Security White Paper for Synappx Meeting and Synappx Go

Sharp Electronics Corporation
April 30, 2020

Contents

Synappx Go and Synappx Meeting Applications

Security White Paper

1. Introduction

Overview

Synappx Go and Synappx Meetings are collaboration, productivity and analytics applications and services. They 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, G Suite and security best practices, your use of the Synappx services helps keep your information safe and secure while helping you enhance productivity in your office.

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

Synappx Go

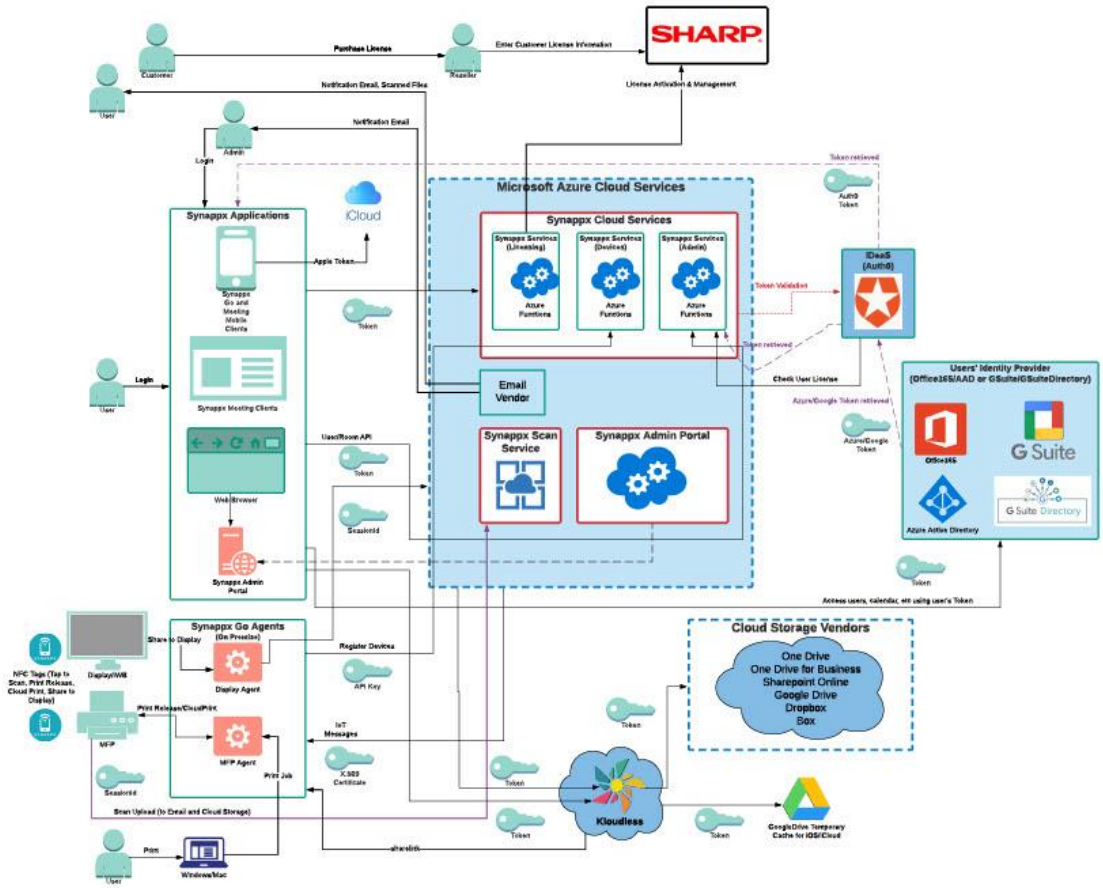
Synappx Go is a mobile-centric service leveraging Near Field Communication (NFC) to enable convenient and time-saving scanning to favorite destinations and print release or printing cloud files to Sharp multifunction printers (MFPs) throughout your office. You are also able to use your mobile phone and app to select and download cloud content to the Sharp display via an NFC tap. Synappx Go cloud software and services leverage the Microsoft Azure database, device provisioning, IoT Hub and many other services.

Synappx Meeting

Synappx Meeting leverages the Azure cloud, rich clients, mobile and voice technologies to help users start meetings on time and be more efficient. With one click of a button, key meeting components are connected. Your PC is automatically mirrored to the Sharp meeting room display, the web conference starts automatically, and you can access meeting materials. Voice commands can be used to save time for common meeting actions. Synappx Meeting uses Microsoft Azure database, storage, Azure functions and more.

2. Overview of Architecture

The following is an overview of the Synappx Platform (powered by Microsoft Azure) including the Synappx Go and Synappx Meeting service components and architecture:



3. Synappx Cloud Services

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

Synappx solutions 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 the Sharp Synappx applications and Synappx Cloud services (hosted on Microsoft Azure) are encrypted via HTTPS (TLS v1.2, AES256), secured through X.509 certificates or MQTT (used by the MFP and Display Agent).

Access to all the Synappx cloud services from client applications require secure keys, certificates, or authentication tokens. After purchasing a Synappx 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 white listed 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.

Synappx Go and/or Synappx Meeting customer specific data stored in the secure Azure cloud databases include the following:

Both Products:

- User first name, last name and email address (imported from Azure AD orG Suite to Synappx by Admin)
- Admin user first name, last name and email address (imported from Azure AD or G Suite to Synappx by Admin)
- Workspace (meeting room) names, email addresses and locations imported from Microsoft Outlook or G Suite Directory to Synappx by Admin
- Manually added workspace names and locations
- Company domain aliases from Azure AD and G Suite
- Application usage data to generate reports for Admin use
- Synappx license data (e.g. expiration)
- System logs

Synappx Meeting Specific:

- Display IP address and port (if configured by Admin)
- Optional Display account ID and display password (if configured by Admin)
- 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

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, version number, update policy, date last updated)
- NFC tag information (tag ID, type) associated with Admin configured devices

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 cloud 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/

4. Synappx Admin Portal

Administrators (Admins) for Synappx Meeting and Synappx Go configure and manage the Synappx system through the Synappx Admin Portal web pages. Adding 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. Reports help demonstrate Synappx system usage and business value. Downloads (for Synappx Go) are conveniently accessible via these pages. System logs can be downloaded.

4.1 Role Based Access and Log in (For Admin Portal and Clients)

Access to the Synappx Admin Portal system is controlled using tenant-based and role-based authentication processes. Users are set up in each tenant and are associated with a specific customer account and in accordance with their usage roles and permissions. 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, manage Synappx service users and workspaces, view reports, etc. for 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 transmit.

Synappx Meeting and Synappx Go leverage Admins' and users' Microsoft 365 or G Suite credentials to avoid having to set up, manage and protect separate Synappx log-in credentials. By design, Synappx services do not have access to Microsoft 365 or Google G Suite customer passwords. The system leverages Azure Active Directory or G Suite 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 365accounts) or G Suite Directory (for G Suite accounts) through a secure identity partner Auth0 (see below) and user passwords are never stored in the

Synappx nor Auth0 systems. The Synappx Platform securely stores the user email address and first/last name only. No other personally identifiable information about the user is known or stored by the Synappx system.

4.2 Auth0 (Identity Service Provider)

For Synappx services, Sharp is working with Auth0 (https://auth0.com/) for secure identity services to Microsoft Azure AD and G Suite. According to Auth0, they serve 21 million users across 120,000 applications, with 2.5 billion logins per month. It is a highly respected identity service provider.

An overview of the process is as follows:

1. The Admin or user enters Microsoft 365 or G Suite credentials via dialogues when logging into the Synappx Admin Portal or any Synappx client.
2. Auth0 delegates the username and password authentication passed via SSL/TLS 1.2 (port 443) to Azure AD or G Suite which validates the username and password credentials.
3. Auth0 does not know nor store the user password.
4. In collaboration with Azure AD or G Suite, a secure JSON Web Token (JWT) is provided back to the browser (for Synappx Admin Portal access), mobile devices (for Synappx Go and Synappx Meeting) and/or to Windows/Mac clients (for Synappx Meeting).
5. This token enables the application to perform functions without the user having to log on each time they use the applications (except in cases where credentials are changed e.g. password needs to be re-entered, user is no longer valid, the user logs out of the mobile app, or with 30 days of inactivity). No one can tamper with the JWT token without the associated secret key used for signing, which is securely stored on the cloud.

Multiple layers of authentication protection are available. The user's mobile device or computer is protected by a password or biometric (e.g. fingerprint or facial) login. User passwords are not known/stored on any of the Synappx devices and the secure tokens that are provided by Auth0 are based on secure tokens and validation from Microsoft Azure or G Suite.

Auth0 has many certifications for cloud security including: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, EU-US Privacy Shield Framework, Gold CSA STAR, GDPR compliance and more. See the following Auth0 white papers for more information about Auth0 security provisions:

- https://auth0.com/security/
- https://assets.ctfassets.net/kbkgmx9upatd/2KxmM5BICQ4GKgeIwA0sKu/bee69c73669bfdeb26ca8e43df65be27/Auth0_Platform_Operations.pdf

4.3 Granting Synappx Application Privileges

To enable Synappx Meeting and Synappx Go features, the Admin is required to grant Synappx application users selected privileges. The first Admin to log into the system must have Azure AD or G Suite Administrator privileges and consent on the behalf of the organization to the requested permissions for users when accessing the Synappx applications/services.

For Microsoft 365 customers, the permissions and reasons for each are:

Permissions Requested	Definition	Admin Portal	Synappx Meeting	Synappx Go
Azure Active Directory Graph:				
• 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	Allows the app to collect domain aliases from Azure AD (needed for multi-domain support) and allows the app to read data in Azure AD such as users, groups and apps.	Yes	No	No
Microsoft Graph:				
• Calendars.ReadWrite.Shared	Allows the app to create, read, update and delete events in all calendars the user has permissions to access. This includes delegated and shared calendars.	No	Yes	No
• Files.ReadWrite.All	Allows the app to read, create, update, and delete all files the signed-in user can access.	No	Yes	No
• 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
• 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.	Yes	Yes	No
• offline_access	Allows the app to read and update user data, even when they are not currently using the app.	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

For G Suite customers, the following is the list of API scopes that are required and reason for each:

Google API Scopes Requested	Definition	Admin Portal	Synappx Meeting	Synappx Go
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.	No	Yes	No
https://www.googleapis.com/auth/calendar.events	Allows the app to have read/write access to events on a calendar and update the calendar (e.g. extend the meeting time).	No	Yes	No
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	No
https://www.googleapis.com/auth/drive.file	Allows app to have access to files created or opened by the app for downloading and uploading. File authorization is granted on a per-user basis and is revoked when the user deauthorizes the app.	No	Yes	No
https://www.googleapis.com/auth/userinfo.profile	Allows app to use personal information user has made publicly available to get username and avatar image.	No	Yes	Yes

4.4 Importing Users or Workspaces from Azure AD or G Suite

Synappx Go licenses the service on a user basis while Synappx Meeting licenses based on workspaces/meeting rooms. Admins can save time and reduce typing errors by directly importing Users (for Synappx Go) and Workspaces (e.g. Rooms) for both applications from Microsoft 365 (Azure AD) or G Suite. Manual entry of Workspaces is also permitted. Only users in the supported domains and in Azure AD or G Suite can be added as licensed Synappx Go users. Communications with Microsoft Azure and G Suite for User and/or Workspace import is via HTTPS (port 443).

4.5 Synappx Go Agent Downloads

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). See the Synappx Go Agents section for more details on agent related security.

4.6 Synappx Reports

Synappx Meeting and Synappx Go feature reports to help Admins understand Synappx application usage and value. Data that generate the Synappx reports is stored on secure Microsoft servers. Data is retained until 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 Reports 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.

4.7 Synappx Supported Domains

For Microsoft 365 accounts and G Suite, Synappx collects information on the domain aliases supported in the account's Azure AD or G Suite system. For Microsoft 365 accounts, n the Admin Setting/Supported Domains web page, after initial permission opt in, 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.

4.8 Synappx System Logs

Synappx Go and Synappx Meeting include a system log containing information about system events of potential interest to Administrators. 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.

5. Windows and Apple Mac Clients for Synappx Meeting

Synappx Meeting helps connect to the display in the meeting room, start web conference and operate applications by simple voice commands. They provide a broad range of security features including:

- All Synappx Meeting client access to cloud resources is via HTTPS (port 443)
    - Azure (Gets meeting room information from Synappx Admin)
    - Auth0 (User authentication delegation to Azure AD)
    - Azure AD (User authentication with Microsoft 365 account) or G Suite (User authentication with G Suite account)
    - Microsoft Graph APIs (Gets meeting information and files for meeting from Microsoft Office 365) or Google API Scopes (Gets meeting information and files for meeting from G Suite)
    - Amazon Web Services for voice command queue access
- Access to local display
    - Enables control of AQUOS BOARD® interactive display systems with voice control. Protocol is telnet (Port 10008)
- User authenticates with Microsoft 365 or G Suite passwords the first time he/she uses the Synappx app, when there are credential changes (e.g. password update), they log out of the client app and/or after 3 days with no app use
- User passwords are not stored on the mobile device; instead a secure JWT token is provided after user password validation with Azure AD or G Suite system via a partner Auth0.
    - User access token is stored on local computer
        - ID/Password for proxy are stored on local storage. (encrypted using AES128)

6. Synappx Go and Synappx Meeting Mobile

With the pervasive use of mobile devices in business, smartphones are now commonly used to access and share business content. Users expect intuitive mobile services to help them accomplish their work faster. Synappx Go mobile app users can scan to frequent destinations, print release or print supported cloud files to any Synappx Go configured device and share cloud files to configured Sharp displays. The Synappx Meeting mobile app lets users start their meeting, start web conferences and access documents quickly. Several security features associated with the mobile clients are:

Synappx Meeting and Synappx Go:

- Mobile device requires entry of user passwords or biometric (e.g. fingerprint, facial recognition) authentication to access apps
- Users authenticate with Microsoft 365 or G Suite 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. Leverages:
    - Auth0 (User authentication delegation to Azure AD)
    - Azure AD (User authentication with Microsoft 365 account) or G Suite (User authentication with G Suite account)
- User passwords are not stored on the mobile device; instead a secure JWT token is provided after user password validation with Azure AD or G Suite system via a partner Auth0.
- All access to system encrypted via TLS v1.2 AES256 (Port 443)

Synappx Go Specific:

- User mobile access is controlled centrally via the Synappx Admin Portal. Admins can remove a user license at any time to block subsequent use of the Synappx Go mobile features.
- Users are requested to grant access to their mobile contacts list in order to create scan to email destinations without having to re-enter target user emails. This saves time and reduces typing errors.
- To scan to a cloud storage folder, print selected cloud files, or share cloud files to Sharp displays, users can elect to configure Synappx Go to access files from supported cloud storage sites (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box or Google Drive). For the iOS app, iCloud and Local files are already configured.
    - 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 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. Note: The Synappx Go service has no function to delete files or folders from any cloud storage site.
    - Note: Sharp partners with a 3rd party vendor, Kloudless (Kloudless.com) to facilitate efficient Synappx Go connections to multiple cloud storage vendors. Kloudless does not have access to user passwords. Their secure database does include Synappx Go user email addresses. They store minimal file/folder metadata (e.g. file name and ID, modified date) to support viewing Recently Modified files across cloud sites. User file contents are not stored by Kloudless.

Synappx Meeting Specific:

- Mobile apps are available for any user of the service (no license required); however, user must be a valid user in Azure AD or G Suite in the same customer domain.
- Azure meeting room information is accessed from Synappx Admin
- Microsoft Graph API gets meeting information and files for Meeting from Microsoft Office 365. Google API scopes get information and files for Meeting from G Suite.

7. Synappx Go NFC Tags

Synappx Go utilizes special NFC tags provided by Sharp, authorized resellers and/or embedded in selected 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) by the Admin via the Synappx Go mobile app, upon NFC tap by the user, the tag and mobile app together identify the user identity and device associated with the tag/device to enable the Synappx Go use cases such as scanning to email, print release, print cloud files and share to display.

8. Synappx Go MFP Agent

The Synappx Go MFP Agent (including Print Release software) is an on-premise component of the Synappx Go system installed on a customer PC or server to facilitate communications between Synappx Go-enabled MFPs and the Synappx Go cloud to enable mobile and NFC use cases related to Sharp MFPs. Synappx Go eliminates the need to learn and take multiple steps on the MFP front panel to release secure print jobs from any Synappx Go enabled MFP, print selected cloud files and send files to favorite scan destinations. Users can save time for scanning and secure printing, also reducing risk of unauthorized access to the user print jobs.

The Synappx Go MFP Agent is required to support scan and print use cases. One of the core functions 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 and supported MFPs. 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 message by publishing to that identifier topic.

8.1 MFP Agent Install

To install the MFP Agent, the custom install package is downloaded from the Synappx Go Admin Portal with a configuration file unique to the customer. The configuration file contents are secured via encryption algorithms. This MFP Agent installation package is not available from a public web site and is tied to the specific customer account. For most customer installations, there will be one MFP Agent installed per customer site to support a maximum of 50 to 100 MFPs (depending on number of users and print jobs) that can use Synappx Go print and scan capabilities. Customers who wish to support more than 100 MFPs will need to install additional MFP agent(s).

After install, to register itself, the MFP Agent submits its unique identifier, along with agent security credentials, to the Synappx Go Cloud for registration into the Device Registry. Information stored in the Device Registry includes data such as device ID, location, tenant ID, and for MFPs, the MFP agent associated with the MFP.

8.2 MFP Agent Communications

All communications between the Synappx Go MFP Agent and Synappx Go Cloud use either HTTPS (Port 443) or X.509 client security over MQTT. HTTPS is used during initial installation communications between the Synappx Go MFP Agent and the Synappx Go cloud, plus to send MFP information and any error information.

- Agent X.509 private keys never leave the system on which the agent is installed, and thus are never exposed as a result of transmission over the internet.
- All Agent X.509 certificates are signed using the Agent customer's signing certificates. Agents are allowed to auto register only if the X.509 certificate is signed by their associated customer signing the certificate.

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

After automatic provisioning of the agent to the Synappx Go cloud including X.509 certifications, communications between the Agent and cloud are conducted via secure MQTT connections. Sharp Synappx Go X.509 rootCA-signed certificates are used. Certificates signed by a rootCA provide an extra level of attestation that certifies the certificate holder is who they say they are. The use of x.509 certificates offers the greatest security in device authentication, as the private key of each Agent device never leaves the device and cannot be compromised. The Synappx Go Agent tenant root CA signing certificate is generated by the Synappx Go Tenant Provisioning Service and stored in the Azure Key Vault.

- Advantages of MQTT and X.509 certificates include that Agents are permitted to subscribe only to their own unique device ID topic; this means Synappx Go agents receive messages published ONLY to their respective deviceID. The agent cannot receive content from any other endpoint.

8.3 MFP Agent Requirements

The Synappx Go Agent is designed with the following requirements by the Azure cloud:

- Before a device can connect to Azure cloud, the device MUST be registered
- Before a device can be registered, the device MUST be provisioned (by a customer Admin)
- Before a device can be provisioned, the device MUST have security certificates (via the system)

8.4 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 range 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

8.5 MFP Agent Print Release and Scan Documents

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 file 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 having access to the computer via normal PC/server password protection.

The customer network impacts are related to use of Synappx Go user scan and print 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)

9. Synappx Go Display Agent

The Synappx Go Display Agent is an on-premise component of the Synappx Go system installed on a customer Display PC or server to facilitate communications between Synappx Go-enabled PCs and the Synappx Go cloud—enabling mobile and NFC related Share to Sharp Displays. Synappx Go allows the user to simply set up connections to all of their favorite cloud storage sites once and be able to find the file(s) across sites to share and/or edit (for most cloud storage sites) on Sharp displays—all from their private mobile device and with a simple NFC tap to download the files. Users save time that can be better spent on collaboration around the file content, also reducing the risk of others in the meeting seeing sensitive file names that are also in their cloud folders. And, multiple users can download and edit files (in most cases) on the same Display PC for collaborative editing or to compare file content.

9.1 Display Agent Installation

To enable Share to Display use cases, the Synappx Display agent must be installed on the Display Windows PC or server. 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.

To install the Display Agent, the custom install package is downloaded from the Synappx Go Admin Portal with a configuration file unique to the customer. This Display installation package is not available from a public web site and is tied to the specific customer account. After install, to register itself, the Display Agent submits its unique identifier, along with agent security credentials, to the Synappx Go Cloud for registration into the Device Registry. Information stored in the Device Registry includes data such as PC/server name, unique PC/server ID and tenant ID.

9.2 Display Agent Communication

All communications between the Synappx Go Display Agent and Synappx Go Cloud use either HTTPS (Port 443) or X.509 client security over MQTT. HTTPS is used during initial installation communications between the Synappx Go Display Agent and the Synappx Go cloud, plus to send any error information.

- See the X509 and other communications details in the MFP Agent section above. The Display Agent has the same security features as the MFP Agent described there.

9.3 Display Agent Contents Share

For the Display Agent, the following additional security features are implemented for Share to Display:

- Once the user has configured their desired cloud storage repositories (e.g. SharePoint Online, Dropbox) via their mobile device, when the user accesses the Share to Display function, the secure user token(s) in the Synappx Go mobile app are temporarily shared with a secure Synappx Cloud cache. The cache is only accessible with secure keys. The user token is removed from the Sharp Synappx cloud cache a short time following usage and the user token is never downloaded to the Display Agents.
- When a user selects a file(s) from their cloud storage site via the Synappx Go app to download to the Display PC, the Synappx Cloud generates a download URL including a session ID to get the selected user file(s). The files are automatically opened on the Display Agent PC for viewing and/or editing (for most cloud storage sites). The files are stored in a temp folder in the Display PC.
- Files that can be downloaded via the Synappx Go service for viewing or editing are limited to the following:
    - Plain Text, Microsoft Office files (Word, PowerPoint, Excel, OneNote), PDF, Image files (JPEG, TIFF, GIF, BMP, PNG) & Video files (MP4, AVI, WMV, MOV)
    - Note: Executable or script files are <u>not</u> supported and cannot be downloaded via this service.
- Files that can be downloaded via the Synappx Go service for viewing only are limited to the following:
    - For iOS, iCloud and Local Files storage: same file list as above
    - For G Suite files stored in Google Drive: Google Docs, Google Slides, Google Sheets, Google Drawing, Google Jamboard
    - Note: Executable or script files are <u>not</u> supported and cannot be downloaded via this service.

- If the user elects to save an editable file after making changes on the Display PC, it will be saved back to the same cloud folder location from which is was downloaded as either a new version and/or with an appended file name (subject to the policy of each cloud storage site).
- If a user saves a supported editable file back to the cloud or closes a file without saving, it will be removed from the temporary Display PC folder.
- Multiple users with Synappx Go licenses/apps can each download cloud files to the same Display Agent for viewing, copying and pasting editable content, comparing files before saving back to the respective cloud sites.

10.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's and our valued business partner's information assets and is regularly researching, reviewing, and investing in procedural and technical countermeasures to provide assurance and security. 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.

11.Corporate Policies and Practices

Sharp has implemented several policies and procedures to ensure the security of Sharp's, and our business associates', information assets. All of Sharp's policies and procedure 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 27001:2013 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 27001:2013 certified

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.

12.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 admin 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 administrators 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

13.Sharp Privacy Policy

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

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

14.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**