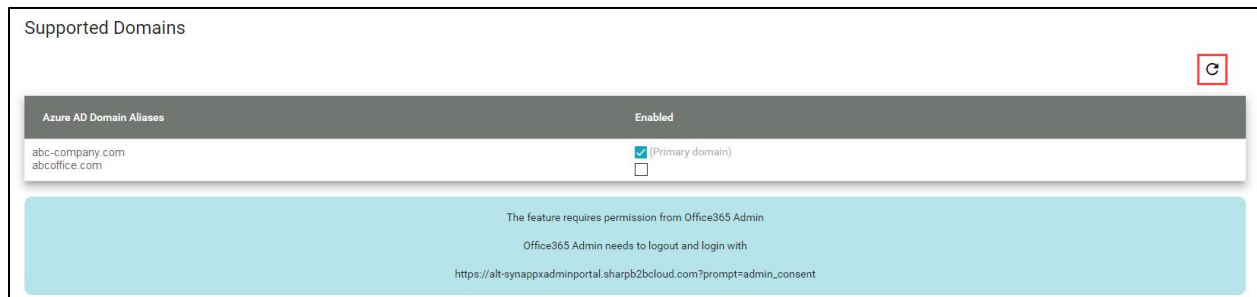
The **Supported Domains** page automatically collects domain aliases from Azure Active Directory or Google Workspace. The default setting is to enable all domains.

Caution: 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.



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.

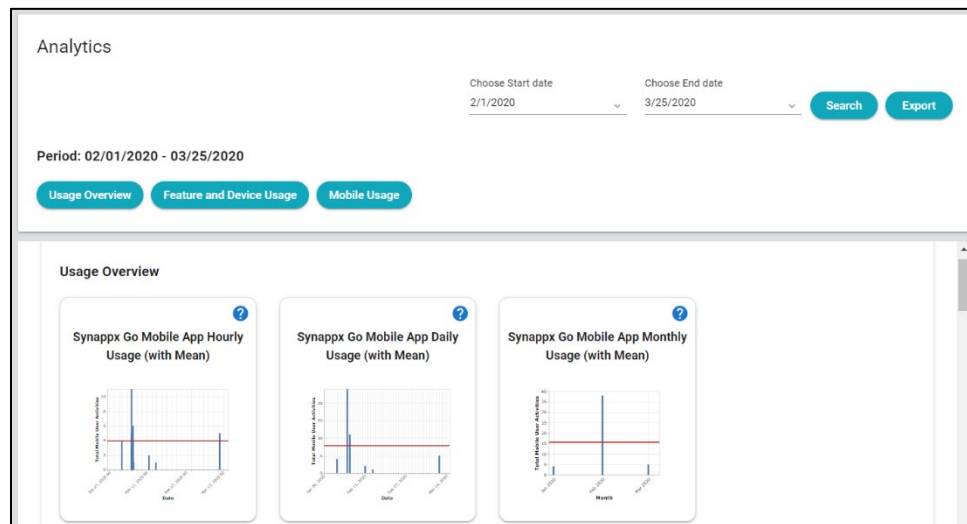


Analytics

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.

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

Usage Overview

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.

Feature and Device Usage

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

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.

Appendix A: Windows Defender Firewall Configuration

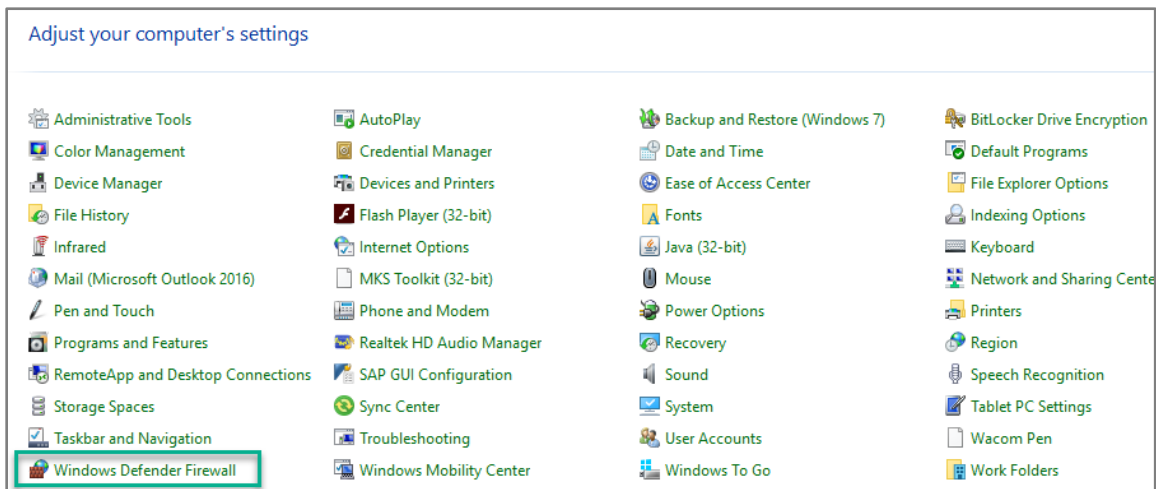
Background

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.

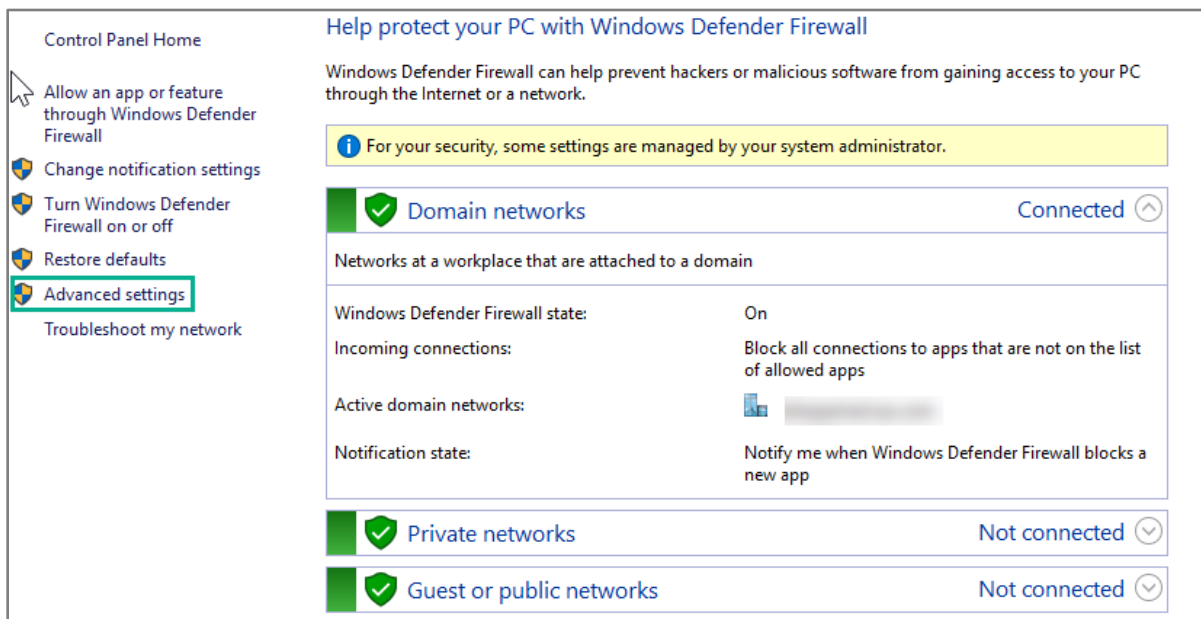
Note: From version 2.0, the agent automatically opens the inbound port as part of the installation.

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

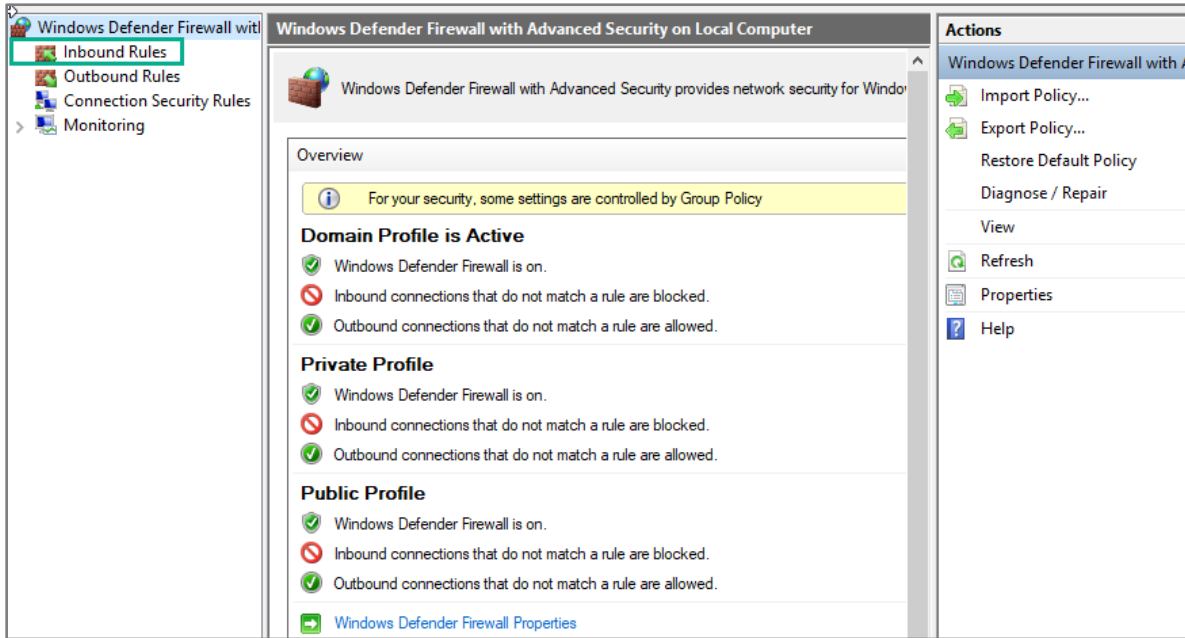
1. Launch the **Windows Defender Control Panel**. Then launch the **Windows Firewall** applet.



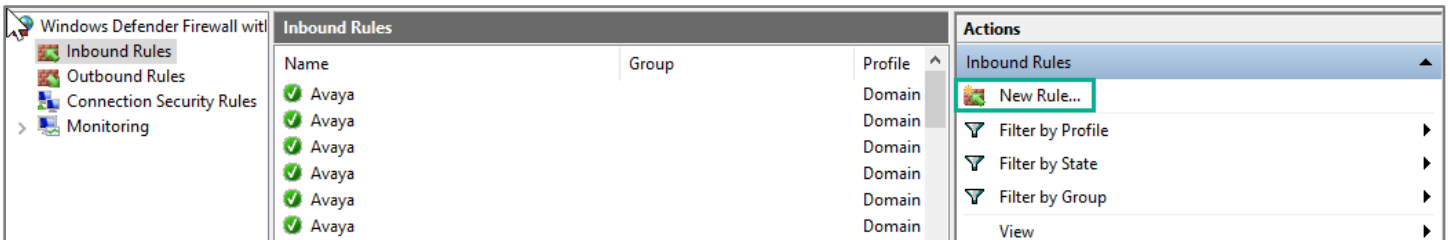
2. The main **Windows Defender Firewall** interface is shown below. Select **Advanced Settings**.



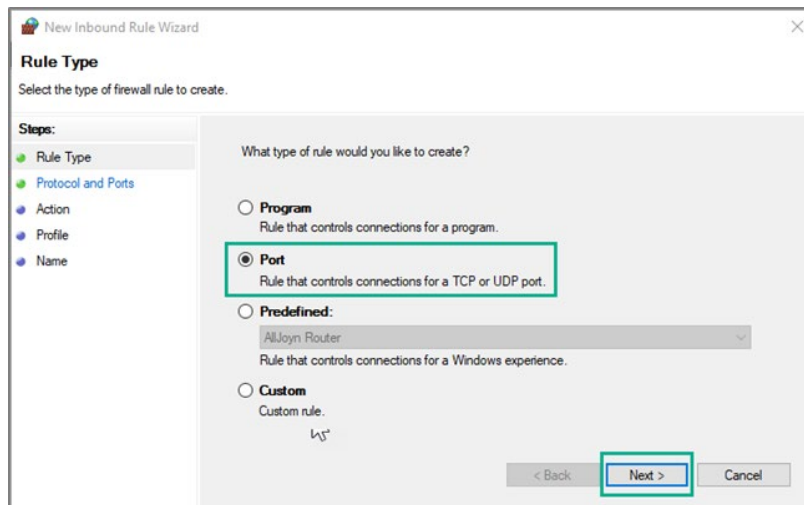
- The **Advanced Security** window will pop up. Select **Inbound Rules**. The goal is to allow inbound TCP traffic to the MFP agent on either or both ports 9100 and 515. This allows print jobs to be sent securely and held at the MFP agent until they are released for printing by the Synappx Go mobile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



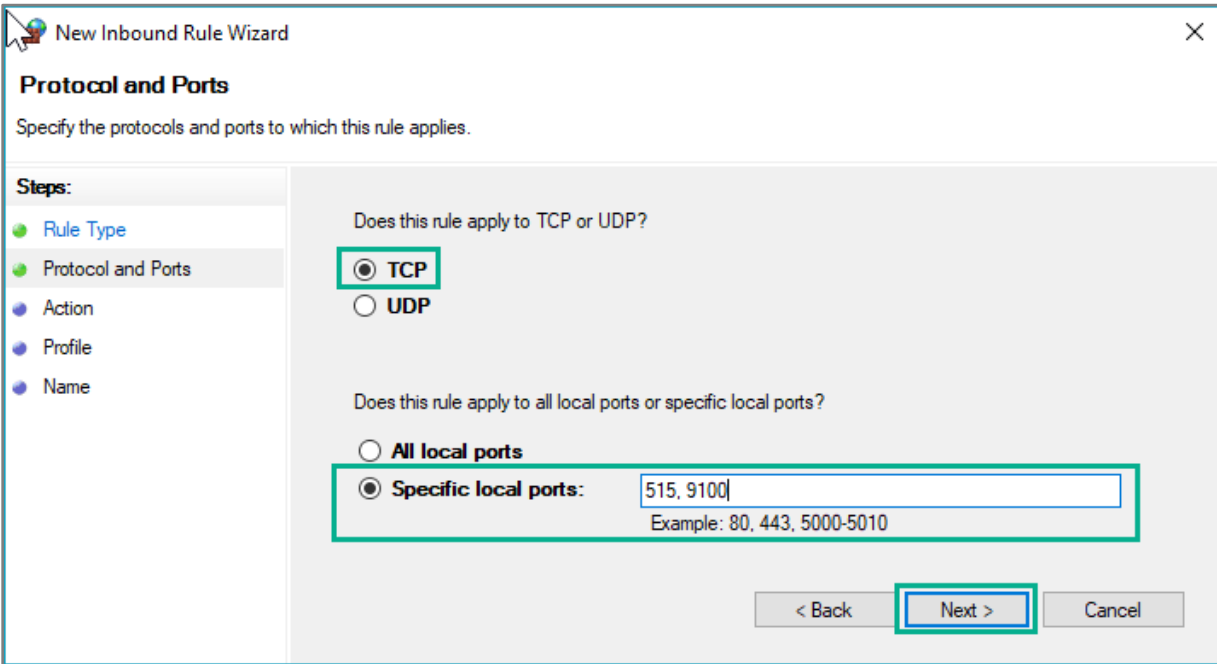
- Select the **New Rule** option on the **Actions** pane at the far right.



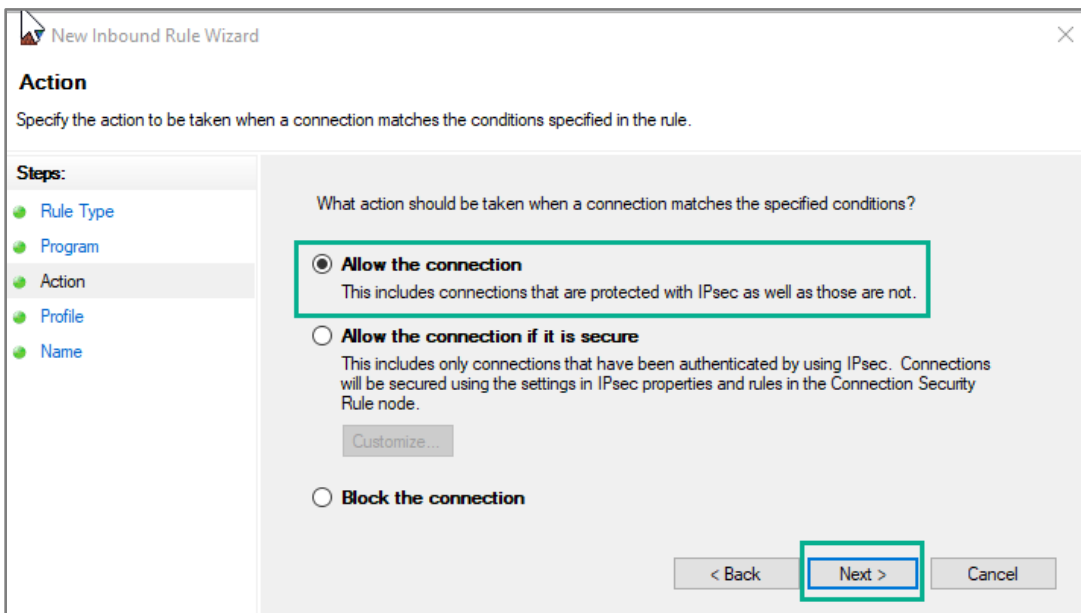
- The **Rule Type** window will pop open. Select the **Port** rule type. Then select **Next**.



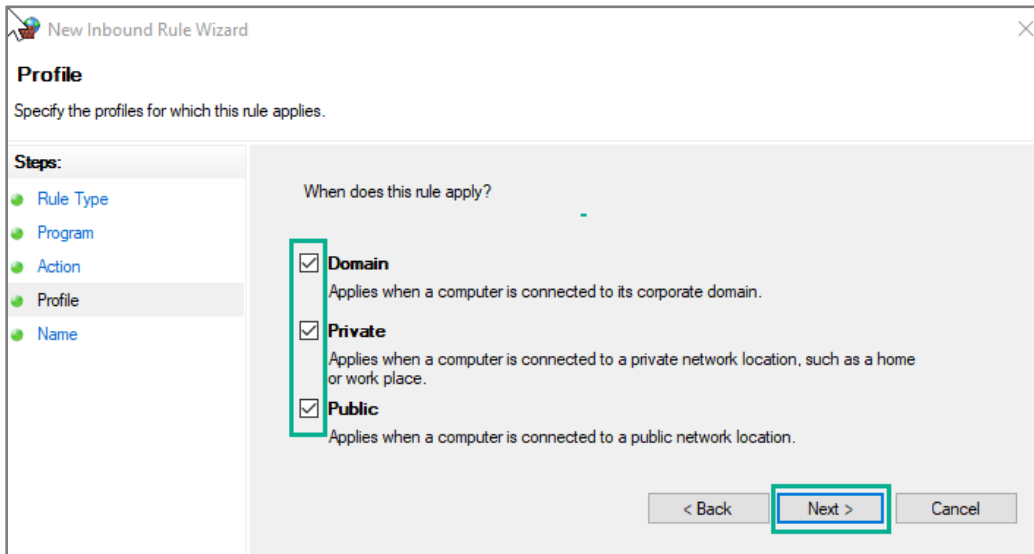
- On the Protocol and Ports window, select the **TCP** option and then select the **Specific local ports** option. In the adjacent field, enter the port(s) you wish to open for traffic. You can select 9100 (RAW), 515 (LPR) or both. The example below uses both ports. Select **Next** when finished.



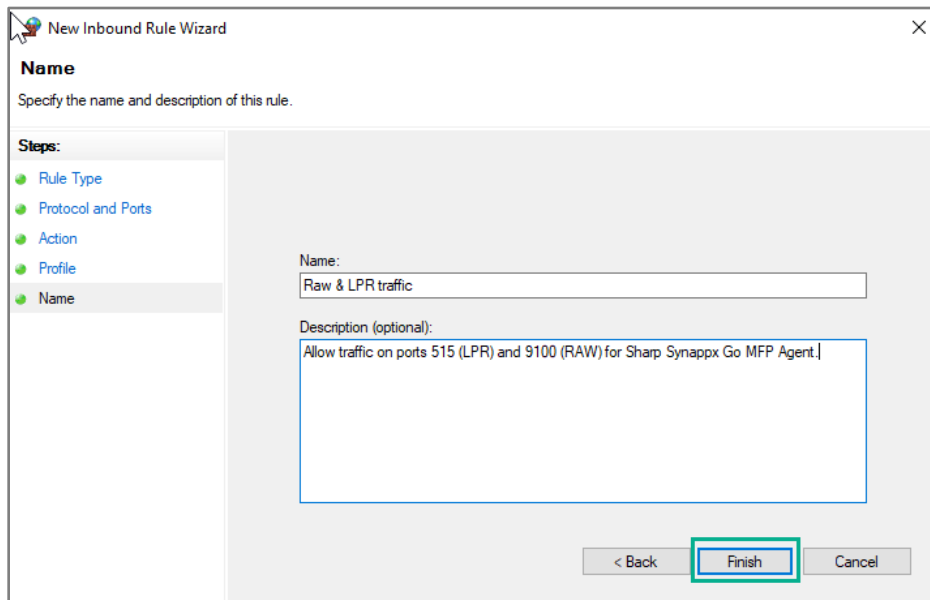
- Select **Allow the connection** and then select **Next**.



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



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



- 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. In many cases, users do not know the correct input for the display PC or may not be able to find the remote. This time-saving 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. 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)

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.

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

Supported With	LAN Telnet	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

Supported With	RS-232	Inputs											Power Controls	
Model	Display Gender	HDM I 1	HDM I 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

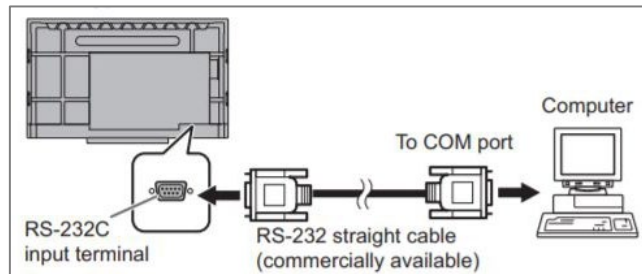
Notes

- RS-232C 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)**.

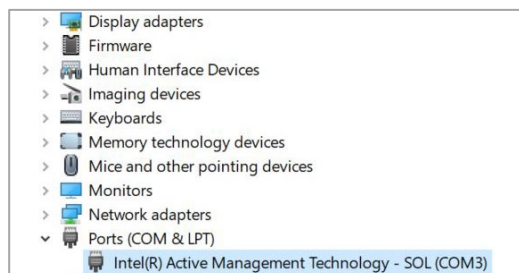
Note: Computers without serial ports may require USB-to-serial converters to allow compatibility with RS-232C serial devices. Before obtaining a USB connector, note the RS-232C (9-pin) connector on your display (connector gender varies). Note the cable recommendations in the [Supported IWB Models and Input Options](#) table.

2. Ensure all RS-232C 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**.

- For displays supporting **Application** mode, select the **Application** input. Open the **Settings/Setup** menu on the display.
- 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.
 - Display agents must already be installed and configured with Synappx Go workspaces before configuring displays for auto-input switch on the admin portal.
- Log in to the Synappx Admin Portal with your Microsoft® 365 or Google Workspace™ credentials.
 - If both Synappx Go and Meeting are licensed, choose **Synappx Go**.
 - Go to **Workspaces**.
 - Select **Devices & Agents**.
 - Select the **Display** radio button. The **Summary of Devices and Agents** display page will show all configured display agents.

Device / Agent PC	Agent ID / IP Address	Version	Updates	Display Information	Workspace
PC-C	d-20192631025 192.168.1.3	1.4.433.0		Configure	Office_3

- To set up auto-input switching information for each display, select **Configure** in the **Display Information** column. A dialog box will open.
- Be sure to choose the connection type: **Telnet LAN** or **RS-232C**. Enter the relevant information for the display.
- Select **OK** to save the settings. Auto-input switching is now available for Go users.

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. **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.
7. **Note** (optional): Add applicable notes.

Display Information
Input display information

Connection Type: LAN RS-232C

Display Name: _____ 🔍

IP Address (*): _____ 🔍

Port (*): 10008

User Name: _____

Password: _____

Go Agent PC Input: Manual ▾

Note: _____

(*) Mandatory

OK Cancel

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.

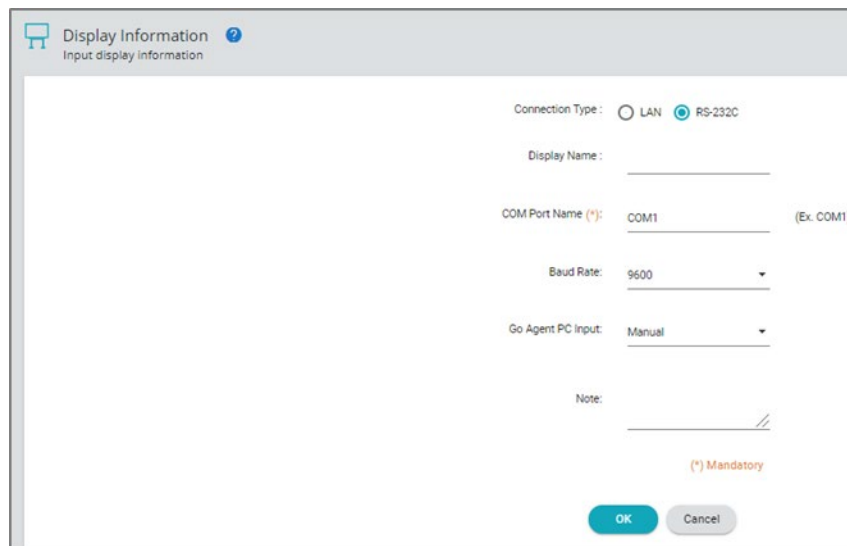
192.168.1.234 🔍

Display Name	IP Address	Port	User Name	Password	Go Agent PC Input	Workspace	Note
<input type="radio"/> Display1	192.168.1.234	10008	test	Manual	Office A	

OK Cancel

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. **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.
5. **Note** (optional): Add applicable notes.



The screenshot shows a configuration window titled "Display Information" with the subtitle "Input display information". The window contains the following fields and controls:

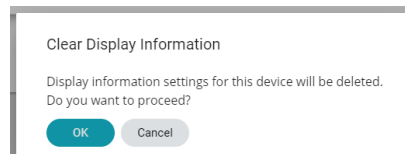
- Connection Type:** Radio buttons for "LAN" and "RS-232C". "RS-232C" is selected.
- Display Name:** A text input field.
- COM Port Name (*):** A text input field containing "COM1". A note "(Ex. COM1)" is to the right.
- Baud Rate:** A dropdown menu showing "9600".
- Go Agent PC Input:** A dropdown menu showing "Manual".
- Note:** A text area for entering notes.
- Buttons:** "OK" and "Cancel" buttons at the bottom.
- Legend:** A red asterisk (*) indicates "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.

Device / Agent PC	Agent ID / IP Address	Log	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.



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.

Agent PC/Server Name	Agent ID	Device	Display Information	NFC Tag ID	NFC Tag Action
oobstgfw10	d-201926310251011	Display	Edit Clear	c520571-9e86-43af-b84e-8674a62e9116	Share

Automatic Input Switch Usage

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

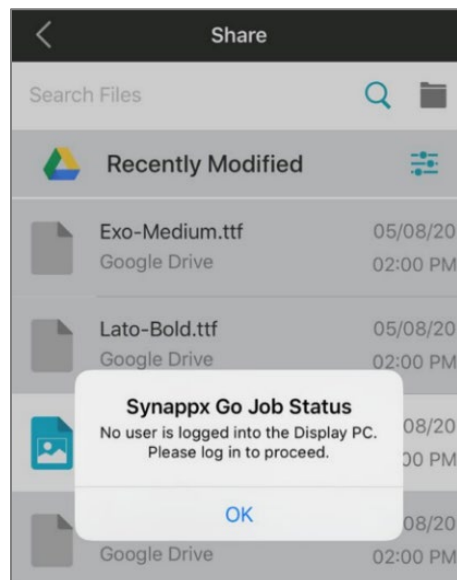
Auto input switching is supported in the following environments:

- Display and Display PC is 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.

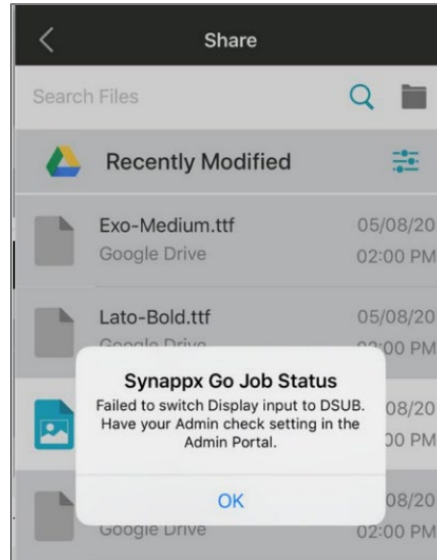
The NFC tap initiates auto-input switching if the display is not already on the defined Go agent PC input. Both tap first and tap last (i.e., foreground and background operation) are supported.

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.



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



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.

S Y N A P P X™



For more information, visit the [Synappx support site](#).

Access the [Synappx Terms of Use](https://business.sharppusa.com/synappx-support/about/termsofuse) at <https://business.sharppusa.com/synappx-support/about/termsofuse>.

Access the [Synappx Privacy Policy](https://business.sharppusa.com/synappx-support/About/Privacy) at <https://business.sharppusa.com/synappx-support/About/Privacy>.

Access the [Synappx End User License Agreement](https://business.sharppusa.com/synappx-support/about/EULA) at <https://business.sharppusa.com/synappx-support/about/EULA>.

©2020 Sharp Electronics Corporation. All rights reserved.

Design and specifications subject to change without notice. Some images appearing in this document are simulated. Sharp, Synappx, MICASSM, OSA[®] and all related trademarks are trademarks or registered trademarks of Sharp Corporation and/or its affiliated companies. Adobe[®] and Adobe[®] PDF are registered trademarks of Adobe in the United States and other countries. Amazon, Alexa and all related logos are trademarks of Amazon.com, Inc. or its affiliates. Android, Google Workspace[™], Google, Google Chrome[™], Google Docs[™], Google Drive[™], Google Sheets[™], and Google Slides[™] are trademarks of Google, Inc. Apple[®], iCloud[®], Mac[®], macOS[®] and iPhone[®] are registered trademarks of Apple Inc., registered in the U.S. and other countries. Azure, Microsoft[®], Microsoft[®] 365, Microsoft Teams, Outlook[®], OneDrive[®], PowerPoint[®], Sharepoint, Windows[®] and Windows[®] 10 are registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries. Box is a trademark of Box, Inc. Crestron[®] and the Crestron logo are trademarks or registered trademarks of Crestron Electronics, Inc. in the United States, other countries or both. Dropbox is a trademark of Dropbox, Inc. GoToMeeting[®] is a registered trademark of LogMeIn, Inc., in the United States and other countries. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. Shuttle is a registered trademark of Shuttle Inc. WEBEX, CISCO, Cisco WebEx, the CISCO logo, and the Cisco WebEx logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliated 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.