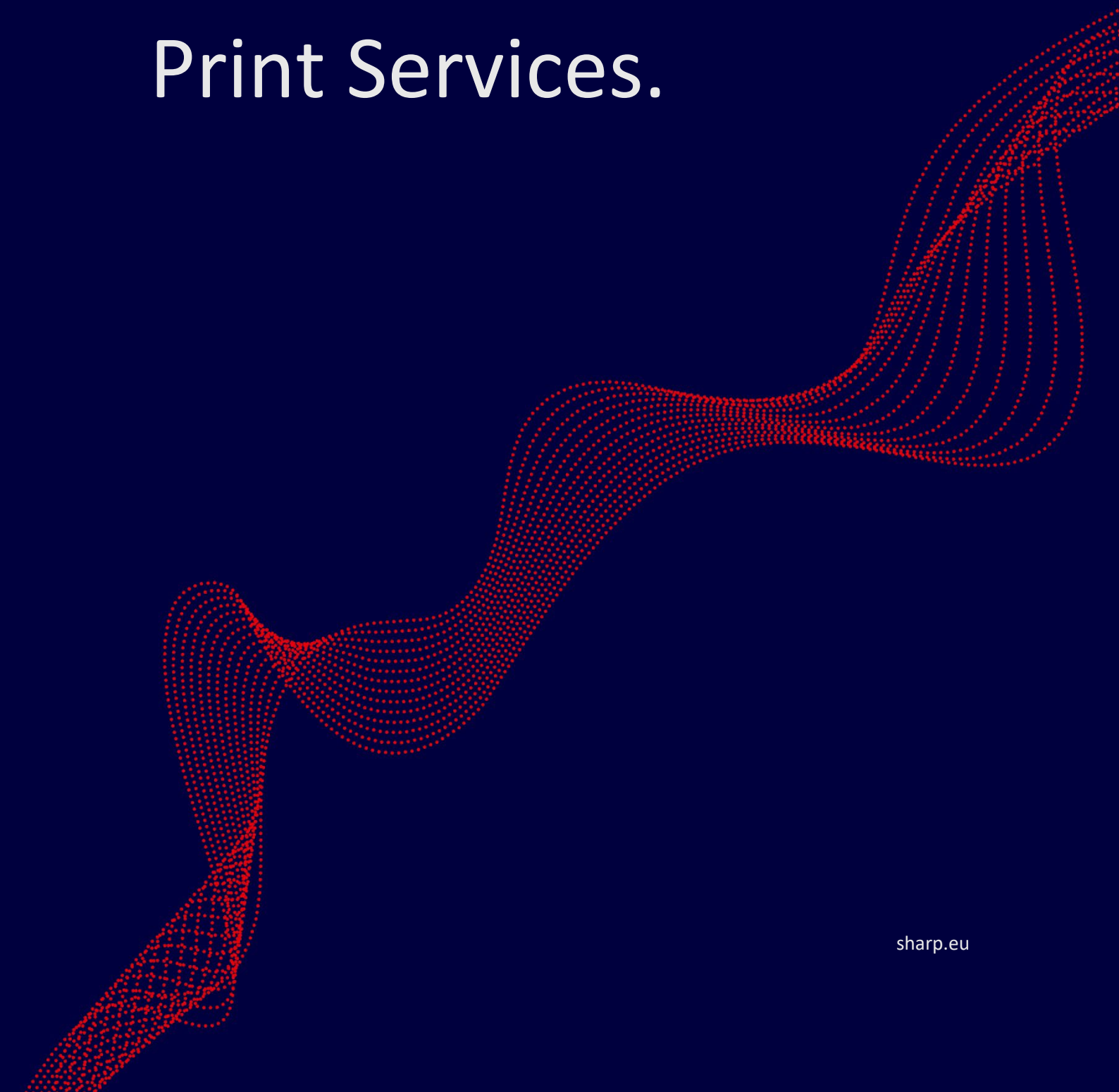
SHARP

Security White Paper for Synappx Cloud Print Services.



sharp.eu

SHARP

Contents

Synappx Cloud Print Security White Paper

1. Introduction

Overview

Synappx application services help bring smarter office experiences, optimising hybrid collaboration and productivity. The 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. Using a combination of world-class technology providers including Microsoft Azure, Google Workspace and security best practices, 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 Cloud Print

Synappx Cloud Print leverages the Azure cloud and rich client technologies to help users increase productivity and work efficiently. Synappx Cloud Print is an agentless cloud-based print management solution for Sharp multifunction printers (MFPs) and compatible 3rd party devices. For MFPs, it enables convenience, time saving and security features including secure print release, scanning to favourite destinations, printing cloud files and copying using Sharp MFPs throughout your office. Synappx Cloud Print users can also use their mobile device to print corporate documents stored in the cloud as well as documents in the mobile phone storage. Synappx Cloud Print software and services leverage the Microsoft Azure database, device provisioning and other services.

This document was created based on Synappx Cloud Print version 1.8 and will be updated annually based on the latest version available.

2. Synappx Cloud Services

Synappx applications utilise several Azure services including the Azure Cosmos database, storage, IoT Services, Key Vault, Security Centre monitoring, backup.

Synappx applications are hosted in secure Microsoft Azure data centres located the West Germany European Region. The data centres are protected through Microsoft's security practices and are GDPR compliant. Each data centre 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 v1.3, 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).Synappx Cloud Print does not store documents in the cloud and only metadata is shared by design.

Access to Synappx Cloud Print does not require a client application. Licenses are required for each sharp MFP or printer in the system, which are managed with a secure license key between the device and cloud application.

After purchasing Synappx Cloud Print licenses, the customers administrator can run MFP discovery on their local network and assign licenses as required. 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 required access permissions.

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

Common to all Synappx Cloud Print applications:

- User first name, last name, email address (imported from EntraID or Google Workspace to Synappx by Admin) and IP address
- Admin user first name, last name and email address (imported from EntraID or Google Workspace to Synappx by Admin)
- Automatic PIN generation is assigned to each user and admin to authenticate and unlock the MFP
- Card / badge ID associated with each user and admin to authenticate and unlock the MFP
- Company domain aliases from EntraID 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)
- MFP information (model name, IP address, serial number) discovered via Admin initiated SNMP discovery or manually added

Synappx Cloud Print Windows Client Session & Token Lifecycle Management:

-
- The client application implements **secure access token caching** to maintain authenticated sessions without persisting user credentials locally.
- Upon successful authentication via the Identity Provider (IdP)[1], a **short-lived OAuth 2.0 access token (JWT)** is issued and securely stored within the application runtime context.
- A corresponding **refresh token**, subject to stricter protection controls and longer validity, is used to obtain new access tokens upon expiration without requiring user re-authentication.
- The application automatically performs **silent token renewal** (token refresh flow) prior to or upon access token expiry, ensuring **continuous session usability** while maintaining security boundaries.
- No user interaction is required during this process, enabling a **seamless Single Sign-On (SSO) experience** across sessions until explicit logout or token revocation occurs.
- Token handling follows **least privilege and limited lifetime principles**, reducing the attack surface associated with token leakage or replay.
- All tokens are stored using **secure, platform-specific storage mechanisms** (e.g., OS-protected keystore, encrypted memory), preventing unauthorized access or extraction.
- Session termination (logout) triggers **token invalidation and secure deletion**, enforcing proper session closure and preventing reuse.
- This approach aligns with **Zero Trust Architecture**, ensuring that authentication is continuously validated via token lifecycle controls rather than persistent credentials.Data in Synappx databases is only accessible to active customers via the Synappx Cloud Print administration portal 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:

[1] EntraID or Google Workspace for enterprise environments

- 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 Cloud Print Admin Portal

Administrators (Admins) use, configure and manage the Synappx Cloud Print services through the Synappx Admin Portal web pages. Managing users, MFPs and Printers, security rules, additional Admins and more are performed via these secure web pages. In addition, license information and status can be accessed and managed. Analytic reports can be generated to provide insights into system usage, security and business value. Logs and reports can be downloaded for further analysis.

Synappx Cloud Print Supported Domains

When using Microsoft 365 and Google Workspace accounts, Synappx Cloud Print services collect information relating to domain aliases supported in the account's EntraID or Google Workspace system.

With Microsoft 365 accounts, the Azure Global Admin is required to accept permissions in admin settings/supported domains.

Currently, Synappx Cloud Print only supports the primary domain and not secondary domains.

Identity Delegation, Federated Authentication & Custom IdP Support

- All authentication within Synappx Cloud Print is **centrally delegated to Auth0 (Okta Customer Identity platform)**, which operates as the **primary identity broker and Custom Identity Provider (IdP) abstraction layer** across the platform.
- For enterprise customers, Auth0 enables **federation with external Identity Providers**, such as **Microsoft Entra ID (Microsoft 365)** and **Google Workspace Directory**, ensuring that authentication is performed directly by the customer's trusted IdP. In this model, Synappx services **never store, process, or access user passwords**, relying exclusively on **OAuth 2.0 / OpenID Connect (OIDC) tokens** for identity validation.
- For small and medium-sized customers without an external corporate IdP, Auth0 provides **built-in identity services acting as the Custom IdP**, enabling authentication using **social or email-based identities** (e.g., *@gmail.com, @outlook.com*). This allows seamless onboarding without requiring dedicated identity infrastructure.
- In these Custom IdP scenarios, credential management is fully handled within Auth0. All passwords are **securely stored using strong, salted, adaptive hashing algorithms** (e.g., bcrypt, Argon2), and are **never accessible to Synappx services**.
- Auth0 enforces **modern authentication controls**, including optional **multi-factor authentication (MFA), anomaly detection, bot protection, and adaptive access**

policies, ensuring consistent security across both federated and standalone identity scenarios.

- Synappx maintains a **minimal identity footprint**, storing only essential user attributes (e.g., email address, first/last name, and IP address) required for service delivery. No credential data or unnecessary personally identifiable information (PII) is stored within the platform.
- All authentication events result in the issuance of **signed tokens (JWTs)**, which are validated by Synappx services using strict checks on **issuer, audience, scope, and expiration**, ensuring **secure, stateless, and time-bound access control**.
- This unified identity architecture provides a **flexible and scalable model**, supporting both **enterprise-grade federated identity** and **lightweight identity onboarding for SMB customers**, while maintaining consistent security controls aligned with **Zero Trust principles**.
- The Auth0 platform adheres to industry-recognized security and privacy certifications, including **ISO/IEC 27001, ISO/IEC 27018, SOC 2 Type II, CSA STAR, and GDPR**, ensuring enterprise-level assurance for identity and access management.

For more information about Auth0 and security provisions, go to:
https://auth0.com/security/

Role Based Access

Access to the Synappx Admin Portal and Synappx applications is controlled using tenant-based and role-based authentication processes. The Primary (first) Administrator is nominated during the customer onboarding process. Additional Admins can be added after a successful log in to the Synappx portal by the primary Administrator.

Only admins designated or assigned by the customer can access, configure, license and manage Synappx service users, view reports, etc. from their account via the secure web portal. All communications with the Admin Portal are via HTTPS/SSL (TLS1.3) port 443 to protect data in transit.

Admin User Types:

- Primary Admin: The first admin (one nominated person per tenant). This user role has the same privileges as 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 Analytic reports.
- Group Admin: This user role can manage users and user groups.

User Types:

- User: This user role can log in and use Synappx Windows client, Synappx portal and Synappx Cloud Print mobile.

Admins and Users can use their normal Microsoft 365 or Google Workspace credentials to access Synappx features after the admin adds and activates them.

Granting Synappx Cloud Print Services Privileges

Microsoft 365 Users

To use Synappx Cloud Print services including Admin Portal, Cloud Print Windows PC Client and Cloud Print Mobile app, the user is required to grant the permissions shown in the table below. A permission consent screen is shown for every user for the first-time log-in or according to the company security authentication policies.

Permissions Requested	**Definition**	**Admin Portal**	**Cloud Print Windows PC Client**	**Cloud Print 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 permission to access. This includes delegated and shared calendars.	No	**No**	**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	**Yes**	Yes
• Directory.Read.All	Allows 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 organisation's directory, and people from recent communications (such as email and Skype).	No	No	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 organisation 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 organisation 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**	**No**	**No**
• email	Allows the app to read your users' primary email address.	**Yes**	No	No
• 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 EntraID (previous Azure AD).	**Yes**	Yes	Yes

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

・Group search for users and workspaces

・Automatically sub-domains are listed in the "Supported Domains" page. This page is available for future evolution of the service. Currently only primary domains are supported.

・

Permissions Requested	**Definition**
Microsoft Graph:	
• Directory.Read.All	Allows the app to read data in your organisation'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.
• User.Read.All	Allows the app to read the full set of profile properties, reports, and managers of other users in your organisation, on behalf of the signed-in user.

Google Workspace Users

To use Synappx applications including Admin Portal, Cloud Print Windows and Cloud Print 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	Cloud Print Windows	Cloud Print Mobile
https://www.googleapis.com/auth/admin.directory.domain.readonly	Allows the app to read domain information for supporting multi-domain feature.	No	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.	No	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	No	No
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	No	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	No	Yes
https://www.googleapis.com/auth/directory.readonly	Allows app to see and download your organization's Google Workspace directory	No	No	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	No	No

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. This page is available for future evolution of the service. Currently, only the primary domain is supported.

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

Synappx Cloud Print - Summary of Ports Used

Information on the ports used by Synappx Cloud Print is summarised below. The information is based on Synappx

Cloud Print v1.8 (April 2026 release), we split between Inbound and Outbound.

Inbound

Transport	Port	Listening Component	Caller (Inbound)	Use Case	Application Protocol
TCP	57100	PC Client	Printer Driver	Pull Printing	Custom
TCP	57200	PC Client	IPP Virtual Printer	Third-party printer support	IPP (custom port)
TCP	58080	Tomcat	MFP Browser	MFP app requests	HTTP
TCP	58181	Tomcat	MFP Browser	MFP app requests (secure)	HTTPS
TCP	10080	MFP APP	MFP Browser	MFP registration / heartbeat	HTTP
TCP	10443	MFP APP	MFP OSA	MFP registration / heartbeat (secure)	HTTPS
TCP	8000	Tomcat / MFP APP	MFP Browser	MFP app access (legacy/internal)	HTTP

Outbound

Transport	Remote Port	Listening Component	Caller (Outbound)	Use Case	Application Protocol
TCP	443	Web API	PC Client	API access / IPP over HTTPS	HTTPS (IPP over HTTPS)
TCP	9100	PC Client	Third-party MFPs	Third-party printer support (RAW printing)	JetDirect / RAW
UDP	161	MFP	PC Client	Device discovery / monitoring	SNMP
TCP	443	Web API	MFP App	Calling backend APIs	HTTPS
TCP	8080	MFP App Server	MFP App	Device registration /	HTTP

				heartbeat (“Act Hello”)	
TCP	10080	MFP Service	MFP App	Mobile printing – job polling	HTTP

Importing Users or from EntraID (previous Azure AD) or Google Workspace

Admins can directly import Users (for Synappx Cloud Print) from Microsoft 365 (EntraID or Google Workspace. Manual entry of users is also permitted. Users in the supported domains and in EntraID or Google Workspace can be added. Synappx Cloud Print users can be activated / deactivate without any license required. Communications with Microsoft EntraID and Google Workspace for User import is via HTTPS (port 443). Users with Microsoft 365 and Google Workspace can also be manually added from the Active Directory of the customer. The procedure on how to import users is covered in the Administrator Guide, which it can found here: Admin Support Guide | Synappx Support Centre

Synappx Cloud Print Analytics Reports

Synappx helps Admins understand Synappx Cloud Print service 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 services or recover data) User usage specific information in the reports is only available to Admins within the company via the Analytics pages. Anonymized summary data about customers’ service usage is available to Sharp for purposes of support and product enhancement over time. See Sharp Corporate Security, and Sharp Privacy Policy for more details.

Synappx Cloud Print System Logs, Admin Logs

Synappx Cloud Print includes a System Log containing information about system events. The system log includes 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.

An admin log is also provided containing information about administrator interactions with the Admin Portal. Since 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.

Synappx Cloud Print Zero Trust Architecture Design

Synappx Cloud Print is secure by design. Sharp has implemented a Zero Trust Design, which is a security framework that requires all users, whether in or outside the customers network, to be authenticated, authorised, and continuously validated for security authorisation before being granted access to applications or data.

There are several components that comprise this approach, first, all authentication and identity management is handled through an Active Directory, ensuring the user is authenticating to the solution using their network assigned authentication. Identity Management is in the Cloud and Synappx Cloud Print is connected with Entra ID or Google Workspace.

Secondly, only metadata concerning the print job is sent to the cloud. This means, no matter where a user releases a print, they are only sending an instruction to the cloud saying it is released. The document to be printed never leaves the company network.

The third and final step is at the device itself, which we think is a very important step and there are several options to help security. Secure Print Release means that a user must authenticate themselves at the device, whether via password, pin number or card / badge. Additionally, this is supported by an array of administrator controls that can define levels of security, such as adding two-factor authentication, for example. At this point, the device (MFP) using IPP protocol, will pull the print job from the users laptop over the local area network.

In cases where the user uses the mobile app, the first step is managed by EntraID or Google Workspace providing users access, based on their permissions to select files to print from corporate cloud-based file systems. The final step, at the device requires the user to authenticate using a password, PIN or ID card to retrieve and print the file from the network location. Zero trust is maintained throughout this process with no files leaving the customer network environment.

4. Agentless Communications and Secure process

Synappx Cloud Print does not require an agent installed in the customer network.

All communications between the Synappx Cloud Print Windows application, Sharp devices and Synappx Cloud Print Administration portal and back in cloud, use IPP, HTTPS (Port 443), or MQTT Over WebSocket, AMQP or AMQP Over WebSocket.

The Synappx Cloud Print cloud services maintain separate signing certificates for each Synappx customer.

Synappx Cloud Print MFP Device Discovery

To automate the collection of MFP information (needed to configure the Synappx Cloud Print MFP services), the Synappx Cloud Print Windows client includes the ability for administrators to find MFPs using SNMP discovery. Discovery is automatically initiated after the administrator adds the IP ranges in the Synappx Cloud Print Administrator Portal. This will trigger SNMP in the backend of the Synappx Cloud Print Windows Client and send it to the network. As part of the Zero Trust Design, this action will retrieve all MFPs in the Synappx Cloud Print Administrator portal. The following information about the MFP is collected as part of this process and sent to the Synappx Cloud Print cloud:

- 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

Synappx Cloud Print: Secure Device Onboarding and Registration (Direct Connect)

Synappx Cloud Print implements a secure, token-based device onboarding mechanism designed to ensure controlled provisioning, strong authentication, and minimal attack surface exposure during device registration.

End-to-End Provisioning Flow

Device onboarding is initiated by an authorized administrator through the Synappx Cloud Print Admin Portal. The administrator generates a **Direct Connect provisioning link** for a specific tenant environment. This link is constructed following a custom tokenization model and configured with a short expiration time and usage constraints.

The provisioning link is transferred to the target Multi-Function Printer (MFP), either manually (e.g., pasting into the device interface) or via guided on-device instructions. Upon execution, the device establishes a secure connection to the Synappx Cloud Print registration endpoint and presents the embedded token alongside its device identity.

The Synappx Cloud Print backend validates the request through multiple security controls, including:

- Enforcement of usage constraints (e.g., single-use or limited-use tokens)
- Evaluation of registration quotas tied to tenant licensing

Once validated, the system securely associates the device with the target tenant and issues **short-lived device credentials**, enabling authenticated communication with Synappx Cloud Print services.

Following successful registration, the device is immediately visible within the Admin Portal, where it can be managed, assigned policies, and allocated licenses in accordance with organizational governance.

Security Controls and Operational Safeguards

Synappx Cloud Print incorporates a defense-in-depth approach to secure the device onboarding process:

Strong Cryptographic Controls

- All provisioning tokens are signed using the HS256/**RS256 algorithm**, ensuring integrity and authenticity.
- Private signing keys are securely stored and managed within Azure Key Vault, providing hardware-backed protection and controlled access.
- Cryptographic keys are rotated periodically in accordance with defined key management policies.

Token Security and Abuse Prevention

- Tokens include strict validation of claims such as issuer (iss), audience (aud), and expiration (exp).
- Each token is uniquely identifiable via a jti (JWT ID), enabling enforcement of **single-use or limited-use policies** to prevent replay attacks.
- Token lifetime is intentionally short to reduce exposure risk.

Registration Control and Licensing Enforcement

- Device registration is tightly coupled with tenant licensing. The system enforces a **maximum registration limit per token**, aligned with available entitlements.
- Attempts to exceed licensed capacity are automatically blocked, ensuring compliance with contractual and operational constraints.

Network and API Protection

- Registration endpoints are protected industry-standard controls, including:
    - Web Application Firewall (WAF) rules to mitigate common web threats
    - Rate limiting to prevent abuse and denial-of-service conditions
- Continuous monitoring is implemented to detect anomalous registration patterns and potential misuse.

Minimal Data Exposure and Credential Hygiene

- Only essential device attributes are collected and stored during registration, adhering to the principle of **data minimization**.
- Devices are issued **short-lived credentials**, which are periodically rotated to reduce the risk of credential compromise.

- All communications between devices and SCP services are secured using industry-standard encryption protocols (e.g., TLS 1.2+).

Security Design Principles

The Synappx Cloud Print Direct Connect onboarding mechanism is designed in alignment with key security principles:

- **Zero Trust Architecture**: Every registration request is explicitly verified; no implicit trust is granted based on network location.
- **Least Privilege**: Tokens and device credentials are scoped with minimal permissions required for operation.
- **Secure by Default**: Short-lived tokens, enforced quotas, and strict validation are applied automatically.
- **Auditability and Traceability**: Token usage (jti) and registration events are tracked to support monitoring, auditing, and forensic analysis

The Synappx Cloud Print Direct Connect onboarding mechanism demonstrates strong alignment with ISO/IEC 27001:2022 Annex A across key domains:

- **Identity and access management** through tokenized, controlled provisioning
- **Cryptographic assurance** via secure signing and key management practices
- **Secure application design** with strict validation and enforcement logic
- **Network and operational protection** through monitoring, WAF, and rate limiting
- **Data minimization and asset control** ensuring reduced exposure and full lifecycle visibility

This mapping confirms that Synappx Cloud Print's onboarding architecture follows **industry-recognized security controls and best practices**, supporting compliance and audit readiness.

Application Security

All communication between endpoints and Synappx Cloud Print services are secured and encrypted via TLS v1.3 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 they use 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 EntraID (previous Azure AD), Google Workspace and for Synappx non-enterprise guest user database)
- EntraID (previous 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 EntraID (previous Azure AD) or Google Workspace system via a partner Auth0.

Synappx Cloud Print Windows Web and Local Client – Authentication and Credential Handling

The **Synappx Cloud Print Windows Web and Local application (PC client)** is designed following modern zero-trust and token-based authentication principles. The client does **not store or process user credentials (ID/password)** locally at any time.

Authentication Flow and Token Handling:

- The client leverages a **federated authentication model** using an external Identity Provider (IdP) via **Auth0**.
- During login, the user is **redirected to the IdP authentication page** (e.g., **Microsoft Entra ID** or **Google Workspace**).
- User credentials are entered **directly into the IdP interface**, ensuring that:
  - Credentials are never exposed to or handled by the Synappx Cloud Print client.
  - Authentication is performed entirely by the trusted identity provider.
- Upon successful authentication:
  - The IdP issues an **OAuth 2.0 / OpenID Connect access token** (via Auth0), typically in the form of a **JSON Web Token (JWT)**.
  - This token is **cryptographically signed using RS256 (asymmetric RSA signature)** to ensure integrity and authenticity.
- The Synappx Cloud Print Web and PC client:
  - Receives the Auth0-issued token.
  - Exchanges or transforms it into a **Synappx Cloud Print (SCP) API access token**, which is:
    - Signed using **HS256 (HMAC with SHA-256)** for internal service authentication.

    - Uses this SCP token exclusively for **authorized API communication** with backend services.

Credential and Token Storage:

- **No user ID or password is stored locally** on the client.
- Tokens are handled in accordance with secure session management practices:
    - Stored temporarily in memory or secure OS-protected storage (implementation dependent).
    - Subject to expiration and revocation policies enforced by the authentication system.
- No use of **AES128 or AES256 encryption** is applied to the SCP access token itself, as token security is ensured through **signature-based integrity (RS256 / HS256)** rather than encryption.

Data Exchange and Privacy:

- Communication between the client and the Synappx Cloud Print cloud backend is performed over **secure HTTPS (TLS 1.2 or higher)** channels.
- Only **necessary metadata and job-related information** is transmitted to support print operations.
- Document content handling follows service-specific processing rules and is not exposed beyond required processing scope.

Security Principles Applied

- Zero credential storage on endpoint
- Federated identity and delegated authentication
- Token-based authorization (OAuth 2.0 / OIDC)
- Strong cryptographic signing (RS256 / HS256)
- Secure transport (TLS)

The Synappx Cloud Print Windows Web and Local client application align strongly with ISO 27001 Annex A[2] by:

- Eliminating local credential storage
- Leveraging federated identity and trusted IdPs
- Enforcing token-based, least-privilege access

[2] See Appendix

- Applying strong cryptographic signing mechanisms
- Minimizing data exposure and endpoint risk

Synappx Cloud Print Mobile Application

Synappx Cloud Print mobile app offers features including print/copy/scan on Sharp MFPs. Security features associated with the Synappx Cloud Print mobile clients are:

- User login into the application using the EntraID or Google Workspace authentication, token is created via partner system Auth0. No password and ID are stored on the Mobile app.
- For cloud storage service's file and folder access, users can configure Synappx mobile 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 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.
      You can find all cloud storage options that the user can configure, here: App Setup | Synappx Support Centre

- File print from cloud location.
    - Synappx Cloud Print can print up to ten files across configured cloud storage sites, (100MB file size limitation). Files from iCloud, local iOS device storage, and Google Drive have a 30MB file size limit. Supported Google files stored in Google Drive only can be selected for cloud file printing.
    - Some Sharp device models may require additional expansion kits:
        - Direct Print Expansion Kit
        - Adobe PostScript 3 Expansion Kit

- File formats supported are:

File Extensions	Google Applications
• .txt • .tiff • .jpeg • .png • .pdf* • .ps* • .docx** • .pptx** • .xlsx**	• Google Docs*** • Google Slides*** • Google Sheets*** • Google Drive*** • Google Jamboard*

- Authenticate to Synappx Cloud Print at the MFP using PIN, Card etc [View Image].
- Select the 'mobile print' option on the MFP panel [View Image].
- Select Print Cloud Files [View Image].
- The Recently Modified list displays files modified within the last 30 days from all configured sites with the most recent files shown at the top.
- Teams shows files created or modified by you within the last 30 days. Only files you created or modified in Teams folders will display in Recently Modified to print.
- New file uploads may not be immediately reflected in the Recently Modified list.
- Files from some configured cloud sites begin to display from the date of first access.
- SharePoint and Dropbox files are not included in Recently Modified list but can be selected for printing by browsing to the folder with the targeted file(s).
- iCloud and local files on iOS devices do not appear on the Recently Modified list. Those files are only accessible through the browse feature.
- The device will load recently modified files from your configured cloud storage folders. Select up to ten files from the cloud folder browsing, search feature, or Recently Modified list. Then select Print [View Image].
- Scan the QR code on the MFP panel to start the print job.

The documents selected to print on the customer cloud storage is not storage on Synappx Cloud Print and it is delivered directly after authentication from customer cloud storage to the Sharp device as part of the Zero Trust Design.

Synappx Cloud Print Chrome Extension (Chromebook / ChromeOS)

Overview

Synappx Cloud Print extends secure pull printing to Chromebook and ChromeOS environments via a purpose-built Google Chrome extension. The extension follows the same security-by-design principles as other clients: zero-trust authentication, metadata-only cloud communication, and local document storage with secure, authenticated release.

Distribution and Integrity

- The extension is published via the Google Chrome Web Store and undergoes Google's review for each release.
- Integrity is enforced through CRX package signing by the Chrome Web Store. The extension package is digitally signed using an RSA key pair, and the Extension ID is deterministically derived from the associated public key, ensuring a stable and verifiable Extension ID across installations and updates.
- Automatic updates are delivered through the Chrome Web Store to keep users on a verified version.

User Authentication

- Users authenticate through the Auth0-brokered identity flow, delegating to Microsoft Entra ID or Google Workspace. Synappx does not store user passwords.
- Upon authentication, a session token is issued and managed within the extension runtime for secure API access.

Data Handling and Local Storage

- Print jobs captured by the extension are stored locally on the device in the browser's IndexedDB.
- Only job metadata (e.g., job name, timestamp, user identity, print settings) is transmitted to Synappx Cloud Print services over HTTPS (TLS 1.3, AES-256).
- No document content is uploaded to or stored in the cloud.

Transport Security

- All extension-to-cloud communications are encrypted via HTTPS (TLS 1.3) on port 443.
- The extension uses the same hardened API endpoints as other SCP clients.

Pull Printing and Secure Release

- Jobs remain local on the Chromebook until the user authenticates at a Sharp MFP and explicitly selects jobs for release.
- Upon secure release, the MFP retrieves the document from the user's device over the local network, ensuring documents print only in the user's physical presence.

Silent Printing Policy

- ChromeOS supports Silent Printing to bypass user confirmation prompts.
- This is controlled exclusively by IT via the Google Admin Console policy PrintingAPIExtensionsAllowlist and applied at the Google Workspace domain level.
- The permission is tied to the extension's verified Extension ID. Users cannot enable or change this setting themselves.

Permissions Model

- The extension requests only the minimum Chrome API permissions required for operation, declared in manifest.json.
- Permissions are reviewed during the Chrome Web Store publishing process.
- The extension does not request access to browsing history or cookies beyond what is necessary for print capture and authentication.

MFP Configuration Requirements

- System Settings > Authentication Settings > Default Settings > Enable IPP Authentication Except for Printer Driver: Unchecked
- System Settings > Security Settings > SSL/TLS Settings > TLS 1.3: Unchecked (this is only required for device CR5.0 without latest firmware)
- System Settings > Authentication Settings > Default Settings > Cache Authentication Information for External Service Connect: Unchecked

Alignment with Zero-Trust Architecture

The Chrome extension adheres to Synappx Cloud Print zero-trust principles: identity validated by the customer's IdP, metadata-only cloud transit, documents remain local, and secure device-side release. The extension relies on Google's extension security model and signing review, adding no additional trust assumptions.

Synappx Cloud Print QR Code Generation

Synappx Cloud Print platform uses the QR Code standard to provide an easy method to authenticate and validate the end user on the different process. As soon as the QR Code is generated and linked to a specific user, based on the standard, the back platform generates a new QR Code. This procedure happens in real time across all MFPs activated with Synappx Cloud Print solution.

If you are interested the standard associated with QR Code technology, please check Standard section here: QR code - Wikipedia

5. 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 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.

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.

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.

Business Continuity Management

Because Synappx is hosted on Azure, part of the continuity assurance comes from the cloud provider.

Microsoft Azure is certified under ISO 22301 (Business Continuity Management).

Microsoft states that Azure, Office 365, and several cloud services were independently audited and awarded ISO 22301 certification covering their business-continuity processes.

The certification includes:

- disaster recovery processes
- backup validation
- operational monitoring
- incident response procedures
- staff training and BCM governance

Azure even highlighted that it was the first hyperscale cloud provider to achieve ISO 22301 certification for business continuity management.

This means:

Layer	Certification
Azure infrastructure	ISO 22301 BCM certified

Synappx application layer	relies on Azure infrastructure
Sharp product security	ISO 27001 aligned

Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Synappx Cloud Print is a **cloud-based Print Management solution delivered as a Software-as-a-Service (SaaS)**. The service is designed to eliminate the need for on-premises infrastructure while providing secure printing and print accounting capabilities for distributed workplaces.

The service is hosted on **Microsoft Azure cloud infrastructure** and integrates with cloud identity platforms such as **Microsoft Entra ID (Azure AD) and Google Workspace**.

Business Continuity and Data Protection

Because Synappx Cloud Print operates as a cloud-native SaaS platform hosted on Azure infrastructure, business continuity and disaster recovery mechanisms leverage the **high-availability and resilience features of the underlying cloud platform**, including:

- redundant cloud infrastructure
- regional availability zones
- automated backup and recovery capabilities
- encrypted communication and Zero Trust architecture for protecting print data and device interactions

RTO and RPO Considerations

For Synappx Cloud Print, recovery objectives depend primarily on the **cloud infrastructure resilience model** and the **stateless nature of print jobs and print queues**.

Typical operational characteristics include:

Recovery Time Objective (RTO)

- The service is designed for **rapid restoration of cloud services through Azure high-availability architecture**, minimizing downtime in the event of infrastructure failure.

Recovery Point Objective (RPO)

- Print jobs are typically **processed in near real-time and stored temporarily**, which minimizes potential data loss.
- Administrative data such as user configuration, reporting, and print accounting are stored in cloud services that rely on **persistent storage and backup mechanisms provided by the hosting platform**.

Operational Continuity

In the event of a temporary service interruption:

- Print jobs remain protected through **secure release printing**, preventing unauthorized document access.
- All print activity and reporting data are maintained through **cloud-based auditing and management services**.

Sharp Privacy Policy

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

Document	Sharp Europe URL
Synappx Terms of Use	https://synappx-support.sharp.eu/en/terms-of-use
Synappx Privacy Policy	https://synappx-support.sharp.eu/en/privacy-policy
Support Centre Privacy	https://synappx-support.sharp.eu/en/synappx-support-centre-privacy-policy

6. Summary

Core Service Overview

Synappx Cloud Print is a full agentless cloud print management solution specifically designed for Sharp multifunction printers (MFPs) and compatible 3rd Party devices. It leverages Microsoft Azure cloud services and rich client technologies to facilitate hybrid collaboration, enabling features like secure print release, scanning to cloud destinations, and mobile printing.

Zero Trust Architecture and Security Design

The service is built on a Zero Trust Design framework, requiring all users to be authenticated and authorised regardless of whether they are inside or outside the corporate network.

- **Identity Management**: Synappx integrates directly with Microsoft Entra ID (formerly Azure AD) and Google Workspace for authentication.
- **Authentication Delegation**: It uses Auth0 to handle user identity verification, ensuring that user passwords are never stored within the Synappx or Auth0 systems. Instead, secure JWT tokens are used to maintain sessions.
- **Role-Based Access Control (RBAC)**: Access to the Admin Portal and specific applications is strictly governed by tenant-based roles, such as Primary Admin, Admin, and User.

Data Protection and Encryption

A critical security feature of Synappx Cloud Print is that **no print documents are stored in the cloud**.

- **Metadata Only:** Only metadata related to print jobs is transmitted to the cloud backend; the actual document remains within the customer's local network.
- **Encryption Standards:** All communications between client applications, MFPs, and the cloud are encrypted using HTTPS (TLS v1.3, AES256) or secured through X.509 certificates for MQTT and AMQP protocols.
- **Data Residency**: Services are hosted in secure Microsoft data centres in West Germany, which are fully GDPR compliant and provide local data redundancy.

Application Security

- **Windows Application**: Operates behind the customer's firewall and uses SNMP discovery (initiated by an admin) to find MFPs on the local network.
- **Mobile Application**: Allows users to print documents from cloud storage (e.g., OneDrive, Google Drive, Teams). When a user releases a print job via the mobile app, the document is pulled directly from the cloud storage or local network to the MFP, maintaining the Zero Trust model.
- **Secure Release**: Users must authenticate at the MFP using a **PIN, card/badge, or QR code** to release their documents, ensuring no sensitive information is left unattended.

Compliance and Business Continuity

- **Certifications**: Sharp maintains an ISO/IEC 27001 certification for its information security management systems.
- **Governance**: Sharp IT and support staff have strictly limited, role-based access to customer data, which is restricted to the minimum necessary for troubleshooting.
- **Resilience**: As a SaaS platform, Synappx relies on the ISO 22301-certified business continuity processes of Microsoft Azure, including redundant infrastructure and automated backup capabilities.
- **Data Retention**: Most logs and analytics data are retained for specific periods (e.g., 30 to 90 days), and customer data is deleted 45 days after a subscription ends.

Design and specifications subject to change without notice.

Sharp Electronics (Europe) Limited

4 Furzeground Way

Stockley Park, Uxbridge, Middlesex, UB11 1EZ, U.K.

www.sharp.eu

APPENDIX

Synappx Cloud Print (SCP) - ISO/IEC 27001:2022 Annex A Control Mapping

(Device Onboarding + Windows Web and Local Client Authentication)

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Identity & Access Management	Device Onboarding (Direct Connect)	J Customer unique token short-lived	A.5.16 Identity management	Devices are uniquely identified and onboarded using cryptographically secure tokens, ensuring controlled identity lifecycle.
		Single-use / limited-use tokens (jti tracking)	A.5.15 Access control	Prevents replay attacks and enforces strict access control.
		Device-to-tenant association	A.5.19 Information access restriction	Ensures tenant-level isolation and restricted access to resources.
		Short-lived device credentials	A.5.18 Access rights	Access is time-bound and aligned with least privilege principles.
	Windows Web and Local Client Authentication	Authentication via Microsoft Entra ID / Google Workspace	A.5.16 Identity management	Centralized identity providers manage user identities securely.
		No password storage in client	A.5.17 Authentication information	Sensitive authentication data is not stored locally, reducing compromise risk.
		JWT/OAuth tokens used post-authentication	A.5.15 Access control	Token-based access ensures secure session management.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
		Role-based access control (RBAC)	A.5.18 Access rights	User permissions are enforced based on assigned roles.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Cryptography & Key Management	Device Onboarding	Customer unique token short-lived	A.8.24 Use of cryptography	Ensures integrity and authenticity of provisioning tokens.
		Customer unique token short-lived	A.8.25 Key management	Secure storage and lifecycle management of cryptographic keys.
		Key rotation policies	A.8.25 Key management	Periodic rotation reduces risk of key compromise.
	Windows Web and Local Client Authentication	Secure token issuance (OAuth/JWT)	A.8.24 Use of cryptography	Tokens are cryptographically protected during authentication flows.
		TLS encryption for authentication flows	A.8.24 Use of cryptography	Protects credentials and tokens in transit.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Application & Secure Development	Device Onboarding	Customer unique token short-lived	A.8.28 Secure coding	Prevents token tampering and replay vulnerabilities.
		Backend enforcement of quotas and constraints	A.8.29 Security testing in development and acceptance	Ensures logic is validated and secure before acceptance.

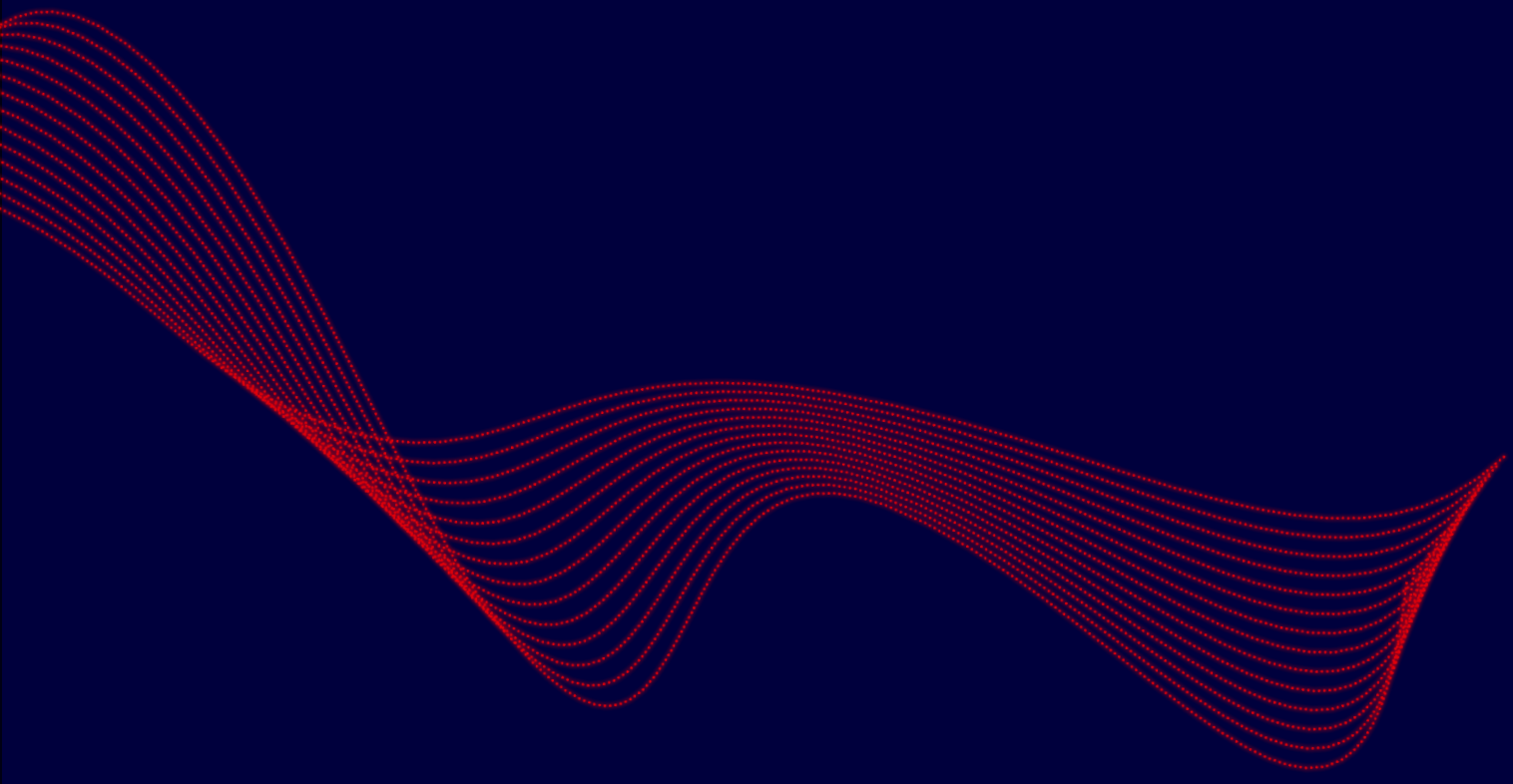
Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
		Tenant isolation enforcement	A.8.31 Separation of environments	Logical separation prevents cross-tenant access risks.
	Windows Web and Local Client Authentication	Secure client design (no credential storage)	A.8.28 Secure coding	Reduces attack surface on endpoint devices.
		Use of trusted identity providers	A.8.30 Outsourced development	Reliance on secure, externally managed authentication services.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Network Security	Device Onboarding	WAF protection on registration endpoints	A.8.20 Network security	Protects against web-based attacks.
		API rate limiting	A.8.23 Web filtering	Prevents abuse and denial-of-service attempts.
		TLS-secured communication	A.8.24 Use of cryptography	Ensures confidentiality and integrity in transit.
	Windows Web and Local Client Authentication	Secure communication with identity providers	A.8.20 Network security	Authentication flows are protected over secure channels.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Monitoring & Operations Security	Device Onboarding	Monitoring anomalous registration activity	A.8.16 Monitoring activities	Detects suspicious onboarding behavior.
		Token usage logging (jti tracking)	A.8.15 Logging	Provides traceability and forensic capability.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
		Device registration audit trails	A.8.15 Logging	Ensures accountability and audit readiness.
	Windows Web and Local Client Authentication	Authentication event logging	A.8.15 Logging	Tracks login attempts and access patterns.
		Integration with identity provider logs	A.8.16 Monitoring activities	Enables centralized monitoring and alerting.

Domain	SCP Capability	Control Implementation (SCP)	ISO 27001 Annex A Control	Mapping Description
Compliance & Governance	Device Onboarding	License-based registration limits	A.5.31 Legal, statutory, regulatory requirements	Ensures compliance with contractual constraints.
		Policy-driven device management	A.5.1 Policies for information security	Devices operate under defined governance policies.
	Windows Web and Local Client Authentication	Use of enterprise IdP compliance controls	A.5.36 Compliance with policies and standards	Aligns authentication with enterprise security frameworks.



SHARP