Informe sobre seguridad

Synappx™ Go y Synappx™ Meeting

www.sharp.es

SHARP
Be Original.

Índice

1. Presentación

Descripción general

Synappx Go y Synappx Meetings son aplicaciones y servicios de colaboración, productividad y análisis. Están protegidos por un sistema de seguridad sólido y por capas para garantizar que el entorno y sus componentes no ofrecen puntos de entrada vulnerables para sus datos y redes. Mediante una combinación de proveedores de tecnología de talla mundial, incluidos Microsoft Azure y G Suite, y las mejores prácticas de seguridad, el uso de los servicios de Synappx le ayuda a mantener su información segura y protegida, al tiempo que contribuye a mejorar la productividad de su oficina. En este informe se describen las características de seguridad relacionadas con Synappx.

Synappx Go

Synappx Go es un servicio orientado a los dispositivos móviles que aprovecha la tecnología Near Field Communication (NFC) para permitir la digitalización práctica y rápida de documentos, y su envío a destinos favoritos, así como la liberación de impresiones y la impresión de archivos guardados en la nube en cualquier impresora multifunción de su oficina. También puede utilizar su teléfono móvil y la aplicación para seleccionar y descargar contenido guardado en la nube en una pantalla de Sharp mediante un toque gracias a NFC. Los servicios y el software de nube de Synappx Go aprovechan la base de datos, el aprovisionamiento de dispositivos, IoT Hub y muchos otros servicios de Microsoft Azure.

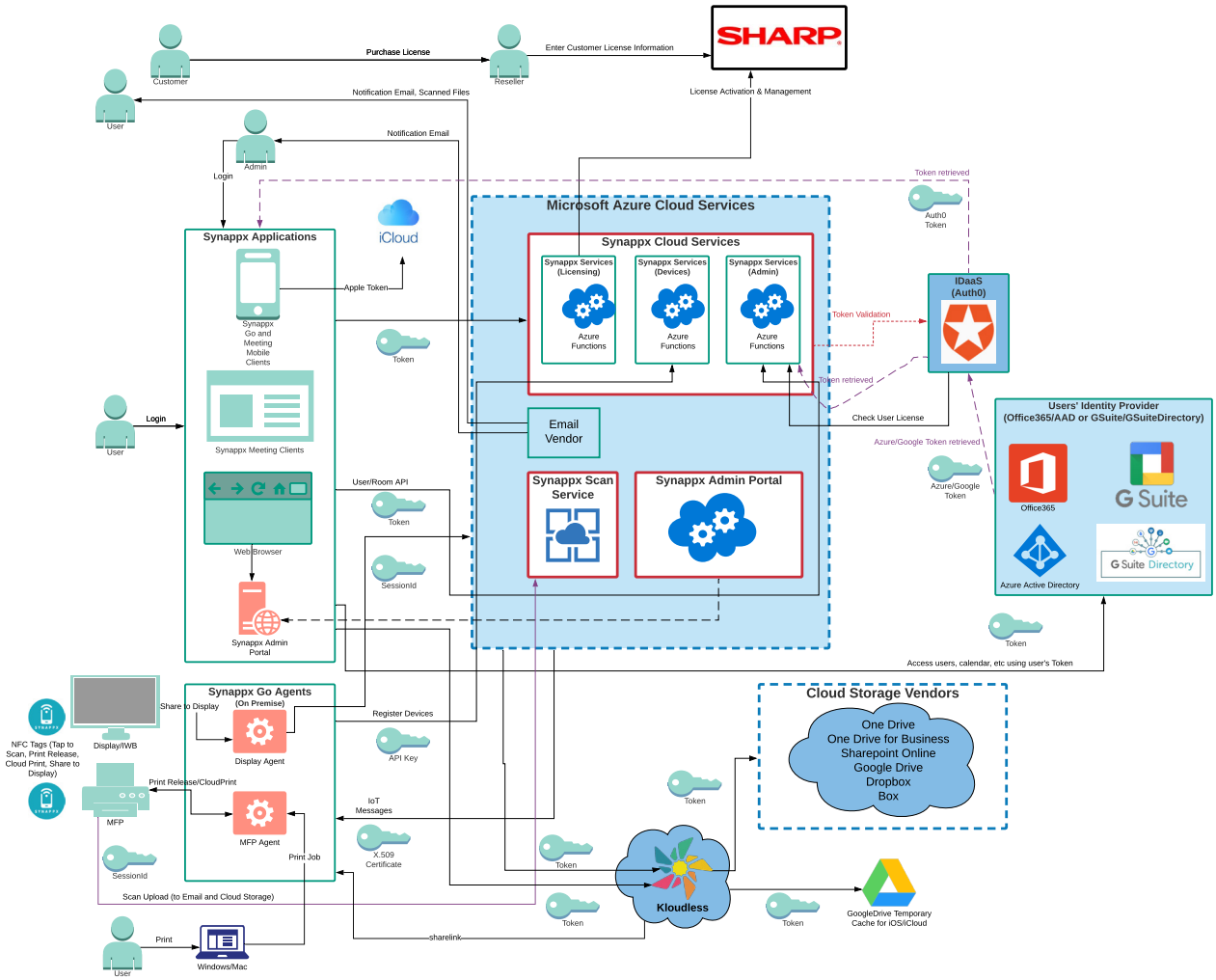
Synappx Meeting

Synappx Meeting aprovecha las tecnologías móviles y de voz*, así como los clientes mejorados y la nube de Azure para ayudar a los usuarios a iniciar reuniones a tiempo y aumentar su eficiencia. Con el clic de un botón se pueden conectar componentes clave de reuniones. Su PC se duplica automáticamente en la pantalla de la sala de reuniones de Sharp, la conferencia web se inicia automáticamente y el usuario puede acceder a materiales de la reunión. Se pueden utilizar comandos de voz* para realizar acciones habituales en reuniones a fin de ahorrar tiempo. Synappx Meeting utiliza, entre otras cosas, la base de datos, el sistema de almacenamiento y las funciones de Microsoft Azure.

* El control por voz no está actualmente disponible en Europa.

2. Descripción general de la arquitectura

A continuación, se presenta una descripción general de la plataforma Synappx (basada en Microsoft Azure), incluidos los componentes de servicio y la arquitectura de Synappx Go y Synappx Meeting:



3. Servicios de nube de Synappx

Synappx Meeting y Synappx Go aprovechan los servicios de la plataforma de nube de Microsoft Azure como base para los servicios de nube de Synappx. Microsoft Azure es un servicio de nube global muy respetado con un amplio conjunto de funciones utilizadas por la familia de productos Synappx de Sharp, incluidos, entre otros, la base de datos, el sistema de almacenamiento, varios servicios de IoT, Key Vault, la funcionalidad de supervisión y el sistema de copia de seguridad de Security Centre de Azure Cosmos.

Las soluciones de Synappx se alojan en centros de datos seguros de Microsoft ubicados en Europa. Los centros de datos y el servicio de nube de Microsoft Azure están protegidos con las prácticas de seguridad de Microsoft. Cada centro de datos proporciona redundancia local de datos. Por otra parte, todas las comunicaciones entre las aplicaciones de Sharp Synappx y los servicios de nube de Synappx (alojados en Microsoft Azure) se cifran a través de HTTPS (TLS v1.2, AES256), con protección mediante certificados X.509 o MQTT (usados por el agente de pantallas y el agente de impresoras multifunción).

El acceso a todos los servicios de nube de Synappx desde aplicaciones cliente requiere claves seguras, certificados y tokens de autenticación. Después de comprar un servicio de Synappx, se asigna a cada cliente un certificado exclusivo para las comunicaciones que se almacena en Microsoft Key Vault para permitir un acceso seguro y limitado al cliente. El acceso a la base de datos de Synappx Azure se limita a direcciones IP incluidas en listas blancas desde servicios de aplicaciones seguros de Azure. Microsoft Key Vault se utiliza para almacenar certificados SSL, certificados de firma de X.509, claves privadas y otro contenido que requiera la máxima seguridad. El acceso a Microsoft Azure Key Vault se limita a las entidades servicio de Sharp y a los usuarios de sistemas con permisos de acceso asociado.

Datos específicos de cliente de Synappx Go o Synappx Meeting almacenados en las bases de datos de nube seguras de Azure:

Synappx Meeting y Synappx Go

- El nombre, el apellido y la dirección de correo electrónico del usuario (importados desde Azure AD o G Suite a Synappx por el administrador)
- El nombre, el apellido y la dirección de correo electrónico del administrador (importados desde Azure AD o G Suite a Synappx por el administrador)
- Los nombres de espacio de trabajo (sala de reuniones), las direcciones de correo electrónicos y las ubicaciones importados desde Microsoft Outlook o G Suite Directory a Synappx por el administrador
- Los nombres y las ubicaciones de los espacios de trabajo añadidas manualmente
- Los alias de dominio de la empresa de Azure AD y G Suite
- Los datos de uso de las aplicaciones para generar informes para uso del administrador
- Los datos de las licencias de Synappx (p. ej., el vencimiento)
- Los registros del sistema

Datos específicos de Synappx Meeting:

- La dirección IP y el puerto de la pantalla (si el administrador lo ha configurado)
- El ID de la cuenta opcional de la pantalla y la contraseña de la pantalla (si el administrador lo ha configurado).
- El tipo de remitente de proyección, la dirección IP y el PIN (si el administrador lo ha configurado)
- El nombre de la reunión, la duración real de la reunión (hora de inicio y hora de finalización), el nombre de la ubicación de la reunión y la dirección de correo electrónico de los asistentes.

Datos específicos de Synappx Go

- Información de la impresora multifunción (nombre del modelo, dirección IP y número de serie) descubiertos a través del proceso de descubrimiento SNMP iniciado por el administrador
- La información del agente de impresoras multifunción (nombre del ordenador, ID de la impresora, número de versión, política de actualización y última fecha de actualización)
- La información del agente de pantallas (nombre del ordenador, ID de la impresora, número de versión, política de actualización y última fecha de actualización)
- Información de la etiqueta NFC (ID y tipo de la etiqueta) asociada a los dispositivos configurados por el administrador

Los datos de la base de datos de Synappx solo están accesibles para los clientes con licencia a través de las aplicaciones de Synappx y a personal limitado de Sharp si es necesario para fines de asistencia.

En términos generales, el sistema de gobernanza de Sharp para los servicios de nube de Synappx se limita al personal mínimo para fines de despliegue y asistencia. Consulte las seccione sobre políticas de seguridad de Sharp para obtener más detalles.

Para obtener más información sobre la seguridad de Microsoft Azure, consulte los siguientes enlaces relacionados con las funciones utilizadas por los servicios de Synappx:

- Descripción general: https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Cifrado de datos en reposo: https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest
- Seguridad de red de Azure: https://docs.microsoft.com/en-us/azure/security/security-network-overview
- Funciones y seguridad de la plataforma sin servidor de Azure: https://docs.microsoft.com/en-us/azure/security/abstract-serverless-platform-security
- Guía de seguridad de Azure Storage: https://docs.microsoft.com/en-us/azure/security/security-storage-overview

Administración de la seguridad en Azure: https://docs.microsoft.com/en-us/azure/security/azure-security-management

- Gobernanza de administración de Azure: https://docs.microsoft.com/en-us/azure/governance/

4. Portal del administrador de Synappx

Los administradores de Synappx Meeting y Synappx Go configuran y administran el sistema Synappx a través de las páginas web del portal del administrador de Synappx. Estas páginas web seguras permiten añadir espacios de trabajo o salas de reuniones, usuarios, dispositivos, administradores adicionales, etc. La administración de licencias se realiza a través del portal del administrador y el estado de licencia puede verse aquí. Los informes ayudan a demostrar el uso del sistema de Synappx y su valor empresarial. Las descargas (para Synappx Go) están cómodamente accesibles a través de estas páginas. Se pueden descargar registros del sistema.

4.1 Acceso e inicio de sesión basados en funciones (para el portal del administrador y los clientes)

El acceso al sistema del portal del administrador de Synappx se controla en función de procesos de autenticación basados en inquilinos y funciones. Los usuarios se configuran en cada inquilino y se asocian a una cuenta de cliente específica, y de acuerdo con sus funciones de uso y permisos. El administrador inicial es identificado como parte del proceso de órdenes de pedido. El administrador inicial puede añadir administradores adicionales después de su registro correcto en el portal de Synappx.

Solo los administradores designados o asignados por el cliente pueden acceder, configurar, otorgar licencias, administrar usuarios y espacios de trabajo de servicios de Synappx, ver informes, etc. para su cuenta a través del portal web seguro. Todas las comunicaciones con el portal del administrador se realizan a través de HTTPS/SSL (TLS1.2) (puerto 443) para proteger los datos en tránsito.

Synappx Meeting y Synappx Go aprovechan las credenciales de los administradores y usuarios de Microsoft 365 o G Suite para evitar tener que establecer, gestionar y proteger credenciales de inicio de sesión independientes. Por su diseño, los servicios de Synappx no tienen acceso a las contraseñas de cliente Microsoft 365 ni de Google G Suite. El sistema aprovecha Azure Active Directory o G Suite Directory y se basa en tokens de autenticación para identificar a los administradores y usuarios (para el acceso de clientes). La identificación del usuario se confirma con Microsoft Azure AD (para las cuentas de Microsoft 365) o G Suite Directory (para las cuentas de G Suite) a través de un socio de autenticación seguro de Auth0 (véase a continuación) y las contraseñas de los usuarios no se almacenan nunca en los sistemas de Synappx ni de Auth0. La plataforma Synappx almacena de forma segura únicamente la dirección de correo electrónico del usuario, y su nombre y apellido. El sistema Synappx no conoce ni almacena ninguna otra información personalmente identificable sobre el usuario.

4.2 Auth0 (proveedor de servicio de identidad)

Para los servicios de Synappx, Sharp colabora con Auth0 (https://auth0.com/) a fin de garantizar servicios de identidad seguros para Microsoft Azure AD y G Suite. Según Auth0, prestan servicio a 21 millones de usuarios a través de 120 000 aplicaciones con 2500 millones de inicios de sesión al mes. Se trata de un proveedor de servicios de identidad muy respetado.

A continuación, se presenta una descripción general del proceso:

1. El administrador o el usuario introduce las credenciales de Microsoft 365 o G Suite a través de cuadros de diálogo al iniciar sesión en el portal del administrador de Synappx o cualquier cliente de Synappx.

2. Auth0 delega la autenticación del nombre de usuario y la contraseña transmitidos a través de SSL/TLS 1.2 (puerto 443) a Azure AD o G Suite que valida las credenciales.

3. Auth0 no conoce ni almacena la contraseña de los usuarios.

4. En colaboración con Azure AD o G Suite, se devuelve un JSON Web Token (JWT) al navegador (para el acceso al portal del administrador de Synappx), a los dispositivos móviles (para Synappx Go y Synappx Meeting) o a los clientes Windows o Mac (para Synappx Meeting).

5. Este token permite a la aplicación realizar funciones sin que el usuario tenga que iniciar sesión cada vez que utiliza las aplicaciones (excepto en los casos en los que se cambian las credenciales, por ejemplo, cuando se necesita volver a introducir las contraseñas, cuando el usuario deja de ser válido, cuando el usuario cierra sesión en la aplicación móvil o tras 30 días de inactividad). Nadie puede manipular el token JWT sin la clave secreta asociada para firmar, que se almacena de forma segura en la nube.

Existen varias capas de autenticación disponibles. El dispositivo móvil del usuario o del ordenador están protegidos mediante una contraseña o mediante un inicio de sesión biométrico (cara o huella dactilar). Las contraseñas de los usuarios no se conocen ni se almacenan en ninguno de los dispositivos de Synappx y los tokens seguros proporcionados por Auth0 se basan en tokens seguros y validación de Microsoft Azure o G Suite.

Auth0 cuenta con una gran cantidad de certificaciones de seguridad en la nube, entre ellas: ISO27001, ISO27018, SOC 2 Tipo II, HIPAA BAA, el marco del escudo de privacidad UE-EE. UU., Gold CSA STAR, compatibilidad con el RGPD, etc. Consulte los siguientes informes de Auth0 para obtener más información sobre las disposiciones de seguridad de Auth0:

- https://auth0.com/security/

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

4.3 Concesión de privilegios para la aplicación Synappx

Para activar las funciones de Synappx Meeting y Synappx Go, el administrador debe conceder a los usuarios de las aplicaciones Synappx privilegios concretos. El primer administrador en iniciar sesión en el sistema debe tener privilegios de administrador de Azure AD o G Suite y conceder en nombre de la organización los permisos solicitados para los usuarios cuando acceden a las aplicaciones o servicios de Synappx.

Para los clientes de Microsoft 365, los permisos y los motivos para cada uno son:

Permisos solicitados	Definición	Portal del administrador	Synappx Meeting	Synappx Go
Azure Active Directory Graph:				
User.Read	Permite al usuario registrarse en la aplicación y a la aplicación leer el perfil de los usuarios registrados. También permite a la aplicación leer información básica de los usuarios registrados de la empresa.	Sí	Sí	Sí
Directory.Read.All	Permite a la aplicación recopilar alias de dominio desde Azure AD (necesarios para la compatibilidad multidominio) y a la aplicación leer datos en Azure AD como los usuarios, los grupos y las aplicaciones.	Sí	No	No
Microsoft Graph:				
Calendars.ReadWrite.Shared	Permite a la aplicación crear, leer, actualizar y eliminar eventos en todos los calendarios a los que el usuario tenga permiso de acceso. Aquí se incluyen calendarios delegados y compartidos.	No	Sí	No
Files.ReadWrite.All	Permite a la aplicación leer, crear, actualizar y eliminar todos los archivos a los que el usuario registrado pueda acceder.	No	Sí	No
Group.Read.All	Permite a la aplicación enumerar grupos y leer sus propiedades y todas las pertenencias a grupos en nombre del usuario registrado. También permite a la aplicación leer el calendario, las conversaciones, los archivos y otro contenido de grupo de todos los grupos a los que el usuario registrado pueda acceder.	Sí	No	No
User.Read.All	Permite a la aplicación leer el conjunto completo de propiedades de perfil, informes y directores de otros usuarios de la organización, en nombre del usuario registrado.	Sí	Sí	No
offline_access	Permite a la aplicación leer y actualizar los datos de usuario, incluso si no están actualmente utilizando la aplicación.	Sí	Sí	Sí
email	Permite a la aplicación leer la dirección de correo electrónico principal de los usuarios.	Sí	Sí	Sí
openid	Permite a los usuarios registrarse en la aplicación con sus cuentas de trabajo o institución escolar, y a la aplicación ver información de perfil básica de los usuarios.	Sí	Sí	Sí
profile	Requerido para obtener información de perfil del usuario (p. ej., el nombre y los apellidos de los usuarios, así como su dirección de correo electrónico) de Azure AD.	Sí	Sí	Sí

Para los clientes de G Suite, la siguiente lista incluye los ámbitos de API requeridos y el motivo para cada uno de ellos:

Ámbitos de API de Google solicitados	Definición	Portal del administrador	Synappx Meeting	Synappx Go
https://www.googleapis.com/auth/admin.directory.domain.readonly	Permite a la aplicación leer la información de dominio para facilitar la función multidominio.	Sí	No	No
https://www.googleapis.com/auth/admin.directory.group.readonly	Permite a la aplicación recuperar el grupo, el alias de grupo y la información de miembro para añadir grupos a través del portal del administrador.	Sí	No	No
https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly	Permite a la aplicación recuperar recursos de calendario para añadir espacios de trabajo a través del portal del administrador.	Sí	No	No
https://www.googleapis.com/auth/admin.directory.user.readonly	Permite a la aplicación recuperar usuarios o alias de usuario para añadir usuarios a través del portal del administrador.	Sí	No	No
https://www.googleapis.com/auth/calendar.readonly	Permite a la aplicación disponer de acceso de solo lectura a los calendarios.	No	Sí	No
https://www.googleapis.com/auth/calendar.events	Permite a la aplicación leer accesos de lectura y escritura a eventos de un calendario y actualizar el calendario (por ejemplo, ampliar el tiempo de la reunión).	No	Sí	No
https://www.googleapis.com/auth/drive	Permite a la aplicación disponer de acceso a archivos de Google Drive del usuario autorizado (excluida la carpeta Application Data) para enumerar los archivos.	No	Sí	No
https://www.googleapis.com/auth/drive.file	Permite a la aplicación disponer de acceso a los archivos creados o abiertos por la aplicación para carga y descarga. Se concede autorización en función del usuario y se revoca cuando el usuario retira la autorización a la aplicación.	No	Sí	No
https://www.googleapis.com/auth/userinfo.profile	Permite a la aplicación utilizar información personal que el usuario ha puesto disposición pública para obtener el nombre de usuario y la imagen del avatar.	No	Sí	Sí

4.4 Importación de usuarios o espacios de trabajo desde Azure AD o G Suite

Synappx Go otorga la licencia de servicio por usuario, mientras que Synappx Meeting lo hace por espacios de trabajo o salas de reunión. Los administradores pueden ahorrar tiempo y reducir errores tipográficos importando directamente los usuarios (para Synappx Go) y los espacios de trabajo (p. ej., salas) para ambas aplicaciones desde Microsoft 365 (Azure AD) o G Suite. También se permite la introducción manual de espacios de trabajo. Solo los usuarios de los dominios admitidos y de Azure AD o G Suite pueden añadirse como usuarios de Synappx Go con licencia. Las comunicaciones con Microsoft Azure y G Suite para los usuarios o espacios de trabajo se importan a través de HTTPS (puerto 443).

4.5 Descargas de agentes de Synappx Go

Los agentes de impresoras multifunción y pantallas de Synappx se pueden descargar desde la página de descargas del portal del administrador de Synappx. Los agentes descargados no están disponibles desde los sitios web públicos y solo pueden ser descargados por administradores autorizados de Synappx. Se empaqueta un archivo de configuración cifrado (SHA-256) con el archivo comprimido que contiene información específica del inquilino, así como información introducida por el cliente para permitir el descubrimiento automático de impresoras multifunción a través de SNMP (para el agente de impresoras multifunción). Consulte la sección sobre los agentes de Synappx Go para obtener más información sobre la seguridad relacionada con los agentes.

4.6 Informes de Synappx

Synappx Meeting y Synappx Go incluyen informes para ayudar a los administradores a entender el uso y el valor de la aplicación Synappx. Los datos que generan los informes de Synappx se almacenan en servidores seguros de Microsoft. Los datos se retienen hasta 45 días después de que el cliente se dé de baja del servicio (para permitir la renovación de la licencia si el cliente lo desea). La información específica incluida en los informes solo está a disposición de los administradores de la empresa a través de la página Reports (Informes). Los datos de resumen anonimizados sobre el uso de la aplicación de los clientes están a disposición de Sharp para fines de asistencia y mejora de los productos a lo largo del tiempo. Consulte Seguridad corporativa de Sharp, Acceso a datos del administrador de Sharp y Política de privacidad de Sharp para obtener más detalles.

4.7 Dominios admitidos por Synappx

Para las cuentas de Microsoft 365 y G Suite, Synappx recopila información sobre los alias de dominio compatibles en el sistema de cuentas de Azure AD o G Suite. Para las cuentas de Microsoft 365, en la página de ajustes del administrador o dominios admitidos, tras aceptar el permiso inicial, los administradores pueden seleccionar alias de dominio adicionales, más allá del dominio de Azure AD primario bajo el cual se creó la cuenta de Synappx. Esto permite importar los usuarios y espacios de trabajo desde dominios concretos para su uso con los servicios Synappx.

4.8 Registros de sistema de Synappx

Synappx Go y Synappx Meeting incluyen un registro del sistema con información sobre eventos del sistema de interés potencial para los administradores. Entre estos eventos, se incluyen condiciones que podrían requerir la intervención de los administradores para corregir un problema o realizar tareas de resolución de incidencias. El administrador puede exportar los registros del sistema como un archivo .CSV para análisis adicionales. Synappx conserva los registros del sistema durante 30 días.

5. Clientes de Windows y Apple Mac para Synappx Meeting

Synappx Meeting ayuda a establecer conexión con la pantalla en la sala de reuniones, a iniciar una conferencia web y a gestionar las aplicaciones mediante comandos de voz*. Estos comandos proporcionan una amplia gama de funciones de seguridad, incluido:

- Todos los accesos de cliente de Synappx Meeting a los recursos de la nube se realizan a través de HTTPS (puerto 443)
  - Azure (obtiene información de la sala de reuniones del administrador de Synappx)
  - Auth0 (delegación de la autenticación de usuarios a Azure AD)
  - Azure AD (autenticación de usuarios con una cuenta de Microsoft 365) o G Suite (autenticación de usuarios con una cuenta de G Suite)
  - API de Microsoft Graph (obtienen información de reuniones y archivos para reuniones de Microsoft Office 365) o alcances de las API de Google (obtienen información de reuniones y archivos para reuniones de G Suite)
  - Amazon Web Services para acceso a la cola de comandos de voz*

- Acceso a la pantalla local
  - Permite el control de los sistemas de pantalla interactivos BIG PAD con control de voz*. El protocolo es telnet (puerto 10008)

- El usuario se autentica con contraseñas de Microsoft 365 o G Suite la primera vez que utiliza la aplicación Synappx, cuando se producen cambios de credenciales (p. ej., cuando se actualiza la contraseña), cuando cierra sesión en la aplicación cliente o tras tres días sin utilizar la aplicación.

- Las contraseñas de usuario no se almacenan en el dispositivo móvil; en su lugar se proporciona un token de JWT tras la validación de la contraseña del usuario con el sistema Azure AD o G Suite a través de un Auth0 de socio.
  - El token de acceso del usuario se almacena en un ordenador local.
  - El ID y la contraseña para el proxy se almacenan en el almacén local. (cifrado con AES128)

* El control por voz no está actualmente disponible en Europa.

6. Synappx Go y Synappx Meeting para dispositivos móviles

Con el uso cada vez más extendido de dispositivos móviles en las empresas, es habitual utilizar los smartphones para acceder a contenido empresarial y compartirlo. Los usuarios esperan que servicios móviles intuitivos les ayuden a completar su trabajo de forma más rápida. La aplicación móvil Synappx Go permite a los usuarios digitalizar documentos y enviarlos a destinos frecuentes, liberar impresiones o imprimir archivos compatibles con nubes en cualquier dispositivo configurado para Synappx Go, así como compartir archivos almacenados en nube en pantallas configuradas de Sharp. La aplicación móvil Synappx Meeting permite a los usuarios empezar su reunión, iniciar conferencias web y acceder a documentos rápidamente. Varias funciones de seguridad asociadas con los clientes móviles:

Synappx Meeting y Synappx Go:

- El dispositivo móvil requiere la introducción de contraseñas de usuario o autenticación biométrica (p. ej., huellas dactilares o reconocimiento facial) para acceder a las aplicaciones.

- Los usuarios se autentican con las credenciales de Microsoft 365 o G Suite la primera vez que utilizan la aplicación Synappx, cuando se modifican las credenciales (p. ej., cuando se actualizan las contraseñas), cuando cierran sesión en la aplicación móvil o después de 30 días o más sin utilizar la aplicación.
  Aprovecha los servicios de:
  - Auth0 (delegación de la autenticación de usuarios a Azure AD)
  - Azure AD (autenticación de usuarios con una cuenta de Microsoft 365) o G Suite (autenticación de usuarios con una cuenta de G Suite)
- Las contraseñas de usuario no se almacenan en el dispositivo móvil; en su lugar se proporciona un token de JWT tras la validación de la contraseña del usuario con el sistema Azure AD o G Suite a través de un Auth0 de socio.

- Todos los accesos al sistema se cifran mediante TLS v1.2 AES256 (puerto 443)

Datos específicos de Synappx Go

- El acceso móvil de los usuarios se controla de manera central a través del portal del administrador de Synappx Los administradores pueden eliminar una licencia de usuario en cualquier momento para bloquear el uso posterior de las funciones móviles de Synappx Go.

- Se solicita a los usuarios que concedan acceso a su lista de contactos móviles para digitalizar documentos y enviarlos a destinos de correo electrónico sin necesidad de volver a introducir los correos electrónicos de los destinatarios. Este proceso ahorra tiempo y reduce los errores tipográficos.

- Para digitalizar documentos y enviarlos a una carpeta de almacenamiento en la nube, para imprimir archivos concretos almacenados en la nube o para compartir los archivos almacenados en la nube en las pantallas de Sharp, los usuarios pueden configurar Synappx Go a fin de acceder a los archivos desde centros de almacenamiento en la nube compatibles (One Drive for Business, One Drive, SharePoint Online, Dropbox, Box o Google Drive). Para la aplicación iOS, los archivos locales y de iCloud ya están configurados.

  - Para centros de almacenamiento de interés, los usuarios pueden introducir su nombre de usuario y contraseña validados con dichos centros. Si se validan, se proporcionará un token seguro, que se almacenará en Synappx Go para que el usuario no tenga que volver a introducir las credenciales, a menos que dejen de resultar válidas (p. ej., en caso de cambio de contraseña, desactivación de la cuenta, etc.)
  - Sharp y los proveedores de componentes no disponen de acceso a las contraseñas de los centros de almacenamiento en nube de los usuarios.
  - Para cada servicio de almacenamiento en la nube, se solicitará al usuario que conceda permisos seleccionados a fin de que la aplicación de Synappx pueda acceder y actualizar los archivos que el usuario desee descargar para ver y editar. Nota: El servicio Synappx Go no incluye ninguna función para eliminar archivos o carpetas de ningún centro de almacenamiento en la nube.
  - Nota: Sharp se asocia con el proveedor externo Kloudless (Kloudless.com) para facilitar conexiones eficientes de Synappx Go con varios proveedores de almacenamiento en la nube. Kloudless no dispone de acceso a las contraseñas de los usuarios. Esta base de datos segura no incluye las direcciones de correo electrónico de los usuarios de Synappx Go. Almacenan metadatos de archivos y carpetas mínimos (p. ej., el nombre y el ID del archivo o la fecha de modificación) para permitir ver archivos recientemente modificados a través de los centros en nube. Kloudless no almacena el contenido de los archivos de los usuarios.

Datos específicos de Synappx Meeting:

- Las aplicaciones móviles están disponibles para cualquier usuario del servicio (no se requiere ninguna licencia); sin embargo, el usuario debe ser un usuario válido de Azure AD o de G Suite en el mismo dominio del cliente.
- A la información de la sala de reuniones de Azure se accede desde el administrador de Synappx.
- La API de Microsoft Graph obtiene la información y los archivos para Meeting de Microsoft Office 365. Los alcances de la API de Google obtienen la información y los archivos para Meeting de G Suite.

7. Etiquetas NFA de Synappx Go

Synappx Go utiliza etiquetas NFC especiales proporcionadas por Sharp o distribuidores autorizados, o que vengan integrados en determinados modelos de impresoras multifunción. Las etiquetas contienen un identificador único y son de solo lectura (no puede reprogramarse). Cada etiqueta solo puede asociarse a un dispositivo a la vez. Una vez configurado a un dispositivo (p. ej., una impresora multifunción o un PC de visualización) por el administrador a través de la aplicación móvil Synappx Go, cuando el usuario toca NFC, la etiqueta y la aplicación móvil identifican conjuntamente al usuario y al dispositivo asociado a la etiqueta y al dispositivo para permitir que Synappx Go utilice funciones como digitalizar documentos y enviarlos a un correo electrónico, liberar tareas de impresión, imprimir archivos almacenados en una nube o compartirlos a una pantalla.

8. Agente de impresoras multifunción de Synappx Go

El agente de impresoras multifunción de Synappx (incluido el software de liberación de impresiones) es un componente local del sistema Synappx Go instalado en un servidor o PC del cliente para facilitar las comunicaciones entre las impresoras multifunción habilitadas para Synappx Go y la nube de Synappx Go, y permitir casos de uso móviles y con NFC relacionados con las impresoras multifunción de Sharp. Synappx Go elimina la necesidad de aprender y tener que completar varios pasos en el panel frontal de la impresora multifunción para liberar de forma segura los trabajos de impresión de cualquier impresora multifunción de Synappx Go, imprimir archivos concretos almacenados en la nube y enviar archivos a destinos de digitalización favoritos. Los usuarios pueden ahorrar tiempo para las tareas de digitalización e impresión segura, además de reducir el riesgo de accesos no autorizados a sus trabajos de impresión.

El agente de impresoras multifunción de Synappx Go es necesario para permitir casos de uso de digitalización e impresión. Una de las funciones principales del agente es establecer un canal de comunicación seguro con la nube de Synappx. El agente interactúa con la nube para registrar y proteger las comunicaciones de los dispositivos y enviar o recibir mensajes entre el agente y las impresoras multifunción compatibles. Cada agente tiene un identificador único, que el sistema de nube de Synappx Go utiliza para identificar a qué agentes enviar mensajes. Los agentes escuchan mensajes mediante suscripción a su tema de identificación único y los servicios en nube envían mensajes mediante la publicación en dicho tema de identificación.

8.1 Instalación del agente de impresoras multifunción

Para instalar el agente de impresoras multifunción, se descarga el paquete de instalación personalizado desde el portal del administrador de Synappx Go con un archivo de configuración único para el cliente. El contenido del archivo de configuración está protegido por algoritmos de cifrado. Este paquete de instalación del agente de impresoras multifunción no está disponible desde un sitio web público y está vinculado a la cuenta específica del cliente. Para la mayor parte de las instalaciones de cliente, habrá un agente de impresoras multifunción instalado por centro del cliente que permitirá a un máximo de 50 a 100 impresora multifunción (dependiendo del número de usuarios y trabajos de impresión) usar las funciones de impresión y digitalización de Synappx Go. Los clientes que deseen utilizar más de 100 impresoras multifunción necesitarán instalar agentes de impresora multifunción adicionales.

Después de su instalación, para registrarse, el agente de impresoras multifunción envía su identificador único, junto con las credenciales de seguridad del agente a la nube de Synappx Go para su registro en el registro de dispositivos. La información almacenada en el registro de dispositivos incluye datos como el ID del dispositivo, el ID del inquilino y, para las impresoras multifunción, el agente de impresoras multifunción asociado a la impresora multifunción.

8.2 Comunicaciones del agente de impresoras multifunción

Todas las comunicaciones entre el agente de impresoras multifunción de Synappx Go y la nube de Synappx Go utilizan HTTPS (puerto 443) o el cliente de seguridad X.509 sobre MQTT. HTTPS se utiliza durante las comunicaciones de la instalación inicial entre el agente de impresoras multifunción de Synappx Go y la nube de Synappx Go, además de para enviar información de la impresora multifunción y cualquier información de error.

- Las claves privadas de X.509 del agente nunca abandonan el sistema en el que está instalado el agente, por lo que nunca se exponen como resultado de la transmisión a través de Internet.

- Todos los certificados X.509 del agente se firman con ayuda de los certificados de firma del cliente del agente. Los agentes solo se pueden autoregistrar si el certificado X.509 es firmado por su cliente asociado suscriptor del certificado.

Los servicios de nube de Synappx Go mantienen certificados de firma separados para cada cliente de Synappx Go. Así se garantiza que los agentes solo se aprovisionen dentro de su registro de inquilino asociado.

Tras aprovisionar automáticamente el agente en la nube de Synappx Go, incluidos los certificados de X.509, las comunicaciones entre el agente y la nube se realizan a través de conexiones MQTT seguras. Se utilizan certificados firmados por una CA raíz X.509 de Synappx Go. Los certificados firmados por una CA raíz proporcionan un nivel adicional de autenticación que certifica que el titular del certificado es quien dice ser. El uso de certificados X.509 ofrece la máxima seguridad en términos de autenticación del dispositivo, pues la clave privada de cada dispositivo agente no sale nunca del dispositivo y no se puede ver comprometida. El certificado de firma de la CA raíz del inquilino del agente de Synappx Go es generado por el servicio de aprovisionamiento de inquilinos de Synappx Go y se almacena en Azure Key Vault.

- Entre las ventajas de los certificados X.509 y MQTT, se incluye la posibilidad de que los agentes se suscriban solo a su propio tema de ID de dispositivo único. Como resultado, los agentes de Synappx Go reciben mensajes publicados ÚNICAMENTE en su ID de dispositivo respectivo. El agente no puede recibir contenido desde ningún otro terminal.

8.3 Requisitos del agente multifunción

El agente de Synappx Go se ha diseñado con los siguientes requisitos por la nube de Azure:

- Para que un dispositivo puede conectarse a la nube de Azure, DEBE registrarse.
- Para que un dispositivo pueda registrarse, el dispositivo DEBE aprovisionarse (por parte de un administrador del cliente).
- Para que un dispositivo pueda aprovisionarse, el dispositivo DEBE contar con certificados de seguridad (a través del sistema).

8.4 Descubrimiento de dispositivos del agente de impresoras multifunción

Para automatizar la recopilación de información sobre las impresoras multifunción (necesaria para configurar los servicios de las impresoras multifunción de Synappx Go), el agente de impresoras multifunción incluye capacidad para encontrar impresoras multifunción mediante la función de descubrimiento SNMP. La operación de descubrimiento se inicia automáticamente tras la instalación inicial del agente. El administrador introduce la IP inicial y final a través del portal del administrador que buscar. También puede volver a buscar a petición (esta búsqueda también es iniciada por el administrador a través de la consola de administración) utilizando el puerto 443. Como parte de este proceso, se recopila la siguiente información sobre la impresora multifunción y se envía a la nube de Synappx Go:

- El ID del agente de impresoras multifunción, el ID de la impresora multifunción que crea el sistema (p. ej., Sharp MX-C301W 63004882), el fabricante, el nombre del modelo, el número de serie, el nombre del dispositivo (si está establecido), la ubicación (si está establecida) y la dirección IP de la red.

8.5 Liberación de tareas de impresión y digitalización de documentos del agente de impresoras multifunción

Un administrador o un usuario puede configurar un controlador de impresora de Sharp para que apunte al servidor o PC de liberación de impresión/agente de Synappx Go. Al enviar trabajos al controlador de liberación de tareas de impresión, los archivos de impresión de los usuarios de Synappx Go con licencia se almacenan automáticamente en una carpeta para cada usuario del servidor o PC del agente. Los usuarios pueden liberar los archivos en cualquier impresora multifunción con etiqueta de Synappx configurada.

- Los archivos de impresión (en formato .prn) almacenados en el servidor se eliminarán automáticamente a las 24 horas.
- Los archivos .prn solo están visibles para los administradores autorizados con acceso al ordenador a través de protección normal con contraseña para el PC o el servidor.

La carga sobre la red del cliente dependerá de las tareas de impresión y digitalización del usuario de Synappx Go. Entre las cargas estimadas se incluye:

- Digitalizaciones a destinos favoritos (por usuario): se estima una media de 1 MB por documento digitalizado (puede variar)
- Impresiones seguras (por usuario y por trabajo): se estima una media de 1,2 MB por trabajo de impresión (podría variar)
- Impresiones de archivos en la nube (por usuario y por trabajo): se estima una media de 1,2 MB por trabajo de impresión (podría variar)

9. Agente de pantallas de Synappx Go

El agente de pantallas de Synappx es un componente local del sistema Synappx Go instalado en un servidor o PC de visualización del cliente para facilitar las comunicaciones entre los PC con Synappx Go habilitado y la nube de Synappx Go, y permitir el uso compartido desde dispositivos móviles y NFC a pantallas de Sharp. Synappx Go permite a los usuarios configurar de forma sencilla conexiones con todos sus almacenes en nube favoritos una vez y encontrar el archivo o los archivos deseados a través de los sitios para compartirlos o editarlos (en la mayoría de los almacenes en nube) en pantallas de Sharp, todo desde sus dispositivos móviles privados y con un sencillo toque (NFC) para descargar los archivos. Los usuarios ahorran tiempo que pueden dedicar a tareas de colaboración en torno al contenido del archivo, además de reducirse el riesgo de que otros participantes de la reunión pueden ver nombres de archivo confidenciales también almacenados en sus carpetas en la nube. Y varios usuarios pueden descargar y editar archivos (en la mayor parte de los casos) en el mismo PC de visualización para realizar tareas de edición en colaboración o comparar el contenido de los archivos.

9.1 Instalación del agente de pantallas

Para permitir la función de compartir a pantalla, el agente de pantallas de Synappx debe estar instalado en el PC o servidor de visualización de Windows. Una de las funciones principales del agente es establecer un canal de comunicación seguro con la nube de Synappx.

- El agente interactúa con la nube para registrar y proteger las comunicaciones de los dispositivos, y enviar o recibir mensajes desde y hasta el agente. Cada agente tiene un identificador único, que el sistema de nube de Synappx Go utiliza para identificar a qué agentes enviar mensajes.
- Los agentes escuchan mensajes mediante suscripción a su tema de identificación único y los servicios en nube envían mensajes mediante la publicación a dicho tema de identificación.

Para instalar el agente de pantallas, se descarga el paquete de instalación personalizado desde el portal del administrador de Synappx Go con un archivo de configuración único para el cliente. Este paquete de instalación del agente de pantallas no está disponible desde un sitio web público y está vinculado a la cuenta específica del cliente. Después de su instalación, para registrarse, el agente de pantallas envía su identificador único, junto con las credenciales de seguridad del agente a la nube de Synappx Go para su registro en el registro de dispositivos. La información almacenada en el registro del dispositivo incluye datos como el nombre del PC o el servidor, el ID único del PC o el servidor y el ID del inquilino.

9.2 Comunicación del agente de pantallas

Todas las comunicaciones entre el agente de pantallas de Synappx Go y la nube de Synappx Go utilizan HTTPS (puerto 443) o el cliente de seguridad X.509 sobre MQTT. HTTPS se utiliza durante las comunicaciones de la instalación inicial entre el agente de pantallas de Synappx Go y la nube de Synappx Go, además de para enviar cualquier información de error.

- Consulte X509 y otros detalles relacionados con las comunicaciones en la sección del agente de impresoras multifunción más arriba. El agente de pantallas tiene las mismas funciones de seguridad que el agente de impresoras multifunción allí descrito.

9.3 Uso compartido del agente de pantallas

Se han introducido las siguientes características adicionales de seguridad para la función de compartir a pantalla en el agente de pantallas:

- Una vez que el usuario ha configurado sus repositorios de almacenamiento en nube deseados (p. ej., SharePoint Online o Dropbox) a través de su dispositivo móvil, cuando accede a la función de compartir a pantalla, se comparten temporalmente uno o varios tokens de usuario seguros de la aplicación móvil de Synappx Go con una caché segura de la nube de Synappx. La caché solo resulta accesible mediante claves seguras. El token de usuario se retira de la caché de la nube de Sharp Synappx poco después del siguiente uso y el token de usuario no se descarga nunca a los agentes de pantalla.

- Cuando un usuario selecciona un archivo o archivos del centro de almacenamiento en la nube a través de la aplicación de Synappx Go para descargar al PC de visualización, la nube de Synappx genera una URL que incluye un ID de sesión para obtener el archivo o archivos seleccionados del usuario. Los archivos se abren automáticamente en el PC del agente de pantallas para su visualización o edición (en la mayor parte de los centros de almacenamiento). Los archivos se almacenan en una carpeta temporal en el PC de visualización.

    - Los archivos que se pueden descargar a través del servicio de Synappx Go para su visualización o edición se limitan a los siguientes:
        - Texto sin formato, archivos de Microsoft Office (Word, PowerPoint, Excel y OneNote), PDF, archivos de imágenes (JPEG, TIFF, GIF, BMP y PNG) y archivos de vídeo (MP4, AVI, WMV y MOV)
        - Nota: No se admiten archivos ejecutables ni de secuencia de comandos, y no pueden descargarse a través de este servicio.

    - Los archivos que se pueden descargar a través del servicio de Synappx Go para su visualización se limitan a los siguientes:
        - Para iOS, iCloud y almacenamiento de archivos locales: los mismos archivos listados arriba
        - Para los archivos de G Suite almacenados en Google Drive: Google Docs, Google Slides, Google Sheets, Google Drawing y Google Jamboard
        - Nota: No se admiten archivos ejecutables ni de secuencia de comandos, y no pueden descargarse a través de este servicio.

    - Si el usuario opta por guardar un archivo editable tras realizar cambios en el PC de visualización, se volverá a guardar en la misma ubicación de carpeta en la nube desde la que se descargó bien en forma de una nueva versión o con un nombre de archivo añadido (en función de la política de cada sitio de almacenamiento en la nube).

    - Si un usuario guarda un archivo compatible editable en la nube o cierra un archivo sin guardarlo, se eliminará de la carpeta del PC de visualización temporal.

    - Varios usuarios con licencias o aplicaciones de Synappx Go pueden cada uno descargar archivos de la nube al mismo agente de pantallas para visualizar, copiar y pegar contenido editable, y comparar archivos antes de volver a guardarlos en sus respectivos sitios de almacenamiento.

10. Seguridad corporativa

Sharp aplica un sólido programa de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de todos los recursos de información procesados o almacenados en el seno de los sistemas empresariales de Sharp. Sharp reconoce la rapidez a la que evolucionan y crecen los riesgos asociados a la protección de los recursos de información propios y de nuestros estimados socios empresariales, e investiga, revisa e invierte en contramedidas técnicas y de procedimiento para proporcionar garantías y seguridad. Un equipo de profesionales dedicado evalúa continuamente el entorno empresarial aplicando su competencia profesional para ampliar y mejorar continuamente su posición de seguridad con respecto a la información de Sharp. Además de estos esfuerzos internos, Sharp utiliza asociaciones estratégicas con proveedores de servicio líderes para probar, supervisar y auditar nuestros programas de seguridad de la información implementados.

11. Acceso a los datos del administrador de Sharp

Puede que los servicios de TI y asistencia de Sharp necesiten acceder ocasionalmente a sus datos para proporcionarle asistencia sobre cuestiones técnicas. Los permisos de acceso para este tipo de cuestiones se limitarán a los mínimos necesarios para resolver el problema. A los administradores de Sharp se les proporciona estrictos permisos basados en su función para garantizar la seguridad de los datos del cliente:

- Capacidad para ver y actualizar la información de cuenta del cliente, como el estado de la cuenta y la dirección de correo electrónico, pero no a los archivos del cliente
- Capacidad para ver el árbol de archivos y los nombres de archivo, pero no para ver ni descargar archivos concretos
- Los usuarios, administradores y administradores de los distribuidores de Synappx disponen todos de acceso adecuado a los elementos de su ámbito de autoridad y nada más. La administración del sistema está estrictamente controlada y limitada al personal autorizado de Sharp. Los administradores de Sharp solo pueden acceder a información crítica para la gestión del sistema. En ningún otro momento se permitirá a los usuarios del sistema acceder a la base de datos ni a otros componentes del sistema directamente.
- Nota: Los datos relacionados con los servicios de Synappx del cliente se eliminarán 45 días después de la fecha de finalización de la suscripción.

12. Política de privacidad de Sharp

Consulte las condiciones de uso y la política de privacidad del servicio de Synappx en:

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

13. Resumen

Migrar a servicios de reuniones y colaboración sobre la marcha basados en nube ofrece a las empresas una forma económica de ayudar a su personal cada día más móvil. Sin lugar a dudas, desarrollar un entorno de oficina con capacidad de respuesta, y adoptar la nube y la tecnología móvil es una tendencia que no tiene vuelta atrás.

Las organizaciones que adoptan servicios basados en la nube aprovechan al máximo todas sus inversiones en tecnología actuales, incluidos ordenadores, dispositivos móviles, sistemas de pantalla interactivos e impresoras multifunción. En combinación con los servicios basados en suscripciones de Synappx, la eliminación de gastos de capital relacionados con los recursos de TI internos reduce aún más el coste total de propiedad. Sin embargo, a algunos responsables de la toma de decisiones les cuesta asumir las implicaciones asociadas los despliegues en nube a la hora de equilibrar la comodidad con las cuestiones de accesibilidad y seguridad. Los servicios de Sharp Synappx ayudan a eliminar estas barreras con una arquitectura orientada a la seguridad y sinergia de hardware y software, que permite desarrollar grupos de trabajo ágiles, capaces de responder con rapidez a las demandas empresariales.

www.sharp.es

SHARP

Be Original.