

SMARTSHIELD



Tecnología integrada de seguridad
en impresión

Para impresoras ColorWave y PlotWave

Canon

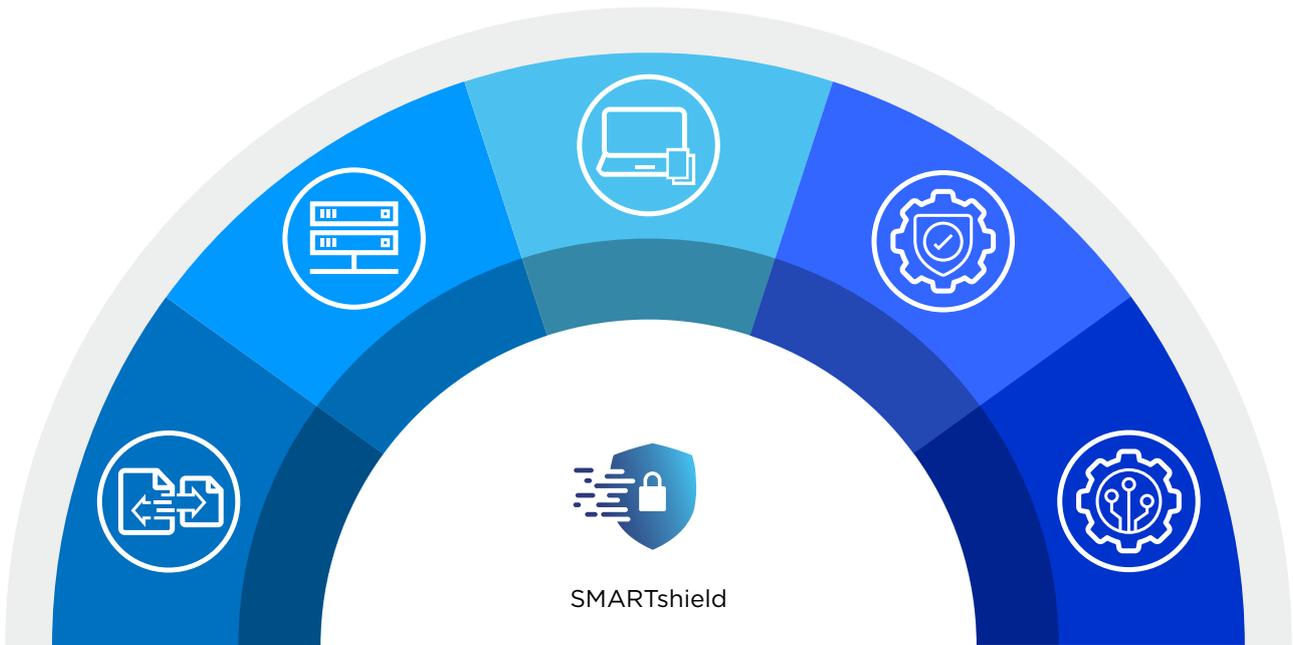
SEGURIDAD DE IMPRESIÓN DE PRIMERA CLASE

Nuestras impresoras de gran formato líderes en el mercado abordan los problemas de seguridad que preocupan a los usuarios de documentos técnicos que gestionan datos confidenciales de los clientes.

SMARTshield es un conjunto de funciones de seguridad integradas en el flujo de trabajo de impresión de los sistemas PlotWave y ColorWave más recientes. Están diseñadas para mantener la seguridad de tus sistemas, hoy y en el futuro.



ColorWave 3800



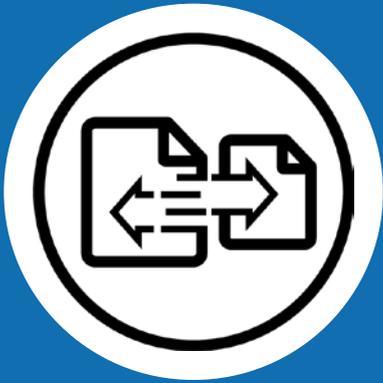
Ahora más que nunca, tanto las empresas como las organizaciones gubernamentales con impresoras de gran formato necesitan proteger la información más importante y confidencial de sus oficinas y redes. Esto incluye la información que se envía desde lugares de trabajo individuales y otros dispositivos a la impresora, así como los datos almacenados en la misma. También es fundamental que los sistemas estén protegidos contra cualquier acceso no autorizado a los datos de impresión, a la información impresa y a la propia infraestructura de TI del usuario final a través de las impresoras. Por estas razones, las organizaciones necesitan una impresora de gran formato segura que le haga la vida más sencilla al administrador de TI, a los usuarios y a la gestión en sí.

SMARTshield es una tecnología de seguridad de impresión completamente integrada que está presente en todas nuestras impresoras de gran formato, diseñada especialmente para satisfacer dichas necesidades.

Esta tecnología incluye varias medidas de seguridad diseñadas para mantener la seguridad de los datos y de la información.

Gracias a SMARTshield, evitarás cualquier riesgo de seguridad en cualquier etapa del flujo de trabajo.

SMARTshield te protege tanto ahora como en el futuro.



ENVÍO SEGURO

Protege los datos al enviar archivos a tu impresora desde cualquier dispositivo.

Gracias a las aplicaciones de flujo de trabajo ClearConnect, los usuarios pueden enviar los archivos desde su ordenador o cualquier dispositivo móvil. Debido a este nivel de flexibilidad y acceso móvil, es fundamental que los datos valiosos se envíen de forma segura a la impresora en cualquier momento y desde cualquier dispositivo.

- Compatibilidad con Internet Protocol Security (IPSec)
- Compatibilidad con IPv6 y IPv4
- HTTPS





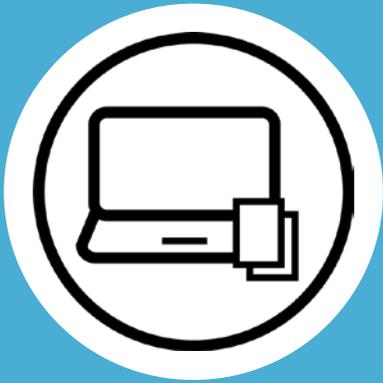
ALMACENAMIENTO Y ELIMINACIÓN SEGUROS

Protege los datos confidenciales almacenados en el disco duro de la impresora.

Es importante proteger los datos confidenciales almacenados en la impresora contra robos o filtraciones accidentales de la empresa o del departamento. SMARTshield cifra los datos y restringe el acceso mediante la identificación de los usuarios para garantizar la seguridad de todos tus datos. Al eliminar correctamente los datos, los usuarios pueden estar seguros de que sus archivos confidenciales están fuera del alcance de compañeros no autorizados.

- Eliminación segura de archivos
- Destrucción de datos electrónicos
- Disco duro extraíble
- Arranque seguro
- Cifrado de datos
- Destrucción del disco duro al final del contrato





AUTORIZACIÓN

La autorización de usuarios de SMARTshield restringe el acceso a archivos confidenciales a usuarios no autorizados.

Además, al solicitar la autenticación de los usuarios, puedes mantener un control más ajustado de tus actividades. También puedes limitar las funciones y los protocolos a los que pueden acceder, así como supervisar los gastos de cada usuario.



- Bloqueo del acceso al panel de control
- Impresión segura mediante credenciales de dominio (Active Directory)
- Impresión segura mediante tarjeta inteligente (solo para el lector)
- Archivos de impresión disponibles solo en tu buzón inteligente
- Escaneo a tu carpeta de inicio personal
- Impresión desde tu carpeta de inicio personal
- Desactivación de puertos e interfaces
- Software de terceros, como uniFLOW



PREVENCIÓN DE ATAQUES INFORMÁTICOS

Uno de los mayores desafíos de seguridad a los que se enfrentan todas las empresas es mantener a raya a los hackers. Debido a la gran cantidad de datos valiosos que se imprimen, es fundamental restringir el acceso a la impresora, así como a los datos almacenados en el disco duro.

Obviamente, quieres asegurarte de que no se realice un uso fraudulento de tu impresora ni se utilice contra tu red. SMARTshield aborda el desafío de la prevención de ataques informáticos de varias maneras:

- Desactivación de protocolos no utilizados
- SNMP v3
- Compatibilidad con IEEE 802.1x
- Antivirus McAfee (opcional)
- McAfee Application Control en listas blancas (opcional)





SEGURO TANTO AHORA COMO EN EL FUTURO

La seguridad nunca es estática. Los hackers tratan constantemente de encontrar nuevas formas de acceder a tu información valiosa. Por lo tanto, SMARTshield se ha diseñado para mantener la seguridad de dicha información tanto ahora como en el futuro.

Y, por supuesto, nuestros especialistas de la seguridad supervisan de forma constante los riesgos más recientes para ayudarte a garantizar que tus datos e impresoras estén a salvo. Las funciones actuales incluyen:

- Software de control Windows 10 IoT Enterprise LTSC
- Compatibilidad al menos hasta el año 2029 o más
- Actualizaciones de seguridad del control remoto
- On Remote Service

Comprendemos la preocupación que tienes por la seguridad, así que hemos combinado un conjunto de funciones para afrontar los riesgos a los que se enfrenta tu empresa en todas las etapas del flujo de trabajo. Tanto ahora como en el futuro.



Canon es tu compañero para lograr un entorno seguro de impresión.

COMPATIBLE CON SMARTSHIELD

SMARTshield está integrado en los siguientes sistemas:

ColorWave 3600



ColorWave 3800



Serie PlotWave 3000



Serie PlotWave 5000



PlotWave 7500



SMARTSHIELD

EN DETALLE

ENVÍO SEGURO

Compatibilidad con Internet Protocol Security (IPsec)

Compatibilidad con IPv6 y IPv4

HTTPS

El IPsec es un protocolo que ofrece autenticación, integridad y confidencialidad de los datos en la comunicación de red entre el controlador y otros dispositivos.

Protocolo Internet, versión 4 (IPv4) es uno de los protocolos principales de los métodos de interconexión de redes basados en estándares de Internet y otras redes con conmutación de paquetes. Utiliza direcciones de 32 bits. IPv6 es la versión más reciente y utiliza direcciones de 128 bits, por lo que puede abarcar muchos más dispositivos.

Para impedir que el tráfico de red de WebTools Express, Publisher Express y Publisher Select con el protocolo HTTP sea interceptado ni modificado, se puede utilizar el protocolo HTTPS en lugar del tráfico HTTP no con el controlador. Además, se pueden integrar en el controlador los certificados seguros por parte de una autoridad de certificación para evitar un ataque de intermediario, en el que un usuario malintencionado, que casualmente se encuentra en la ruta al servidor del controlador, finge ser dicho controlador.

ALMACENAMIENTO Y ELIMINACIÓN SEGUROS

Eliminación segura de archivos

Destrucción de datos electrónicos

Disco duro extraíble

Arranque seguro

Cifrado de datos

Destrucción del disco duro al final del contrato

Elimina automáticamente los trabajos de impresión, escaneo y copia del buzón inteligente tras el tiempo definido por el usuario. La eliminación de archivos es segura cuando se activa la destrucción de datos electrónicos.

La destrucción de datos electrónicos es una función de seguridad que permite al sistema sobrescribir los datos de impresión/copia/escaneado de cualquier usuario tras haberlos eliminado. Esta función evita la recuperación de cualquier dato que haya eliminado el usuario, incluidos el contenido y los atributos de los archivos, en caso de robo del disco duro.

El kit de disco duro extraíble opcional permite a los administradores la extracción física del disco duro interno del dispositivo para almacenarlo en un lugar seguro fuera del horario de trabajo. El disco se podrá volver a instalar fácilmente para usarlo durante el horario de trabajo normal.

El arranque seguro es una norma de seguridad que garantiza que el dispositivo se inicia utilizando únicamente un software seguro. Cuando la impresora se enciende, el software de control comprueba el distintivo de cada parte del software de arranque.

El cifrado del disco duro del controlador POWERsync cifra todos los archivos del mismo (incluidos el sistema operativo y todos sus datos; cifrado del espacio usado). El mecanismo de cifrado se basa en un módulo de plataforma segura (TPM) y un mecanismo BitLocker de Microsoft conforme con la certificación FIPS 140-2. Se utiliza el método de cifrado AES 256.

Bajo demanda del cliente, el disco duro interno del controlador POWERsync se puede eliminar y destruir de forma física para garantizar que no quedan restos de sus datos de impresión en la impresora una vez sale de sus instalaciones.

AUTORIZACIÓN

Bloqueo del acceso al panel de control

Impresión segura mediante credenciales de dominio (Active Directory)

Impresión segura mediante tarjeta inteligente (solo para el lector)

Archivos de impresión disponibles solo en tu buzón inteligente

Escaneo a tu carpeta de inicio personal

Impresión desde tu carpeta de inicio personal

Desactivación de puertos e interfaz

Software de terceros como uniFLOW

Cuando se activa la función de gestión de acceso, solo se puede acceder al panel de control del usuario tras el desbloqueo mediante credenciales de dominio o tarjeta inteligente.

Los trabajos de impresión «sensibles» que envía el propietario del trabajo no se imprimen hasta que este los autentica en el panel de usuario del sistema con las credenciales de usuario correctas y los libera para su impresión.

Los trabajos de impresión «sensibles» que envía el propietario del trabajo no se imprimen hasta que este los autentica en el panel de usuario del sistema pasando e insertando la tarjeta inteligente y los libera para su impresión.

Al desactivar la «impresión directa» en WebTools Express, el archivo de impresión permanecerá en tu buzón inteligente hasta que se active desde el panel de usuario de ClearConnect o WebTools Express. Esta función impide que otros trabajadores de la oficina obtengan la impresión accidentalmente.

La función Escanear a carpeta de inicio está disponible mediante el método de autenticación de nombre de usuario y contraseña. Tras introducir la autenticación en el panel de la impresora, el usuario podrá escanear un archivo a su directorio de inicio en la red según lo haya configurado en su cuenta en el MS Windows Active Directory.

La función Imprimir desde carpeta de inicio está disponible mediante el método de autenticación de nombre de usuario y contraseña. Tras introducir la autenticación en el panel de la impresora, el usuario podrá imprimir desde su directorio de inicio en la red según lo haya configurado en su cuenta en el MS Windows Active Directory.

Para proteger el controlador POWERsync contra accesos no autorizados, se desactivan todos los puertos e interfaces de red sin usar.

Los sistemas de impresión PlotWave y ColorWave que cuentan con una interfaz de usuario se pueden integrar en entornos uniFLOW del cliente. Esto proporciona a los usuarios funcionalidades adicionales, lo que les ayuda a controlar y reducir los gastos de impresión y copia, aumentar la seguridad de los documentos y a mejorar la productividad de los empleados.



PREVENCIÓN DE ATAQUES INFORMÁTICOS

Desactivación de protocolos no utilizados

Los administradores de red reciben la capacidad de configurar los protocolos específicos accesibles. Como resultado, la comunicación de dispositivos no deseados y los accesos al sistema mediante protocolos de transporte específicos se pueden bloquear de forma eficaz.

SNMP V3

Versión segura de SNMP que proporciona autenticación e integridad entre la estación de gestión de red (NMS) y las impresoras gestionadas.

Autenticación de dispositivo IEEE 802.1X

Proporciona un mecanismo de autenticación basado en puertos (según el estándar IEEE802.1X) que permite a un dispositivo ser autenticado por una autoridad central para comunicarse en la red con los demás dispositivos.

Antivirus McAfee (opcional)

Posibilidad opcional de instalar el software antivirus McAfee en el controlador POWERSync como medida de protección adicional contra virus.

McAfee Application Control en listas blancas (opcional)

Función de seguridad opcional que se activa mediante licencia. Al activarla y habilitarla, crea una lista detallada de todos los archivos del controlador y evita cualquier cambio no autorizado, ya sea malware, un virus o usuarios no autorizados. Comprueba de forma continua la integridad de los archivos en la lista, y bloqueará cualquier modificación o cambio no autorizado.

SEGURO TANTO AHORA COMO EN EL FUTURO

Software de control Windows 10 IoT Enterprise LTSC

El controlador POWERSync de la impresora utiliza Windows 10 IoT Enterprise LTSC.

Compatibilidad hasta el año 2029 o más

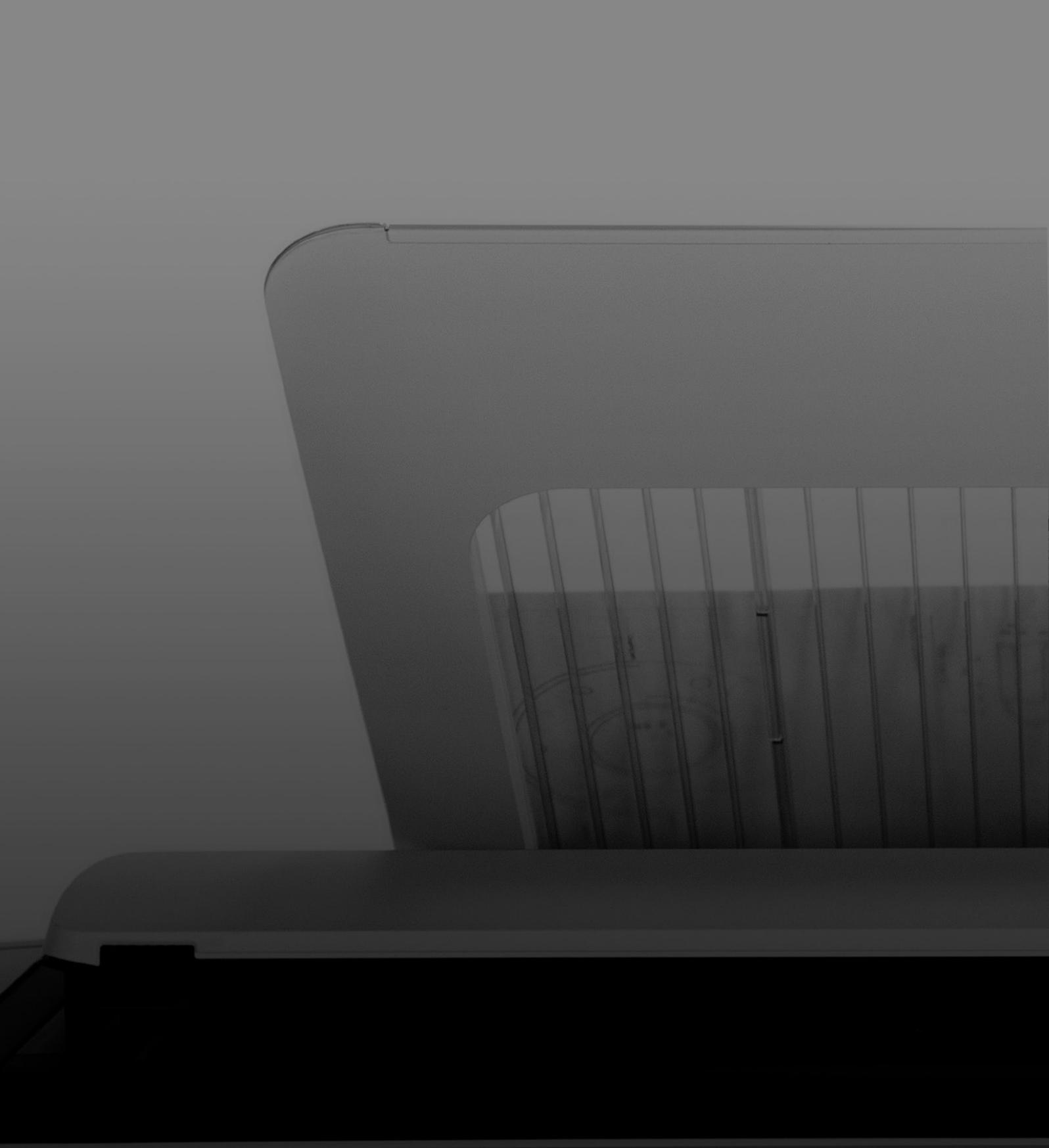
Microsoft garantiza la compatibilidad de Windows 10 IoT Enterprise LTSC hasta el año 2029 o más. Por lo tanto, proporcionará las actualizaciones de seguridad durante este periodo.

Actualizaciones de seguridad del control remoto

Mediante WebTools Express, el administrador del sistema puede cargar e instalar las actualizaciones de seguridad de forma remota. De esta forma se logra una reacción rápida y un tiempo de actividad elevado, ya que no es necesario que el técnico de servicio realice ninguna interacción física con la impresora.

On Remote Service

Canon ha desarrollado On Remote Service para garantizar el mayor tiempo de actividad de tu sistema Canon. Como aplicación integrada del controlador, este servicio te ofrece asistencia a distancia, incluido el diagnóstico remoto, la lectura remota del medidor y la asistencia remota. Los resultados que se obtienen son una mayor disponibilidad del sistema, administración reducida, mejores e inmediatas soluciones de servicio, tiempos de respuesta más rápidos y, sobre todo, tranquilidad.



© 2020 Canon Production Printing

Canon es una marca comercial registrada de Canon Inc. Arizona es una marca comercial o marca comercial registrada de Canon Production Printing Netherlands B.V. Las marcas comerciales restantes pertenecen a sus respectivos propietarios y se reconocen en este documento.

Queda prohibida la copia, modificación, reproducción o transmisión en cualquier forma o por cualquier medio, electrónico, manual o de otro tipo, de cualquier parte de esta publicación sin el consentimiento previo y por escrito de Canon Production Printing. Las ilustraciones y las imágenes de resultados de impresión están simuladas y no se refieren necesariamente a los productos y servicios ofrecidos en cada mercado local. El contenido de esta publicación no debe ser interpretado como un seguro o garantía con respecto a propiedades o especificaciones determinadas ni de rendimiento técnico o idoneidad para aplicaciones particulares. El contenido de esta publicación puede estar sujeto a cambios ocasionales sin previo aviso. Canon Production Printing no será responsable de ningún daño directo, indirecto o consecuente de carácter natural ni de las pérdidas o gastos que resulten del uso de los contenidos de esta publicación.

Canon

Canon España, S.A.
Avda. de Europa, 6
28108 Alcobendas (Madrid)
Tel.: 91 538 45 00
Fax: 91 564 01 17
canon.es
Spanish edition