PaperCut

23.0

NUEVAS FUNCIONES

- **Habilitar la impresión para VDI**
- **Nuevas funciones que son seguras por defecto**
- **Habilitación de las mejores prácticas de autenticación**

Habilitar la impresión para VDI

La infraestructura de escritorio virtual (VDI) ya no es solo para las empresas Fortune 500. Organizaciones de todos los tamaños están utilizando la virtualización de escritorio para mejorar la seguridad de las aplicaciones y los datos, reducir los costos de infraestructura, empoderar a los trabajadores remotos e híbridos en todo el espectro de dispositivos BYO y reducir los costos relacionados con la impresión. carga de apoyo.

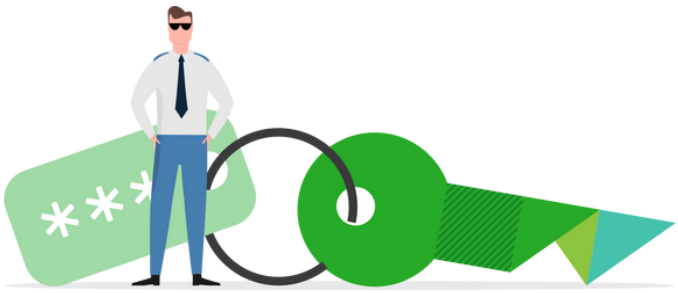
Print Deploy ahora ofrece la capacidad completa de impresión de PaperCut MF para garantizar que sus usuarios obtengan la impresora adecuada, con el controlador adecuado y en el lugar correcto cuando utilicen las plataformas VDI más populares del mundo, como Citrix, VMware Horizon, Azure Virtual Desktop y Servicios de escritorio remoto de Microsoft (RDS).

Esto es un gran problema en el sector sanitario, donde los escritorios virtuales son omnipresentes entre los proveedores de servicios clínicos, de diagnóstico y de distribución que utilizan la impresión para iniciar flujos de trabajo en papel críticos para los pacientes. VDI es igualmente importante en organizaciones empresariales distribuidas y de gran tamaño, donde proporcionar a cada usuario las impresoras que necesita, dondequiera que necesite trabajar, es esencial para la productividad..

ACOX

PaperCut MF | 23.0

Nuevas características de seguridad



Las amenazas a la ciberseguridad han seguido evolucionando, y nosotros también. PaperCut MF 23.0 trae mejoras adicionales de nuestro extenso programa de mejora de la seguridad, que implica revisiones continuas de arquitectura y código internas y externas, pruebas de penetración a gran escala y consultas con expertos en ciberseguridad.

Si bien la mayoría de estas mejoras se realizan detrás de escena, reduciendo silenciosamente las posibles superficies de ataque y migrando las configuraciones de seguridad principales de las interfaces web a alternativas más seguras, actualizando dependencias, etc., verá otras.

Los administradores ahora deben volver a autenticarse antes de cambiar la contraseña de un administrador o crear nuevas cuentas de administrador. Todas las contraseñas almacenadas en el archivo security.properties, al que solo un administrador puede acceder localmente, ahora se cifran automáticamente.

Habilitación de las mejores prácticas de autenticación

La autenticación multifactor (MFA) se ha convertido en la mejor práctica para los sistemas de línea de negocio, ya que ofrece protección en capas contra el acceso no autorizado.

Al requerir múltiples métodos de verificación, MFA reduce significativamente el riesgo de violaciones, incluso si una contraseña está comprometida.

PaperCut MF ahora admite flujos MFA para todas las interfaces web de administrador y usuario cuando se utiliza Azure AD como proveedor de identidad.