Whitepaper over de beveiliging

Synappx™ Go en Synappx™ Meeting

www.sharp.nl

SHARP
Be Original.

Inhoud

1. Inleiding

Overzicht

Synappx Go en Synappx Meetings zijn samenwerking, productiviteit en analytische toepassingen en diensten. Een robuust, gelaagd veiligheidssysteem beschermt de programma's om ervoor te zorgen dat er in het systeem en zijn componenten geen kwetsbaarheden ontstaan voor uw gegevens of netwerken. Door een combinatie van technologieleveranciers van wereldklasse, waaronder Microsoft Azure, Google Workspace en best practices op het gebied van beveiliging, houdt u met de Synappx-services uw informatie veilig en beveiligd. Op hetzelfde moment verbeteren de programma's de productiviteit op kantoor. De veiligheidsvoorschriften met betrekking tot Synappx zijn beschreven in deze whitepaper.

Synappx Go

Synappx Go is een mobiel-georiënteerde service die gebruik maakt van Near Field Communication (NFC) om handig en tijdbesparend te kunnen scannen naar favoriete bestemmingen, om cloudbestanden vrij te geven om te printen of om bestanden te printen op Sharp multifunctionele printers (MFP's) in uw kantoor. U kunt uw mobiele telefoon en app ook gebruiken om cloudcontent te selecteren en te downloaden naar het Sharp-display door op een NFC-tag te tikken. De Synappx Go-cloudsoftware en -diensten maken gebruik van de Microsoft Azure database, apparaatinrichting, IoT-Hub en vele andere diensten.

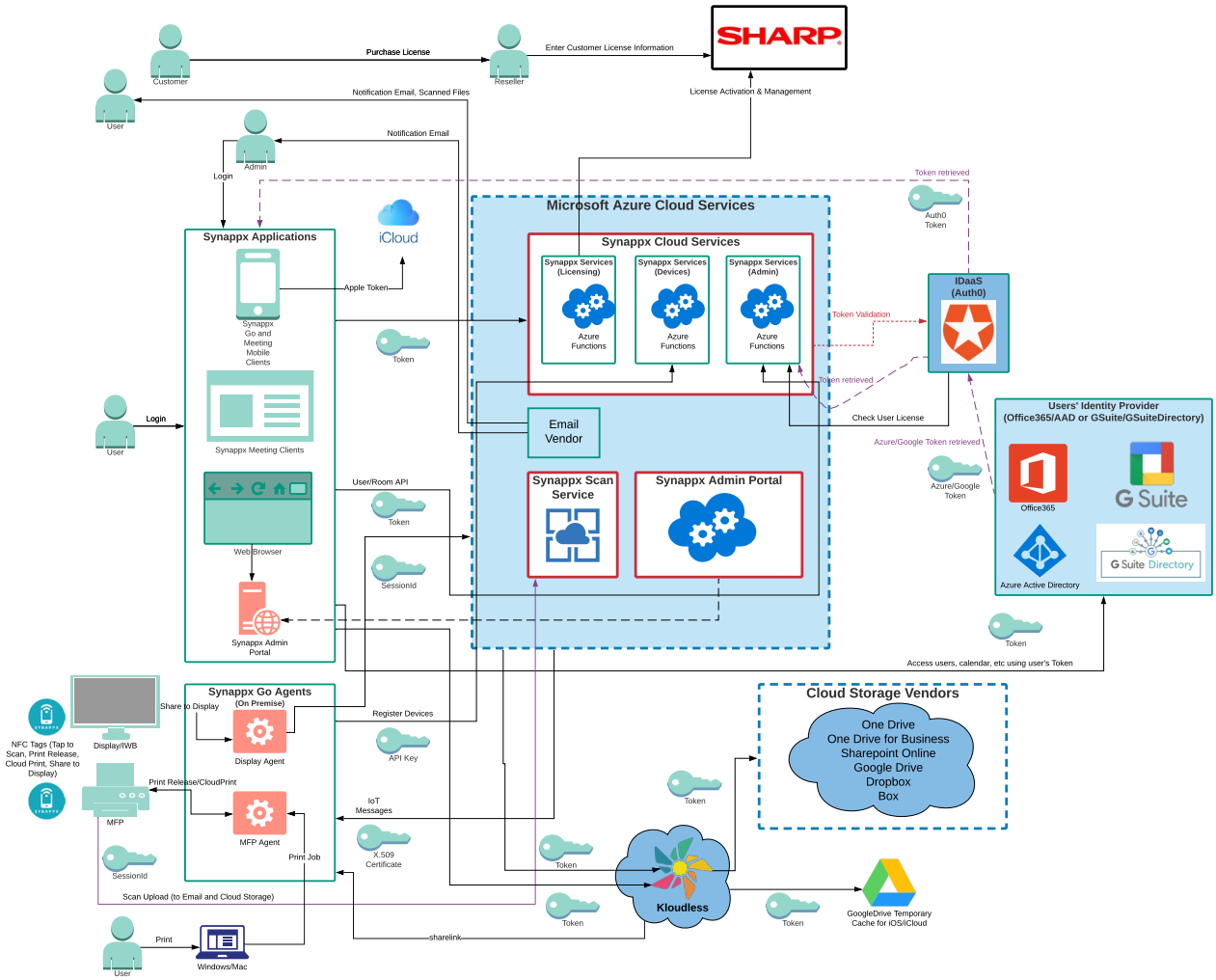
Synappx Meeting

Synappx Meeting maakt gebruik van de Azure-cloud, rich clients, mobiele technologieën en spraakbediening* om gebruikers te helpen op tijd te starten met vergaderingen en efficiënter te zijn. Met één druk op de knop worden de belangrijkste vergaderingsonderdelen verbonden. Uw PC wordt automatisch weergegeven op het Sharp-display in de vergaderruimte, de online vergadering start automatisch en u hebt toegang tot vergadermateriaal. U kunt spraakopdrachten* gebruiken om tijd te besparen voor veelvoorkomende vergaderacties. Synappx Meeting maakt gebruik van Microsoft Azure-database, -opslag, Azure-functies en meer.

* Spraakbediening is momenteel niet beschikbaar in Europa.

2. Overzicht van de architectuur

Onderstaand volgt een overzicht van het Synappx-platform (draaiend op Microsoft Azure) inclusief de servicecomponenten en -architectuur van Synappx Go en Synappx Meeting:



3. Synappx Cloud Services

Synappx Meeting en Synappx Go maken gebruik van de cloudplatformdiensten van Microsoft Azure als basis voor de Synappx Cloud-diensten. Microsoft Azure is een gerenommeerde, wereldwijde cloudservice met een breed scala aan functies die Sharp gebruikt in zijn Synappx-productfamilie. Sharp Synappx gebruikt onder andere de Azure Cosmos-database, opslag, verschillende IoT-services, Key Vault, Security Centre-monitoring, back-up en nog veel meer.

Beveiligde Microsoft-datacenters in Europa hosten de Synappx-oplossingen. Microsoft Azure's cloud- en datacenters worden beschermd door de beveiligingspraktijken van Microsoft. Elk datacenter zorgt voor lokale dataredundantie. Daarnaast is alle communicatie tussen de Sharp Synappx-applicaties en de Synappx Cloud Services (gehost op Microsoft Azure) versleuteld via HTTPS (TLS v1.2, AES256), beveiligd met X.509-certificaten of MQTT (gebruikt door de MFP en de display-agent).

Voor toegang tot alle Synappx Cloud Services vanuit clienttoepassingen zijn veilige sleutels, certificaten of authenticatietokens nodig. Na de aankoop van een Synappx-service krijgt elke klant een uniek certificaat voor communicatie dat wordt opgeslagen in Microsoft Key Vault om veilige, alleen voor de klant toegankelijke toegang mogelijk te maken. Toegang tot de Synappx Azure-database is beperkt tot toegestane IP-adressen op een whitelist van beveiligde Azure-appservices. Microsoft Key Vault wordt gebruikt voor de opslag van SSL-certificaten, X.509-signeercertificaten, persoonlijke sleutels en andere inhoud die de hoogste mate van beveiliging vereisen. De toegang tot de Microsoft Azure Key Vault is beperkt tot Sharp-servicepersoneel en systeemgebruikers met bijbehorende toegangsrechten.

Klantspecifieke gegevens van Synappx Go en/of Synappx Meeting die zijn opgeslagen in de beveiligde clouddatabases van Azure omvatten het volgende:

Synappx Meeting en Synappx Go

- Voornaam, achternaam en e-mailadres van de gebruiker (door de beheerder uit Azure AD of Google Workspace geïmporteerd naar Synappx)
- Voornaam, achternaam en e-mailadres van de beheerder (door de beheerder uitAzure AD of Google Workspace geïmporteerd naar Synappx)
- Namen van werkruimtes (vergaderruimte), e-mailadressen en locaties die de beheerder uit Microsoft Outlook of Google Workspace Directory naar Synappx heeft geïmporteerd
- Handmatig toegevoegde namen en locaties van werkruimtes
- Bedrijfsdomein-aliassen van Azure AD en Google Workspace
- Applicatiegebruiksgegevens voor het genereren van rapporten voor gebruik door de beheerder
- Synappx-licentiegegevens (bijv. vervaldatum)
- Systeemlogboeken

Specifiek voor Synappx Meeting:

- IP-adres en poort van het display (indien geconfigureerd door de beheerder)
- Optioneel account-ID en wachtwoord van het display (indien geconfigureerd door de beheerder)
- Type castingzender, IP-adres en PIN-code (indien geconfigureerd door de beheerder)
- Naam van de vergadering, daadwerkelijke duur van de vergadering (begin- en eindtijd), naam van de vergaderlocatie, naam van de deelnemer en e-mailadres van de deelnemer

Specifiek voor Synappx Go:

- MFP-informatie (modelnaam, IP-adres, serienummer) ontdekt via een door de beheerder geïnitieerde SNMP-scan
- MFP-agentinformatie (computernaam, computer-ID, versienummer, updatebeleid, datum laatst bijgewerkt)
- Display-agentinformatie (computernaam, computer-ID, versienummer, updatebeleid, datum laatst bijgewerkt)
- NFC-taginformatie (tag-ID, type) gekoppeld aan door de beheerder geconfigureerde apparaten

Gegevens in Synappx-databases zijn uitsluitend toegankelijk voor klanten met een licentie via de Synappx-applicaties en beperkt Sharp-personeel indien dit nodig is voor ondersteuningsdoeleinden.

Over het algemeen beperken Sharp-beheerders van de Synappx Cloud Services de toegang tot het systeem tot een minimum aantal personeelsleden voor implementatie- en ondersteuningsdoeleinden. Raadpleeg de sectie over Sharp's beveiligingsbeleid voor meer details.

Klik voor meer informatie over Microsoft Azure-beveiliging op de volgende koppelingen met betrekking tot functies die de Synappx-services gebruiken:

- Overzicht: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Gegevensversleuteling door Rest: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Azure-netwerkbeveiliging: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Azure-functies en serverloze platformbeveiliging: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Gids over beveiliging van Azure-opslag: https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Beveiligingsmanagement in Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Azure-governance: https://docs.microsoft.com/en-us/azure/governance/

4. Synappx Admin Portal

Beheerders (admins) van Synappx Meeting en Synappx Go configureren en beheren het Synappx-systeem via het Synappx Admin Portal. Via deze beveiligde webpagina's voegen zij werkruimtes/vergaderruimtes, gebruikers, apparaten, extra beheerders en meer toe. Licentiebeheer gebeurt via het Admin Portal en de licentiestatus kan hier bekeken worden. Rapporten helpen om het gebruik van het Synappx-systeem en de bedrijfswaarde inzichtelijk te maken. Downloads (voor Synappx Go) zijn via deze pagina's gemakkelijk toegankelijk. Ook systeemlogboeken kunnen gedownload worden.

4.1 Rolgebaseerde toegang en inloggen (voor het Admin Portal en voor klanten)

De toegang tot het Synappx Admin Portal wordt gecontroleerd met behulp van authenticatieprocessen voor huurders (tenants) en rollen voor gebruikers. De gebruikers worden per huurder (tenant) ingesteld en zijn gekoppeld aan een specifiek klantaccount. in overeenstemming met hun gebruikersrollen en -rechten. Als onderdeel van het bestelproces wordt er een eerste beheerder aangewezen. Er kunnen extra beheerders toegevoegd worden nadat de eerste beheerder succesvol is ingelogd op het Synappx Portal.

Alleen door de klant aangewezen of toegewezen beheerders kunnen via het beveiligde webportaal toegang krijgen tot Synappx-gebruikers en -werkruimtes, deze in licentie geven, beheren, rapporten bekijken, etc. voor hun account. Alle communicatie met het Admin Portal verloopt via HTTPS/SSL (TLS1.2) poort 443 ter bescherming van de gegevens bij het verzenden.

Synappx Meeting en Synappx Go maken gebruik van de Microsoft 365- of Google Workspace-inloggegevens van beheerders en gebruikers om te voorkomen dat zij afzonderlijke Synappx-inloggegevens moeten instellen, beheren en beschermen. Door het ontwerp hebben de Synappx-services geen toegang tot Microsoft 365- of Google Workspace-wachtwoorden van klanten. Het systeem maakt gebruik van Azure Active Directory of Google Workspace Directory en vertrouwt op authenticatietokens om beheerders en gebruikers te identificeren (voor client-toegang). De gebruikersidentiteit wordt bevestigd met uw Microsoft Azure AD (voor Microsoft 365-accounts) of Google Workspace Directory (voor Google Workspace-accounts) via een beveiligde identiteitspartner Auth0 (zie hieronder). Gebruikerswachtwoorden worden nooit opgeslagen in de Synappx- of Auth0-systemen. Het Synappx-platform slaat alleen het e-mailadres en de voor-/achternaam van de gebruiker veilig op. Er is geen andere identificeerbare persoonlijke informatie over de gebruiker bekend en het Synappx-systeem slaat dit ook niet op.

4.2 Auth0 (Identity Service Provider)

Voor Synappx-services werkt Sharp samen met Auth0 (https://auth0.com/) voor veilige identiteitsdiensten naar Microsoft Azure AD en Google Workspace. Auth0 bedient naar eigen zeggen 21 miljoen gebruikers in 120.000 applicaties, met 2,5 miljard aanmeldingen per maand. Het is een uiterst gerenommeerde identiteitsdienstverlener.

Een overzicht van het proces:

1. De beheerder of gebruiker voert de Microsoft 365- of Google Workspace-inloggegevens in via een dialoogvenster bij het inloggen op het Synappx Admin Portal of een Synappx-client.

2. Auth0 delegeert de authenticatie van de gebruikersnaam en het wachtwoord die via SSL/TLS 1.2 (poort 443) doorgegeven wordt aan Azure AD of Google Workspace. Azure AD of Google Workspace valideert vervolgens op zijn beurt de gebruikersnaam en het wachtwoord.

3. Auth0 kent het gebruikerswachtwoord niet en slaat dit ook niet op.

4. In samenwerking met Azure AD of Google Workspace wordt een veilig JSON Web Token (JWT) teruggegeven aan de browser (voor toegang tot Synappx Admin Portal), mobiele apparaten (voor Synappx Go en Synappx Meeting) en/of aan Windows/Mac clients (voor Synappx Meeting).

5. Met dit token voert de applicatie functies uit zonder dat de gebruiker zich bij elk gebruik van de applicaties hoeft aan te melden (behalve als de gegevens gewijzigd worden, bijvoorbeeld wanneer het wachtwoord opnieuw ingevoerd moet worden, wanneer de gebruiker niet meer geldig is, wanneer de gebruiker uitlogt uit bij de mobiele app of wanneer er 30 dagen geen activiteit is). Niemand kan met het JWT-token knoeien zonder de bijbehorende geheime sleutel die voor de ondertekening wordt gebruikt. Deze is veilig in de cloud opgeslagen.

De authenticatiebescherming heeft meerdere lagen. Het mobiele apparaat of de computer van de gebruiker is beveiligd met een wachtwoord of een biometrische inlogmethode (bijv. vingerafdruk of gezicht). Gebruikerswachtwoorden zijn niet bekend/worden niet opgeslagen op de Synappx-apparaten. De beveiligde tokens die Auth0 levert, zijn gebaseerd op beveiligde tokens en validatie van Microsoft Azure of Google Workspace.

Auth0 heeft talrijke certificeringen voor cloudbeveiliging, waaronder: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, EU-US Privacy Shield Framework, Gold CSA STAR, AVG en meer. Bekijk de volgende Auth0-whitepapers voor meer informatie over de Auth0-veiligheidsvoorschriften:

- https://auth0.com/security/

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

4.3 Het toekennen van privileges binnen de Synappx-app

Om de functies Synappx Meeting en Synappx Go in te schakelen, moet de beheerder de gebruikers van de Synappx-applicatie geselecteerde rechten toekennen. De eerste beheerder die zich aanmeldt op het systeem moet Azure AD-of Google Workspace-beheerdersrechten hebben en namens de organisatie gebruikers toestemming verlenen bij toegang tot de Synappx- applicaties/-services.

Voor Microsoft 365-klanten zijn de toestemmingen en redenen:

Aangevraagde toestemmingen	Definitie	Admin Portal	Synappx Meeting	Synappx Go
Grafiek Azure Active Directory:				
User.Read	Hiermee kunnen gebruikers inloggen bij de app en kan de app het profiel van de ingelogde gebruikers lezen. Het stelt de app ook in staat om basis bedrijfsinformatie van ingelogde gebruikers te lezen.	Ja	Ja	Ja
Directory.Read.All	Hiermee kan de app domeinextensies van Azure AD verzamelen (nodig voor ondersteuning van meerdere domeinen) en kan de app gegevens in Azure AD lezen, zoals gebruikers, groepen en apps.	Ja	Nee	Nee
Microsoft Graph:				
Calendars.ReadWrite. Shared	Hiermee kan de app gebeurtenissen aanmaken, lezen, bijwerken en verwijderen in alle agenda's waar de gebruiker toegang toe heeft. Dit omvat gedelegeerde en gedeelde kalenders.	Nee	Ja	Nee
Files.ReadWrite.All	Hiermee kan de app alle bestanden waar de ingelogde gebruiker toegang tot heeft, lezen, aanmaken, bijwerken en verwijderen.	Nee	Ja	Nee
Group.Read.All	Hiermee kan de app een lijst van groepen maken en hun eigenschappen en alle groepslidmaatschappen namens de ingelogde gebruiker lezen. Ook kan de app de agenda, gesprekken, bestanden en andere groepscontent lezen voor alle groepen waartoe de ingelogde gebruiker toegang heeft.	Ja	Nee	Nee
User.Read.All	Hiermee kan de app de volledige set van profieleigenschappen, rapporten en managers van andere gebruikers in uw organisatie lezen, namens de ingelogde gebruiker.	Ja	Ja	Nee
offline_access	Hiermee kan de app de gebruikersgegevens lezen en bijwerken, zelfs als zij de app op dat moment niet gebruiken.	Ja	Ja	Ja
email	Hiermee kan de app het primaire e-mailadres van uw gebruikers lezen.	Ja	Ja	Ja
openid	Hiermee kunnen gebruikers inloggen bij de app met hun werk- of schoolaccounts en kan de app basisinformatie over het gebruikersprofiel zien.	Ja	Ja	Ja
profile	Vereist voor het verkrijgen van informatie over het gebruikersprofiel (bijv. voor- en achternaam van de gebruiker, e-mailadres) van Azure AD.	Ja	Ja	Ja

Onderstaande is een lijst van de benodigde API-scopes met de bijbehorende redenen voor Google Workspace-klanten:

Vereiste Google API-scopes	Definitie	Admin Portal	Synappx Meeting	Synappx Go
https://www.googleapis.com/auth/admin.directory.domain.readonly	Hiermee kan de app domeininformatie lezen ter ondersteuning van de multi-domeinfunctie.	Ja	Nee	Nee
https://www.googleapis.com/auth/admin.directory.group.readonly	Hiermee kan de app groeps-, groepsalias- en ledeninformatie opvragen om groepen toe te voegen via het Admin Portal.	Ja	Nee	Nee
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Hiermee kan de app agenda-informatie ophalen om werkruimtes toe te voegen via het Admin Portal.	Ja	Nee	Nee
https://www.googleapis.com/auth/admin.directory.user.readonly	Hiermee kan de app gebruikers ophalen of aliassen van gebruikers toevoegen via het Admin Portal.	Ja	Nee	Nee
https://www.googleapis.com/auth/calendar.readonly	Hiermee heeft de app alleen-lezen toegang tot de agenda's.	Nee	Ja	Nee
https://www.googleapis.com/auth/calendar.events	Hiermee heeft de app lees-/schrijftoegang tot evenementen in een agenda en kan de app de agenda bijwerken (bijv. de vergadertijd verlengen).	Nee	Ja	Nee
https://www.googleapis.com/auth/drive	Hiermee heeft de app toegang tot de Google Drive-bestanden van de geautoriseerde gebruiker (met uitzondering van de map met toepassingsgegevens) om bestanden in een lijst op te nemen.	Nee	Ja	Nee
https://www.googleapis.com/auth/drive.file	Hiermee heeft de app toegang tot bestanden die door de app zijn aangemaakt of geopend om te downloaden en te uploaden. De bestandsautorisatie wordt verleend per gebruiker en wordt ingetrokken wanneer de gebruiker de autorisatie voor de app intrekt.	Nee	Ja	Nee
https://www.googleapis.com/auth/userinfo.profile	Hiermee kan de app persoonsgegevens gebruiken die de gebruiker openbaar heeft gemaakt om een gebruikersnaam en een avatarafbeelding te krijgen.	Nee	Ja	Ja

4.4 Gebruikers of werkruimtes importeren vanuit Azure AD of Google Workspace

Synappx Go verleent licenties voor de service op gebruikersbasis, terwijl Synappx Meeting licenties verleent op basis van werkruimtes/vergaderruimtes. Beheerders besparen tijd en maken minder typefouten door gebruikers (voor Synappx Go) en werkruimtes (bijv. Rooms) voor beide applicaties rechtstreeks te importeren vanuit Microsoft 365 (Azure AD) of Google Workspace. Het is ook toegestaan om werkruimtes handmatig in te voeren. Alleen gebruikers in de ondersteunde domeinen en in Azure AD of Google Workspace kunnen toegevoegd worden als gelicentieerde Synappx Go-gebruikers. De communicatie met Microsoft Azure en Google Workspace voor het importeren van gebruikers en/of werkruimtes verloopt via HTTPS (poort 443).

4.5 Synappx Go-agent downloaden

De Synappx Go MFP- en display-agents zijn te downloaden via de downloadpagina van het Synappx Admin Portal. De gedownloade agents zijn niet beschikbaar op publieke websites en zijn alleen te downloaden door geautoriseerde Synappx-beheerders. Een gecodeerd configuratiebestand (SHA-256) wordt samen met het *.zip-bestand met huurderspecifieke informatie en klantgegevens samengevoegd om automatische MFP-detectie via SNMP mogelijk te maken (voor de MFP-agent). Zie de sectie Synappx Go-agents voor meer details over de beveiliging van agents.

4.6 Synappx-rapporten

Synappx Meeting en Synappx Go kunnen rapporteren genereren om het gebruik en de waarde van de Synappx-applicaties inzichtelijk te maken voor beheerders. De gegevens waarop de Synappx-rapporten gebaseerd zijn, worden opgeslagen op beveiligde Microsoft-servers. De gegevens worden tot 45 dagen na beëindiging van de service door de klant bewaard (voor voldoende tijd om de licentie eventueel te verlengen). Gebruikersspecifieke informatie in de rapporten is alleen beschikbaar voor beheerders binnen het bedrijf via de pagina "Reports" (Rapporten). Geanonimiseerde, samengevatte gegevens over het gebruik van de applicaties van klanten zijn beschikbaar voor Sharp ten behoeve van ondersteuning en productverbetering in de loop van de tijd. Zie Sharp Bedrijfsbeveiliging, Sharp Toegang tot Beheerdersgegevens en Sharp Privacybeleid voor meer details.

4.7 Synappx-ondersteunde domeinen

Voor Microsoft 365- en Google Workspace-accounts verzamelt Synappx informatie over de domein-aliassen die worden ondersteund in het Azure AD- of Google Workspace-systeem van het account. Voor Microsoft 365-accounts kunnen beheerders op de webpagina "Admin Setting"/"Supported Domains" (Instellingen Beheerder/Ondersteunde domeinen) na het verlenen van de eerste toestemming extra domein-aliassen selecteren buiten het primaire Azure AD-domein waaronder het Synappx-account is aangemaakt. Hierdoor is het mogelijk om gebruikers en werkruimtes te importeren uit geselecteerde domeinen voor gebruik met Synappx-services.

4.8 Synappx-systeemlogboeken

Synappx Go en Synappx Meeting bevatten een systeemlogboek met informatie over systeemgebeurtenissen die voor beheerders van belang kunnen zijn. Dit zijn onder meer voorwaarden die een interventie van de beheerder kunnen vereisen om een probleem te corrigeren of om problemen op te lossen. Beheerders kunnen de systeemlogboeken exporteren als een *.csv-bestand voor verdere analyse. Het Synappx-systeem bewaart de systeemlogboeken gedurende 30 dagen.

5. Windows- en Apple Mac-clients voor Synappx Meeting

Synappx Meeting helpt om verbinding te maken met het display in de vergaderruimte, om online vergaderingen te starten en om applicaties te bedienen met eenvoudige spraakopdrachten*. Er is een breed scala aan veiligheidsfuncties beschikbaar, waaronder:

- Elke Synappx Meeting-toegang tot cloudbronnen vindt plaats via HTTPS (poort 443)
  - Azure (krijgt vergaderruimte-informatie van Synappx Admin)
  - Auth0 (delegeren van de gebruikersauthenticatie naar Azure AD)
  - Azure AD (gebruikersauthenticatie met Microsoft 365-account) of Google Workspace (gebruikersauthenticatie met Google Workspace-account)
  - Microsoft Graph APIs (krijgt vergaderinformatie en vergaderbestanden van Microsoft Office 365) of Google API-scopes (krijgt vergaderinformatie en vergaderbestanden van Google Workspace)
  - Amazon Web Services voor toegang tot de spraakopdrachtens* in de wachtrij

- Toegang tot lokaal display
  - Maakt spraakbediening* van BIG PAD interactieve displaysystemen mogelijk. Protocol is telnet (poort 10008)

- De gebruiker logt de eerste keer dat hij/zij de Synappx-app gebruikt in met de Microsoft 365- of Google Workspace-inloggegevens, wanneer inloggegevens zij gewijzigd (bijv. wachtwoordupdate), wanneer hij/zij uitlogt uit de clientapplicatie en/of na 3 dagen zonder gebruik van de app

- Gebruikerswachtwoorden worden niet opgeslagen op het mobiele apparaat; in plaats daarvan wordt een veilig JWT-token verstrekt na validatie van het gebruikerswachtwoord met het Azure AD- of Google Workspace-systeem via de partner Auth0.
  - Het toegangstoken voor gebruikers wordt opgeslagen op de lokale computer
  - ID/wachtwoord voor proxy's worden opgeslagen in de lokale opslag. (gecodeerd met behulp van AES128)

* Spraakbediening is momenteel niet beschikbaar in Europa.

6. Synappx Go en Synappx Meeting voor mobiele apparaten

Door het alomtegenwoordige gebruik van mobiele apparaten in het bedrijfsleven worden smartphones nu vaak gebruikt voor toegang tot zakelijke content en om deze content te delen. Gebruikers verwachten intuïtieve mobiele diensten die hen helpen hun werk sneller te doen. Met de Synappx Go-app kunnen gebruikers scannen naar frequente bestemmingen, printtaken vrijgeven of ondersteunde cloudbestanden printen via elk voor Synappx Go geconfigureerd apparaat en cloudbestanden delen naar geconfigureerde Sharp-displays. Met de Synappx Meeting-app kunnen gebruikers hun vergadering starten, online vergaderingen starten en snel toegang krijgen tot documenten. Diverse beveiligingsfuncties van de mobiele clients zijn onder andere:

Synappx Meeting en Synappx Go:

- Op het mobiel apparaat moet de gebruiker een wachtwoord invoeren of een biometrische authenticatie (bijv. vingerafdruk, gezichtsherkenning) ondergaan voor toegang tot apps
- De gebruiker logt de eerste keer dat hij/zij de Synappx-app gebruikt in met de Microsoft 365- of Google Workspace-inloggegevens, wanneer inloggegevens zij gewijzigd (bijv. wachtwoordupdate), wanneer hij/zij uitlogt uit de mobiele applicatie en/of na 30 dagen zonder gebruik van de app.
  Voordelen:
  - Auth0 (delegeren van de gebruikersauthenticatie naar Azure AD)
  - Azure AD (gebruikersauthenticatie met Microsoft 365-account) of Google Workspace (gebruikersauthenticatie met Google Workspace-account)
- Gebruikerswachtwoorden worden niet opgeslagen op het mobiele apparaat; in plaats daarvan wordt een veilig JWT-token verstrekt na validatie van het gebruikerswachtwoord met het Azure AD- of Google Workspace-systeem via de partner Auth0.
- Alle toegang tot het systeem is gecodeerd via TLS v1.2 AES256 (poort 443)

Specifiek voor Synappx Go:

- De mobiele toegang van de gebruiker wordt centraal geregeld via het Synappx Admin Portal. Beheerders kunnen een gebruikerslicentie op elk moment verwijderen om het gebruik van de mobiele functies van Synappx Go te blokkeren.
- Gebruikers krijgen het verzoek om toegang te verlenen tot hun contactpersonenlijst om een bestemming aan te maken voor het scannen naar een e-maildistributielijst zonder dat ze de e-mails van de betreffende gebruikers opnieuw hoeven in te voeren. Dit bespaart tijd en verkleint de kans op typefouten.
- Om te scannen naar een cloudopslagmap, geselecteerde cloudbestanden te printen of cloudbestanden te delen op Sharp-displays, kunnen gebruikers ervoor kiezen Synappx Go te configureren voor toegang tot bestanden van ondersteunde cloudopslagsites (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box of Google Drive). Voor de iOS-app zijn iCloud en lokale bestanden al geconfigureerd.
  - Voor opslagsites die interessant zijn, kunnen gebruikers hun gebruikersnaam en wachtwoord invoeren voor de betreffende cloudopslagsites. Na het inloggen wordt er een veilig token verstrekt en opgeslagen in Synappx Go om te voorkomen dat de gebruiker deze gegevens opnieuw moet invoeren, tenzij deze niet meer geldig zijn (bijv. wijziging van het wachtwoord, deactivering van het account, enz.)
  - Sharp en componentenleveranciers hebben geen toegang tot de wachtwoorden van de gebruikers van de cloudopslagsites
  - Voor elke cloudopslagdienst krijgt de gebruiker de vraag om de Synappx-app bepaalde rechten te verlenen voor toegang tot door de gebruiker gekozen bestanden om deze te downloaden en te bewerken. Opmerking: De Synappx Go-service heeft geen functie om bestanden of mappen te verwijderen van een cloudopslagsite.
  - Opmerking: Sharp werkt samen met een derde leverancier, Kloudless (Kloudless.com) om efficiënte Synappx Go-verbindingen met meerdere leveranciers van cloudopslag mogelijk te maken. Kloudless heeft géén toegang tot gebruikerswachtwoorden. Hun beveiligde database bevat wel de e-mailadressen van gebruikers van Synappx Go. Kloudless slaat minimale bestand-/map-metadata op (bijv. bestandsnaam en ID, gewijzigde datum) om het bekijken van recentelijk gewijzigde bestanden op verschillende cloudsites te ondersteunen. Kloudless slaat de inhoud van het gebruikersbestand niet op.

Specifiek voor Synappx Meeting:

- Mobiele apps zijn beschikbaar voor elke gebruiker van de service (geen licentie vereist); de gebruiker moet echter een geldige gebruiker zijn in Azure AD of Google Workspace binnen hetzelfde klantendomein.
- Informatie over Azure-vergaderruimtes is toegankelijk via Synappx Admin
- Microsoft Graph API krijgt vergaderinformatie en vergaderbestanden van Microsoft Office 365. Google API-scopes krijgen informatie en vergaderbestanden voor van Google Workspace.

7. Synappx Go NFC-tags

Synappx Go maakt gebruik van speciale NFC-tags, die worden geleverd door Sharp of geautoriseerde wederverkopers en/of die zijn ingebed in geselecteerde MFP-modellen. De tags bevatten een unieke identificatiecode en zijn Read Only (niet herprogrammeerbaar). Elke tag kan slechts aan één apparaat tegelijk worden gekoppeld. Zodra de beheerder van de Synappx Go-app de tag eenmaal geconfigureerd heeft op een apparaat (bijv. MFP of display-PC), identificeren de tag en de mobiele app bij een tik op de NFC-tag door de gebruiker samen de identiteit van de gebruiker en het apparaat dat aan de tag/het apparaat is gekoppeld, zodat Synappx Go kan scannen naar e-mail, printopdrachten kan vrijgeven, bestanden vanuit de cloud kan printen en delen.

8. Synappx Go MFP-agent

De Synappx Go MFP-agent (inclusief software voor het vrijgeven van printopdrachten) is een on-premise component van het Synappx Go-systeem. De agent is geïnstalleerd op een PC of server van de klant om de communicatie tussen MFP's die Synappx Go ondersteunen en de Synappx Go-cloud te vergemakkelijken om mobiele taken en NFC-taken voor Sharp MFP's mogelijk te maken. Met Synappx Go hoeft u geen training meer te volgen en meerdere stappen te doorlopen op het MFP-bedieningspaneel om veilig printopdrachten vrij te geven vanaf elke MFP die Synappx Go ondersteunt, om geselecteerde bestanden uit de cloud te printen en bestanden te verzenden naar uw favoriete scanbestemmingen. Gebruikers besparen tijd met het scannen en beveiligd printen, waardoor ook het risico op onbevoegde toegang tot de printopdrachten van de gebruiker wordt beperkt.

De Synappx Go MFP-agent is nodig voor de ondersteuning van scan- en printopdrachten. Eén van de kernfuncties van de agent is het opzetten van een veilig communicatiekanaal naar de Synappx-cloud. De agent heeft een interface met de cloud om de communicatie met het apparaat te registreren en te beveiligen, en om berichten van en naar de agent en ondersteunde MFP's te verzenden/ontvangen. Elke agent heeft een unieke identificatie. Het Synappx Go-cloudsysteem gebruikt deze identificatie om vast te stellen naar welke agents berichten gestuurd moeten worden. Agents detecteren berichten door zich te abonneren op hun unieke identifier topic. De clouddiensten sturen een bericht door naar het betreffende identifier topic te publiceren.

8.1 De MFP-agent installeren

Om de MFP-agent te installeren, downloadt u het aangepaste installatiepakket van het Synappx Go Admin Portal met een configuratiebestand dat uniek is voor de klant. De inhoud van het configuratiebestand is beveiligd door middel van encryptie-algoritmen. Dit installatiepakket voor de MFP-agent is niet beschikbaar op een publieke website en is gekoppeld aan de specifieke klantaccount. Bij de meeste klanteninstallaties wordt er één MFP-agent per klantlocatie geïnstalleerd ter ondersteuning van maximaal 50 tot 100 MFP's (afhankelijk van het aantal gebruikers en printopdrachten) die gebruik kunnen maken van de print- en scanmogelijkheden van Synappx Go. Klanten die meer dan 100 MFP's willen ondersteunen, dienen extra MFP-agents te installeren.

Na de installatie dient de MFP-agent zijn unieke identificatiecode in - samen met de veiligheidsgegevens van de agent - bij de Synappx Go Cloud voor registratie in het apparaatregister. De informatie in het apparaatregister omvat gegevens zoals apparaat-ID, locatie, huurders-ID en voor MFP's, de MFP-agent die aan de MFP is gekoppeld.

8.2 Communicatie van de MFP-agent

Alle communicatie tussen de Synappx Go MFP-agent en Synappx Go-cloud maakt gebruik van HTTPS (poort 443) of X.509-clientbeveiliging via MQTT. HTTPS wordt gebruikt tijdens de eerste installatiecommunicatie tussen de Synappx Go MFP-agent en de Synappx Go-cloud, plus om MFP-informatie en eventuele foutinformatie te verzenden.

- Persoonlijke sleutels van Agent X.509 verlaten nooit het systeem waarop de agent is geïnstalleerd. Deze sleutels worden dus nooit blootgesteld als gevolg van de overdracht via het internet.
- Alle certificaten van Agent X.509 worden ondertekend met behulp van de handtekeningcertificaten van de klant van de Agent. Agents mogen zich alleen automatisch registreren als het X.509-certificaat is ondertekend, waarbij de bijbehorende klant het certificaat ondertekent.

De Synappx Go-cloudservices houden voor elke Synappx Go-klant een apart certificaat bij. Dit zorgt ervoor dat de agents alleen binnen het bij hen aangesloten huurdersregister worden ingericht.

Nadat de agent automatisch is ingericht op de Synappx Go-cloud inclusief X.509-certificaten, verloopt de communicatie tussen de agent en de cloud via beveiligde MQTT-verbindingen. Er worden Sharp Synappx Go X.509 rootCA-certificaten gebruikt. Door een rootCA ondertekende certificaten geven een extra mate van attestation dat certificeert dat de certificaathouder is wie hij/zij zegt te zijn. Het gebruik van x.509-certificaten biedt de grootste veiligheid bij de authenticatie van apparaten, aangezien de persoonlijke sleutel van elk agent-apparaat het apparaat nooit verlaat en niet kan worden gecompromitteerd. De Synappx Go Tenant Provisioning Service genereert het Synappx Go-agent tenant root CA-handtekeningcertificaat en slaat dit op in de Azure Key Vault.

- Voordelen van MQTT- en X.509-certificaten zijn onder andere dat agents zich alleen mogen abonneren op hun eigen unieke apparaat-ID-topic; dit betekent dat agents van Synappx Go berichten ontvangen die ALLEEN op hun respectievelijke apparaat-ID worden gepubliceerd. De agent kan geen inhoud van een ander eindpunt ontvangen.

8.3 Vereisten van de MFP-agent

De Synappx Go Agent is ontworpen aan de hand van de volgende vereisten van de Azure-cloud:

- Alvorens een apparaat verbinding kan maken met de Azure-cloud, MOET het apparaat geregistreerd worden
- Alvorens een apparaat geregistreerd kan worden, MOET het apparaat ingericht worden (door een beheerder van de klant)
- Alvorens een apparaat ingericht kan worden, MOET het apparaat veiligheidscertificaten hebben (via het systeem)

8.4 Apparaatdetectie MFP-agent

Om het verzamelen van MFP-informatie te automatiseren (nodig om de Synappx Go MFP-services te configureren), heeft de MFP-agent de mogelijkheid om MFP's te detecteren met behulp van een SNMP-scan. De detectie wordt automatisch gestart na de eerste installatie van de agent. De beheerder voert het begin- en eind-IP-bereik in via het Admin Portal om te zoeken. On-demand kan hij/zij ook opnieuw zoeken (ook geïnitieerd door de beheerder via de Admin Console) met behulp van poort 443. De volgende informatie over de MFP wordt verzameld als onderdeel van dit proces. Deze informatie wordt verzonden naar de Synappx Go-cloud:

- MFP-agent-ID, MFP-ID die het systeem maakt (bijv. Sharp MX-C301W 63004882), fabrikant, modelnaam, serienummer, apparaatnaam (indien ingesteld), locatie (indien ingesteld), IP-adres van het netwerk

8.5 Printopdrachten vrijgeven en documenten scannen via de MFP-agent

Een beheerder of gebruiker kan een Sharp-printerstuurprogramma configureren om naar de Synappx Go-agent/PC of server voor het vrijgeven van printtaken te verwijzen. Bij het verzenden van opdrachten naar het stuurprogramma voor het vrijgeven van printtaken wordt het printbestand van gelicentieerde Synappx Go-gebruikers automatisch opgeslagen in een map voor elke gebruiker op de agent-PC/-server. De gebruiker moet deze vrijgeven via elke MFP die geconfigureerd is met een Synappx-tag.

- Printbestanden (*.prn-formaat) die op de server zijn opgeslagen, worden na 24 uur automatisch verwijderd.
- De *.prn-bestanden zijn alleen zichtbaar voor geautoriseerde beheerders die toegang hebben tot de computer via een normale PC-/server-wachtwoordbeveiliging.

De invloed op het klantnetwerk hangt samen met het gebruik van de Synappx Go-functies om te scannen en te printen. De geschatte invloed omvat:

- Scannen naar favoriete bestemmingen (per gebruiker) – geschat op gemiddeld 1 MB per scan (kan variëren)
- Veilig printen (per gebruiker per printtaak) – geschat op gemiddeld 1,2 MB per printtaak (kan variëren)
- Printen van cloudbestanden (per gebruiker per printtaak) – geschat op gemiddeld 1,2 MB per printopdracht (kan variëren)

9.Synappx Go Display-agent

De Synappx Go Display-agent is een on-premise component van het Synappx Go-systeem. De agent is geïnstalleerd op een display-PC of -server van de klant om de communicatie tussen PC's die Synappx Go ondersteunen en de Synappx Go-cloud te vergemakkelijken – om delen op een Sharp-display via een mobiel apparaat of via NFC mogelijk te maken. Met Synappx Go kan de gebruiker eenvoudigweg eenmalig verbindingen opzetten met al zijn favoriete cloudopslagsites. Zo kan hij/zij het bestand of de bestanden op de verschillende sites vinden om het bestand/de bestanden te delen en/of te bewerken (voor de meeste cloudopslagsites) op Sharp-displays – dit alles vanaf zijn/haar eigen mobiele apparaat en met een eenvoudige tik op een NFC-tag om de bestanden te downloaden. Gebruikers besparen kostbare tijd die zij beter kunnen besteden aan het samenwerken aan de bestandsinhoud. Dit beperkt bovendien het risico dat andere deelnemers aan de vergadering gevoelige bestandsnamen zien die ook in hun cloudmappen staan. Meerdere gebruikers kunnen bestanden downloaden en bewerken (in de meeste gevallen) op dezelfde Display-PC om samen te werken of om de inhoud van bestanden te vergelijken.

9.1 De Display-agent installeren

Om de functie "Share to Display" (Delen op een display) mogelijk te maken, moet de Synappx Display-agent op de Windows display-PC of -server geïnstalleerd worden. Eén van de kernfuncties van de agent is het opzetten van een veilig communicatiekanaal naar de Synappx-cloud.

- De agent heeft een interface met de cloud om de communicatie met het apparaat te registreren en te beveiligen, en om berichten van en naar de agent te verzenden/ontvangen Elke agent heeft een unieke identificatie. Het Synappx Go-cloudsysteem gebruikt deze identificatie om vast te stellen naar welke agenten berichten gestuurd moeten worden.
- Agents detecteren berichten door zich te abonneren op hun unieke identifier topic. De clouddiensten sturen berichten door naar het betreffende identifier topic te publiceren.

Om de Display-agent te installeren, downloadt u het aangepaste installatiepakket van het Synappx Go Admin Portal met een configuratiebestand dat uniek is voor de klant. Dit installatiepakket voor de Display-agent is niet beschikbaar op een publieke website en is gekoppeld aan de specifieke klantaccount. Na de installatie dient de Display-agent zijn unieke identificatiecode in - samen met de veiligheidsgegevens van de agent - bij de Synappx Go Cloud voor registratie in het apparaatregister. De informatie in het apparaatregister omvat gegevens zoals de naam van de PC/server, de unieke PC/server-ID en de huurders-ID.

9.2 Communicatie van de Display-agent

Alle communicatie tussen de Synappx Go Display-agent en Synappx Go-cloud maakt gebruik van HTTPS (poort 443) of X.509-clientbeveiliging via MQTT. HTTPS wordt gebruikt tijdens de eerste installatiecommunicatie tussen de Synappx Go Display-agent en de Synappx Go-cloud, plus om eventuele foutinformatie te verzenden.

- Raadpleeg de details van X509 en andere communicatiedetails in het bovenstaande gedeelte van de MFP-agent. De Display-agent heeft dezelfde beveiligingsfuncties als de daar beschreven MFP-agent.

9.3 Het delen van content via een Display-agent

Voor de Display-agent zijn de volgende extra beveiligingsfuncties geïmplementeerd voor de functie "Share to Display" (Delen op een display):

- Zodra de gebruiker de gewenste cloudopslagplaatsen (bijv. SharePoint Online, Dropbox) via zijn mobiele apparaat heeft geconfigureerd, worden de beveiligde gebruikersmarkering(en) in de mobiele app van Synappx Go tijdelijk gedeeld met een beveiligde Synappx Cloud-cache. De cache is uitsluitend toegankelijk met beveiligde sleutels. Het gebruikerstoken wordt korte tijd na gebruik verwijderd uit de Sharp Synappx-cloudcache en het gebruikerstoken wordt nooit gedownload naar de Display-agents.

- Wanneer een gebruiker een bestand/meerdere bestanden van zijn cloudopslagsite selecteert via de Synappx Go-app om te downloaden naar de display-PC, genereert de Synappx-cloud een download-URL inclusief een sessie-ID om het geselecteerde gebruikersbestand/de geselecteerde gebruikersbestanden op te halen. De bestanden worden automatisch geopend op de Display-agent-PC om te bekijken en/of bewerken (voor de meeste cloudopslagsites). De bestanden worden opgeslagen in een tijdelijke map op de display-PC.

    - Bestanden die via de Synappx Go-service gedownload kunnen worden om te worden bekeken of bewerkt, zijn beperkt tot de volgende formaten:
        - Platte tekstbestanden, Microsoft Office-bestanden (Word, PowerPoint, Excel, OneNote), PDF, afbeeldingsbestanden (JPEG, TIFF, GIF, BMP, PNG) & videobestanden (MP4, AVI, WMV, MOV)
        - Opmerking: Uitvoerbare of scriptbestanden worden niet ondersteund en kunnen niet via deze service worden gedownload.

    - Bestanden die via de Synappx Go-service gedownload kunnen worden alleen te bekijken, zijn beperkt de volgende:
        - Voor opslag via iOS, iCloud en lokale bestanden: dezelfde bestandenlijst als hierboven
        - Voor Google Workspace-bestanden opgeslagen op Google Drive: Google Docs, Google Slides, Google Sheets, Google Drawing, Google Jamboard
        - Opmerking: Uitvoerbare of scriptbestanden worden niet ondersteund en kunnen niet via deze service worden gedownload.

    - Als de gebruiker ervoor kiest om een bewerkbaar bestand op te slaan na het aanbrengen van wijzigingen op de display-PC, dan wordt dit bestand op dezelfde locatie in de cloudmap opgeslagen als waarvan het gedownload is. Het bestand wordt als een nieuwe versie en/of met een aangepaste bestandsnaam (met inachtneming van het beleid van elke cloudopslagsite) opgeslagen.

    - Als een gebruiker een ondersteund bewerkbaar bestand opslaat in de cloud of een bestand sluit zonder op te slaan, dan wordt dit verwijderd uit de tijdelijke map op de display-PC.

    - Meerdere gebruikers met Synappx Go-licenties/-apps kunnen elk cloudbestand downloaden naar dezelfde Display-agent om het bestand te bekijken, om bewerkbare inhoud te kopiëren en plakken. Hierbij worden bestanden vergeleken voordat deze opgeslagen worden op de respectievelijke cloudsites.

10. Bedrijfsbeveiliging

Sharp onderhoudt een robuust informatiebeveiligingsprogramma ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van alle informatiemiddelen die in de bedrijfssystemen van Sharp verwerkt en/of opgeslagen worden. Het management van Sharp onderkent de snel evoluerende en groeiende risico's die gepaard gaan met de bescherming van de informatiemiddelen van Sharp en onze gewaardeerde zakenpartners. Sharp onderzoekt, beoordeelt en investeert regelmatig in procedurele en technische tegenmaatregelen om zekerheid en beveiliging te bieden. Een team van toegewijde professionals beoordeelt voortdurend de bedrijfsomgeving met behulp van hun professionele expertise om de informatiebeveiliging van Sharp continu te verbeteren. Naast deze interne inspanningen maakt Sharp gebruik van strategische partnerschappen met toonaangevende dienstverleners binnen de branche om de door ons geïmplementeerde informatie te testen, te monitoren en te controleren Beveiligingsprogramma's.

11. Gegevenstoegang van Sharp-beheerders

Het kan zijn dat Sharp IT of Support af en toe toegang tot uw gegevens nodig heeft om ondersteuning te bieden bij technische problemen. Toegangsrechten voor dit soort zaken worden beperkt tot de minimale rechten die nodig zijn om uw probleem op te lossen. Sharp-beheerders krijgen zorgvuldige, op rollen gebaseerde toestemmingen om de beveiliging van de gegevens voor de klant te waarborgen:

- De mogelijkheid om klantgegevens te bekijken en bij te werken, zoals de accountstatus en het e-mailadres, maar niet de klantenbestanden
- De mogelijkheid om de bestandsstructuur en de bestandsnamen te zien, maar niet om de eigenlijke bestanden te bekijken of te downloaden
- Synappx-gebruikers, -beheerders en beheerders van dealers hebben allemaal passende toegang tot items die onder hun bevoegdheid vallen en niets anders. Het systeembeheer wordt strikt gecontroleerd en is beperkt tot het bevoegde personeel van Sharp. Sharp-beheerders hebben uitsluitend toegang tot informatie die cruciaal is voor de werking van het systeem. Op geen enkel moment hebben gebruikers van het systeem direct toegang tot de database of andere systeemcomponenten.
- Opmerking: Gegevens met betrekking tot uw Synappx-diensten worden 45 dagen na een beëindigingsdatum van het abonnement verwijderd

12. Sharp Privacybeleid

Raadpleeg de Synappx-servicevoorwaarden en het privacybeleid op:

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

13. Samenvatting

De overstap naar cloudgebaseerde, on-the-go samenwerking en vergaderdiensten biedt bedrijven een economische manier om steeds mobielere arbeidskrachten te ondersteunen. Inderdaad: om samenwerkende, responsieve kantooromgevingen op te zetten, is het gebruik van cloud- en mobiele technologie geen geval van "als" maar van "wanneer".

Organisaties die cloudgebaseerde diensten omarmen, maken volledig gebruik van hun bestaande investeringen in technologie, waaronder computers, mobiele apparaten, interactieve displaysystemen en MFP's. In combinatie met de Synappx-services op basis van abonnementen betekent het wegvallen van investeringsuitgaves in interne IT-middelen nóg lagere totale eigendomskosten. Toch worstelen sommige beleidsmakers met wat cloudimplementatie inhoudt, als het gaat om het evenwicht tussen gemak en toegankelijkheid en veiligheid. Sharp Synappx-services helpen deze barrières weg te nemen met een veiligheidsgedreven architectuur en synergie tussen hardware en software die flexibele werkgroepen mogelijk maakt, zodat zij snel kunnen reageren op de eisen van het bedrijfsleven.

www.sharp.nl

SHARP

Be Original.