Raport na temat bezpieczeństwa

Synappx™ Go oraz Synappx™ Meeting

www.sharp.pl

SHARP
Be Original.

Spis treści

1. Wprowadzenie

Omówienie

Synappx Go i Synappx Meetings to aplikacje i usługi z zakresu współpracy, produktywności i analityki. Są chronione przez solidny, wielopoziomowy system zabezpieczeń, aby zagwarantować, że system i jego elementy nie będą stanowiły słabych punktów bezpieczeństwa Twoich danych lub sieci. Dzięki połączeniu światowej klasy dostawców technologii, w tym Microsoft Azure, Google Workspace i najlepszych praktyk w zakresie bezpieczeństwa, korzystanie z usług Synappx pomaga utrzymać bezpieczeństwo informacji i jednocześnie zwiększyć wydajność pracy w biurze. Zasady bezpieczeństwa związane z usługami Synappx opisane są w tym raporcie.

Synappx Go

Synappx Go to usługa zorientowana na mobilność, wykorzystująca technologię Near Field Communication (NFC), która umożliwia wygodne i oszczędzające czas skanowanie do ulubionych lokalizacji oraz drukowanie plików przechowywanych w chmurze na urządzeniach wielofunkcyjnych firmy Sharp w całym biurze. Za pomocą telefonu komórkowego i aplikacji można również wybierać i pobierać pliki z chmury, które mają zostać wyświetlone na ekranie urządzenia Sharp, dzięki zbliżeniu taga NFC. Oprogramowanie i usługi Synappx Go w chmurze wykorzystują bazę danych Microsoft Azure, udostępnianie urządzeń, sieć czujników IoT i wiele innych usług.

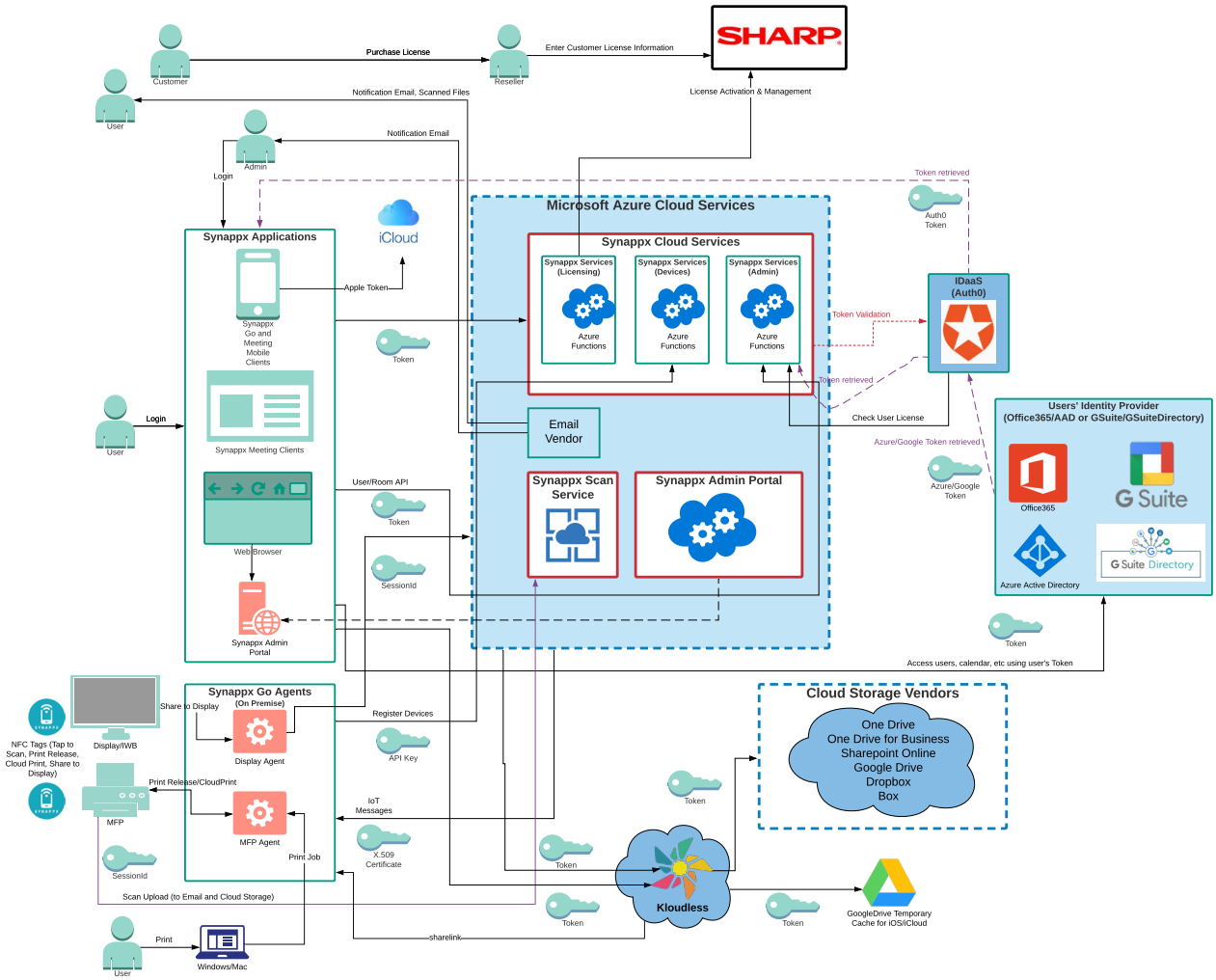
Synappx Meeting

Synappx Meeting wykorzystuje chmurę Azure, rozbudowane aplikacje klienckie, technologie mobilne i głosowe*, aby pomóc użytkownikom rozpocząć spotkania na czas i być bardziej efektywnym Jedno kliknięcie pozwala na połączenie kluczowych elementów spotkania. Ekran twojego komputera jest automatycznie klonowany na monitor konferencyjny firmy Sharp, spotkania on-line rozpoczynają się automatycznie, a Ty masz dostęp do materiałów na spotkania. Polecenia głosowe* mogą być wykorzystywane aby zaoszczędzić czas na typowych czynności podczas spotkań. Synappx Meeting korzysta z bazy danych Microsoft Azure, pamięci masowej, funkcji Azure i innych.

* Sterowanie głosowe obecnie niedostępne w Europie.

2. Omówienie architektury Synappx

Poniżej przedstawiono omówienie platformy Synappx (zasilanej przez Microsoft Azure), w tym komponentów i architektury usług Synappx Go i Synappx Meeting:



3. Usługi Synappx w chmurze

Synappx Meeting i Synappx Go korzystają z usług przetwarzania w chmurze Microsoft Azure jako podstawy dla usług chmurowych Synappx. Microsoft Azure to ciesząca się dużym uznaniem globalna usługa w chmurze o szerokim zakresie funkcji, z której korzysta rodzina produktów Sharp Synappx, w tym: baza danych Azure Cosmos, pamięć masowa, kilka usług IoT, Key Vault, monitorowanie w Security Centre, tworzenie kopii zapasowych i inne.

Rozwiązania Synappx są obsługiwane w bezpiecznych centrach danych Microsoft znajdujących się w Europie. Microsoft Azure Cloud i centra danych są chronione zgodnie z praktykami bezpieczeństwa firmy Microsoft. Każde centrum danych zapewnia lokalną redundancję danych. Ponadto cała komunikacja między aplikacjami Sharp Synappx i usługami Synappx w chmurze (obsługiwanymi przez Microsoft Azure) jest szyfrowana za pomocą protokołu HTTPS (TLS v1.2, AES256) i zabezpieczona certyfikatami X.509 lub MQTT (używanymi przez agenta MFP i agenta monitora).

Dostęp do wszystkich usług w chmurze Synappx z aplikacji klienckich wymaga bezpiecznych kluczy, certyfikatów lub tokenów uwierzytelniających. Po zakupie usługi Synappx każdy klient otrzymuje unikalny certyfikat, który jest przechowywany w Microsoft Key Vault w celu umożliwienia bezpiecznego dostępu wyłącznie dla klientów. Dostęp do bazy danych Synappx Azure jest ograniczony do wymienionych na białej liście adresów IP z bezpiecznych usług Azure App Services. Microsoft Key Vault służy do przechowywania certyfikatów SSL, certyfikatów podpisu X.509, kluczy prywatnych i innej zawartości wymagającej najwyższego poziomu bezpieczeństwa. Dostęp do Microsoft Azure Key Vault jest ograniczony tylko do usługodawców firmy Sharp i użytkowników systemu z odpowiednimi uprawnieniami dostępu.

Indywidualne dane klientów Synappx Go i/lub Synappx Meeting przechowywane w bezpiecznych bazach danych Azure cloud zawierają następujące elementy:

Synappx Meeting oraz Synappx Go

- Imię, nazwisko i adres e-mail użytkownika (importowane z Azure AD albo Google Workspace do Synappx przez administratora)
- Imię, nazwisko i adres e-mail administratora (importowane z Azure AD albo Google Workspace do Synappx przez administratora)
- Nazwy miejsc pracy (sal konferencyjnych), adresy e-mail i lokalizacje zaimportowane z Microsoft Outlook lub Google Workspace Directory do Synappx przez administratora
- Ręcznie dodawane nazwy i lokalizacje przestrzeni roboczej
- Firmowe aliasy domeny z Azure AD i Google Workspace
- Dane dotyczące wykorzystania aplikacji w celu wygenerowania raportów na użytek administratora
- Dane dotyczące licencji Synappx (np. wygaśnięcie)
- Rejestr systemu

Synappx Meeting:

- Wyświetlanie adresu IP i portu (jeśli został skonfigurowany przez administratora)
- Opcjonalny identyfikator konta monitora i hasło monitora (jeśli został skonfigurowany przez administratora)
- Typ nadawcy udostępniającego, adres IP i PIN (jeśli został skonfigurowany przez administratora)
- Nazwa spotkania, rzeczywisty czas trwania spotkania (godzina rozpoczęcia i zakończenia), nazwa miejsca spotkania, nazwisko uczestnika i adres e-mail uczestnika

Synappx Go

- Informacje o urządzeniach wielofunkcyjnych (model, adres IP, numer seryjny) wykryte za pomocą inicjowanego przez administratora wykrywania SNMP
- Informacje o agencie urządzenia wielofunkcyjnego (nazwa komputera, identyfikator komputera, numer wersji, zasady aktualizacji, data ostatniej aktualizacji)
- Informacje o agencie monitora (nazwa komputera, identyfikator komputera, numer wersji, zasady aktualizacji, data ostatniej aktualizacji)
- Informacje o tagach NFC (identyfikator i typ tagu) powiązanych z urządzeniami skonfigurowanymi przez administratora

Dane w bazach danych Synappx są dostępne tylko dla licencjonowanych klientów za pośrednictwem aplikacji Synappx i dla ograniczonej liczby pracowników firmy Sharp, jeśli jest to wymagane dla celów wsparcia.

Ogólnie rzecz biorąc, Sharp zarządza usługami w chmurze Synappx, ograniczając dostęp do systemu do minimalnej liczby pracowników w celu wdrożenia i wsparcia. Więcej informacji na ten temat można znaleźć w sekcjach dotyczących polityki bezpieczeństwa firmy Sharp.

Więcej informacji na temat bezpieczeństwa Microsoft Azure można znaleźć za pośrednictwem następujących linków dotyczących funkcji wykorzystywanych przez usługi Synappx:

- Omówienie: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Szyfrowanie danych w spoczynku: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Bezpieczeństwo Sieci Azure: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Funkcje Azure i bezpieczeństwo platformy bezserwerowej: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Przewodnik bezpieczeństwa magazynów Azure: https://docs.microsoft.com/en-us/azure/security/security-storage-overview
- Zarządzanie bezpieczeństwem w Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management
- Zarządzanie i ład na platformie Azure:: https://docs.microsoft.com/en-us/azure/governance/

4. Portal administratora Synappx

Administratorzy Synappx Meeting i Synappx Go konfigurują i zarządzają systemem Synappx za pośrednictwem stron internetowych portalu administratora Synappx. Za pomocą tych bezpiecznych stron internetowych można dodawać przestrzenie robocze /pokoje spotkań, użytkowników, urządzenia, dodatkowych administratorów i inne. Zarządzanie licencjami odbywa się poprzez portal administratora, można też sprawdzić tutaj ich status. Raporty pomagają przedstawić wykorzystanie systemu Synappx i wartość biznesową. Pliki do pobrania (dla Synappx Go) są wygodnie dostępne za pośrednictwem tych stron. Logi systemowe są dostępne do pobrania.

4.1 Dostęp i logowanie w oparciu o role (dla portalu administratora i klientów)

Dostęp do systemu portalu administratora Synappx jest kontrolowany za pomocą procesów uwierzytelniania opartych na dzierżawie i rolach. Użytkowników zakłada się przy każdej dzierżawie i przypisuje do konkretnego konta klienta oraz zgodnie z ich rolami i uprawnieniami użytkowania. Początkowy administrator zostaje zidentyfikowany w ramach procesu składania zamówienia. Dodatkowych Administratorów można dodać po pomyślnym zalogowaniu się do portalu Synappx przez pierwszego Administratora.

Tylko administratorzy wyznaczeni lub przydzieleni przez klienta mogą uzyskać dostęp do: użytkowników i przestrzeni roboczych usług Synappx, zarządzania nimi, ich konfiguracji i licencjonowania oraz przeglądać raporty, itp. dla swojego konta za pośrednictwem bezpiecznego portalu internetowego. Cała komunikacja z portalem administratora odbywa się za pośrednictwem portu HTTPS/SSL (TLS1.2) 443 w celu ochrony danych w trakcie przesyłania.

Synappx Meeting i Synappx Go wykorzystują dane uwierzytelniające administratorów i użytkowników pakietu Microsoft 365 lub Google Workspace, aby uniknąć konieczności konfigurowania, zarządzania i ochrony osobnych danych uwierzytelniających do logowania w systemie Synappx. Z założenia usługi Synappx nie mają dostępu do haseł klientów Microsoft 365 lub Google Workspace. System wykorzystuje Azure Active Directory lub Google Workspace Directory i opiera się na tokenach uwierzytelniających do identyfikacji administratorów i użytkowników (przy dostępie do klienta). Tożsamość użytkownika jest potwierdzana w systemie Microsoft Azure AD (dla kont Microsoft 365) lub Google Workspace Directory (dla kont Google Workspace) za pośrednictwem bezpiecznego partnera uwierzytelniającego Auth0 (szczegóły poniżej), a hasła użytkowników nigdy nie są przechowywane w systemach Synappx ani Auth0. Platforma Synappx bezpiecznie przechowuje tylko adres e-mail użytkownika oraz imię i nazwisko. Żadne inne dane osobowe użytkownika nie są znane ani przechowywane przez system Synappx.

4.2 Auth0 (dostawca tożsamośći) 7

Przy realizacji usług Synappx firma Sharp współpracuje z Auth0 (https://auth0.com/) w zakresie bezpiecznych usług uwierzytelniania dla pakietów Microsoft Azure AD i Google Workspace. Auth0 podaje, że obsługuje 21 milionów użytkowników w 120 000 aplikacji, osiągając 2,5 miliarda logowań miesięcznie. Jest to dostawca tożsamości, który cieszy się dużym uznaniem.

Proces uwierzytelniania przebiega w następujący sposób:

1. Podczas logowania do portalu administratora Synappx lub dowolnego klienta Synappx administrator lub użytkownik wprowadza dane uwierzytelniające do pakietu Microsoft 365 lub Google Workspace poprzez okna dialogowe.

2. Auth0 przekazuje uwierzytelnienie nazwy użytkownika i hasła przesyłane za pośrednictwem SSL/TLS 1.2 (port 443) do Azure AD lub Google Workspace, który zatwierdza dane uwierzytelniające - nazwę użytkownika i hasło.

3. Auth0 nie zna ani nie przechowuje hasła użytkownika.

4. We współpracy z Azure AD lub Google Workspace, bezpieczny JSON Web Token (JWT) jest dostarczany z powrotem do przeglądarki (przy dostępie do Synappx Admin Portal), urządzeń mobilnych (dla Synappx Go i Synappx Meeting) i/lub do klientów Windows/Mac (dla Synappx Meeting).

5. Token ten umożliwia korzystanie z funkcji aplikacji bez konieczności logowania się za każdym razem, gdy użytkownik korzysta z aplikacji (z wyjątkiem przypadków, w których następuje zmiana danych uwierzytelniających, np. konieczność ponownego wprowadzenia hasła, utrata ważności, wylogowanie się z aplikacji mobilnej lub 30-dniowy brak aktywności). Nikt nie może ingerować w token JWT bez powiązanego z nim tajnego klucza używanego do podpisywania, który jest bezpiecznie przechowywany w chmurze.

Dostępnych jest wiele poziomów ochrony uwierzytelniania. Urządzenie przenośne lub komputer użytkownika jest chroniony hasłem lub logowaniem biometrycznym (np. odciskiem palca lub rozpoznawaniem twarzy). Hasła użytkowników nie są znane/zachowywane na żadnym z urządzeń Synappx, a bezpieczne tokeny dostarczane przez Auth0 są oparte na bezpiecznych tokenach i uwierzytelnianiu z Microsoft Azure lub Google Workspace.

Auth0 posiada wiele certyfikatów dotyczących bezpieczeństwa w chmurze, w tym: ISO27001, ISO27018, SOC 2 Type II, HIPAA BAA, Tarcza Prywatności UE – USA, Gold CSA STAR, zgodność z RODO i inne. Więcej informacji na temat przepisów bezpieczeństwa Auth0 można znaleźć w następujących raportach Auth0:

- https://auth0.com/security/

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

4.3 Przyznawanie uprawnień aplikacji Synappx.

Aby aktywować funkcje Synappx Meeting i Synappx Go, administrator musi nadać użytkownikom aplikacji Synappx wybrane uprawnienia. Pierwszy Administrator, który zaloguje się do systemu, musi mieć uprawnienia administratora Azure AD lub Google Workspace i wyrazić zgodę w imieniu organizacji na wymagane uprawnienia dla użytkowników podczas dostępu do aplikacji/usług Synappx.

W przypadku klientów Microsoft 365 uprawnienia ich uzasadnienie są następujące:

Prośby o uprawnienia	Definicja	Portal administratora	Synappx Meeting	Synappx Go
Azure Active Directory Graph:				
User.Read	Umożliwia użytkownikom zalogowanie się do aplikacji i pozwala na odczytanie profilu zalogowanych użytkowników. Pozwala również na odczytanie podstawowych informacji służbowych zalogowanych użytkowników.	Tak	Tak	Tak
Directory.Read.All	Umożliwia aplikacji zbieranie aliasów domen z Azure AD (potrzebnych do obsługi wielu domen) i pozwala aplikacji na odczytywanie danych w Azure AD, takich jak użytkownicy, grupy i aplikacje.	Tak	Nie	Nie
Microsoft Graph:				
Calendars.ReadWrite. Shared	Pozwala na tworzenie, odczytywanie, aktualizowanie i usuwanie zdarzeń we wszystkich kalendarzach, do których użytkownik ma dostęp. Obejmują one delegowane i wspólne kalendarze.	Nie	Tak	Nie
Files.ReadWrite.All	Pozwala na odczytywanie, tworzenie, aktualizację i usuwanie wszystkich plików, do których zalogowany użytkownik ma dostęp.	Nie	Tak	Nie
Group.Read.All	Pozwala aplikacji na sporządzanie list grup oraz odczytywanie ich właściwości i wszystkich rodzajów członkostwa w grupie w imieniu zalogowanego użytkownika. Aplikacja umożliwia również odczytywanie kalendarza, rozmów, plików i innej zawartości grupy we wszystkich grupach, do których zalogowany użytkownik ma dostęp.	Tak	Nie	Nie
User.Read.All	Pozwala aplikacji na odczytanie pełnego zestawu właściwości profilu, raportów i menadżerów innych użytkowników w Twojej organizacji, w imieniu zalogowanego użytkownika.	Tak	Tak	Nie
offline_access	Pozwala aplikacji odczytywać i aktualizować dane użytkownika, nawet jeśli nie korzysta on obecnie z aplikacji.	Tak	Tak	Tak
email	Pozwala aplikacji na odczytanie głównego adresu e-mail użytkownika.	Tak	Tak	Tak
openid	Umożliwia użytkownikom zalogowanie się do aplikacji przy użyciu ich kont służbowych lub szkolnych oraz pozwala aplikacji zobaczyć podstawowe informacje o profilu użytkownika.	Tak	Tak	Tak
profile	Wymagane do uzyskania informacji o profilu użytkownika (np. imię i nazwisko użytkownika, adres e-mail) od Azure AD.	Tak	Tak	Tak

Dla klientów pakietu Google Workspace poniżej znajduje się lista wymaganych zakresów interfejsów API oraz uzasadnienie dla każdego z nich:

Żądane zakresy interfejsów Google API	Definicja	Portal administratora	Aplikacja Synappx Meeting	Aplikacja Synappx Go
https://www.googleapis.com/auth/admin.directory.domain.readonly	Umożliwia aplikacji odczytywanie informacji o domenie w celu obsługi funkcji obejmujących wiele domen.	Tak	Nie	Nie
https://www.googleapis.com/auth/admin.directory.group.readonly	Pozwala aplikacji na pobieranie grup, aliasów grup i informacji o członkach w celu dodania grup za pośrednictwem portalu administratora.	Tak	Nie	Nie
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Pozwala aplikacji na pobieranie zasobów kalendarza w celu dodawania obszarów roboczych poprzez portal administratora.	Tak	Nie	Nie
https://www.googleapis.com/auth/admin.directory.user.readonly	Pozwala aplikacji na pobieranie użytkowników lub aliasów użytkowników aby dodać użytkowników poprzez portal administratora.	Tak	Nie	Nie
https://www.googleapis.com/auth/calendar.readonly	Umożliwia aplikacji dostęp do kalendarzy tylko do odczytu.	Nie	Tak	Nie
https://www.googleapis.com/auth/calendar.events	Pozwala aplikacji na odczyt/zapis zdarzeń w kalendarzu i aktualizację kalendarza (np. wydłużenie czasu spotkania).	Nie	Tak	Nie
https://www.googleapis.com/auth/drive	Umożliwia aplikacji dostęp do plików z dysku Google Drive autoryzowanego użytkownika (z wyjątkiem folderu Application Data) w celu sporządzenia listy plików.	Nie	Tak	Nie
https://www.googleapis.com/auth/drive.file	Pozwala aplikacji na dostęp do plików utworzonych lub otwartych przez aplikację w celu ich pobrania i przesłania. Autoryzacja plików jest udzielana dla każdego użytkownika i jest odwoływana, gdy użytkownik dezaktywuje aplikację.	Nie	Tak	Nie
https://www.googleapis.com/auth/userinfo.profile	Pozwala aplikacji do korzystania z danych osobowych użytkownik udostępnił publicznie, aby uzyskać nazwę użytkownika i obraz awatara.	Nie	Tak	Tak

4.4 Importowanie użytkowników lub obszarów roboczych z Azure AD lub Google Workspace

Synappx Go licencjonuje usługę w oparciu o użytkowników, natomiast Synappx Meeting na zasadzie obszarów roboczych/sal konferencyjnych. Administratorzy mogą oszczędzać czas i redukować błędy podczas pisania, importując bezpośrednio użytkowników (dla Synappx Go) i przestrzenie robocze (np. pokoje) dla obu aplikacji z Microsoft 365 (Azure AD) lub Google Workspace. Dozwolone jest również ręczne wprowadzanie przestrzeni roboczych. Tylko użytkownicy w obsługiwanych domenach i w Azure AD lub Google Workspace mogą być dodawani jako licencjonowani użytkownicy Synappx Go. Komunikacja z Microsoft Azure i Google Workspace for User i/lub Workspace odbywa się za pomocą protokołu HTTPS (port 443).

4.5 Pobieranie agenta Synappx Go

Agent urządzeń wielofunkcyjnych i agent monitora Synappx Go może zostać pobrany ze strony z plikami do pobrania w portalu administratora Synappx. Pobrany agent nie jest dostępny na publicznych stronach internetowych i może być pobrany tylko przez upoważnionych administratorów Synappx. Zaszyfrowany (SHA-256) plik konfiguracyjny jest pakowany w pliku zip zawierającym informacje specyficzne dla dzierżawcy oraz informacje wprowadzone przez klienta w celu umożliwienia automatycznego wykrycia urządzenia wielofunkcyjnego za pomocą SNMP (dla agenta urządzenia wielofunkcyjnego). Więcej szczegółów na temat zabezpieczeń związanych z agentami można znaleźć w sekcji poświęconej agentom Synappx Go.

4.6 Raporty Synappx

Raporty Synappx Meeting i Synappx Go pomagają administratorom zrozumieć wykorzystanie i wartość aplikacji Synappx. Dane, które są podstawą do generowania raportów Synappx są przechowywane na bezpiecznych serwerach firmy Microsoft. Dane są przechowywane do 45 dni po rozwiązaniu usługi przez klienta (aby dać czas na odnowienie licencji w razie potrzeby). Informacje dotyczące poszczególnych użytkowników w raportach są dostępne tylko dla wewnętrznych administratorów firmy za pośrednictwem stron z raportami. Firma Sharp ma dostęp do anonimowych, zbiorczych danych na temat korzystania z aplikacji klienta w celu zapewnienia wsparcia i udoskonalenia produktu w miarę upływu czasu. Więcej szczegółów można znaleźć w sekcjach Bezpieczeństwo korporacyjne Sharp , Dostęp administratora Sharp do danych oraz Polityka prywatności firmy Sharp.

4.7 Domeny wspierane przez Synappx

W przypadku kont Microsoft 365 i pakietu Google Workspace firma Synappx gromadzi informacje na temat aliasów domen obsługiwanych w systemie Azure AD lub Google Workspace konta. W przypadku kont Microsoft 365, na stronie Ustawienia administratora/Wspierane domeny, po wstępnym zezwoleniu, administratorzy mogą wybrać dodatkowe aliasy domen poza główną domeną Azure AD, pod którą zostało utworzone konto Synappx. Pozwala to na importowanie użytkowników i obszarów roboczych z wybranych domen, które mają być używane z usługami Synappx.

4.8 Rejestr systemu Synappx

Synappx Go i Synappx Meeting zawierają rejestr systemowy z informacjami o zdarzeniach systemowych, które mogą zainteresować administratorów. Należą do nich sytuacje, które mogą wymagać interwencji administratora w celu skorygowania problemu lub przeprowadzenia diagnostyki. Rejestr systemowy może być wyeksportowany przez administratora jako plik .CSV do dalszej analizy. Rejestr systemowy jest przechowywany przez system Synappx przez 30 dni.

5. Aplikacje klienckie Windows i Apple Mac dla Synappx Meeting

Synappx Meeting pomaga połączyć się z monitorem w sali konferencyjnej, rozpocząć spotkanie on-line i obsługiwać aplikacje za pomocą prostych poleceń głosowych*. Zapewniają one szeroki wachlarz zabezpieczeń, w tym:

- Dostęp aplikacji klienckiej Synappx Meeting do zasobów chmury odbywa się za pośrednictwem protokołu HTTPS (port 443).
  - Azure (Otrzymuje informacje o sali konferencyjnej od administratora Synappx)
  - Auth0 (Przekazanie uwierzytelnienia użytkownika do Azure AD)
  - Azure AD (uwierzytelnianie użytkownika za pomocą konta Microsoft 365) lub Google Workspace (uwierzytelnianie użytkownika za pomocą konta Google Workspace)
  - Interfejsy API Microsoft Graph (pobieranie informacji o spotkaniach i plików na spotkania z pakietu Microsoft Office 365) lub Zakresy interfejsu Google API (pobieranie informacji o spotkaniach i plików na spotkania z pakietu Google Workspace)
  - Amazon Web Services dla dostępu do kolejki poleceń głosowych*

- Dostęp do lokanego monitora
  - Umożliwia sterowanie systemami interaktywnych wyświetlaczy BIG PAD za pomocą głosu*. Wykorzystywany protokół to telnet (Port 10008)

- Użytkownik uwierzytelnia się za pomocą haseł Microsoft 365 lub Google Workspace przy pierwszym użyciu aplikacji Synappx, jeśli nastąpią zmiany w danych uwierzytelniających (np. aktualizacja hasła), użytkownik zostaje wylogowany z aplikacji klienckiej a także/lub po 3 dniach bez użycia aplikacji.

- Hasła użytkownika nie są zapisywane w urządzeniu przenośnym. Zabezpieczony token JWT jest dostarczany po zatwierdzeniu hasła użytkownika w systemie Azure AD lub Google Workspace za pośrednictwem partnera Auth0.
  - Token dostępu użytkownika jest przechowywany na lokalnym komputerze
  - Identyfikator/hasło do serwera proxy są przechowywane w pamięci lokalnej. (szyfrowane przy użyciu AES128)

* Sterowanie głosowe obecnie niedostępne w Europie.

6. Synappx Go oraz Synappx Meeting Mobile

Dzięki wszechobecnemu wykorzystaniu urządzeń mobilnych w biznesie, smartfony są obecnie powszechnie używane do uzyskiwania dostępu i udostępniania treści biznesowych. Użytkownicy oczekują intuicyjnych usług mobilnych, które pomogą im szybciej wykonywać pracę. Dzięki aplikacji mobilnej Synappx Go użytkownicy mogą skanować do często używanych miejsc docelowych, uwalniać zadania druku lub drukować obsługiwane pliki przechowywane w chmurze na dowolnym skonfigurowanym w Synappx Go urządzeniu i udostępniać pliki w chmurze na skonfigurowanych monitorach Sharp. Aplikacja mobilna Synappx Meeting umożliwia użytkownikom szybkie rozpoczynanie spotkań on-line oraz szybki dostęp do dokumentów. Kilka funkcji bezpieczeństwa związanych z klientami mobilnymi to:

Synappx Meeting oraz Synappx Go

- Urządzenie przenośne wymaga wprowadzenia hasła użytkownika lub uwierzytelnienia biometrycznego (np. odcisk palca, rozpoznawanie twarzy) w celu uzyskania dostępu do aplikacji.
- Użytkownicy uwierzytelniają się za pomocą danych Microsoft 365 lub Google Workspace przy pierwszym użyciu aplikacji Synappx, lub jeśli nastąpią zmiany w danych uwierzytelniających (np. aktualizacja hasła), użytkownik zostaje wylogowany z aplikacji klienckiej lub po 30 dniach bez użycia aplikacji.
  Wykorzystywane technologie:
  - Auth0 (Przekazanie uwierzytelnienia użytkownika do Azure AD)
  - Azure AD (uwierzytelnianie użytkownika za pomocą konta Microsoft 365) lub Google Workspace (uwierzytelnianie użytkownika za pomocą konta Google Workspace)
- Hasła użytkownika nie są zapisywane w urządzeniu przenośnym. Zabezpieczony token JWT jest dostarczany po zatwierdzeniu hasła użytkownika w systemie Azure AD lub Google Workspace za pośrednictwem partnera Auth0.
- Cały dostęp do systemu szyfrowany przez TLS v1.2 AES256 (port 443)

Synappx Go

- Dostęp mobilny użytkownika jest kontrolowany centralnie przez portal administratora Synappx. Administratorzy mogą w każdej chwili usunąć licencję użytkownika, aby zablokować późniejsze korzystanie z funkcji aplikacji mobilnej Synappx Go.
- Użytkownicy są proszeni o udzielenie dostępu do swojej listy kontaktów w telefonie komórkowym w celu utworzenia miejsc docelowych skanowania do poczty elektronicznej bez konieczności ponownego wpisywania adresów e-mail użytkowników docelowych. Oszczędza to czas i zmniejsza liczbę błędów przy wpisywaniu adresów.
- Aby skanować do folderu pamięci masowej w chmurze, drukować wybrane pliki przechowywane w chmurze lub udostępniać pliki przechowywane w chmurze wyświetlaczom firmy Sharp, użytkownicy mogą skonfigurować Synappx Go, aby uzyskać dostęp do plików z obsługiwanych witryn pamięci masowej w chmurze (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box lub Google Drive). Dla aplikacji iOS, iCloud i pliki lokalne są już skonfigurowane.
  - Aby korzystać z wybranej pamięci w chmurze, użytkownicy mogą wprowadzić swoją nazwę użytkownika i hasło, które są zatwierdzane za pomocą wybranej witryny pamięci w chmurze. Po uwierzytelnieniu, dostarczony zostaje bezpieczny token i jest on przechowywany w Synappx Go, aby uniknąć konieczności ponownego wprowadzania przez użytkownika tych danych, chyba że utracą one ważność (np. przy zmianie hasła, dezaktywacji konta itp.).
  - Firma Sharp i dostawcy komponentów nie mają dostępu do haseł dostępu do miejsc przechowywania danych w chmurze użytkowników
  - Dla każdej usługi przechowywania w chmurze użytkownik zostanie poproszony o nadanie aplikacji Synappx wybranych uprawnień do dostępu i aktualizacji plików, które użytkownik wybierze do pobrania, a następnie wyświetlenia i edycji. * Uwaga: Usługa Synappx Go nie ma funkcji umożliwiającej usuwanie plików lub folderów z dowolnego miejsca przechowywania w chmurze.
  - Uwaga: Firma Sharp współpracuje z zewnętrznym dostawcą - Kloudless (kloudless.com)- aby ułatwić efektywne połączenia Synappx Go z wieloma dostawcami pamięci masowych w chmurze. Kloudless nie ma dostępu do haseł użytkowników. Ich bezpieczna baza danych zawiera adresy e-mail użytkowników Synappx Go. Kloudless przechowuje minimalne metadane plików/folderów (np. nazwę i ID pliku, datę modyfikacji), aby umożliwić przeglądanie ostatnio zmodyfikowanych plików w witrynach chmury. Natomiast zawartość plików użytkownika nie jest przechowywana.

Synappx Meeting:

- Aplikacje mobilne są dostępne dla każdego użytkownika usługi (nie jest wymagana licencja); jednakże użytkownik musi być użytkownikiem w Azure AD lub Google Workspace w tej samej domenie klienta.
- Dostęp do informacji dotyczących sali konferencyjnej Azure można uzyskać od administratora Synappx.
- Microsoft Graph API pobiera z pakietu Microsoft Office 365 informacje o spotkaniach i pliki do spotkań. Zakresy Google API otrzymują informacje i pliki do Spotkań z pakietu Google Workspace.

7. Tagi NFC Synappx Go

Synappx Go korzysta ze specjalnych tagów NFC dostarczanych przez firmę Sharp, autoryzowanych sprzedawców i/lub wbudowanych w wybrane modele urządzeń wielofunkcyjnych. Tagi zawierają unikalny identyfikator i są tylko do odczytu (nie można ich przeprogramować). Każdy tag może być przypisany tylko do jednego urządzenia naraz. Po skonfigurowaniu urządzenia (np. urządzenia wielofunkcyjnego lub komputera PC z monitorem) przez administratora za pomocą aplikacji mobilnej Synappx Go, po zbliżeniu tagu NFC przez użytkownika, tag i aplikacja mobilna razem identyfikują tożsamość użytkownika i urządzenie powiązane z tagiem/urządzeniem, aby umożliwić korzystanie z urządzeń Synappx Go w takich przypadkach, jak skanowanie do poczty e-mail, uwalnianie zadań druku, drukowanie plików przechowywanych w chmurze i udostępnianie do wyświetlania.

8. Agent MFP Synappx Go

Agent MFP Synappx Go (w tym oprogramowanie do druku podążającego) to element systemu Synappx Go instalowany na komputerze klienta lub serwerze w celu ułatwienia komunikacji między urządzeniami wielofunkcyjnymi obsługującymi technologię Synappx Go a chmurą Synappx Go, aby umożliwić korzystanie z urządzeń mobilnych i tagów NFC powiązanych z urządzeniami wielofunkcyjnymi firmy Sharp. Synappx Go eliminuje potrzebę nauki obsługi i wykonywania wielu czynności na przednim panelu urządzenia wielofunkcyjnego, aby zwolnić bezpieczne zadania drukowania z dowolnego urządzenia wielofunkcyjnego z włączoną funkcją Synappx Go, drukować wybrane pliki przechowywane w chmurze i wysyłać pliki do ulubionych miejsc docelowych skanowania. Użytkownicy mogą zaoszczędzić czas na skanowaniu i bezpiecznym drukowaniu, a także zmniejszyć ryzyko nieautoryzowanego dostępu do zadań drukowania użytkownika.

Agent MFP Synappx Go jest wymagany do obsługi operacji skanowania i drukowania. Jedną z podstawowych funkcji agenta jest ustanowienie bezpiecznego kanału komunikacyjnego z chmurą Synappx. Agent łączy się z chmurą w celu rejestrowania i zabezpieczania komunikacji z urządzeniem oraz wysyłania/odbierania wiadomości do i od agenta oraz obsługiwanych urządzeń wielofunkcyjnych. Każdy z agentów posiada unikalny identyfikator, którego System Synappx Go Cloud używa do ustalenia, do których agentów mają być wysyłane wiadomości. Agenty oczekują na wiadomości poprzez subskrypcję tematu z ich unikalnym identyfikatorem, a usługi w chmurze wysyłają wiadomość poprzez publikację tematu z tym identyfikatorem.

8.1 Instalacja agenta MFP

Aby zainstalować agenta MFP, wymagane jest pobranie specjalnego pakietu instalacyjnego z portalu Synappx Go Admin Portal z unikalnym dla klienta plikiem konfiguracyjnym. Zawartość pliku konfiguracyjnego jest zabezpieczona za pomocą algorytmów szyfrujących. Pakiet instalacyjny agenta MFP nie jest dostępny na publicznej stronie internetowej i jest powiązany z konkretnym kontem klienta. W przypadku większości instalacji dla klientów, na każdego klienta przypadnie jeden agent MFP obsługujący maksymalnie od 50 do 100 urządzeń wielofunkcyjnych (w zależności od liczby użytkowników i zadań drukowania), które mogą korzystać z funkcji drukowania i skanowania Synappx Go. Klienci, którzy chcą obsługiwać więcej niż 100 urządzeń wielofunkcyjnych, będą musieli zainstalować dodatkowego agenta MFP (lub więcej).

Po zainstalowaniu, w celu samodzielnej rejestracji, agent urządzenia wielofunkcyjnego przesyła swój unikalny identyfikator wraz z danymi uwierzytelniającymi agenta do chmury Synappx Go w celu rejestracji w Rejestrze Urządzeń. Informacje przechowywane w rejestrze urządzeń obejmują takie dane, jak identyfikator urządzenia, lokalizacja, identyfikator dzierżawy, a w przypadku urządzeń wielofunkcyjnych - agent MFP powiązany z tym urządzeniem.

8.2 Komunikacja z agentem MFP

Wszelka komunikacja pomiędzy agentem MFP Synappx Go a chmurą Synappx Go odbywa się za pomocą HTTPS (Port 443) lub X.509 poprzez MQTT. Protokół HTTPS jest wykorzystywany podczas wstępnej komunikacji instalacyjnej między agentem MFP Synappx Go a chmurą Synappx Go oraz do przesyłania informacji o urządzeniach wielofunkcyjnych i wszelkich informacji o błędach.

- Klucze prywatne agenta X.509 nigdy nie opuszczają systemu, w którym zainstalowany jest agent, a tym samym nie są nigdy ujawniane w wyniku transmisji przez Internet.
- Wszystkie certyfikaty agenta X.509 są podpisywane za pomocą certyfikatu podpisanego przez klienta Agenta. Agenty mogą dokonać automatycznej rejestracji tylko wtedy, gdy certyfikat X.509 jest podpisany przez powiązanego z nimi klienta.

Usługi chmury Synappx Go utrzymują oddzielne certyfikaty podpisu dla każdego klienta Synappx Go. Gwarantuje to, że Agenci są zaopatrywani tylko w ramach rejestru powiązanego z ich dzierżawą.

Po automatycznym powiązaniu agenta z chmurą Synappx Go, w tym za pomocą certyfikatów X.509, komunikacja pomiędzy agentem a chmurą odbywa się za pomocą bezpiecznych połączeń MQTT. Stosowane są certyfikaty Sharp Synappx Go X.509 podpisane przez rootCA. Certyfikaty podpisane przez rootCA zapewniają dodatkowy poziom weryfikacji, że posiadacz certyfikatu jest tym, za kogo się podaje. Zastosowanie certyfikatów x.509 oferuje największe bezpieczeństwo w uwierzytelnianiu urządzeń, ponieważ prywatny klucz każdego agenta nigdy nie opuszcza urządzenia i nie może zostać ujawniony. Certyfikat dzierżawy agenta Synappx Go podpisany przez root CA jest generowany przez Synappx Go Tenant Provisioning Service i przechowywany w Azure Key Vault.

- Zalety certyfikatów MQTT i X.509 polegają na tym, że agenci mogą subskrybować tylko swój własny unikalny temat identyfikatora urządzenia; oznacza to, że agenci Synappx Go otrzymują wiadomości publikowane TYLKO na ich identyfikator urządzenia. Agent nie może otrzymywać treści z żadnego innego punktu końcowego.

8.3. Wymagania agenta MFP

Agent Synappx Go jest zaprojektowany według następujących wymagań chmury Azure:

- Zanim urządzenie zostanie podłączone do chmury Azure, MUSI zostać zarejestrowane.
- Zanim urządzenie będzie mogło być zarejestrowane, MUSI być udostępnione (przez administratora klienta)
- Zanim urządzenie będzie mogło zostać udostępnione, MUSI ono posiadać certyfikaty bezpieczeństwa (poprzez system)

8.4 Wykrywanie urządzeń przez agenta MFP

Aby zautomatyzować zbieranie informacji o urządzeniach wielofunkcyjnych (potrzebnych do skonfigurowania usług Synappx Go MFP), agent MFP posiada możliwość wyszukiwania urządzeń wielofunkcyjnych za pomocą wykrywania SNMP. Wykrywanie jest inicjowane automatycznie po wstępnej instalacji agenta. Administrator wprowadza początkowy i końcowy zakres IP za pośrednictwem portalu administratora w celu wyszukania i może również przeprowadzić ponowne wyszukiwanie na żądanie (również inicjowane przez administratora za pośrednictwem konsoli administratora) przy użyciu portu 443. W ramach tego procesu zbierane są następujące informacje o urządzeniu wielofunkcyjnym i przesyłane do chmury Synappx Go:

- Identyfikator agenta MFP, identyfikator urządzenia wielofunkcyjnego, który tworzy system (np. Sharp MX-C301W 63004882), producent, model, numer seryjny, nazwa urządzenia (jeśli jest ustawiona), lokalizacja (jeśli jest ustawiona), adres IP.

8.5 Agent MFP oraz druk podążający i skanowanie dokumentów

Administrator lub użytkownik może skonfigurować sterownik drukarki Sharp tak, aby wskazywał komputer lub serwer z agentem Synappx Go. Podczas wysyłania zadań do sterownika druku plik wydruku użytkownika Synappx Go jest automatycznie zapisywany w folderze dla każdego użytkownika na komputerze z agentem/serwerze, który ma zostać uwolniony przez użytkownika na dowolnym urządzeniu wielofunkcyjnym skonfigurowanym do obsługi tagów NFC Synappx.

- Pliki do druku (format .prn) zapisane na serwerze zostaną automatycznie usunięte po 24 godzinach.
- Pliki prn. są widoczne tylko dla autoryzowanych administratorów mających dostęp do komputera za pomocą zwykłego hasła do PC/serwera.

Obciążenie sieci klienta jest powiązane z korzystaniem przez użytkowników z usług skanowania i drukowania za pomocą Synappx Go. Szacowane obciążenia sieci obejmują:

- Skanowanie do ulubionych miejsc docelowych (na użytkownika) - szacunkowo średnio 1 MB na każde skanowanie (dane mogą się różnić)
- Bezpieczne drukowanie (na użytkownika na zadanie drukowania) - szacowane na 1,2 MB na zadanie drukowania średnio (dane mogą się różnić)
- Drukowanie pliku w chmurze (na użytkownika na zadanie drukowania) - szacowane na 1,2 MB na zadanie drukowania średnio (dane mogą się różnić)

9 Agent monitora Synappx Go

Agent monitora Synappx Go to element systemu Synappx Go zainstalowany na komputerze klienta z monitorem lub serwerze w celu ułatwienia komunikacji między komputerami PC obsługującymi technologię Synappx Go a chmurą Synappx Go, aby umożliwić udostępnianie treści na monitorach Sharp za pomocą urządzeń mobilnych i tagów NFC. Aplikacja Synappx Go umożliwia użytkownikowi łatwe skonfigurowanie połączeń do wszystkich ulubionych miejsc pamięci masowej w chmurze i odnalezienie plików do udostępnienia i/lub edycji (dla większości usług pamięci masowej w chmurze) na monitorach firmy Sharp - wszystko to z prywatnego urządzenia przenośnego i za pomocą prostego zbliżenia tagu NFC w celu pobrania plików. Użytkownicy oszczędzają czas, który można lepiej wykorzystać na wspólną pracę nad zawartością plików, a także zmniejszają ryzyko, że inne osoby na spotkaniu zobaczą poufne nazwy plików, które znajdują się również w ich folderach w chmurze. Ponadto wielu użytkowników może pobierać i edytować pliki (w większości przypadków) na tym samym komputerze z agentem monitora w celu wspólnej edycji lub porównania zawartości pliku.

9.1 Instalacja agenta monitora

Aby umożliwić udostępnianie na monitorze, agent monitora Synappx musi być zainstalowany na komputerze z monitorem z systemem Windows lub na serwerze. Główną funkcją agenta jest ustanowienie bezpiecznego kanału komunikacyjnego z chmurą Synappx.

- Agent łączy się z chmurą w celu rejestrowania i zabezpieczania komunikacji z urządzeniem oraz wysyłania/odbierania wiadomości do i od agenta. Każdy z agentów posiada unikalny identyfikator, którego System Synappx Go Cloud używa do ustalenia, do których agentów mają być wysyłane wiadomości.
- Agenty oczekują na wiadomości poprzez subskrypcję tematu z ich unikalnym identyfikatorem, a usługi w chmurze wysyłają wiadomości poprzez publikację tematu z tym identyfikatorem.

Aby zainstalować agenta monitora wymagane jest pobranie specjalnego pakietu instalacyjnego z portalu Synappx Go Admin Portal z unikalnym dla klienta plikiem konfiguracyjnym. Pakiet instalacyjny agenta monitora nie jest dostępny na publicznej stronie internetowej i jest powiązany z konkretnym kontem klienta. Po zainstalowaniu, w celu samodzielnej rejestracji, agent monitora przesyła swój unikalny identyfikator wraz z danymi uwierzytelniającymi agenta do chmury Synappx Go w celu rejestracji w Rejestrze Urządzeń. Informacje przechowywane w rejestrze urządzeń obejmują dane takie jak nazwa komputera/serwera, unikalny identyfikator komputera/serwera oraz identyfikator dzierżawcy.

9.2 Komunikacja z agentem monitora

Wszelka komunikacja pomiędzy agentem monitora Synappx Go a chmurą Synappx Go odbywa się za pomocą HTTPS (Port 443) lub X.509 poprzez MQTT. Protokół HTTPS jest wykorzystywany podczas wstępnej komunikacji instalacyjnej między agentem monitora Synappx Go a chmurą Synappx Go oraz do przesyłania informacji o błędach.

- Więcej informacji na temat X509 i innych szczegółów dotyczących komunikacji można znaleźć w sekcji poświęconej agentowi urządzeń wielofunkcyjnych. Agent monitora posiada te same funkcje bezpieczeństwa, co opisany powyżej agent urządzeń wielofunkcyjnych.

9.3 Udostępnianie treści przez agenta monitora

W przypadku agenta monitora zaimplementowano następujące dodatkowe funkcje zabezpieczające udostępnianie treści na monitorze:

- Po skonfigurowaniu przez użytkownika pożądanych repozytoriów pamięci masowej w chmurze (np. SharePoint Online, Dropbox) za pośrednictwem własnego urządzenia mobilnego, gdy użytkownik korzysta z funkcji udostępniania na monitorze, bezpieczne tokeny użytkownika w aplikacji mobilnej Synappx Go są tymczasowo przekazywane do bezpiecznej pamięci podręcznej Synappx Cloud. Pamięć podręczna jest dostępna tylko przy użyciu bezpiecznych kluczy. Token użytkownika jest usuwany z pamięci podręcznej chmury Sharp Synappx w krótkim czasie po użyciu, a token użytkownika nigdy nie jest pobierany do serwera agentów monitora.

- Gdy użytkownik wybiera plik(i) z usługi przechowywania w chmurze do pobrania na komputer z agentem monitora za pomocą aplikacji Synappx Go, Synappx Cloud generuje adres URL do pobierania zawierający identyfikator sesji, aby pobrać wybrany plik(i) użytkownika. Pliki są automatycznie otwierane na komputerze z agentem monitora w celu ich wyświetlenia i/lub edycji (dla większości usług przechowywania w chmurze). Pliki są przechowywane w folderze tymczasowym na komputerze z agentem monitora.

    - Pliki, które można pobrać za pomocą usługi Synappx Go do przeglądania lub edycji, są ograniczone do następujących:
        - Plik tekstowy, pliki Microsoft Office (Word, PowerPoint, Excel, OneNote), PDF, obrazy (JPEG, TIFF, GIF, BMP, PNG) & oraz wideo (MP4, AVI, WMV, MOV)
        - Uwaga: Pliki wykonywalne lub skrypty nie są obsługiwane i nie mogą być pobierane za pośrednictwem tej usługi

    - Pliki, które można pobrać za pomocą usługi Synappx Go jedynie do przeglądania, są ograniczone do następujących:
        - Dla iOS, iCloud oraz pamięci plików lokalnych: taka sama lista plików jak powyżej
        - W przypadku plików Google Workspace przechowywanych na dysku Google Drive: Google Docs, Google Slides, Google Sheets, Google Drawing, Google Jamboard
        - Uwaga: Pliki wykonywalne lub skrypty nie są obsługiwane i nie mogą być pobierane za pośrednictwem tej usługi

    - Jeśli użytkownik zdecyduje się na zapisanie edytowanego pliku po dokonaniu zmian na komputerze z agentem monitora, zostanie on zapisany z powrotem w tej samej lokalizacji folderu chmury, z której został pobrany jako nowa wersja i/lub ze zmienioną nazwą pliku (zgodnie z polityką każdej usługi przechowywania w chmurze).

    - Jeśli użytkownik zapisze obsługiwany, edytowalny plik z powrotem do chmury lub zamknie plik bez zapisu, zostanie on usunięty z folderu tymczasowego komputera z agentem monitora

    - Wielu użytkowników z licencjami/aplikacjami Synappx Go może pobierać pliki w chmurze do tego samego Agenta monitora w celu przeglądania, kopiowania i wklejania edytowanych treści, porównując pliki przed zapisaniem ich z powrotem w odpowiednich usługach w chmurze.

10. Bezpieczeństwo korporacyjne

Firma Sharp prowadzi rzetelny program bezpieczeństwa informacji w celu ochrony poufności, integralności i dostępności wszystkich zasobów informacyjnych przetwarzanych i/lub przechowywanych w systemach biznesowych firmy Sharp. Zarząd firmy Sharp dostrzega szybko zmieniające się i rosnące ryzyko związane z ochroną zasobów informacyjnych firmy Sharp i naszych cenionych partnerów biznesowych i regularnie bada, analizuje i inwestuje w proceduralne i techniczne środki zaradcze w celu zapewnienia bezpieczeństwa. Zespół zaangażowanych profesjonalistów stale ocenia środowisko biznesowe, wykorzystując swoją wiedzę fachową w celu udoskonalenia i ciągłej poprawy pozycji firmy Sharp w zakresie bezpieczeństwa informacji. Oprócz tych wewnętrznych działań, firma Sharp wykorzystuje strategiczne partnerstwa z wiodącymi w branży dostawcami usług w celu testowania, monitorowania i audytowania wdrożonych przez nas programów bezpieczeństwa.

11. Dostęp administratora Sharp do danych

Dział informatyczny lub dział pomocy technicznej firmy Sharp może od czasu do czasu potrzebować dostępu do danych użytkownika w celu udzielenia pomocy w kwestiach technicznych. Pozwolenia na tego typu sytuacje będą ograniczone do minimum niezbędnego do rozwiązania danego problemu. Administratorzy firmy Sharp otrzymują ścisłe uprawnienia w oparciu o role, aby zapewnić bezpieczeństwo danych klienta:

- Możliwość przeglądania i aktualizowania informacji o koncie klienta, takich jak status konta i adres e-mail, ale nie plików klienta.
- Możliwość zobaczenia drzewa plików i ich nazw, ale nie przeglądania ani pobierania samych plików
- Użytkownicy Synappx, administratorzy i administrator dealerów mają przydzielony odpowiedni dostęp w ramach swoich uprawnień i nic więcej. Zarządzanie systemem jest ściśle kontrolowane i ograniczone do upoważnionego personelu firmy Sharp. Administratorzy firmy Sharp mają dostęp tylko do informacji krytycznych dla działania systemu. W żadnym momencie użytkownicy systemu nie mają bezpośredniego dostępu do bazy danych lub innych składników systemu.
- Uwaga: Dane związane z Państwa usługami Synappx zostaną usunięte po 45 dniach od daty zakończenia subskrypcji.

12. Polityka prywatności firmy Sharp

Proszę zapoznać się z warunkami korzystania z usług Synappx i polityką prywatności na stronie:

- https://www.sharp.pl/synappx/privacy
- https://www.sharp.pl/synappx/terms

13. Podsumowanie

Przejście na usługi współpracy i spotkań w chmurze oferuje przedsiębiorstwom ekonomiczny sposób wspierania coraz bardziej mobilnych pracowników. Aby budować współpracujące ze sobą i reagujące na zmiany środowiska biurowe, wdrożenie technologii w chmurze i technologii mobilnej nie jest kwestią "czy", ale "kiedy".

Organizacje, które korzystają z usług w chmurze, w pełni wykorzystują swoje inwestycje technologiczne, takie jak komputery, urządzenia mobilne, interaktywne monitory i urządzenia wielofunkcyjne. W połączeniu z usługami abonamentowymi Synappx, eliminacja nakładów inwestycyjnych na wewnętrzne zasoby IT oznacza jeszcze niższy całkowity koszt posiadania. Niektórzy decydenci zmagają się jednak z tym, co pociąga za sobą wdrożenie usług w chmurze, jeśli chodzi o zrównoważenie wygody z dostępnością i bezpieczeństwem. Usługi Sharp Synappx pomagają usunąć te bariery dzięki architekturze opartej na bezpieczeństwie oraz synergii sprzętowo-programowej, która umożliwia tworzenie sprawnych grup roboczych, które mogą szybko reagować na potrzeby biznesowe.

www.sharp.pl

SHARP

Be Original.