Security White Paper for Synappx Manage Services

Sharp Electronics Corporation
June 2025

Contents

Synappx Manage Security White Paper

1. Introduction

Overview

Synappx Manage is a device management service. Synappx 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, Okta (Auth0) 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 Manage are described in this white paper.

2. Synappx Cloud Services

Synappx applications 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) use HTTPS (TLS v1.2, AES256) or WSS (WebSocket Secure).

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 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, user principal name email address (imported from Entra ID or Google Workspace to Synappx by Admin), email aliases (proxy addresses) and IP address
- Admin user first name, last name and user principal name email address (imported from Entra ID or Google Workspace to Synappx by Admin) and email aliases (proxy addresses)
- Company domain aliases from Entra ID 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 Manage Specific:

- User first name, last name, email address (imported from Custom Account to Synappx by Admin)
- Admin first name, last name, email address (imported from Custom Account to Synappx by Admin)
- Gathering device status and log data
- Provide security policy remote configuration function
- Copy and save device configuration data
- Update device configuration data
- Access Maintenance interface, data and receive alert
- Provide notifications based on device status
- Provide Report/Analytics based on historical device data
- Provide security policy check, Notification
- Print Driver Distribution
- MFP information (model name, IP address, serial number) discovered via Admin initiated SNMP discovery
- Synappx Manage gather only device specific information (Status, Data, Logs, Security Policy, configuration, Alert Data)
- Provide Print Driver distribution with default configuration

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
- Securing Azure Functions: https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts
- 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) and service providers use, configure and manage the Synappx applications through the Synappx Admin Portal web pages. Managing 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 are conveniently accessible via these pages. System and Admin logs can be downloaded.

3.1 Synappx Supported Domains

For Microsoft 365 accounts and Google Workspace, Synappx collects information on the domain aliases supported in the account's Microsoft Entra ID or Google Workspace system. For Microsoft 365 accounts, in the Admin Setting/Supported Domains web page, after initial permission opt in, Admins can select additional domain aliases beyond the primary Microsoft Entra ID domain under which the Synappx account was created. Even if the Admin has not opted in for additional permissions, the ability to manually add Supported domains (instead of automatic acquisition of domain information) is available. This allows users and workspaces to be imported from selected domains to be used with Synappx services.

3.2 User Authentication

Synappx supports Microsoft 365, Google Workspace, and Custom Account as Identity Providers. By design, Synappx services do not have access to Microsoft 365 or Google Workspace customer passwords. The system leverages Microsoft Entra ID, 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 Entra ID (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 the Synappx nor Auth0 systems. The Synappx Platform securely stores the user email address, user name and password (when custom account is used), 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, EU-US Privacy Shield Framework, Gold CSA STAR, GDPR compliance and more.

3.3 Role Based Access

Access to the Synappx Admin Portal and Synappx applications are controlled using tenant-based and role-based authentication processes. The service provider gains tenant access upon tenant creation. Tenant access for the service provider is strictly managed through Sharp-Start, which is exclusively available to authorized Sharp dealers and SIICA administrators. As part of the purchase order process, the service provider can add the initial administrator. Additional administrators can be added by the initial customer administrator after successfully logging in to the Synappx portal.

Only service provider and Admins designated or assigned by the customer can access, configure, license, manage Synappx 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.

Admin User Types:

- Primary Admin: The first Admin who is only one person in one tenant. This user role has the same privileges as IT Main.
- IT main: This user role can manage users, roles, licenses and data entities. Also this user role can see Admin log, System log and Analytics reports.
- IT Helpdesk: This user role can see data entities and Admin log and System log.

Guest Admin User Types (Synappx Manage Only):

- Service Main: Main user role of Service provider for tenant. This user role adds permissions to the IT Main, granting access to the service portal functionality.
- Service Support: Support member of Service provider for tenant. This user role adds permissions to the IT helpdesk, granting access to the Device Cloning and Storage Backup features.
- Service View Only: Status checker of Service provider for tenant. This user role can see data entities only.

Guest Admins can use their Sharp-Start login to access Synappx Manage features. Upon Single Sign On to Sharp-Start, Synappx Manage validates that the added service users are eligible to access the tenant. The Synappx user login and password are stored in a secure Auth0 database only when using custom database IdP. Sharp-Start is handled as a social OIDC (OpenID Connect) IdP, therefore the user login (id) and password are not stored in Auth0 database.

3.4 Granting Synappx Application Privileges

3.4.1 Microsoft 365 Users

To use Synappx applications including Admin Portal and Synappx Manage, 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, Synappx Manage
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
• 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
• Directory.Read.All	Allow the app to read sub domains.	**Yes***

• Files.ReadWrite.All	Allows the app to read, create, update, and delete all files the signed-in user can access.	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***
• 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
• Team.ReadBasic.All	Allows app to get a list of Teams to retrieve documents for the user to share.	No
• 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***
• 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**
• 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**
• email	Allows the app to read your users' primary email address.	**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**
• profile	Required to obtain user profile information (e.g. user first and last name, email address) from Entra ID.	**Yes**

* These permissions are optional. On the Admin Portal, Azure Global Administrator can grant global permission shown in the table below. If granted, he/she would gain access to the features under "Automatically sub-domains are listed" in the "Supported Domains" page.

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 and Synappx Manage, 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, Synappx Manage
https://www.googleapis.com/auth/admin.directory.domain.readonly	Allows the app to read domain information for supporting multi-domain feature.	Yes
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
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
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
https://www.googleapis.com/auth/calendar.readonly	Allows the app to have read-only access to Calendars.	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
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
https://www.googleapis.com/auth/directory.readonly	Allows app to see and download your organization's Google Workspace directory	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.	Yes

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

- 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 Synappx Analytics Reports

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 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.

3.6 Synappx Admin Logs, Operation Logs and Device Logs

Synappx Manage includes an admin log that contains information about administrators’ interactions with the Synappx Manage Admin Portal. Because multiple Admins can be assigned and provided access to the Synappx Admin Portal, this log captures major actions taken by the administrators. Admin Logs can also be exported as a .CSV file for analysis. Admin logs are retained by the Synappx System for 90 days.

There is also an operation log that contains information about which users have performed which Synappx Manage functions. Finally, there is also a Device Log that records response information coming from the device because of the operation. Each log is retained by the Synappx system for 90 days.

4. Synappx Cloud Communication

4.1 Agent Communications

Installed on premise, 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 is secured via encryption. After install and verification, the agent submit its unique identifier, along with agent security credentials, to the Synappx Manage for registration into the device registry. Information stored in the device registry includes data such as device ID, location, and tenant ID.

All communications between the agent and Synappx Manage use either HTTPS (Port 443) or WSS (WebSocket Secure)

4.2 Direct Connection

Direct connection provides device to Synappx cloud service communication without requiring on-premise software installations. All direct connection communications are encrypted using HTTPS/TLS.

4.3 Summary of Ports Used

Information on the ports used by Synappx Manage is summarized below. The information is based on Synappx Manage v1.9. (June 2025 release)

Agent listening ports:

TCP/UDP	Listening Port (*Default)	Use Case	Caller	Callee	Protocol	require FW permissions
TCP	8088	Technical service functions(*1)	Sharp-MFP	Agent	HTTPS	inbound to Agent PC
TCP	8088	Agent administration	Agent operation dialog	Agent	HTTPS	-

Agent connects ports:

TCP/UDP	Destination Port (*Default)	Use Case	Caller	Callee	Protocol	require FW permissions
TCP	443	Synappx Manage Agent Service	Agent	Synappx Manage cloud server	WebSocket/HTTPS	outbound from Agent PC outbound from LAN to Internet
UDP	161	MFP search/management	Agent	MFP	SNMP	outbound from Agent PC
TCP	80/443	Device cloning / Storage backup/ Security control / Power management / Service report	Agent	Sharp-MFP	HTTP/HTTPS* (*2)	outbound from Agent PC
TCP	6080~6089(*3)	Device cloning /Storage backup (data channel)	Agent	Sharp-MFP	HTTP/HTTPS	outbound from Agent PC
TCP	5900*	Remote operation	Agent	MFP (with VNC service)	RFB	outbound from Agent PC
TCP	443	Embedded web page access	Agent	Sharp MFP	HTTPS	outbound from Agent PC
TCP	51003	MFP management	Agent	Sharp-MFP (BP-1200/1250M/ 1360M)	Custom interface for BP-1200/1250M/ 1360M	outbound from Agent PC
TCP	10008*/10022(*4)	Display management	Agent	Display with S-Format	S-Format (BS-Telnet)/SSH (*4)	outbound from Agent PC
TCP	7142*/10022(*4)	Display management	Agent	Display with N-Format	N-Format (PDCON)/SSH (*4)	outbound from Agent PC

*1: This information is intended for service persons and this communication is not for general user use.

*2: For some legacy models, Http is used

*3: Port dynamically determined by Sharp MFPs

*4: If SSH is enabled, port is 10022

MFP Direct connection ports:

TCP/UDP	Destination Port (*Default)	Use Case	Caller	Protocol	require FW permissions	require FW permissions
TCP	443	Direct connection Technical service functions	Sharp-MFP (Enhanced FSS supported)	HTTPS	outbound from LAN to Internet	outbound from LAN to Internet

5. Data Security

Synappx Manage store data in the Azure Cosmos DB, Azure Storage and Azure Databricks Delta Tables where the data is automatically and seamlessly encrypted. Device password related information is encrypted before storing in Azure Cosmos DB, providing double layered security.

Sharp does not have access or any capability to see printed, faxed, and copied contents processed by MFPs using Synappx Manage. A service provider or Sharp authorized technician may gain access to job related features via storage back up feature; however the target data is job programs not actual jobs processed by the MFP, therefore service providers and Sharp personnel cannot access job files using Synappx Manage.

6. Synappx Manage Features

6.1 Synappx Manage Agent Download

The Synappx Manage 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. The configuration file is packaged with a zip file containing tenant specific information to enable automatic MFP discovery via SNMP and tenant connection. For specific MFP data collection, agent communicate with device via HTTP(S)/SNMP(v1/v3)/RFB/Telnet. The agent communicates with cloud server via HTTPS.

6.2 Synappx Manage Agent Device Discovery For MFP

SNMP discovery is used to collect MFP data and information when agent is used. The admin can configure broadcast address or IP ranges via the Admin Portal to search and can also perform on-demand search using port 161. Upon device discovery, the following information will be sent to the Synappx cloud with Agent ID:

- MFP Model Name, MFP Serial Number, Device Friendly Name(if set), Location(if set), Country, Language, Product Family Name, MAC address, IP address, Option Information, Error Information, uptime, engine PPM, cover status, Finisher information, Device Icon Image, SNMP-Alert, Life Count, Tonner information, Tray Information, and printing counters.

6.3 Synappx Manage Agent Device Search for Display devices

An agent is used to search, connect and collect display device information and data. IP address and port (See "**4.3 Summary of Ports Used**" for detail.) are used to find and connect the device. The following information is collected and sent to the Synappx Manage services with Agent ID:

- Display Model Name, Display Serial Number, MAC address, IP address, Firmware Version, Portrait/Landscape, Power Status, Input Information, Volume, Brightness, Temperature Sensor, Uptime.

6.4 Synappx Manage Print Driver Download

Synappx Manage service keeps configured print drivers for the driver distribution feature. When an administrator uploads a print driver via HTTP and then configures data input using web UI, the Synappx Manage application service creates a configuration file. An encrypted (SHA-256) configuration file is packaged with the print driver zip file.

6.5 Remote Operation via internet (Agent install is required)

All communications for the Remote Operation feature are encrypted using WSS (Websocket over TLS) both between the browser and Synappx cloud and between Synappx cloud and the Agent. In addition, MFP settings allow users to accept or reject the accessed communication on the MFP operation panel.

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'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.

7.1 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 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 27001:2013 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.

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 administrators 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.

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 device management, 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**