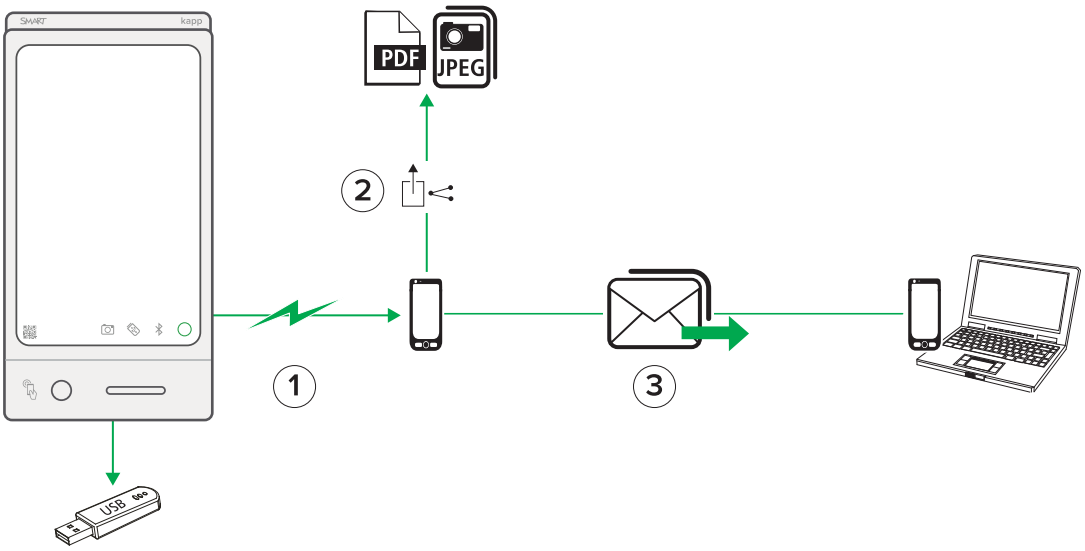
Información sobre seguridad

SMART kapp

SMART kapp® incluye características de protección de datos diseñadas para mantener el contenido controlado de forma predecible. En este documento se explican las características de seguridad que SMART kapp emplea para mantener sus datos más seguros.

Seguridad de los datos de un extremo a otro

La arquitectura de seguridad de SMART kapp emplea prácticas de seguridad muy conocidas estándares en el sector con el fin de proteger sus datos mientras se comparten entre la pizarra SMART kapp, un dispositivo móvil, el correo electrónico o servicio de terceros y las sesiones de uso compartido. De este modo, se logra que sus datos estén seguros de un extremo a otro.



1 Cómo protege SMART kapp los datos desde la pizarra hasta un dispositivo móvil

Para proteger la información que usted escribe en la pizarra, la pizarra tiene las siguientes características de seguridad:

Memoria interna

La pizarra tiene su propia memoria interna, donde se almacena temporalmente su información. Al borrar la pizarra, la tinta digital queda permanentemente eliminada de la memoria de la pizarra.

NOTAS

- Al hacer instantáneas presionando **Captura** en la pizarra, los datos no se guardan en la memoria interna de la pizarra.
- La única forma de guardar instantáneas sin tener que conectar un dispositivo móvil es conectar una unidad USB directamente al puerto USB de la pizarra.

Sincronización Bluetooth®

La pizarra utiliza sincronización Bluetooth para comunicarse con su dispositivo móvil. No se conecta directamente a ninguna red. Eso significa que no tiene que preocuparse por ninguna interrupción de la seguridad de la red que puedan afectar a la comunicación entre su dispositivo móvil y la pizarra.

NOTA

Aunque la conexión Bluetooth entre su dispositivo móvil y la pizarra no requiere una conexión de red, su dispositivo móvil sí necesitará estar conectado a una red para iniciar la sesión compartida o compartir cualquier instantánea de la sesión.

Cada pizarra se conecta con un solo dispositivo móvil cada vez y tiene un código QR exclusivo, etiqueta NFC y ID de la pizarra. Estos identificadores exclusivos garantizan que, al sincronizar su dispositivo móvil escaneando el código QR, pulsando la etiqueta NFC o introduciendo manualmente la ID exclusiva de la pizarra, la comunicación entre el dispositivo sincronizado y la pizarra sea más segura.

La sincronización entre su dispositivo móvil y la pizarra emplea una conexión Bluetooth cifrada para evitar cualquier interceptación. SMART kapp protege esta sincronización Bluetooth utilizando el método estándar en el sector “Secure Simple Pairing” (SSP). Para proporcionar todavía más protección, SMART kapp añade una capa de cifrado Advanced Encryption Standard (AES) de 128 o 256 bits, criptografía asimétrica de curva elíptica y encapsulado de claves para la conexión Bluetooth, lo cual elimina de forma eficaz el riesgo de interceptación de datos inalámbricos.

2 Cómo asegura SMART kapp las instantáneas compartidas

Al hacer instantáneas presionando **Captura** en la pizarra o en la aplicación SMART kapp, sus datos se guardarán en la biblioteca de sesiones de la aplicación. SMART kapp no comparte instantáneas guardadas con otras aplicaciones sin su permiso. Sus instantáneas solo se comparten si las exporta desde la aplicación SMART kapp a través del correo electrónico o un servicio de terceros, como las aplicaciones en la nube que tiene en su dispositivo móvil. Cuando comparte instantáneas por correo electrónico o un servicio de terceros, la protección de datos estándar que ofrece su proveedor de correo electrónico o servicio de terceros ayuda a proteger la información. Después, los destinatarios pueden guardar sus instantáneas en los dispositivos locales. Al guardar estas instantáneas, el cifrado de su dispositivo local o la protección en espacios aislados específica de su sistema operativo* ayuda a mantener los datos seguros.

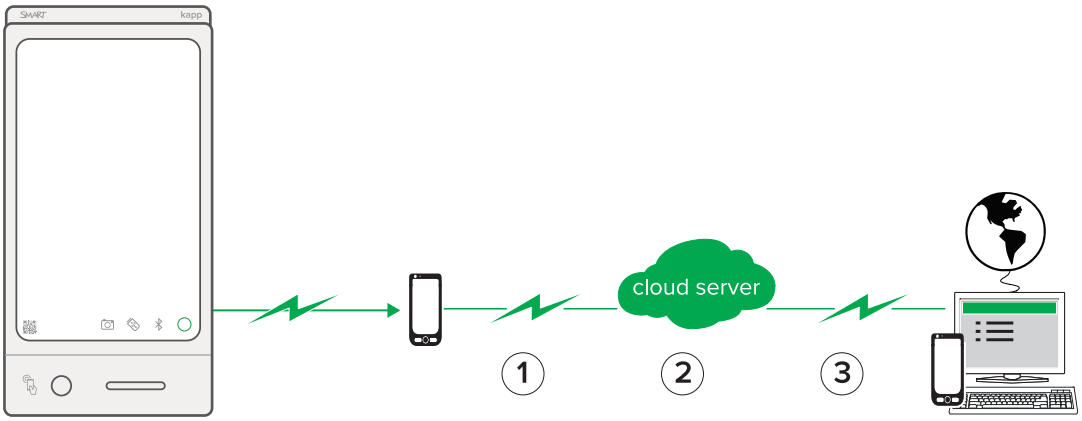
3 Cómo asegura SMART kapp las invitaciones a sesiones compartidas

Cuando inicie una sesión compartida desde la aplicación SMART kapp puede enviar la URL de la sesión a otros participantes por correo electrónico o cualquier otro servicio de terceros. Cuando las demás personas reciba la invitación para visualizar su sesión, presionarán o harán clic en la URL para ver su pizarra y las instantáneas de la sesión en su explorador web. SMART kapp protege esta URL mediante protocolos de comunicación cifrados (HTTPS). Cuando envía la invitación a una sesión por correo electrónico o un servicio de terceros, la protección de datos estándar que ofrece su proveedor de correo electrónico o servicio de terceros ayuda a proteger la información.

Seguridad de los datos durante las sesiones compartidas

Durante una sesión compartida, sus datos se transfieren desde la pizarra a su dispositivo móvil mediante una conexión Bluetooth segura y, después, desde su dispositivo móvil hasta el servidor de la nube kappboard.com y, en último lugar, al explorador del participante de la sesión compartida.

*Por protección en espacios aislados se entiende un mecanismo de seguridad que protege frente a programas potencialmente dañinos que pueden contener un virus o código perjudicial mediante la restricción del acceso del programa a los recursos del dispositivo local (por ejemplo, los descriptores de archivo o la memoria de un dispositivo).



Cómo asegura SMART kapp los datos durante las sesiones compartidas

Para aumentar la seguridad de su información confidencial en todo momento durante la transmisión desde su dispositivo móvil hasta el explorador de un participante, SMART kapp protege sus datos de las siguientes formas:

1	**En tránsito hacia el servidor en la nube**	SMART kapp solamente usa protocolos de comunicación cifrados (HTTPS) para enviar información al servidor en la nube de kappboard.com.
2	**El servidor de la nube**	El servidor de la nube de SMART kapp está alojado en Amazon Web Services (AWS) y utiliza un cifrado estándar en el sector proporcionado con AWS para proteger sus datos en la nube. Los datos de sucesión están disponibles desde la nube solamente durante esa sesión compartida. Una vez que la sesión compartida termine, solamente los participantes de dicha sesión podrán descargar una copia de la misma desde la ventana del explorador que utilizaron para visualizar la sesión. Después de terminar una sesión y de que todos los participantes hayan cerrado sus exploradores, sus datos dejan de estar accesibles de cualquier forma desde el servidor de la nube.
3	**En tránsito hacia el explorador web del participante**	La URL que los participantes utilizan para unirse a su sesión compartida está asegurada mediante HTTPS. Esta URL contiene un identificador alfanumérico exclusivo creado específicamente para cada una de las sesiones. Si tiene una suscripción premium a la aplicación, puede convertir esta URL en estática (es decir, se utilizará la misma URL para todas sus sesiones compartidas) o en dinámica (cada URL nueva será exclusiva y no secuencial). Los suscriptores a la aplicación premium también pueden proteger las sesiones con un PIN. **NOTA** Si desea obtener más información sobre las diferencias que hay entre la aplicación premium y la básica, visite smartkapp.com/app.

Preguntas frecuentes sobre seguridad

¿Qué ocurre si pierdo mi dispositivo móvil y dentro tenía imágenes guardardas JPGE de instantáneas o archivos PDF?

La seguridad del sistema operativo de su dispositivo móvil protege los datos de la sesión guardados en la biblioteca interna de su dispositivo móvil. Los dispositivos Android utilizan cifrado y los dispositivos iOS utilizan protección de espacios aislados. Los datos que haya guardado en su dispositivo móvil estarán protegidos con la seguridad que proporcione automáticamente su dispositivo o mediante las características de seguridad que haya configurado en el mismo (como, por ejemplo, un PIN). Si se pierde su dispositivo, siga los procedimientos de seguridad de datos de su empresa para pérdida de dispositivos que contengan información confidencial.

¿La pizarra requiere un software antivirus?

No, la pizarra no es vulnerable a los virus porque no tiene un sistema operativo tradicional. El único software que se puede ejecutar en la pizarra es el firmware de SMART kapp.

¿En qué casos debo usar el puerto USB de la pizarra? ¿Están seguros los archivos que se guardan en la unidad USB?

Si no desea conectar un dispositivo móvil o pizarra, puede insertar una unidad USB en el puerto USB proporcionado en la pizarra con el fin de guardar las instantáneas que vaya tomando durante la sesión. Estas instantáneas se guardarán en su unidad USB como archivos PDF no asegurados. Algunas unidades USB incluyen sus propias características de seguridad (como cifrado o protección con contraseña), que pueden ayudarle a proteger sus datos si se perdiera la unidad USB. También puede cifrar su unidad USB o añadirle una contraseña a cada archivo manualmente.

¿Es necesario que haya abierto algún puerto específico en la pizarra para poder trabajar?

No, SMART kapp solamente utiliza la red del dispositivo móvil sincronizado para comunicarse y no requiere ninguna red adicional.

¿Conserva SMART kapp alguna información personal, como la Id. del usuario, la dirección IP o el número de teléfono?

No, SMART kapp no guarda ninguna información personal identificable.

¿SMART kapp proporciona informes o auditorías sobre el uso de la pizarra?

Actualmente, SMART kapp no ofrece la posibilidad de crear informes públicos.

smarttech.com/support
smarttech.com/contactsupport