PaperCut

23.0

NOVIDADES

- **Ativação de impressão para VDI**
- **Novos recursos seguros por padrão**
- **Habilitando as melhores práticas de autenticação**

Ativação de impressão para VDI

A infraestrutura de desktop virtual (VDI) não é mais apenas para empresas Fortune 500. Organizações de todos os tamanhos estão usando a virtualização de desktops para melhorar a segurança de aplicativos e dados, reduzir custos de infraestrutura, capacitar trabalhadores remotos e híbridos em todo o espectro de dispositivos BYO e reduzir a carga de suporte relacionada à impressão.

O Print Deploy agora traz a capacidade completa de habilitação de impressão do PaperCut MF para garantir que seus usuários obtenham a impressora certa, com o driver certo, no lugar certo ao usar as plataformas VDI mais populares do mundo, como Citrix, VMware Horizon, Azure Virtual Desktop e Microsoft Remote Desktop Serviços (RDS).

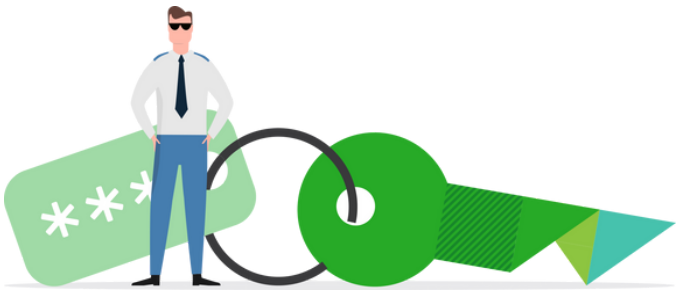
Este é um grande negócio na área da saúde, onde os desktops virtuais são omnipresentes entre os prestadores de serviços clínicos, de diagnóstico e de distribuição que utilizam a impressão para iniciar fluxos de trabalho em papel críticos para os pacientes. A VDI é igualmente grande em organizações empresariais dimensionadas e distribuídas, onde fornecer a cada usuário as impressoras de que precisam, onde quer que precisem trabalhar, é essencial para a produtividade.

ACOX

PaperCut MF | 23.0

Novos recursos de segurança

As ameaças à segurança cibernética continuaram a evoluir, e nós também. PaperCut MF 23.0 traz melhorias adicionais do nosso amplo programa de melhoria de segurança, que envolve arquitetura interna e externa contínua e revisões de código, testes de penetração em grande escala e consulta com especialistas em segurança cibernética.



Embora a maioria dessas melhorias esteja nos bastidores, reduzindo silenciosamente possíveis superfícies de ataque e migrando as principais configurações de segurança das interfaces da web para alternativas mais seguras, atualizando dependências e assim por diante, outras você verá.

Os administradores agora devem autenticar novamente antes de alterar a senha de um administrador ou criar novas contas de administrador. Todas as senhas armazenadas no arquivo security.properties, que só podem ser acessadas localmente por um administrador, agora são criptografadas automaticamente.

Habilitando as melhores práticas de autenticação

A autenticação multifator (MFA) tornou-se a prática recomendada para sistemas de linha de negócios, oferecendo proteção em camadas contra acesso não autorizado.

Ao exigir vários métodos de verificação, a MFA reduz significativamente o risco de violações, mesmo que uma senha seja comprometida.

O PaperCut MF agora dá suporte a fluxos de MFA para todas as interfaces web de administração e usuário quando o Azure AD é usado como provedor de identidade.