Livre blanc sur la sécurité

Synappx™ Go et Synappx™ Meeting

www.sharp.fr

SHARP
Be Original.

Tables des matières

1. Introduction

Aperçu

Synappx Go et Synappx Meetings sont des applications et des services de collaboration, de productivité et d'analyse. Ils sont protégés par un système de sécurité efficace à plusieurs niveaux, afin de garantir que le système et ses composants ne présentent pas de points de vulnérabilité pour vos données ou vos réseaux. Grâce à une combinaison de fournisseurs de technologies de classe mondiale, notamment Microsoft Azure, Google Workspace et des bonnes pratiques de Sharp en matière de sécurité, votre utilisation des services Synappx vous permet de préserver la sécurité de vos informations tout en vous aidant à améliorer la productivité de votre entreprise. Les dispositions de sécurité relatives à Synappx sont décrites dans ce livre blanc.

Synappx Go

Synappx Go est un service mobile qui exploite la technologie NFC pour permettre une numérisation pratique et rapide vers vos destinations favorites et l'impression de fichiers dans le Cloud vers des imprimantes multifonctions Sharp (MFP). Vous pouvez également utiliser votre smartphone et l'application pour sélectionner et télécharger le contenu présent dans cotre espace de stockage Cloud grâce à un tag NFC. Le logiciel et les services cloud Synappx Go s'appuient sur la base de données Microsoft Azure, le provisionnement des dispositifs, le Hub IoT et de nombreux autres services.

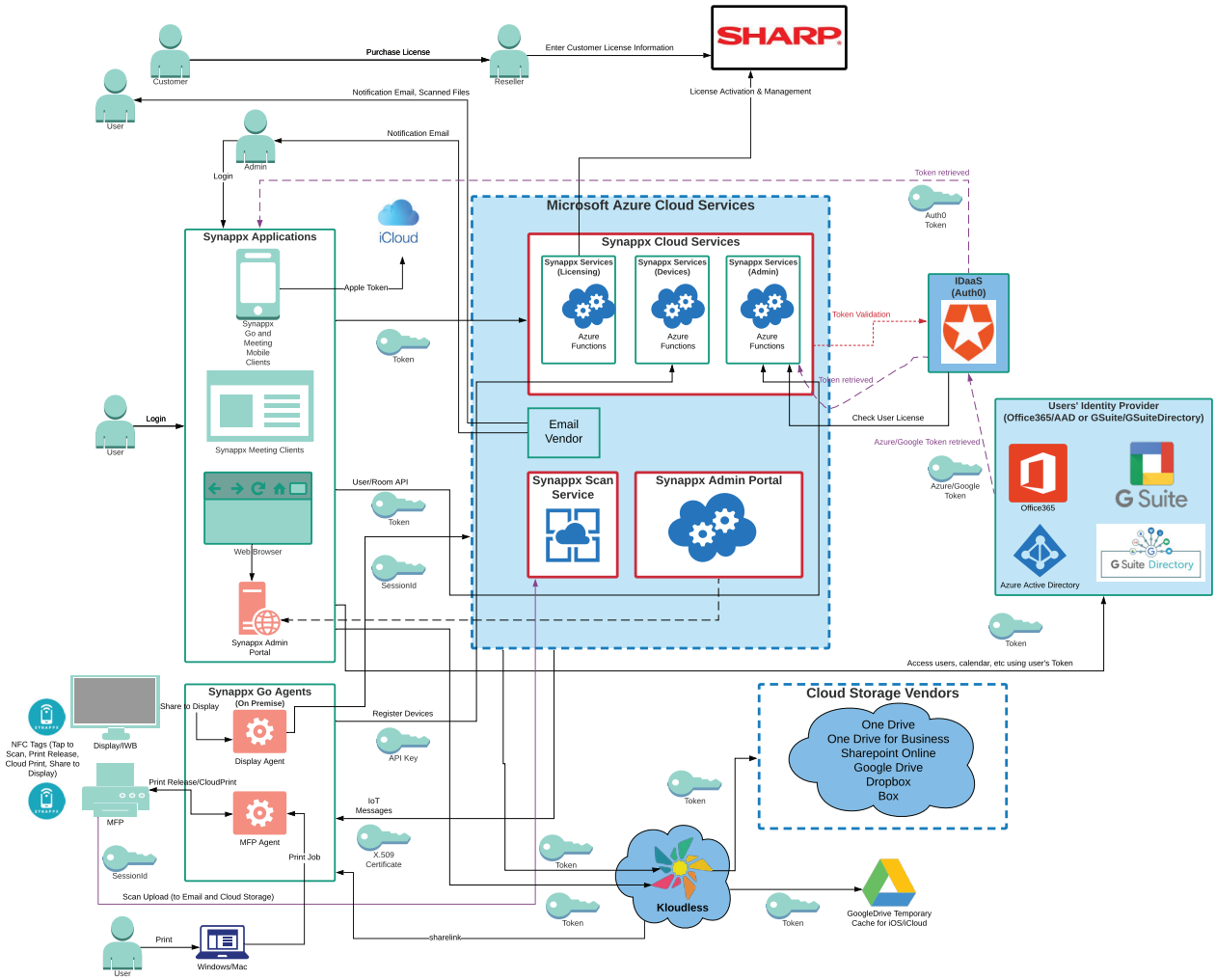
Synappx Meeting

Synappx Meeting exploite le Cloud Azure, les technologies mobiles et vocales* pour aider les utilisateurs à démarrer les réunions à temps et à être plus efficaces. Un simple clic sur un bouton permet de connecter les éléments clés de la réunion. L'affichage miroir se fait automatiquement de votre PC vers l'écran Sharp de la salle de réunion. La conférence en ligne démarre automatiquement et vous pouvez accéder aux documents de la réunion. Les commandes vocales* peuvent être utilisées pour gagner du temps pour les tâches courantes de la réunion. Synappx Meeting utilise la base de données Azure de Microsoft, le stockage, les fonctions Azure et bien plus encore.

* Le contrôle vocal n'est actuellement pas disponible en Europe.

2. Aperçu de l’architecture

Voici un aperçu de la plateforme Synappx (optimisée par Microsoft Azure), dont les composants et l’architecture des services Synappx Go et Synappx Meeting :



3. Services Synappx Cloud

Synappx Meeting et Synappx Go s'appuient sur les services de la plateforme cloud Microsoft Azure comme base des services cloud de Synappx. Microsoft Azure est un service dans le Cloud mondial très respecté, doté d'un large éventail de fonctionnalités utilisées par la famille de produits Sharp Synappx, comprenant la base de données Azure Cosmos, le stockage, plusieurs services IoT, Key Vault, Azure Security Center, et plus encore.

Les solutions Synappx sont hébergées dans des centres de données Microsoft sécurisés situés en Europe. Le « Microsoft Azure Cloud » et les centres de données sont protégés par les pratiques de sécurité de Microsoft. Chaque centre de données présente une redondance locale des données. En outre, toutes les communications entre les applications Sharp Synappx et les services Synappx Cloud (hébergés sur Microsoft Azure) sont cryptées via HTTPS (TLS v1.2, AES256), sécurisées par des certificats X.509 ou MQTT (utilisés par le MFP et l'Agent d'affichage).

L'accès à tous les services dans le Cloud de Synappx à partir d'applications de clients nécessite des clés, des certificats ou des jetons d'authentification sécurisés. Après avoir acheté un service Synappx, chaque client se voit attribuer un certificat unique pour les communications, qui est stocké dans Microsoft Key Vault pour permettre un accès sécurisé et réservé aux clients. L'accès à la base de données Azure de Synappx est limité aux adresses IP figurant sur la liste blanche d'Azure App Services. Microsoft Key Vault est utilisé pour le stockage des certificats SSL, des certificats de signature X.509, des clés privées et d'autres contenus exigeant la plus haute sécurité. L'accès à Microsoft Azure Key Vault est limité à l'administrateur des services Sharp et aux utilisateurs du système disposant des autorisations d'accès associées.

Les données spécifiques aux clients de Synappx Go et/ou Synappx Meeting stockées dans les bases de données sécurisées dans le Cloud Azure sont les suivantes :

Synappx Meeting et Synappx Go

- Le prénom, le nom et l'adresse électronique de l'utilisateur (importés d'Azure AD ou Google Workspace vers Synappx par l'Admin)
- Le prénom, le nom et l'adresse électronique de l'utilisateur Admin (importés d'Azure AD ou Google Workspace vers Synappx par l'Admin)
- Les noms, adresses électroniques et localisations des espaces de travail (salles de réunion) importés de Microsoft Outlook ou Google Workspace Directory vers Synappx par l'Admin
- Les noms et localisations des espaces de travail ajoutés manuellement
- Les alias de domaine des entreprises d'Azure AD et Google Workspace
- Les données d'utilisation des applications pour générer des rapports à l'usage de l'Admin
- Les données de la licence Synappx (ex : la date de son expiration)
- Les journaux du système

Spécificités de Synappx Meeting :

- L'affichage de l'adresse IP et du port (si configuré par l'Admin)
- Affichage facultatif de l'ID du compte et du mot de passe (si configuré par l'Admin)
- Le type d'expéditeur de la diffusion, l'adresse IP et le code PIN (si configuré par l'Admin)
- Le nom de la réunion, la durée réelle de la réunion (heure de début et heure de fin), le nom du lieu de la réunion, le nom et l'adresse électronique des participants

Spécificités de Synappx Go :

- Les informations sur le MFP(nom du modèle, adresse IP, numéro de série) découvertes via la découverte SNMP initiée par l'Admin
- Les informations sur l'Agent du MFP (nom de l'ordinateur, ID de l'ordinateur, numéro de version, politique de mise à jour, date de la dernière mise à jour)
- Les informations sur l'Agent d'affichage (nom de l'ordinateur, ID de l'ordinateur, numéro de version, politique de mise à jour, date de la dernière mise à jour)
- Informations sur les tags NFC (ID de tag, type) associés aux dispositifs configurés par l'Admin

Les données contenues dans les bases de données Synappx ne sont accessibles aux clients sous licence que par l'intermédiaire des applications Synappx et un personnel Sharp limité si nécessaire à des fins de support.

Dans l'ensemble, la stricte gestion des services Cloud de Synappx limite l'accès au système à un personnel minimal pour le déploiement et le support. Voir les sections sur la politique de sécurité de Sharp pour plus de détails.

Pour plus d'informations sur la sécurité de Microsoft Azure, voir les liens suivants relatifs aux fonctionnalités utilisées par les services Synappx :

- Aperçu : https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Cryptage des données au repos : https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Sécurité du réseau Azure : https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Fonctions d'Azure et sécurité des plates-formes sans serveur : https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Sécurité du réseau Azure : https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Gestion de la sécurité dans Azure : https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Gestion- Gouvernance Azure : https://docs.microsoft.com/en-us/azure/governance/

4. Portail Administrateur Sharp

Les administrateurs (Admins) de Synappx Meeting et Synappx Go configurent et gèrent le système Synappx via les pages web du Portail Administrateur Synappx. L'ajout d'espaces de travail/salles de réunion, d'utilisateurs, d'appareils, d'administrateurs supplémentaires et autres s'effectue via ces pages web sécurisées. La gestion des licences se fait via le Portail Administrateur et le statut des licences peut être consulté ici. Les rapports aident à illustrer l'utilisation du système Synappx et sa valeur commerciale. Les téléchargements (pour Synappx Go) sont facilement accessibles via ces pages. Les journaux du système peuvent être téléchargés.

4.1 Accès et connexion basés sur les rôles (pour le Portail Administrateur et les clients)

L'accès au Portail Administrateur Synappx est contrôlé au moyen de processus d'authentification basés sur les comptes titulaires et les rôles. Les utilisateurs sont configurés dans chaque titulaire et sont associés à un compte client spécifique et en fonction de leurs rôles et autorisations d'utilisation. L'administrateur initial est identifié dans le cadre du processus de commande. Des Administrateurs supplémentaires peuvent être ajoutés après une connexion réussie au portail Synappx par le premier Admin.

Seuls les administrateurs désignés ou assignés par le client peuvent accéder, configurer, octroyer des licences, gérer les utilisateurs et les espaces de travail du service Synappx, consulter les rapports, etc. pour leur compte via le portail web sécurisé. Toutes les communications avec le Portail Administrateur se font via le port 443 du HTTPS/SSL (TLS1.2) afin de protéger les données en cours de transmission.

Synappx Meeting et Synappx Go exploitent les informations d'identification des administrateurs et des utilisateurs de la suite Microsoft 365 ou G pour éviter d'avoir à mettre en place, gérer et protéger des identifiants distincts de connexion à Synappx. De par leur conception, les services Synappx n'ont pas accès aux mots de passe des clients de Microsoft 365 ou de Google Workspace. Le système exploite Azure Active Directory ou Google Workspace Directory et s'appuie sur des jetons d'authentification pour identifier les administrateurs et les utilisateurs (pour l'accès des clients). L'identité de l'utilisateur est confirmée avec votre Microsoft Azure AD (pour les comptes Microsoft 365) ou Google Workspace Directory (pour les comptes Google Workspace) par un partenaire d'identité sécurisé Auth0 (voir ci-dessous) et les mots de passe des utilisateurs ne sont jamais conservés dans les systèmes Synappx ou Auth0. La plate-forme Synappx conserve uniquement en toute sécurité l'adresse électronique et le nom/prénom de l'utilisateur. Aucune autre information personnelle identifiable sur l'utilisateur n'est connue ou conservée par le système de Synappx.

4.2 Auth0 (Fournisseur de services d'identité)

Pour les services Synappx, Sharp travaille avec Auth0 (https://auth0.com/) pour des services d'identité sécurisés vers Microsoft Azure AD et Google Workspace. Selon Auth0, ils desservent 21 millions d'utilisateurs à travers 120 000 applications, avec 2,5 milliards de connexions par mois. Il s'agit d'un fournisseur de services d'identité très respecté.

Voici un aperçu du processus :

1. L'Admin ou l'utilisateur saisit les informations d'identification de Microsoft 365 ou de la Google Workspace via des dialogues lorsqu'il se connecte au Portail Administrateur Synappx ou à tout client de Synappx.

2. Auth0 délègue l'authentification du nom d'utilisateur et du mot de passe passés via SSL/TLS 1.2 (port 443) à Azure AD ou Google Workspace qui valide les identifiants du nom d'utilisateur et du mot de passe.

3. Auth0 ne connaît pas ni ne conserve le mot de passe de l'utilisateur.

4. En collaboration avec Azure AD ou Google Workspace, un jeton Web JSON (JWT) sécurisé est fourni en retour au navigateur (pour l'accès
   au Portail Administrateur de Synappx), aux appareils mobiles (pour Synappx Go et Synappx Meeting) et/ou aux clients Windows/Mac (pour Synappx Meeting).

5. Ce jeton permet à l'application d'exécuter des fonctions sans que l'utilisateur ait à se connecter à chaque fois qu'il utilise les applications (sauf dans les cas où les informations d'identification sont modifiées, par exemple lorsque le mot de passe doit être saisi à nouveau, lorsque l'utilisateur n'est plus valide, lorsque l'utilisateur se déconnecte de l'application mobile ou en cas de 30 jours d'inactivité). Personne ne peut altérer le jeton JWT sans la clé secrète associée utilisée pour la signature, qui est conservée en toute sécurité dans le Cloud.

Plusieurs niveaux de protection de l'authentification sont à votre disposition. L'appareil mobile ou l'ordinateur de l'utilisateur est protégé par un mot de passe ou un identifiant biométrique (par exemple, empreintes digitales ou reconnaissance faciale). Les mots de passe des utilisateurs ne sont connus/conservés sur aucun des appareils Synappx et les jetons sécurisés fournis par Auth0 sont basés sur des jetons sécurisés et une validation de Microsoft Azure ou Google Workspace.

Auth0 dispose de nombreuses certifications pour la sécurité dans le Cloud, notamment : ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, le bouclier de protection des données UE-US, Gold CSA STAR, la conformité aux exigences du RGPD, entre autres. Voir les livres blancs relatifs à l'Auth0 pour plus d'informations sur les dispositions de sécurité d'Auth0 :

- https://auth0.com/security/

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

4.3 Attribution des privilèges d'application de Synappx

Pour activer les fonctions Synappx Meeting et Synappx Go, l'Admin doit accorder certains privilèges aux utilisateurs de l'application Synappx. Le premier Admin à se connecter au système doit disposer des privilèges d'administrateur d'Azure AD ou Google Workspace et consentir, au nom de l'organisation, aux autorisations requises pour les utilisateurs lors de l'accès aux applications/ services
de Synappx.

Les autorisations requises	Définition	Portail Administrateur	Synappx Meeting	Synappx Go
Azure Active Directory Graph :				
User.Read	Permet aux utilisateurs de se connecter à l'application et permet à l'application de lire le profil des utilisateurs connectés. Il permet également à l'application de lire les informations de base sur les entreprises des utilisateurs connectés.	Oui	Oui	Oui
Directory.Read.All	Permet à l'application de collecter des alias de domaine d'Azure AD (nécessaire pour le support multi-domaine) et permet à l'application de lire des données dans Azure AD telles que les utilisateurs, les groupes et les applications.	Oui	Non	Non
Microsoft Graph :				
Calendars.ReadWrite. Shared	Permet à l'application de créer, lire, mettre à jour et supprimer des événements dans tous les calendriers auxquels l'utilisateur est autorisé à accéder. Cela inclut les calendriers délégués et partagés.	Non	Oui	Non
Files.ReadWrite.All	Permet à l'application de lire, créer, mettre à jour et supprimer tous les fichiers auxquels l'utilisateur connecté est autorisé à accéder.	Non	Oui	Non
Group.Read.All	Permet à l'application de lister les groupes, de lire leurs propriétés ainsi que toutes les adhésions aux groupes au nom de l'utilisateur connecté. L'application permet également de lire le calendrier, les conversations, les fichiers et autres contenus de groupe pour tous les groupes auxquels l'utilisateur connecté est autorisé à accéder.	Oui	Non	Non
User.Read.All	Permet à l'application de lire l'ensemble des propriétés du profil, des rapports et des gestionnaires des autres utilisateurs de votre organisation, au nom de l'utilisateur connecté.	Oui	Oui	Non
offline_access	Permet à l'application de lire et de mettre à jour les données des utilisateurs, même lorsqu'ils ne sont pas en train d'utiliser l'application.	Oui	Oui	Oui
Courriel	Permet à l'application de lire l'adresse électronique principale de vos utilisateurs.	Oui	Oui	Oui
openid	Permet aux utilisateurs de se connecter à l'application avec leur compte professionnel ou scolaire et permet à l'application de voir les informations de base du profil de l'utilisateur.	Oui	Oui	Oui
profile	Requis pour obtenir des informations sur le profil de l'utilisateur (par exemple, nom et prénom de l'utilisateur, adresse électronique) à partir d'Azure AD.	Oui	Oui	Oui

Pour les clients de la Google Workspace, voici la liste des champs d'application de l'API qui sont nécessaires et la raison pour chacun :

Portée de l'API Google demandée	Définition	Portail Administrateur	Synappx Meeting	Synappx Go
https://www.googleapis.com/auth/admin.directory.domain.readonly	Permet à l'application de lire les informations sur le domaine pour prendre en charge la fonction multi-domaine.	Oui	Non	Non
https://www.googleapis.com/auth/admin.directory.group.readonly	Permet à l'application de récupérer les informations sur les groupes, les alias de groupes et les membres pour ajouter des groupes via le Portail Administrateur.	Oui	Non	Non
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Permet à l'application de récupérer les ressources du calendrier pour ajouter des espaces de travail via le portail d'administration.	Oui	Non	Non
https://www.googleapis.com/auth/admin.directory.user.readonly	Permet à l'application de récupérer des utilisateurs ou des alias d'utilisateurs pour ajouter des utilisateurs via le portail d'administration.	Oui	Non	Non
https://www.googleapis.com/auth/calendar.readonly	Permet à l'application d'avoir un accès en lecture seule aux calendriers.	Non	Oui	Non
https://www.googleapis.com/auth/calendar.events	Permet à l'application d'avoir un accès en lecture/écriture aux événements d'un calendrier et de mettre à jour le calendrier (par exemple, prolonger la durée de la réunion).	Non	Oui	Non
https://www.googleapis.com/auth/drive	Permet à l'application d'avoir accès aux fichiers Google Drive de l'utilisateur autorisé (à l'exclusion du dossier Données d'application) pour lister les fichiers.	Non	Oui	Non
https://www.googleapis.com/auth/drive.file	Permet à l'application d'avoir accès aux fichiers créés ou ouverts par l'application pour le téléchargement et le chargement. L'autorisation de fichier est accordée sur une base par utilisateur et est annulée lorsque l'utilisateur supprime l'autorisation de l'application.	Non	Oui	Non
https://www.googleapis.com/auth/userinfo.profile	Permet à l'application d'utiliser les informations personnelles que l'utilisateur a rendues publiques pour obtenir un nom d'utilisateur et une image d'avatar.	Non	Oui	Oui

4.4 Importation d'utilisateurs ou d'espaces de travail d'Azure AD ou Google Workspace

Synappx Go accorde une licence pour le service sur base de l'utilisateur tandis que Synappx Meeting accorde une licence sur base des espaces de travail/salles de réunion. Les administrateurs peuvent gagner du temps et réduire les erreurs de frappe en important directement les utilisateurs (pour Synappx Go) et les espaces de travail (par exemple Rooms) pour les deux applications depuis Microsoft 365 (Azure AD) ou Google Workspace. L'entrée manuelle des espaces de travail est également autorisée. Seuls les utilisateurs des domaines pris en charge dans Azure AD ou Google Workspace peuvent être ajoutés en tant qu'utilisateurs autorisés de Synappx Go.

Les communications avec Microsoft Azure et Google Workspace pour l'importation des utilisateurs et/ou des espaces de travail se font via HTTPS (port 443).

4.5 Téléchargements de l'Agent Synappx Go

Les Agents Synappx Go du MFP et de l'affichage peuvent être téléchargés sur la page de téléchargement du Portail Administrateur de Synappx. Les Agents téléchargés ne sont pas disponibles sur les sites web publics et ne peuvent être téléchargés que par des administrateurs Synappx agréés. Un fichier de configuration crypté (SHA-256) est joint au fichier zip contenant les informations spécifiques au titulaire et les informations saisies par le client afin de permettre la détection automatique du MFP via SNMP pour l'agent du MFP). Voir la section Agents Synappx Go pour plus de détails sur la sécurité liée aux agents.

4.6 Les rapports de Synappx

Les rapports Synappx Meeting et Synappx Go aident les administrateurs à comprendre l'utilisation et la valeur des applications Synappx. Les données qui génèrent les rapports Synappx sont stockées sur des serveurs Microsoft sécurisés. Les données sont conservées jusqu'à 45 jours après la résiliation du service par le client (pour lui laisser le temps de renouveler la licence s'il le souhaite). Les informations spécifiques à l'utilisateur contenues dans les rapports ne sont accessibles qu'aux administrateurs de l'entreprise via les pages des rapports. Des données récapitulatives anonymes sur l'utilisation des applications par les clients sont mises à la disposition de Sharp à des fins de support et d'amélioration des produits au fil du temps. Pour plus de détails, voir La sécurité des entreprises Sharp, l'Accès aux données de l'administration Sharp et la politique de protection de la vie privée de Sharp.

4.7 Domaines pris en charge par Synappx

Pour les comptes Microsoft 365 et la Google Workspace, Synappx collecte des informations sur les alias de domaine pris en charge dans le système Azure AD ou Google Workspace du compte. Pour les comptes Microsoft 365, sur la page web Configuration admin / Domaines pris en charge, après l'autorisation initiale, les administrateurs peuvent sélectionner des alias de domaine supplémentaires en plus du domaine principal Azure AD sous lequel le compte Synappx a été créé. Cela permet aux utilisateurs et aux espaces de travail d'être importés depuis les domaines sélectionnés pour être utilisés avec les services de Synappx.

4.8 Synappx System Logs

Synappx Go et Synappx Meeting comprennent un journal du système contenant des informations sur les événements du système susceptibles d'intéresser les administrateurs. Il s'agit notamment des conditions qui peuvent nécessiter une intervention de l'Admin pour corriger un problème ou effectuer un dépannage. Les journaux du système peuvent être exportés par les administrateurs sous forme de fichier .CSV pour une analyse plus approfondie. Les journaux du système sont conservés par le système Synappx pendant 30 jours.

5. Clients Windows et Apple MAC OS pour Synappx Meeting

Synappx Meeting permet de se connecter à l'écran dans la salle de réunion, de démarrer une conférence web et de faire fonctionner des applications par de simples commandes vocales *. Ils offrent un large éventail de caractéristiques de sécurité, notamment :

- Les accès des clients Synappx Meeting aux ressources du Cloud se font via HTTPS (port 443)
  - Azure (Obtention d'informations sur les salles de réunion auprès de l'administration de Synappx)
  - Auth0 (Délégation de l'authentification des utilisateurs pour Azure AD)
  - Azure AD (authentification de l'utilisateur avec un compte Microsoft 365) ou Google Workspace (authentification de l'utilisateur avec un compte Google Workspace)
  - Microsoft Graph APIs (obtient des informations sur les réunions et des fichiers pour les réunions depuis Microsoft Office 365) ou Google API Scopes (obtient des informations sur les réunions et des fichiers pour les réunions à partir de la Google Workspace)
  - Amazon Web Services pour l'accès à la file d'attente des commandes vocales*

- L'accès à l'affichage local
  - Permet le contrôle des systèmes d'affichage interactif BIG PAD avec commande vocale *. Le protocole est telnet (Port 10008)

- L'utilisateur s'authentifie avec les mots de passe Microsoft 365 ou Google Workspace la première fois qu'il utilise l'application Synappx, lorsqu'il y a des changements d'identification (par exemple, mise à jour du mot de passe), il se déconnecte de l'application client et/ou après 3 jours sans utilisation de l'application

- Les mots de passe des utilisateurs ne sont pas conservés sur l'appareil mobile ; par contre, un jeton JWT sécurisé est fourni après validation du mot de passe de l'utilisateur avec le système Azure AD ou Google Workspace via un partenaire Auth0.
  - Le jeton d'accès de l'utilisateur est conservé sur l'ordinateur local
  - L'ID/Mot de passe pour le proxy sont stockés sur la mémoire locale. (crypté au moyen de l'AES128)

* Le contrôle vocal n'est actuellement pas disponible en Europe.

6. Synappx Go et Synappx Meeting Mobile

Avec l'utilisation généralisée des appareils mobiles dans les entreprises, les smartphones sont désormais couramment utilisés pour accéder et partager des contenus professionnels. Les utilisateurs s'attendent à ce que des services mobiles intuitifs les aident à accomplir leur travail plus rapidement. Avec l'application mobile Synappx Go, les utilisateurs peuvent numériser vers des destinations fréquentes, imprimer des versions ou des fichiers Cloud pris en charge vers n'importe quel appareil configuré par Synappx Go et partager des fichiers Cloud vers des écrans Sharp configurés. L'application mobile Synappx Meeting permet aux utilisateurs de démarrer leur réunion, de lancer des conférences web et d'accéder rapidement à des documents. Plusieurs dispositifs de sécurité sont associés aux clients mobiles :

Synappx Meeting et Synappx Go :

- Les appareils mobiles nécessitent la saisie de mots de passe utilisateur ou une authentification biométrique (par exemple, empreintes digitales, reconnaissance faciale) pour accéder aux applications.

- Les utilisateurs s'authentifient avec des identifiants Microsoft 365 ou Google Workspace la première fois qu'ils utilisent l'application Synappx, lorsqu'il y a des changements d'identifiants (par exemple, mise à jour du mot de passe), ils se déconnectent de l'application mobile et/ou après 30 jours ou plus sans utilisation de l'application.
  Les effets de levier :
  - Auth0 (Délégation de l'authentification des utilisateurs pour Azure AD)
  - Azure AD (authentification de l'utilisateur avec un compte Microsoft 365) ou Google Workspace (authentification de l'utilisateur avec un compte Google Workspace)
- Les mots de passe des utilisateurs ne sont pas conservés sur l'appareil mobile ; par contre, un jeton JWT sécurisé est fourni après validation du mot de passe de l'utilisateur avec le système Azure AD ou Google Workspace via un partenaire Auth0.

- Tous les accès au système sont cryptés via TLS v1.2 AES256 (Port 443).

Spécificités de Synappx Go :

- L'accès mobile des utilisateurs est contrôlé de manière centralisée via le Portail Administrateur Sharp. Les administrateurs peuvent retirer une licence d'utilisateur à tout moment pour bloquer l'utilisation ultérieure des fonctionnalités mobiles de Synappx Go.

- Les utilisateurs sont priés d'accorder l'accès à leur liste de contacts mobiles afin de créer une numérisation vers des destinations de courrier électronique sans avoir à saisir à nouveau les courriers électroniques des utilisateurs cibles. Cela permet de gagner du temps et de réduire les erreurs de frappe.

- Pour numériser vers un dossier de mémoire dans le Cloud, imprimer des fichiers sélectionnés dans le Cloud ou partager des fichiers dans le Cloud vers des écrans Sharp, les utilisateurs peuvent choisir de configurer Synappx Go pour accéder aux fichiers des sites de stockage dans le Cloud pris en charge (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box ou Google Drive). Pour l'application iOS, les fichiers iCloud et locaux sont déjà configurés.

  - Pour les sites de conservation de données présentant un intérêt, les utilisateurs peuvent saisir leur nom d'utilisateur et leur mot de passe, qui sont validés avec les sites de conservation de données dans le Cloud. En cas de validation, un jeton sécurisé est fourni et conservé dans Synappx Go mobile pour éviter à l'utilisateur de devoir saisir à nouveau ces informations d'identification, sauf si elles ne sont plus valables (par exemple, changement de mot de passe, désactivation du compte, etc.).
  - Les fournisseurs de Sharp et de composants n'ont pas accès aux mots de passe des sites de conservation dans le Cloud des données des utilisateurs.
  - Pour chaque service de stockage dans le Cloud, il sera demandé à l'utilisateur de fournir à l'application Synappx les autorisations sélectionnées pour pouvoir accéder et mettre à jour les fichiers qu'il choisit de télécharger pour les afficher et les modifier. Remarque : Le service Synappx Go ne dispose d'aucune fonction permettant de supprimer des fichiers ou des dossiers d'un site de conservation de données dans le Cloud.
  - Remarque : Sharp s'associe à un fournisseur tiers, Kloudless (Kloudless.com), pour faciliter des connexions Synappx Go efficaces avec plusieurs fournisseurs stockage de données dans le Cloud. Kloudless n'a pas accès aux mots de passe des utilisateurs. Leur base de données sécurisée comprend les adresses électroniques des utilisateurs de Synappx Go. Ils conservent des métadonnées minimales sur les fichiers/dossiers (par exemple, le nom et l'ID du fichier, la date de modification) pour permettre la consultation des fichiers récemment modifiés sur les sites dans le Cloud. Le contenu des fichiers des utilisateurs n'est pas conservé par Kloudless.

Spécificités de Synappx Meeting :

- Les applications mobiles sont disponibles pour tout utilisateur du service (aucune licence requise); toutefois, celui-ci doit être un utilisateur légitime d'Azure AD ou Google Workspace dans le même domaine client.
- Les informations sur la salle de réunion Azure sont accessibles à partir de Synappx Admin.
- L'API Microsoft Graph permet d'obtenir des informations et des fichiers pour Meeting depuis Microsoft Office 365.
  Les champs d'application de l'API Google permettent d'obtenir des informations et des fichiers pour Meeting depuis la Google Workspace.

7. Tags NFC de Synappx Go

Synappx Go utilise des tags NFC spéciaux fournis par Sharp, des revendeurs agréés et/ou intégrés dans certains modèles du MFP. Les tags contiennent un identifiant unique et sont en lecture seule (ils ne peuvent pas être reprogrammés). Chaque tag ne peut être associé qu'à un seul appareil à la fois. Une fois configuré sur un appareil (par exemple le MFP ou le PC d'affichage) par l'administrateur via l'application mobile Synappx Go, il suffit à l'utilisateur de rapprocher son smartphone du tag NFC pour que l'application mobile identifie l'identité de l'utilisateur et l'appareil associé au tag pour permettre à Synappx Go d'utiliser des fonctions tels que la numérisation vers courrier électronique, l'impression suivie, l'impression de fichiers depuis le Cloud et le partage vers un écran.

8. Agent MFP pour Synappx Go

L'Agent MFP pour Synappx Go (y compris le logiciel d'impression) est un composant intégré au système Synappx Go installé sur le PC ou le serveur d'un client pour faciliter les communications entre les MFP compatibles avec Synappx Go et le Cloud de Synappx Go afin de permettre l'utilisation des téléphones portables et des NFC pour les cas d'utilisation liés aux MFP de Sharp. Synappx Go supprime la nécessité de se former et de procéder à de multiples étapes sur le panneau avant du MFP pour lancer des travaux d'impression sécurisés à partir de n'importe quel MFP équipée de Synappx Go, imprimer des fichiers sélectionnés dans le Cloud et envoyer des fichiers vers les destinations de numérisation favorites. Les utilisateurs peuvent gagner du temps pour la numérisation et l'impression sécurisée, ce qui réduit également le risque d'accès non autorisé aux travaux d'impression de l'utilisateur.

L'agent MFP Synappx Go est tenu de prendre en charge les cas d'utilisation de la numérisation et de l'impression. L'une des fonctions essentielles de l'agent est d'établir un canal de communication sécurisé vers le Cloud de Synappx. L'agent s'interface avec le Cloud pour enregistrer et sécuriser les communications des appareils et envoyer/recevoir des messages à destination et en provenance de l'agent et des MFP prise en charge. Chaque Agent possède un identifiant unique, et c'est ce que le système Synappx Go Cloud utilise pour identifier les agents à qui envoyer des messages. Les Agents écoutent les messages en s'abonnant à leur sujet d'identification unique et les services dans le Cloud envoient le message en publiant dans ce sujet d'identification.

8.1 Installation de l'Agent MFP

Pour installer l'agent du MFP, le package d'installation personnalisé est téléchargé depuis le portail d'administration de Synappx Go avec un fichier de configuration unique pour le client. Le contenu du fichier de configuration est sécurisé par des algorithmes de cryptage. Ce pack d'installation de l'agent du MFP n'est pas disponible sur un site web public et est lié au compte spécifique du client. Pour la plupart des installations des clients, il y aura un Agent du MFP installé par site client pour prendre en charge un maximum de 50 à 100 MFP(en fonction du nombre d'utilisateurs et des travaux d'impression) qui pourront utiliser les capacités d'impression et de numérisation de Synappx Go. Les clients qui souhaitent prendre en charge plus de 100 MFP devront installer un ou plusieurs agents de MFP supplémentaires.

Après l'installation, pour s'enregistrer, l'agent du MFP soumet son identifiant unique, ainsi que les références de sécurité de l'agent au Cloud de Synappx Go pour l'enregistrement dans le registre des équipements périphériques. Les informations stockées dans le registre des appareils comprennent des données telles que l'ID de l'appareil, l'emplacement, l'ID du titulaire et, pour les MFP l'agent associé au MFP.

8.2 Communications de l'Agent du MFP

Toutes les communications entre l'agent du MFP Synappx Go et le Cloud de Synappx Go utilisent soit le HTTPS (port 443), soit la sécurité client X.509 sur MQTT. Le HTTPS est utilisé lors des communications initiales d'installation entre l'agent du MFP Synappx Go et le Cloud Synappx Go, ainsi que pour envoyer les informations du MFP et toute information relative à des erreurs.

- Les clés privées de l'agent X.509 ne quittent jamais le système sur lequel l'agent est installé, et ne sont donc jamais exposées du fait de la transmission sur Internet.

- Tous les certificats de l'agent X.509 sont signés à l'aide des certificats de signature du client de l'agent. Les Agents ne sont autorisés à s'inscrire automatiquement que si le certificat X.509 est signé par leur client associé qui signe le certificat.

Les services du Cloud Synappx Go conservent des certificats de signature distincts pour chaque client Synappx Go. Cela garantit que les Agents ne sont provisionnés que dans le registre du titulaire qui leur est associé.

Après le provisionnement automatique de l'agent dans le Cloud Synappx Go, dont les certifications X.509, les communications entre l'agent et le Cloud sont effectuées via des connexions MQTT sécurisées. Des certificats Sharp Synappx Go X.509 signés par le certificat racine sont utilisés. Les certificats signés par un certificat racine fournissent un niveau d'attestation supplémentaire qui certifie que le titulaire du certificat est bien celui qu'il prétend être. L'utilisation de certificats x.509 offre la plus grande sécurité dans l'authentification des périphériques, car la clé privée de chaque périphérique Agent ne quitte jamais celui-ci et ne saurait être compromise. Le certificat de signature du CA racine du titulaire de l'agent Synappx Go est généré par le service de provisionnement du titulaire de Synappx Go et stocké dans l'Azure Key Vault.

- Parmi les avantages des certificats MQTT et X.509, les Agents sont autorisés à s'abonner uniquement à leur propre domaine d'ID d'appareil unique ; cela signifie que les Agents Synappx Go reçoivent des messages publiés UNIQUEMENT sur leur ID d'appareil respectif. L'agent ne peut pas recevoir de contenu à partir d'un autre terminal.

8.3 Obligations de l'Agent MFP

L'agent Synappx Go est conçu avec les exigences suivantes par le Cloud Azure :

- Avant qu'un appareil puisse se connecter au Cloud d'Azure, l'appareil DOIT être enregistré
- Avant qu'un appareil puisse être enregistré, il DOIT être provisionné (par un client Admin)
- Avant qu'un dispositif puisse être provisionné, il DOIT disposer de certificats de sécurité (via le système)

8.4 Découverte des dispositifs de l'Agent du MFP

Pour automatiser la collecte des informations du MFP (nécessaire pour configurer les services du MFP de Synappx Go), l'agent du MFP inclut la possibilité de trouver les MFP en utilisant le SNMP discovery. Discovery est automatiquement lancé après l'installation initiale de l'agent. L'administrateur saisit la série d'IP de début et de fin via le portail d'administration pour effectuer des recherches et peut également effectuer des recherches à la demande (également initiées par l'administration via la console d'administration) en utilisant le port 443. Les informations suivantes sur le MFP sont collectées dans le cadre de ce processus et envoyées dans le Cloud de Synappx Go :

- L'ID de l'Agent du MFP, l'ID du MFP que crée le système (par exemple, Sharp MX-C301W 63004882), fabricant, nom du modèle, numéro de série, nom de l'appareil (si défini), emplacement (si défini), adresse IP du réseau

8.5 Impression et numérisation de documents de l'Agent MFP

Un administrateur ou un utilisateur peut configurer un pilote d'imprimante Sharp pour qu'il soit dirigé vers le PC ou l'Agent du serveur Synappx Go Agent/Impression de documents. Lors de l'envoi de travaux au pilote d'impression, le fichier d'impression des utilisateurs de Synappx Go sous licence est automatiquement stocké dans un dossier pour chaque utilisateur sur le PC/serveur de l'agent pour être débloqué par l'utilisateur sur n'importe quelle MFP configurée avec un tag Synappx.

- Les fichiers d'impression (format.prn) sauvegardés sur le serveur seront automatiquement supprimés après 24 heures.
- Les fichiers prn. ne sont visibles que par les administrateurs autorisés ayant accès à l'ordinateur via la protection normale par mot de passe du PC/serveur.

Les impacts sur le réseau des clients sont liés à l'utilisation de Synappx Go pour la numérisation et l'impression. Les impacts estimés incluent :

- La numérisation vers des destinations favorites (par utilisateur) - estimée à 1 Mo par numérisation en moyenne (peut varier)
- L'impression sécurisée (par utilisateur et par travail d'impression) - estimée à 1,2 Mo en moyenne par travail d'impression (peut varier)
- L'impression de fichiers dans le Cloud (par utilisateur et par travail d'impression) est estimée à 1,2 Mo en moyenne par travail d'impression (peut varier)

9. Agent d'affichage Synappx Go

L'agent d'affichage Synappx Go est un composant sur site du système Synappx Go installé sur un PC ou un serveur d'affichage du client pour faciliter les communications entre les PC compatibles Synappx Go et le Cloud de Synappx Go - permettant le partage des smartphones et des appareils compatibles NFC sur les écrans Sharp. Synappx Go permet à l'utilisateur de se connecter une seule fois à tous ses sites de conservation de données en ligne préférés et de trouver le(s) fichier(s) à partager et/ou à modifier (pour la plupart des sites de conservation de données en ligne) sur les écrans Sharp, tout cela à partir de son appareil mobile privé et en appuyant simplement sur le bouton NFC pour télécharger les fichiers. Les utilisateurs gagnent du temps qui peut être mieux utilisé pour la collaboration autour du contenu du fichier, tout en réduisant le risque que les autres participants à la réunion voient des noms de fichiers sensibles se trouvant également dans leurs dossiers dans le Cloud. Enfin, plusieurs utilisateurs peuvent télécharger et modifier des fichiers (dans la plupart des cas) sur le même PC d'affichage pour une édition collaborative ou pour comparer le contenu des fichiers.

9.1 Installation de l'Agent d'affichage

Pour permettre les cas d'utilisation de partage d'écran, l'agent d'affichage Synappx doit être installé sur le PC ou le serveur d'affichage Windows. Une des fonctions essentielles de l'agent est d'établir un canal de communication sécurisé vers le Cloud de Synappx.

- L'agent s'interface avec le Cloud pour enregistrer et sécuriser les communications des appareils et envoyer/recevoir des messages à destination et en provenance de l'agent. Chaque Agent possède un identifiant unique, et c'est ce que le système Synappx Go Cloud utilise pour identifier les agents à qui envoyer des messages.
- Les Agents écoutent les messages en s'abonnant à leur sujet d'identification unique et les services dans le Cloud envoient les messages en publiant dans ce sujet d'identification.

Pour installer l'agent de l'affichage, le package d'installation personnalisé est téléchargé depuis le portail d'administration de Synappx Go avec un fichier de configuration unique pour le client. Ce pack d'installation de l'agent de l'affichage n'est pas disponible sur un site web public et est lié au compte spécifique du client. Après l'installation, pour s'enregistrer, l'agent de l'affichage soumet son identifiant unique, ainsi que les références de sécurité de l'agent au Cloud de Synappx Go pour l'enregistrement dans le registre des équipements périphériques. Les informations stockées dans le registre des dispositifs comprennent des données telles que le nom du PC/serveur, l'ID unique du PC/serveur et l'ID du titulaire.

9.2 Communication de l'Agent d'affichage

Toutes les communications entre l'agent d'affichage Synappx Go et le Cloud de Synappx Go utilisent soit le HTTPS (port 443), soit la sécurité client X.509 sur MQTT. Le HTTPS est utilisé lors des communications initiales d'installation entre l'agent d'affichage Synappx Go et le Cloud Synappx Go, ainsi que pour envoyer toute information relative à des erreurs.

- Voir le X509 et d'autres détails sur les communications dans la section consacrée aux Agents du MFP ci-dessus. L'agent d'affichage possède les mêmes caractéristiques de sécurité que l'agent du MFP qui y est décrit.

9.3 Partage du contenu de l'Agent d'affichage

Pour l'agent d'affichage, les fonctionnalités de sécurité supplémentaires suivantes sont implémentées pour le partage d'écran :

- Une fois que l'utilisateur a configuré les dépôts de données à conserver dans le Cloud qu'il souhaite (par exemple SharePoint Online, Dropbox) via son appareil mobile, lorsqu'il accède à la fonction « Partage d'écran », le ou les jetons d'utilisateur sécurisés de l'application mobile Synappx Go sont temporairement partagés avec un cache Synappx Cloud sécurisé. Le cache n'est accessible qu'avec des clés sécurisées. Le jeton d'utilisateur est retiré du cache du Cloud de Synappx de Sharp peu de temps après l'utilisation et le jeton d'utilisateur n'est jamais téléchargé vers les Agents d'affichage.

- Lorsqu'un utilisateur sélectionne un ou plusieurs fichiers sur son site de conservation des données dans le Cloud via l'application Synappx Go pour les télécharger sur le PC d'affichage, le Cloud de Synappx génère une URL de téléchargement incluant un ID de session pour obtenir le ou les fichiers de l'utilisateur sélectionné. Les fichiers sont automatiquement ouverts sur le PC d'affichage de l'Agent pour être visualisés et/ou modifiés (pour la plupart des sites de conservation des données dans le Cloud). Les fichiers sont conservés dans un dossier temporaire dans le PC d'affichage.

    - Les fichiers pouvant être téléchargés via le service Synappx Go pour être visualisés ou modifiés sont limités à ce qui suit :
        - Les textes bruts, les fichiers Microsoft Office (Word, PowerPoint, Excel, OneNote), PDF, les fichiers images (JPEG, TIFF, GIF, BMP, PNG) et les fichiers vidéo (MP4, AVI, WMV, MOV)
        - Remarque : Les fichiers exécutables ou de script ne sont pas pris en charge et ne peuvent pas être téléchargés via ce service.

    - Les fichiers pouvant être téléchargés via le service Synappx Go pour être uniquement visualisés sont limités à ce qui suit :
        - Pour la conservation des fichiers iOS, iCloud et locaux : même liste de fichiers que ci-dessus
        - Pour les fichiers Google Workspace conservés dans Google Drive : Google Docs, Google Slides, Google Sheets, Google Drawing, Google Jamboard
        - Remarque : Les fichiers exécutables ou de script ne sont pas pris en charge et ne peuvent pas être téléchargés via ce service.

    - Si l'utilisateur choisit d'enregistrer un fichier modifiable après avoir effectué des modifications sur le PC d'affichage, il sera réenregistré dans le même dossier dans le Cloud à partir duquel il a été téléchargé, soit sous la forme d'une nouvelle version, soit avec un nom de fichier annexé (sous réserve de la politique de chaque site de conservation des données dans le Cloud).

    - Si un utilisateur enregistre un fichier modifiable pris en charge dans le Cloud ou ferme un fichier sans l'enregistrer, celui-ci sera supprimé du dossier temporaire du PC de l'affichage.

    - Plusieurs utilisateurs disposant de licences/applications Synappx Go peuvent chacun télécharger des fichiers dans le Cloud vers le même Agent d'affichage pour visualiser, copier et coller du contenu modifiable, en comparant les fichiers avant de les enregistrer à nouveau sur leurs sites respectifs dans le Cloud.

10. Sécurité de l'entreprise

Sharp maintient un programme de sécurité des informations solide afin de protéger la confidentialité, l'intégrité et la disponibilité de toutes les informations traitées et/ou conservées dans les systèmes d'entreprise de Sharp. La direction de Sharp est consciente de l'évolution rapide et de la croissance des risques associés à la protection des actifs d'information de Sharp et de nos précieux partenaires commerciaux. Elle recherche, examine et investit régulièrement dans des contre-mesures procédurales et techniques afin de fournir une assurance et une sécurité. Une équipe de professionnels dévoués évalue en permanence l'environnement des entreprises en utilisant leur expertise professionnelle pour améliorer et renforcer en permanence la posture de Sharp en matière de sécurité de l'information. En plus de ces efforts internes, Sharp utilise des partenariats stratégiques avec les principaux prestataires de services de l'industrie pour tester, contrôler et auditer les programmes de sécurité des informations que nous avons implémentés.

11. Accès aux données par l'administrateur Sharp

Le service informatique ou le support de Sharp peut occasionnellement être amené à accéder à vos données afin de vous fournir une assistance sur des questions techniques. Les autorisations d'accès pour ces types de questions seront limitées à l'autorisation minimale nécessaire pour résoudre votre problème. Les administrateurs de Sharp se voient accorder des autorisations soigneusement définies en fonction de leur rôle afin de préserver la sécurité des données pour le client :

- Aptitude à consulter et à mettre à jour les informations relatives aux comptes des clients, telles que le statut du compte et l'adresse électronique, mais pas les fichiers des clients
- Aptitude à visualiser l'arborescence et les noms de fichiers, sans pour autant visualiser ou télécharger les fichiers eux-mêmes
- Les utilisateurs, les administrateurs et les administrateurs des distributeurs de Synappx ont tous un accès adapté aux éléments qui relèvent de leur compétence et rien d'autre. L'administration du système est strictement contrôlée et limitée au personnel autorisé de Sharp. Les administrateurs de Sharp ne peuvent accéder qu'aux informations essentielles au fonctionnement du système. Les utilisateurs du système ne sont à aucun moment autorisés à accéder directement à la base de données ou à d'autres composants du système.
- Remarque : Les données relatives à vos services Synappx seront supprimées 45 jours après la date de résiliation de l'abonnement

12. Politique de confidentialité de Sharp

Veuillez consulter les conditions d'utilisation du service Synappx et la politique de confidentialité sur les sites :

- www.sharp.fr/synappx/privacy
- www.sharp.fr/synappx/terms

13. Synthèse

Le passage à des services de collaboration et de réunion itinérants basés sur le Cloud offre aux entreprises un moyen économique de soutenir des effectifs de plus en plus mobiles. En effet, pour créer des environnements de travail collaboratifs et réactifs, l'adoption de la technologie mobile et du Cloud n'est pas une question de « si » mais de « quand ».

Les organisations qui adoptent des services basés sur le Cloud utilisent pleinement leurs investissements technologiques existants, notamment les ordinateurs, les appareils mobiles, les systèmes d'affichage interactifs et les MFP. Associée aux services par abonnement de Synappx, la suppression des dépenses d'investissement pour les ressources informatiques internes se traduit par un coût total d'exploitation encore plus faible. Pourtant, certains décideurs ont du mal à comprendre ce que l'implémentation du Cloud implique, en termes d'équilibre entre la fonctionnalité, l'accessibilité et la sécurité. Les services de Sharp Synappx contribuent à éliminer ces obstacles grâce à une architecture axée sur la sécurité et à une synergie matériel/logiciel qui permet de créer des groupes de travail agiles, en mesure de répondre rapidement aux demandes des entreprises.

www.sharp.fr

SHARP
Be Original.