Security White Paper for Synappx Applications and Services

Sharp Electronics Corporation
January 2024

Contents

Synappx Security White Paper

1. Introduction

Overview

Synappx application services help bring smarter office experiences. They are designed to help optimize hybrid collaboration experiences. Synappx application services are protected by a robust, layered security system to ensure the system and its components are not opening points of vulnerability for your data or networks. Through a combination of world-class technology providers including Microsoft Azure, Google Workspace and security best practices, your use of the Synappx application services helps keep your information safe and secure while helping you enhance productivity in your office.

Security provisions related to Synappx application services are described in this white paper.

Synappx Go

Synappx Go leverages the Azure cloud and rich client technologies to help users increase productivity and work efficiently. Synappx Go offers features for Sharp multifunction printers (MFP) and for collaboration with Sharp displays. For MFPs, it enables convenient and time-saving features including scanning to favorite destinations, print release, printing cloud files and copying on Sharp MFPs throughout your office. Collaboration, users can use their mobile phone or laptop to quickly start and participate in meetings via a QR Code, Near Field Communication (NFC), or pairing code. It provides a simplified meeting experience via remote control of the web conference on the meeting room display including the microphone, camera, and screen share from the Synappx mobile or laptop app. You can also select, download, and remotely control cloud content and files on the Sharp display from your mobile. Plus, you can use the mobile app for touchpoint tracking in the office. Synappx Go cloud software and services leverage the Microsoft Azure database, device provisioning, IoT Hub and many other services.

Note: A No Login, Free version of Synappx Go (license not required) is also available. The security features of that Synappx Go variant are described here.

2. Synappx Cloud Services

Synappx application services leverage Microsoft Azure cloud platform services as a foundation. Microsoft Azure is a highly respected global cloud service with a wide range of features that are used by the Synappx applications, including the Azure Cosmos database, storage, several IoT Services, Key Vault, Security Center monitoring, backup and more.

Synappx application services are hosted in secure Microsoft data centers located the U.S. Microsoft Azure cloud and data centers are protected through Microsoft's security practices. Each data center provides local data redundancy. In addition, all communication between Synappx client applications and Synappx cloud services (hosted on Microsoft Azure) are encrypted via HTTPS (TLS v1.2, AES256), or secured through X.509 certificates, when using MQTT or MQTT Over WebSocket, AMQP or AMQP Over WebSocket (used by the MFP and Display Agent).

Access to all the Synappx application services from client applications require secure keys, certificates, or authentication tokens. After purchasing a Synappx subscription service, each customer is assigned a unique certificate for communications that is stored in Microsoft Key Vault to enable secure, customer-only access. Synappx Azure database access is limited to whitelisted IP addresses from secure Azure App Services. Microsoft Key Vault is used for storage of SSL certificates, X.509 signing certificates, private keys, and other content requiring the highest security. Access to Microsoft Azure Key Vault is limited only to Sharp service principals and system users with associated access permissions.

The customer specific data used for the Synappx applications stored in the secure Azure cloud databases include the following:

Common to all Synappx Applications:

- User first name, last name, email address (imported from Azure AD or Google Workspace to Synappx by Admin) and IP address
- Admin user first name, last name and email address (imported from Azure AD or Google Workspace to Synappx by Admin)
- Workspace (meeting room) names, email addresses and locations imported from Microsoft Outlook or Google Workspace Directory to Synappx by Admin
- Manually added workspace names and locations
- Company domain aliases from Azure AD and Google Workspace
- Application usage data to generate reports for Admin use
- Synappx license data (e.g., expiration)
- System and Admin logs (including date and time for log events)
- Display IP address and port (if configured by Admin)
- Optional Display account ID and display password (if configured by Admin)

Synappx Windows Client Specific:

- Casting sender type, IP address and PIN (if configured by Admin)

- Meeting name, actual meeting duration (start time and end time), meeting location name, attendee name and attendee email address. Meeting names, location names, attendee names and email addresses are anonymized so Sharp cannot view those. Only the customer can see the non-anonymized data.

Synappx Go Specific:

- MFP information (model name, IP address, serial number) discovered via Admin initiated SNMP discovery
- MFP Agent information (computer name, computer ID, version number, update policy, date last updated)
- Display Agent information (computer name, computer ID, IP address, version number, update policy, date last updated)
- Check in logs (date/time, username, email address, workspace location, device IP address, activity type)
- NFC tag information (tag ID, type) associated with Admin configured devices and touchpoint tracking
- QR code information associated with display agents
- Temporary storage of meeting organizer email address if they've uploaded attachment changes (4 hours).

Data in Synappx databases is only accessible to licensed customers via the Synappx applications and limited Sharp staff if required for support purposes.

Overall, Sharp governance of the Synappx application services limits system access to minimal staff for deployment and support purposes. See Sharp security policy sections for more details.

For more information on Microsoft Azure security, see the following links related to features used by Synappx services:

- Overview: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Data Encryption at Rest: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Azure Network Security: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Azure Functions and Serverless Platform Security: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Azure Storage Security Guide: https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Security Management in Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Azure Management-Governance: https://docs.microsoft.com/en-us/azure/governance/

3. Synappx Admin Portal

Administrators (Admins) use, configure and manage the Synappx applications through the Synappx Admin Portal web pages. Managing workspaces/meeting rooms, users, devices, additional Admins and more are performed via these secure web pages. License management is done via the Admin Portal and license status can be viewed here (when applicable). Analytics reports help demonstrate Synappx system usage and business value. Downloads (for Synappx Go) are conveniently accessible via these pages. System, Admin and Check In logs can be downloaded.

3.1 Synappx Supported Domains

For Microsoft 365 and Google Workspace accounts, Synappx application services collect information on the domain aliases supported in the account's Azure AD or Google Workspace system. For Microsoft 365 accounts, in the Admin Setting/Supported Domains web page, if the Azure Global Admin does initial permission opt in or manually adds domains, Admins can select additional domain aliases beyond the primary Azure AD domain under which the Synappx account was created. This allows users and workspaces to be imported from selected domains to be used with Synappx services.

3.2 User Authentication

Synappx application services leverage Microsoft 365 or Google Workspace credentials to avoid having to set up, manage and protect separate Synappx log-in credentials. By design, Synappx application services do not have access to Microsoft 365 or Google Workspace customer passwords. The system leverages Azure Active Directory or Google Workspace Directory and relies on authentication tokens to identify Admins and users (for client access). The user identity is confirmed with your Microsoft Azure AD (for Microsoft 365 accounts) or Google Workspace Directory (for Google Workspace accounts) through a secure identity partner Auth0 (see below) and these user passwords are never stored in Synappx nor Auth0 systems. The Synappx platform securely stores the user email address, IP address and first/last name only. No other personally identifiable information about the user is known or stored by the Synappx system. Auth0 has many certifications for cloud security including: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, , Gold CSA STAR, GDPR compliance and more.

For more information about Auth0 and security provisions, go to:

https://auth0.com/security/

3.3 Role Based Access

Access to the Synappx Admin Portal and Synappx applications is controlled using tenant-based and role-based authentication processes. The initial Administrator is identified as part of the purchase order process. Additional Admins can be added after successful log in to the Synappx portal by the initial Admin.

Only Admins designated or assigned by the customer can access, configure, license and manage Synappx service users and workspaces, view reports, etc. from their account via the secure web portal. All communications with the Admin Portal are via HTTPS/SSL (TLS1.2) port 443 to protect data in transit.

Admin User Types:

- Primary Admin: The first Admin who is only one person in one tenant. This user role has the same privileges to Admin.
- Admin: This user role can manage users, roles, licenses, and data entities such as workspaces, MFPs and agents. Also, this user role can see Admin log, System log and Analytics reports.
- Support Admin: This user role can see data entities and Admin log and System log.

User Types:

- User: This user role can log in to Synappx Windows client and Synappx Go mobile and use them.
- Guest User: This user role can log in to Synappx Windows client and Synappx Go mobile and use them.

Guest Admins and Users can use their normal Microsoft 365 or Google Workspace credentials to access Synappx features after Admin configuration or other types of accounts (e.g. social) create a separate Synappx log in and password to use Synappx as a guest. For non-enterprise Synappx guest users only, the Synappx guest user login and password (hashed) are stored in a secure Auth0 database.

3.4 Granting Synappx Application Privileges

3.4.1 Microsoft 365 Users

To use Synappx applications including Admin Portal, Go Windows and Go Mobile, the user is required to grant permissions shown in the table below. Permission consent screen is shown for every user for the first-time log-in.

Permissions Requested	**Definition**	**Admin Portal**	**Go Windows**	**Go Mobile**
Microsoft Graph:				
• Calendars.ReadWrite.Shared	Allows the app to create, read, update (e.g. extend time) and delete events in all calendars the user has permissions to access. This includes delegated and shared calendars.	No	**Yes**	**Yes**
• User.Read	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Yes	**Yes**	Yes

• Directory.Read.All	Allow the app to read sub domains.	**Yes***	No	No
• Files.ReadWrite.All	Allows the app to read, create, update, and delete all files the signed-in user can access.	No	**Yes**	**Yes**
• Group.Read.All	Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.	**Yes***	No	No
• People.Read	Allows the app to read a scored list of people relevant to the signed-in user. The list can include local contacts, contacts from social networking or your organization's directory, and people from recent communications (such as email and Skype).	No	Yes	No
• Team.ReadBasic.All	Allows app to get a list of Teams to retrieve documents for the user to share.	No	No	**Yes**
• User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization and locations on behalf of the signed-in user.	**Yes***	No	No
• User.ReadBasic.All	Allows the app to read a basic set of profile properties of other users in your organization on behalf of the signed-in user. This includes display name, first and last name, email address, open extensions and photo. Also allows the app to read the full profile of the signed-in user.	**Yes**	No	No
• offline_access	Allows the app to read and update user data, even when they are not currently using the app to keep log in state,	**Yes**	**Yes**	**Yes**
• email	Allows the app to read your users' primary email address.	**Yes**	Yes	Yes
• openid	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.	**Yes**	Yes	Yes
• profile	Required to obtain user profile information (e.g. user first and last name, email address) from Azure AD.	**Yes**	Yes	Yes

* These permissions are optional. On the Admin Portal, Azure Global Administrator can grant global permission shown in the table below. If he does so, the following features can be available:

・Group search for users and workspaces

・Automatically sub-domains are listed in the "Supported Domains" page

・Location information of workspaces are available

Permissions Requested	Definition
Microsoft Graph:	
• Directory.Read.All	Allows the app to read data in your organization's directory, such as users, groups and apps.
• Group.Read.All	Allows the app to list groups, and to read their properties and all group memberships on behalf of the signed-in user. Also allows the app to read calendar, conversations, files, and other group content for all groups the signed-in user can access.
• User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.

3.4.2 Google Workspace Users

To use Synappx applications including Admin Portal, Go Windows and Go Mobile, the user is required to grant permissions shown in the table below. A permission consent screen is shown for every user for the first-time logging in.

Google API Scopes Requested	Definition	Admin Portal	Go Windows	Go Mobile
https://www.googleapis.com/auth/admin.directory.domain.readonly	Allows the app to read domain information for supporting multi-domain feature.	Yes	No	No
https://www.googleapis.com/auth/admin.directory.group.readonly	Allows the app to retrieve group, group alias, and member information to add groups via the Admin Portal.	Yes	No	No
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Allows the app to retrieve calendar resources to add workspaces via the Admin Portal.	Yes	No	No
https://www.googleapis.com/auth/admin.directory.user.readonly	Allows the app to retrieve users or user aliases to add users via the Admin Portal.	Yes	No	No
https://www.googleapis.com/auth/calendar.readonly	Allows the app to have read-only access to Calendars.	Yes	**Yes**	**Yes**
https://www.googleapis.com/auth/calendar.events	Allows the app to have read/write access to events on a calendar and update it (e.g. extend the meeting time).	No	**Yes**	**Yes**
https://www.googleapis.com/auth/drive	Allows the app to have access to authorized user's Google Drive files (excluding the Application Data folder) to list files.	No	**Yes**	**Yes**
https://www.googleapis.com/auth/directory.readonly	Allows app to see and download your organization's Google Workspace directory	No	**Yes**	**Yes**
https://www.googleapis.com/auth/userinfo.profile	Allows app to use personal information user has made publicly available to get username and avatar image.	Yes	**Yes**	**Yes**

However, the following features are unavailable until the custom role is assigned to the user.

- Group search for users & workspaces
- Automatically sub-domains are listed in “Supported Domains” page

Custom role requires the permission shown below which can be set from the Google Admin page.

- Admin API privileges – Users.Read, Groups.Read, Domain Management

3.5 Importing Users or Workspaces from Azure AD or Google Workspace

Synappx Go licenses the service on a user basis and Synappx Windows licenses are based on workspaces/meeting rooms. In order for the Synappx collaboration hub experience to support efficient meetings, it requires both Synappx Windows and Synappx Go licenses. Admins can directly import Users (for Synappx Go) and Workspaces (e.g. Rooms) for both applications from Microsoft 365 (Azure AD) or Google Workspace. Manual entry of Workspaces is also permitted. Users in the supported domains and in Azure AD or Google Workspace can be added as licensed Synappx Go users. Communications with Microsoft Azure and Google Workspace for User and/or Workspace import is via HTTPS (port 443). Guest users with Microsoft 365, Google Workspace or Synappx custom credentials can also be manually added.

3.6 Synappx Analytics Reports

Synappx helps Admins understand Synappx application usage and value. Data generated in the Synappx reports is stored on secure Microsoft servers. Data is retained for 45 days after the service is terminated by the customer (to allow time to renew the license if desired). User specific information in the reports is only available to Admins within the company via the Analytics pages. Anonymized summary data about customers’ application usage is available to Sharp for purposes of support and product enhancement over time. See Sharp Corporate Security, Sharp Admin Data Access and Sharp Privacy Policy for more details.

3.7 Synappx System Logs, Admin Logs and Check In Logs

Synappx Go includes a System Log containing information about system events of potential interest to Admins. These include conditions that might require Admin intervention to correct an issue or perform troubleshooting. System logs can be exported by Admins as a .CSV file for further analysis. System logs are retained by the Synappx system for 30 days.

There is also an Admin Log that contains information about Admin interactions with the Admin Portal. Because multiple Admins can be assigned and provided access to the Synappx Admin Portal, this log captures major

actions taken by the Admins. Admin Logs can also be exported as a .CSV file for analysis. Admin logs are retained by the Synappx System for 90 days.

Finally, there is also a Check In log that can be exported as a .CSV file to support Synappx user touchpoint tracking throughout the office. This log is retained by the Synappx system for 30 days.

3.8 Configuration for Tap to Start from Display

Synappx Admin Portal provides the PowerShell script to configure Microsoft 365 meeting room mailbox settings to enable/disable users to directly touch the calendar item shown in Synappx Go Windows app on the In-Room PC. This configuration with the script is optional and needs to be done by Microsoft 365 Admins having Exchange Administrator role of Microsoft 365. The script only changes the properties of the specific mailbox.

What attribute of mailbox to be changed by the script is as follows:

Attribute of the mailbox of the resource account (meeting room calendar)	**Default value**	**Change to (When enable)**	**Description**
AddOrganizerToSubject	True	False	True: Change the meeting subject into organizer's name. False: Do not change. -> This change avoids adding the meeting organizer name to the subject of the meeting in the meeting room (resource account) schedule. (No extra information is added to the meeting title) Synappx Go app doesn't become to do anything new by this change.
DeleteComments	True	False	True: Delete the description of the meeting. False: Do not delete. -> This change keeps any text in the message body of incoming meeting requests in order for Synappx Go app to obtain meeting URL to join.
DeleteSubject	True	False	True: Delete the meeting subject. False: Do not delete. -> This change keeps the meeting title in the meeting room (resource account) schedule. Synappx Go app doesn't become to do anything new by this change.
DeleteAttachments	True	False	True: Delete the attached files. False: Do not delete. -> This change keeps the attachments in the meeting room (resource account) calendar so that Synappx Go app can access the attachments.
ProcessExternalMeetingMessages	False	True	False: Do not be booked. True: The meeting room (resource account) schedule is booked automatically by the scheduled meeting from a sender outside of the organization. -> This change enables Synappx Go app to start the meeting from a sender outside the organization.

4. Agent Communications

Installed on premise, the Synappx agent plays a role to securely connect to endpoints and cloud services to deliver application features. To install the Synappx agent, the custom install package is downloaded from the Synappx Admin Portal with a configuration file unique to the customer. The configuration file contents are secured via encryption algorithms. After install, to register itself, the agent submits its unique identifier, along with agent security credentials, to the Synappx Cloud for registration into the Device Registry. Information stored in the Device Registry includes data such as device ID, location, and tenant ID.

Following agents are available:

- Synappx Go MFP Agent
- Synappx Go Display Agent

All communications between the Synappx Agent and Synappx Cloud use either HTTPS (Port 443), or X.509 client security over MQTT,MQTT Over WebSocket, AMQP or AMQP Over WebSocket.

The Synappx Go cloud services maintain separate signing certificates for each Synappx customer. This ensures agents are provisioned only within their associated tenant registry.

4.1 Synappx Go Agent Download

The Synappx Go MFP and Display Agents can be downloaded from the Synappx Admin Portal's Downloads page. The downloaded agents are not available from public web sites and can only be downloaded by authorized Synappx Admins. An encrypted (SHA-256) configuration file is packaged with the zip file containing tenant specific information and customer entered information to enable automatic MFP discovery via SNMP (for the MFP Agent) and tenant connection. A non-tenant specific version of the Go common installer is also available from the downloads page and is pre-installed on some Sharp display PCs. That agent can only be activated if a valid Admin enters credentials to associate the display agent with that customer account.

4.2 Synappx Go MFP Agent Device Discovery

To automate the collection of MFP information (needed to configure the Synappx Go MFP services), the MFP Agent includes the ability to find MFPs using SNMP discovery. Discovery is automatically initiated after initial agent installation. The admin enters the beginning and ending IP ranges via the Admin Portal to search and can also re-search on-demand (also initiated by the Admin via the Admin Console) using port 443. The following information about the MFP is collected as part of this process and sent to the Synappx Go cloud:

- MFP Agent ID, MFP ID that system creates (e.g. Sharp MX-C301W 63004882), Manufacturer, Model Name, Serial Number, Device Name (If Set), Location (If Set), Network IP Address

4.3 Synappx Go Display Agent

To enable Share to Display use and collaboration features,, the Synappx display agent must be installed on a Windows PC or server connected to a display. A core function of the agent is to establish a secure communication channel to the Synappx cloud.

- The agent interfaces to the cloud to register and secure device communications and send/receive messages to and from the agent. Each agent has a unique identifier, and this is what the Synappx Go cloud system uses to identify which agents to send messages to.
- Agents listen for messages by subscribing to their unique identifier topic and the cloud services send messages by publishing to that identifier topic.

4.4 Synappx Go NFC Tags

Synappx Go utilizes special NFC tags provided by Sharp, authorized resellers and/or embedded in select MFP models. The tags contain a unique identifier and are Read Only (cannot be re-programed). Each tag can only be associated with one device at a time. Once configured to a device (e.g. MFP or display PC) or for check in by the Admin via the Synappx Go mobile app, when a user taps the NFC tag, the tag and mobile app together identify the user identity, device and location associated with the tag/device to enable the Synappx Go use cases such as scanning to email, copy, print release, print cloud files, start/conduct/end meetings, share to display and touchpoint tracking. Note that some Sharp MFPs also have embedded NFC tags that can be used when associated via Synappx Go mobile.

4.5 Synappx Go Print Release, Scan and Copy

An Admin or user can configure a Sharp printer driver to point to the Synappx Go Agent/Print Release PC or server. When sending jobs to the print release driver, licensed Synappx Go users' print files are automatically stored in a folder for each user on the Agent PC/server to be released by the user at any Synappx tag configured MFP.

- Print files (.prn format) stored on the server will be automatically deleted after 24 hours.
- The prn. files are only visible to authorized Admins that have access to the computer via normal PC/server password protection.

The customer network impacts are related to use of Synappx Go user scan, print and copy use. Estimated impacts include:

- Scan to favorite destinations (per user)—estimated at 1 MB per scan average (could vary)
- Secure print (per user per print job)—estimated at 1.2 MB per print job average (could vary)
- Print cloud file (per user per print job)—estimated at 1.2 MB per print job average (could vary)
- Copy file (per user per copy job)—estimated at 1 MB per copy job average (could vary)

5. Synappx Go MFP Lite (No Login)

As an alternative to the fully featured, licensed Synappx Go application, there is an option for users to access Synappx Go No Login without requiring subscription service, agent, and NFC tags. It enables simple copy and scan to email functions by scanning a QR Code.

- No user credentials are needed to access the No Log in features. Users can optionally enter their email address to scan to themselves and that information is stored only in their mobile app.
- Users can optionally approve access to their mobile contact list for convenience in entering email addresses to scan files from MFPs to others.
- Users are asked to provide access to their mobile camera to enable scanning the MFP QR code (to complete scan or copy). MFP QR code is changed with every scan or copy job to ensure jobs are processed on the correct MFP.
- Requires installation of an embedded application for each MFP to be used for scan and copy features. MFP communicates to Amazon Web Services (AWS) cloud application.
    - Communications between MFP and AWS cloud is via HTTPS (port 443)
    - See AWS security whitepapers for other cloud security (https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/introduction-aws-security.pdf

6. Synappx Go for Collaboration

Synappx Go for collaboration allows laptop and mobile-first users to be more productive, providing flexibility and confidence during a meeting though a consistent user experience.

- Microsoft 365 and Google Workspace support
  - Microsoft Graph API is used to get meeting information and files from Microsoft Office 365. Google API scopes get information and files for meetings from Google Workspace.
  - Azure and Google Workspace meeting room information is accessed from the Synappx Admin Portal.
- Synappx Go client application on the in-room PC is logged in with a resource account (Microsoft 365) or user account to which meeting rooms are mapped (Google Workspace). When the user enters a pairing code on their laptop, taps the NFC tag or scans the QR code with their Synappx Go mobile, the system switches Synappx Go to the user account (passed from Synappx Go) to get the meeting information and start the meeting. When the meeting is ended, Synappx Go reverts to the resource account or user account for the room.
- When the in-room PC is also kept logged in with a resource account, it is recommended to take necessary measures to maintain the security and integrity of that PC.
  - Protect unwanted access to applications and Windows features by utilizing Synappx Go's full screen mode combined with the in-room PC security features. Desktop and taskbar access as well as access to Windows registry can be protected.
  - Utilize the reset room feature to clear cache and remove files added to the supported folder locations at the end of the meeting.
  - It is strongly recommended to disable the chat feature (e.g. Microsoft Teams) of the resource account.
- Meeting attachments from the Outlook or Google Calendar invite can be downloaded for viewing or editing. Changes to attachments or saved Pen Software files are sent to Azure and a link to the edited file is provided to the meeting organizer. The link is active for seven (7) days.
- Synappx Go supports several videoconferencing systems: Microsoft Teams, Zoom, Google Meet and GoTo Connect. For Zoom, Synappx uses stored Zoom's access token to access Zoom for automated meeting starts. The token is generated through user log in to Zoom account on the Synappx app.

6.1 Application Security

All communication between endpoints and Synappx application services are secured and encrypted via TLS v1.2 AES256 (Port 443) or X.509 client security over MQTT, MQTT Over WebSocket, AMQP or AMQP Over WebSocket. Synappx users authenticate with Synappx applications using Microsoft 365, Google Workspace or Synappx non-enterprise guest credentials the first time he/she uses the Synappx app, when there are credential changes (e.g. password update), they log out of the mobile app and/or after 30 days or more with no app use. Synappx leverages:

- Auth0 (User authentication delegation to Azure AD, Google Workspace and for Synappx non-enterprise guest user database)
- Azure AD (User authentication with Microsoft 365 account) or Google Workspace (User authentication with Google Workspace account)

User passwords are not stored on the client device; instead, a secure JWT token is provided after user password validation with Azure AD or Google Workspace system via a partner Auth0.

6.2 Synappx Go Windows Application

Synappx Go Windows app is designed to be installed on the in-room PC connected to a meeting room display, or on users' laptop to help connect to the display in the meeting room, start web conference and operate applications. Synappx Go client provides a broad range of security features including:

- Access to local display and in-room PC can be protected using Synappx Go features.
    - Full Screen Mode to display only approved applications.
    - In-room PC Security to minimize unwanted access to Windows components and features.
    - Reset Room to protect privacy and prevent accidental sharing of confidential information.
- User passwords are not stored on the Synappx Go client. A secure JWT token is provided after user password validation with Azure AD or Google Workspace system via a partner Auth0.
    - User access token is stored on local user computer (only for the laptop mode)
        - ID/Password for proxy are stored on local storage. (Encrypted using AES128)

6.3 Synappx Go Mobile Application

Synappx Go mobile app offers features including print/copy/scan on Sharp MFPs and collaboration using Sharp display products. Security features associated with the Synappx Go mobile clients are:

- User mobile access is controlled centrally via the Synappx Admin Portal. Admins can remove a user license to block subsequent use of the Synappx Go mobile features.
- Users are requested to grant access to their mobile contacts list to create scan to email destinations without having to re-enter target user emails. This saves time and reduces typing errors.
- For cloud storage service's file and folder access, users can configure Synappx Go application to access files from supported cloud storage sites. Some cloud sites are pre-configured via Single Sign On (SSO) to minimize set up time.
    - Microsoft 365 users: SSO to One Drive for Business, SharePoint Online and Teams.
    - Google Workspace users: SSO to Google Drive.
    - Apple iPhone users: SSO for iCloud and Local files.
- Optional cloud site set-up (e.g., Dropbox, Box)
    - For storage sites of interest, users can enter their username and password which are validated with the cloud storage sites. If validated, a secure token is provided and stored in Synappx Go mobile (and secure token is also in Azure Key Vault for Box and non-enterprise Google Drive) to avoid the user having to re-enter those credentials unless they are no longer valid (e.g., password change, account deactivated, etc.).
    - Sharp and component suppliers do not have access to user cloud storage site passwords.
    - For each cloud storage service, the user will be requested to give the Synappx app selected permissions to be able to access and update files the user chooses to download to a display and edit or edit via the display PC browser. Note: The Synappx Go service has no function to delete files or folders from any user cloud storage site.

- File Share on Display
    - Files are uploaded to the cloud storage site or Azure cloud via AMQP, AMQP over WebSocket or HTTPS.
    - The files are temporarily stored on the in-room PC.
    - If the user saves a file after making changes, it will be saved back to the same cloud folder location as either a new version and/or with an appended file name (subject to the policy of each cloud storage site). When the file is not saved, it will be removed from the temporary Display PC folder.
    - Alternatively, users can open selected cloud files in the in-room PC's Chrome browser in Incognito mode for direct editing. This feature also requires the user to configure Multi Factor Authentication (MFA) for additional security. Users will be prompted with MFA to get a passcode on their mobile device and send it to the in-room PC (user does not need to log in again to that PC for 14 days (Google user) to 90 days (Microsoft user). Synappx stores an encrypted session cookie for that user login. If the user doesn't want the convenience, he/she can log out of the Chrome browser after finishing browser-based editing and it will invalidate that cookie. Note: User passwords are not stored by the Synappx system.

6.4 Synappx Go NFC Tags, QR Code, and Pairing Code

Users have the following options to start meetings including the launch of supported conferencing systems (if part of the meeting invite):

- With Synappx Go mobile apps, to launch a meeting and/or share content to the display:
    - Tap a configured Synappx NFC tag.
    - Use phone camera to capture the QR code displayed on the in-room display.
    - Note: When starting a meeting via mobile, user can tap the NFC tag or scan the QR code before or after selecting a scheduled meeting depending on preference.
- With Synappx Go Windows, to launch a meeting:
    - After selecting a scheduled meeting or creating an ad hoc meeting, enter the pairing code shown on the display in the prompt on the laptop screen. The display pairing code changes after each use.

Multiple users who are invited can join a meeting using these methods. The QR code and pairing code are refreshed and updated when a meeting session is ended.

7. Corporate Security

Sharp maintains a robust information security program to protect the confidentiality, integrity and availability of all information assets processed and/or stored within Sharp's business systems. Sharp management recognizes the rapidly evolving and growing risks associated with the protection of Sharp and our valued business partners' information assets and is regularly researching, reviewing and investing in procedural and technical countermeasures to help optimize security assurance. A team of dedicated professionals are continuously assessing the business environment utilizing their professional expertise to enhance and continuously improve Sharp's information security posture. In addition to these internal efforts, Sharp utilizes strategic partnerships with industry leading service providers to test, monitor and audit our implemented information security programs.

7.1 Corporate Policies and Practices

Sharp has implemented several policies and procedures to ensure the security of Sharp and our business associates' information assets. All of Sharp's policies and procedures are regularly reviewed internally and updated annually. All of Sharp's policies and procedures are audited annually by our Internal Audit team and by our external auditors, as well as ISO/IEC 27001 certification and compliance.

The following list is a representative example of the policies currently in place as of the date this document was published:

- IT Security
- IT Access Control
- IT Change Management
- IT Threat and Risk Assessment
- IT Incident Handling
- IT Disaster Recovery
- IT Records Management
- IT Computer

Sharp is ISO/IEC 27001 certified (renewed July 22, 2020)
https://global.sharp/corporate/eco/governance/security/

Due to the confidential nature of the content of these policies they are not regularly distributed but can be made available for review with Sharp upon execution of a Nondisclosure Agreement.

7.2 Sharp Administrator Access of Data

Sharp IT or Support may occasionally need to access your data in order to provide support on technical issues. Access permissions for these types of issues will be limited to the minimum permission necessary to resolve your

issue. Sharp administrators are granted careful role-based permissions in order to uphold data security for the customer:

- Ability to view and update customer account information, such as account status and email address, but not customer files.
- Ability to see the file tree and file names, but not view or download the actual files.
- Synappx users, admins and dealer admins all have appropriate access to items within their scope of authority and nothing else. System administration is strictly controlled and limited to Sharp authorized personnel. Sharp admins can only access information critical to the operation of the system. At no time are users of the system allowed to access the database or other system components directly.
- Note: Data related to your Synappx services will be deleted 45 days after a subscription termination date.

7.3 Sharp Privacy Policy

Please see the Synappx service terms of use and privacy policy at:

- https://business.sharpusa.com/synappx-support/about/privacy
- https://business.sharpusa.com/synappx-support/about/termsofuse

8. Summary

Making the move to cloud-based, on-the-go collaboration and meeting services offers businesses an economical way to support increasingly mobile workforces. Indeed, to build collaborative, responsive office environments, adoption of cloud and mobile technology isn't a case of "if" but "when".

Organizations that embrace cloud-based services fully utilize their existing technology investments, including computers, mobile devices, interactive display systems and MFPs. Combined with the Synappx subscription-based services, the elimination of capital expenditures for internal IT resources means even lower total cost of ownership. Yet some decision makers struggle with what cloud implementation entails, in terms of balancing convenience with accessibility and security. Sharp Synappx services help remove these barriers with a security-driven architecture and hardware/software synergy that enables agile workgroups, which can quickly respond to business demands.

Design and specifications subject to change without notice.

SHARP ELECTRONICS CORPORATION

100 Paragon Drive, Montvale, NJ 07495-1163

1-800-BE-SHARP • www.sharpusa.com

Document Number **19147**