Enable Secure Access and Protect Network-Connected Printers

Organizations that efficiently manage access to printers not only affect the bottom line but reduce data loss and security risks.

Organizations spend valuable time and resources working to eliminate external security attacks, but often don't protect one of their most vulnerable internal tools, Multi-Function Printers (MFP), from potential security leaks. By securing access to MFPs and network connected copiers using rf IDEAS® credential readers, enterprises can begin to easily manage sensitive data and track employee usage.

Easily Validate Authorization:
Requiring authentication to activate printing opens the door to better, more secure print management

Your organization uses employee credentials to access doors and restricted areas; now it is easy to also use the same credential to provide authentication and access to printers. As part of the secure print solution, the reader emulates a keyboard and passes the credential ID and/or site code to the backend network for authentication. The information is instantaneously provided to and validated by the company's employee database, Active Directory or Lightweight Directory Access Protocol (LDAP).

Protect Important Information:
Reduce data breaches by controlling printer access

Printer data breaches via an unsecure printer or MFP on the network are common, with 63% of businesses admitting to this type of data breach.* And, without proper controls at the printer, unauthorized access to MFP functions can occur. A secure print software solution that incorporates a credential reader captures not only the ID of the employee accessing the printer, but the time, location and source of the print request. Secure or pull print solutions also ensure confidential documents are not printed and left in the output tray until the person physically waves their credential at the reader connected to the printer. With a credential reader solution for authentication, organizations can better secure information in multi-printer, multi-location configurations and minimize data breach risks to network-connected copiers. Adding information regarding the employee who accesses the printer/copier provides valuable cost center and historical information. Organizations that efficiently manage access to printers not only affect the bottom line but reduce data loss and security risks.

Streamline Printing Operations:
Eliminate the need to enter PIN codes, user names and passwords, reducing identification errors

When a rf IDEAS credential reader, plus print management software, is connected to a single-use or multi-function printer, an employee simply sends a document for printing to a print queue on a print server. With a secure pull printing solution, the employee taps their card or smartphone credential on the reader at the MFP or copier. The credentials are validated, the print queue becomes available to the employee, and the document is released to be printed.

Trust begins here.™

rf IDEAS Readers

MANAGE USER ACCESS TO SECURE MFPS

rf IDEAS' USB and Ethernet readers are easy to integrate with your current credential and printer solutions, and support virtually every proximity and contactless smart card on the market. Our readers are available in various form factors making them suitable for internal integration such as in recessed compartments or external mounting.

Meet Security and Compliance Requirements – Sensitive documents no longer sit in the output tray unattended, reducing unauthorized exposure.

Save Costs Every Day – Paper and toner usage is immediately reduced by not automatically printing unwanted documents.
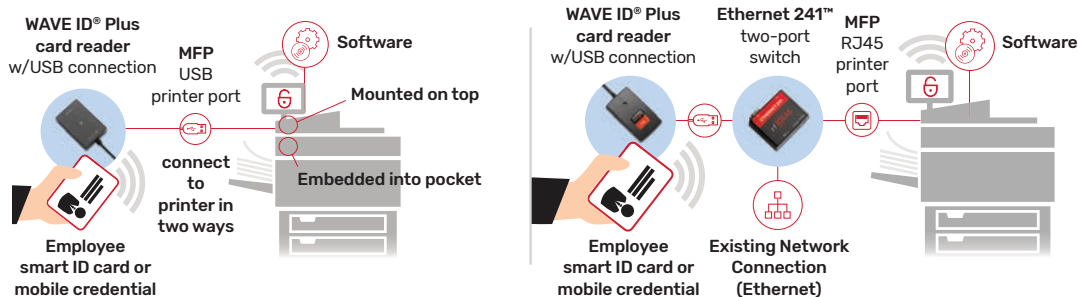
Improve Sustainability Goals – Managed print solutions help encourage everyone to avoid unnecessary printing thereby reducing toner and paper usage costs.

Eliminate Print Boundaries – A print job can be sent from a home office in Chicago, for example, and held in queue on a printer server. The employee travels to another office in Minneapolis, authenticates at that printer and "pulls" the print job.

Data Protection Regulations

Is your printer network and printing policy compliant with HIPAA, PCI or the GDPR? Output of confidential documents, especially those with personal data, to the wrong printer or an unsecured output tray increases the risk of data privacy related violations. Violation of data protection regulations can result in expensive investigations, loss of reputation and financial penalties. Reduce the risk of personal data getting into the wrong hands with a secure print authentication solution.

Secure Print Configurations

WAVE ID® Plus card reader w/USB connection
MFP USB printer port
Software
Mounted on top
Embedded into pocket
connect to printer in two ways
Employee smart ID card or mobile credential

WAVE ID® Plus card reader w/USB connection
Ethernet 241™ two-port switch
MFP RJ45 printer port
Software
Employee smart ID card or mobile credential
Existing Network Connection (Ethernet)

For more information on how rf IDEAS can help you improve your secure print operation, visit **www.rfIDEAS.com**

PARTNERS

rf IDEAS products are an integral part of numerous industry-specific applications. Through our carefully vetted global network of rf IDEAS partners, we ensure that customers have convenient access to secure solutions of proven quality, performance and value. Our partners have the technologies, expertise and support they need to offer the industry's most advanced identification and authentication capabilities for practically any application.

To find a partner or to join the rf IDEAS ENGAGE® Partner Program and incorporate rf IDEAS technologies into your solutions, visit **https://www.rfIDEAS.com/partners**

ENGAGE
rf IDEAS Partner Program

4020 Winnetka Avenue, Rolling Meadows, IL 60008   //   Toll Free: (866) 439-4884   //
Voice: (847) 870-1723   //   Fax: (847) 483-1129   //   Email: sales@rfIDEAS.com   //   rfIDEAS.com

AB-405C