PRINTERON
PRINT SIMPLY ANYWHERE

PrinterOn Enterprise | Express Security

How PrinterOn uses enterprise-grade security methods to provide secure print across your infrastructure

White Paper

Contents

Executive Summary..1

Glossary..2

PrinterOn Enterprise and Express Overview..3

PrinterOn Document Submission..6

Authentication..9

Processing and Encryption..11

Print Release..15

Using an MDM with PrinterOn..18

FAQ..19

Executive Summary

PrinterOn has been providing secure mobile printing solutions since 2001 and has vast experience with both cloud deployment and on-premise deployment. As a result, today PrinterOn offers the broadest range of solutions to address any type of secure mobile printing scenario. This includes the requirements of a secure 100% on premise solution for the enterprise, large or small.

This discussion paper will provide an overview of the PrinterOn on-premise secure mobile print editions: Enterprise and Express. Both use the same architecture and use the same security methods for deployment on one or multiple physical or virtual servers installed in the end customer’s trusted network. For the same information regarding the PrinterOn Hosted Edition, please refer to the companion paper.

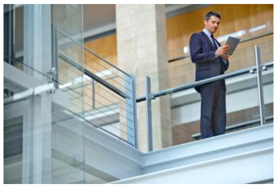
This document is intended for Enterprise Architects, Solution Architects, IT groups or Sales Engineers who require deeper knowledge of the PrinterOn platform and how it provides a secure printing solution for the enterprise. PrinterOn Enterprise and Express provide multiple levels of security at every point of the mobile print workflow from submission to release. This security is described in the following sections:

- Glossary
- PrinterOn Overview
- Document Submission
- Authentication
- Processing and Encryption
- Print Release
- Using an MDM with PrinterOn
- Physical Security

Glossary

Term	Description	Resides Where?
PrinterOn Enterprise	Secure mobile printing solution enabling printing from any device, any platform on any network without the installation of print drivers. Suitable for large and complex needs. Components can be deployed and replicated anywhere in the trusted network	Customer Trusted Network
PrinterOn Express	Simpler and easier version of Enterprise using the same platform and security but more suitable to smaller organizations with simpler needs. Its components are bundled and run on one physical or virtual server in the trusted network	Customer Trusted Network
PrinterOn Directory	A service component that stores all information about printers including drivers.	Customer Trusted Network
Print Delivery Gateway (PDG)	Serves as a protocol gateway to PrinterOn Enterprise printers allowing jobs to be submitted using a number of different methods including iOS print, Google Cloud Print and Windows print protocols	Customer Trusted Network
Central Print Services (CPS)	Primary entry point for all requests submitted to the PrinterOn Enterprise Server	Customer Trusted Network
PrintAnywhere Server (PAS)	Facilitates the receiving and printing of documents and the delivery of the processed documents to a specified printer	Customer Trusted Network
Print Delivery Hub (PDH)	Uses Internet Printing Protocol (IPP) over SSL (Secure Sockets Layer) to provide a secure method of transferring print jobs over disparate networks and through firewalls	Customer Trusted Network
Print Delivery Station (PDS)	Bridges the PrinterOn delivery infrastructure with the physical printer or print queue. Pulls print jobs from PDH and releases them to enabled printers	Printer's LAN
PrintWhere® Driver	Enables traditional File>Print workflow for Windows laptops, desktops and Surface® tablets without installing printer drivers	User's Windows PC or Surface® Tablet

PrinterOn Enterprise and Express Overview



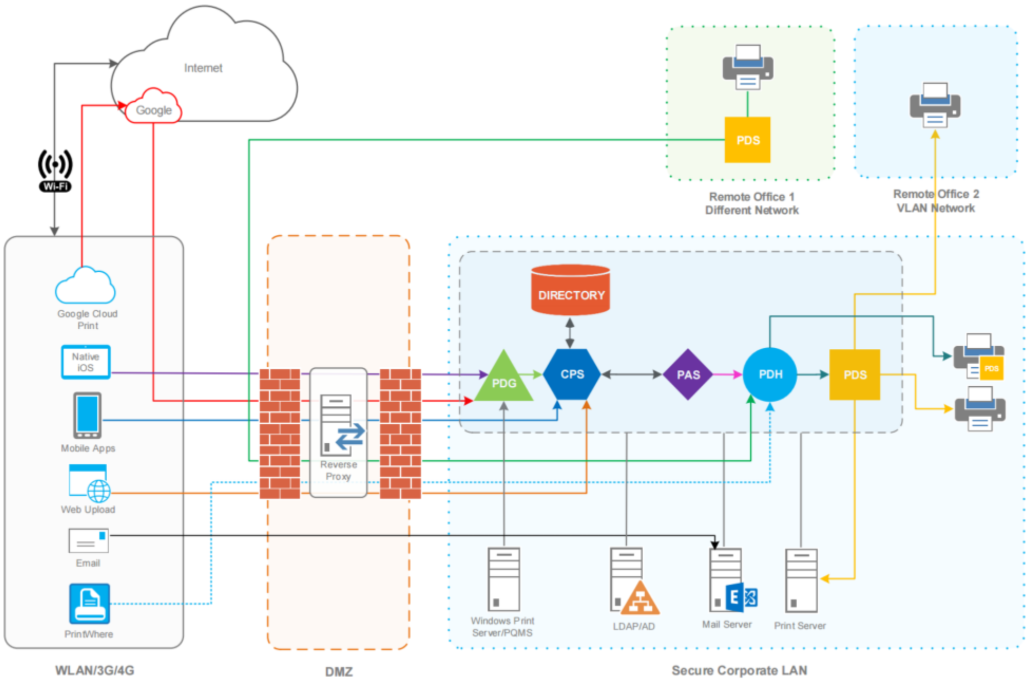
PrinterOn Enterprise and Express make it possible for employees and guests to securely print to corporate printers on a trusted network without having to download print drivers or connect to the secure corporate network.

PrinterOn Enterprise and Express deliver a high level of security by ensuring all documents are submitted, processed, and managed completely within the trusted network. All data is encrypted end-to-end, from submission to delivery, in transit and at rest.

PrinterOn Enterprise and Express include multiple components, all deployed on the trusted network. These components deliver services for printer discovery, document submission, rendering, and delivery. It is this combination of components that makes PrinterOn Enterprise and Express uniquely powerful, flexible, *and secure.* Users are free to securely submit print jobs from anywhere, render them securely inside the trusted network, and deliver them securely anywhere. ***At no time do documents leave the trusted network using PrinterOn Enterprise or Express*.**

PrinterOn Enterprise Architecture

To understand PrinterOn Enterprise and Express security, it is important to understand how its components deliver services for the end-to-end print workflow. All services operate in the background, seamless to the end user. The diagram on the next page depicts a high level overview of the components that constitute the PrinterOn Enterprise and Express services. Most services are port-configurable (except for Directory communications via SSL on port 443). The defaults for each service are noted in the section below.



Central Print Services (CPS)

Central Print Services is the primary entry point for all requests submitted to PrinterOn Enterprise and Express. CPS is responsible for providing a centralized interface for all secure printing, including end-user web print, mobile app printing as well as for third parties who develop integrations to PrinterOn for custom print services.

In addition to providing print service access, CPS also provides a web-based administrative console allowing administrators to manage their service and control how jobs are received and then submitted to the other components.

PrintAnywhere® Services (PAS)

PrintAnywhere is the print engine at the center of the on-premise PrinterOn solution. PrintAnywhere provides job management and print processing of documents as part of PrinterOn print services. The PrintAnywhere service comprises a number of software services that facilitate receiving and printing documents and delivery to a PrinterOn-enabled printer, print management service or Print Delivery Station (PDS). PAS communicates by default on ports 443/631. This is configurable.

Print Delivery Station (PDS)

Print Delivery Station's role is to provide a bridge between the PrinterOn delivery infrastructure and the physical printer, print queue or print management service. PDS secured communications are over SSL and based on the industry standard IPP protocol. Optional job data encryption using PrinterOn extensions is available in addition to using IPP over SSL. PDS communicates by default on ports 443/631. This is configurable.

Print Delivery Hub (PDH)

In some enterprise deployments, delivering print jobs directly from PrinterOn to desired printers on disparate networks may not be possible through the PDS due to network configuration. In other cases, leveraging a simple and rapid deployment of print devices will benefit from the centralized installation of PDH. In this arrangement, print jobs are delivered to the PDH. The PDS services communicate with PDH to detect and download the print jobs. PDH communicates by default on ports 443/631. This is configurable.

In this case the PDH services must be accessible over the network by the PDS servers. The PDH services can be installed in a central network operating center. Access to the PDH will be configured such that the PAS, desktop PrintWhere® clients and PDS deployments can access the PDH server. This configuration generally minimizes network changes, as the PDH is the only service requiring access to incoming network traffic.

Please note that PDH services are available only with Enterprise Edition and not Express.

Architectural Flexibility

PrinterOn Enterprise has the ultimate flexibility for these main components to be placed literally *anywhere* in the enterprise network. All components are deployed behind the enterprise firewall by default but can also be deployed in a DMZ, or even in an external data center. Furthermore, each can be scaled out horizontally for volume or set up in a redundant configuration. This means that no matter the existing enterprise network architecture, PrinterOn Enterprise can be integrated ***without network infrastructure changes***. *Distributing PrinterOn components is only available with Enterprise Edition. PrinterOn Express bundles all these components on a single physical or virtual server.*

Summary of Port Configuration for PrinterOn

PrinterOn Component	Port Configuration
PrintWhere Driver	ports 443/631
PDG (Print Delivery Gateway)	port 6310 using the IPP protocol
PAS (PrintAnywhere Server)	default on ports 443/631
PDH (Print Delivery Hub)	default on ports 443/631
PDS (Print Delivery Station)	default on ports 443/631

PrinterOn Document Submission

One benefit of PrinterOn is its range of document submission methods. Multiple methods means IT can decide which methods to enable for their specific deployment and then let users decide which method suits them best for the particular workflow.

Email - Users submit their print jobs by simply forwarding an email to a printer's email address. This can be done from any computer or mobile device that supports email. The user will receive an email response with release codes, one for the printed body of the email and one for each of the email attachments.

Emails sent from users can be received by a mailbox on a central email server or relayed to a dedicated email server just for print jobs. The PrinterOn email print server acts like a standard mail client communicating with the designated mail server, minimizing its impact on existing email servers. This also enables PrinterOn to leverage trusted and proven 3rd party email security services such as TLS, virus and spam filters.

It is the PrintAnywhere Server (PAS) that monitors a single mailbox to receive and process email print requests. The goal of this deployment approach is to isolate email printing and the PAS from the corporate mail server. PrinterOn can provide a number of deployment scenarios to assist in finding the right deployment for your organization.

Communication ports for email vary by specific email services deployment.

Native iOS – In many cases Apple Bonjour is not a viable option for administrators to connect users between even simple network configurations. The limitations of Bonjour and, as a result, native print for iOS is compounded further when introducing many users and many printers and more complex networks. The result is many times unmanageable or sometimes impossible.

PrinterOn Enterprise and Express provide a secure way for users to print on or off the corporate network using the native print functionality of iOS devices. The Print Delivery Gateway (PDG), can be used to provide the same benefits of the native iOS print workflow, with or without Bonjour. PrinterOn accomplishes this by integrating the native iOS print authentication with Enterprise LDAP/AD, role-based access control, and guest printing rules to inform the iOS devices how and where to find printers on a network.

To provide the ability to print from an iOS device without Bonjour requires a couple of easily accessible tools and information. The configuration is accomplished by "pushing" printer profiles to an iOS device.

Web Print – Documents may also be submitted by uploading documents through the secure web portal. After authenticating, users simply select the desired printer and then upload the document they would like to print.

The web printing service is provided as part of CPS which uses SSL providing additional security. From CPS documents are forwarded to PAS on the trusted network to be rendered and printed. Web submission communicates on Port 443/80. This is configurable.

Mobile Applications – Users may also search for printers and securely submit print jobs to Centralized Print Services (CPS) using PrinterOn mobile applications for iOS or Android. There are also versions of these applications available which are specifically "wrapped" to be deployed through popular Mobile Device Management (MDM) providers' platforms. PrinterOn mobile apps also integrate authentication with LDAP/AD, role-based access control, and guest print rules. Since CPS uses SSL, the mobile applications benefit from the same security as web submission. Mobile apps communicate on ports 443/80. This is configurable.

PrintWhere® Desktop Print Driver – For Windows-based desktop PCs, laptops or Microsoft Surface® tablets users can also securely submit print jobs using the PrinterOn PrintWhere driver. The PrintWhere driver enables users to print using the standard “File | Print” workflow and, with the help of PDH, allows them to securely deliver their print job to any remote print destination set up within PrinterOn Enterprise, even if the destination printer is on a completely different network. The PrintWhere driver provides additional security capability by first compressing, and then encrypting print data on the user’s computer before delivering it to the desired remote print destination. Finally, PrintWhere provides administrative convenience by simplifying configuration to remote printing locations. PrintWhere communicates on ports 443/80. This is configurable.

Google Cloud Print – As an option, for those wanting to bridge the gap between existing Google Cloud Print (GCP) workflows and PrinterOn Enterprise or Express, the PDG service allows users to print seamlessly from any of the GCP client applications (ChromeOS, Chrome Browser etc.) to PrinterOn Enterprise or Express-enabled printers. It also enables administrators to create new GCP printers and map them to PrinterOn printers. *This submission method is entirely optional and does require an Internet connection to communicate with Google Cloud Print services*.

The combination of PrinterOn Enterprise or Express and Google Cloud Print enables management of BYOD environments where devices do not connect exclusively to the existing print infrastructure. Google Cloud Print communicates using HTTPS/XMPP over ports 443/5222.

Print Queue Monitoring Service (PQMS) – The Print Queue Monitoring Service enables jobs submitted to standard Windows print server queues to be delivered to remote printers throughout the PrinterOn Enterprise infrastructure bridging the gap between existing Windows print queues and PrinterOn Enterprise. It allows users to submit jobs using standard Windows workflows (File>Print) leveraging the capabilities of PrinterOn Enterprise to deliver the pre-rendered data content to printers located anywhere in the world. This feature is not available with PrinterOn Express, only Enterprise. PQMS communicates on the PrinterOn PDG port instead of the usual TCP/IP ports. *Please note that PQMS services are available only with Enterprise Edition and not Express*.

IPP Connector – The PDG IPP Connector enables jobs submitted using IPP to be delivered to remote printers through the PrinterOn infrastructure.

The IPP Connector helps bridge the gap between the existing IPP-based client and server workflows and PrinterOn. It allows print users to submit jobs using a variety of clients such as Oracle ERP and Apple Mac® on OS X®. IPP is transported over HTTPS

Authentication

PrinterOn Enterprise and Express provide a number of authentication options. They can use existing LDAP or Active Directory configurations to authenticate users when printing. Authentication services are managed centrally by CPS. CPS is configured to communicate with an existing LDAP or AD server and authenticate users accessing the print services providing a central location for integrating all print methods. This approach allows print jobs to be associated with a user’s existing network login name and enables PrinterOn to be easily integrated into other print management and auditing services that may be deployed in an organization. PrinterOn is a flexible and modular system that can adapt to your specific requirements through the use of authentication APIs available for the service.

Email

There are two options to authenticate or authorize email print users. Both allow email print jobs to be tracked by third party print management solutions, if implemented.

The first option allows PrinterOn to “lookup” a user’s network identifier based on the user’s email address. The server will use the existing LDAP/AD configuration to locate a user based on their email address. The user’s network login will be returned by the server and included with print jobs.

Another option is to configure the service to respond to print jobs with an email containing a link to an authentication web page. Before allowing a job to proceed, the user must access the page and authenticate themselves. The authentication web page is provided by CPS and uses the existing LDAP/AD configuration to authenticate users.

Native iOS

Native iOS printing on its own does not offer enterprise-integrated user authentication. This is just one of the reasons why it is not considered a true enterprise-grade printing solution.

By deploying PrinterOn Enterprise or Express with PDG, user authentication against AD or LDAP is provided as part of the native iOS print workflow.

Mobile Applications

PrinterOn mobile applications for iOS and Android are able to leverage the same LDAP/AD services as other users. The user will be authenticated prior to submitting their print jobs. The user account name will be used as the network login included with print jobs.

Web Submission

Before accessing print services, users are prompted to enter LDAP/AD credentials. CPS validates the credentials using the configured settings before allowing the user to continue.

PrintWhere Driver

Users printing using the PrintWhere driver will automatically be presented with an authentication page for their print jobs. Prior to completing the print request the user will authenticate themselves against the LDAP/AD server using CPS as the intermediary.

Google Cloud Print

After submitting a document for print, the user is authenticated in Google using Gmail or Google Business accounts. That user info is delivered to PrinterOn. Optionally, authentication can take place against a local AD or LDAP where email addresses are matched with internal users. PrinterOn Enterprise or Express then processes the job and delivers it to the printer, print queue or print management server providing secure release.

PQMS (Print Queue Monitoring Service)

Since the Windows print workflows do not offer any means to collect user information and the print queues are normally made accessible only to privileged users, it is expected that the PrinterOn Enterprise service will NOT be required to authenticate the users. Consequently, this workflow is **ONLY** applicable when guest printing is enabled for the printer or authentication is disabled in CPS.

IPP

The IPP connector is designed to deliver print jobs generated by third-party IPP clients and print servers to designated printers located in remote locations. Since the user authentication is already completed through the third-party IPP print server, PrinterOn Enterprise and Express only verifies that the printer does not require authentication before accepting the job data and delivering it to the destination printer. The user's identify can be delivered along with the print job, as part of the request.

Access Control Lists (ACLs)

As an alternative to LDAP/AD authentication PrinterOn provides the ability to add unique Access Control Lists (ACLs) to each PrinterOn-enabled printer. You can add email domains (for email printing only) or individual users using a PrinterOn registered email address. Users may discover and use printing services as described above without the need for an external authentication service.

Processing and Encryption

On-Device Security

Significant efforts have been made to ensure a high degree of security while using the PrinterOn mobile applications for iOS and Android. This includes both on-device storage and network security.

The PrinterOn mobile apps store all user and account information used within the application in the most secure and safest manner possible. This includes a combination of both OS-specific security capabilities as well as PrinterOn specific enhancements.

Account information is encrypted and stored using vendor recommended secure storage, such as the iOS Keychain. In addition to the OS specific tools, PrinterOn additionally encrypts information prior to saving within the OS secure encrypted services, providing two levels of encryption.

Network Security

The PrinterOn Mobile application ensures that all communication is done securely and works with the user to ensure they are informed of their network activity. Users will be notified whenever connecting any discovered services using a self-signed certificate to ensure users are aware of the service identity.

Print Data Encryption

PrinterOn Enterprise or Express can be configured to leverage certificates to generate public/private key data encryption for data at rest. For example, a user uploads a Word document through web print. The job is securely delivered to the PrintAnywhere service using SSL. Once documents are received by PAS, they are rendered and converted to a printable form.

The print data is then compressed and encrypted using 128-bit AES encryption. A unique AES encryption key is generated for every printed job processed by PAS. Finally, the Print Delivery Station (PDS) releases the job to the printer. The PAS communicates to the PDS using SSL. Every PDS service instance generates a unique RSA 2048-bit public and private key pair. The print data AES key is encrypted using the RSA key-pair and is delivered alongside the print data to the PDS. This scheme effectively creates two levels of encryption for every print job.

Print Data Delivery

At its core, PrinterOn Enterprise and Express rely on the Directory service, which will be discussed in more detail further on in this document. The Directory service provides information regarding every printer managed by PrinterOn. This includes settings such as printer model, printing options and location information. Every printer stored in the Directory has a unique and static 12-digit identifier. When configuring PDS, this printer identifier is used to associate the physical printer with a PrinterOn's "virtual printer". When installing the Print Delivery Station software, the user is prompted to provide their PrinterOn administrative credentials.

This information in combination with a unique software serial number is used to ensure that a job sent to a PrinterOn printer can only be accessed by the device or software that has been configured to do so.

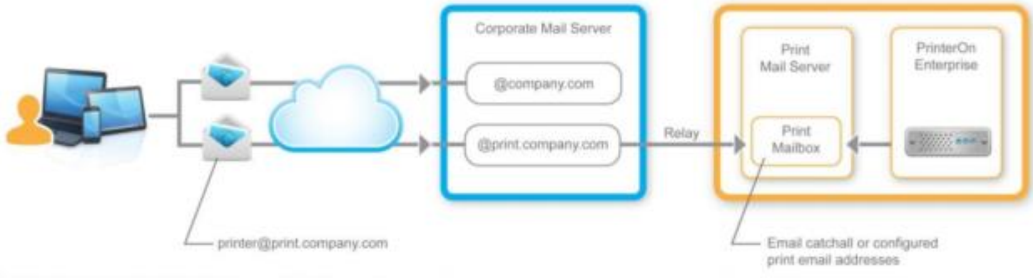
Documents delivered to PDS remain encrypted until a user enters their secure and private release code. By leveraging PrinterOn public/private key encryption technology with private keys stored in the release software, only the PDS that manages the selected printer is capable of decrypting the print job.

Email Security

PrinterOn Enterprise and Express only perform the most basic validation of the email address and domain. It is typically the responsibility of the upstream email server and configured SPAM software to ensure the validity of the incoming email addresses prior to being delivered to PrinterOn. Enterprise and Express email printing is one where PrinterOn simply acts as a mail client much like Outlook or any other mail client. Like these clients, they assume the mail server is providing a level of security prior to delivering the messages. This approach allows PrinterOn to be flexible while leveraging existing SPAM or anti-virus software.

Recommended Email Message Routing Configuration

The PrintAnywhere Server monitors a single mailbox to receive and process email print requests. The diagram below illustrates a recommended deployment and configuration for supporting email printing. Its design is intended to isolate email printing and the PrintAnywhere server from the corporate mail server. PrinterOn can provide a number of deployment scenarios to assist in finding the right deployment for your organization.



The PrinterOn Directory Service

The PrinterOn Directory service is a component used by Enterprise and Express to store information about each printer including drivers and is used in processing every print job.

How PrinterOn Enterprise and Express Utilize the PrinterOn Directory

When the PrinterOn Enterprise or Express receives a print job, it contacts the Directory service and provides the PrinterOn printer name for the job. The Directory returns configuration info for the specific printer in order to render and print the job. This info was entered by the system administrator upon initial system configuration.

With this configuration info, all secure services including Central Print Services (CPS) and remote print release servers may quickly and easily know how to render and release a print job without having to communicate with each other. The Directory info retrieved includes:

- Printer make and model and the appropriate driver (if required)
- Administrator-configured finishing options including color settings, duplex options, available paper sizes, job cover page
- Optionally, additional service URLs required to integrate with third party authentication/authorization services including alternate network locations used to deliver the generated print data.
- This may include alternate network locations if pushing print data directly to a release client or using the Print Delivery Hub (PDH) delivery services to deliver print jobs across disparate networks.

In order to retrieve exact details for the specific installation, this info is also sent:

- Software license serial number, version, and operating system
- PrinterOn printer name for the print job
- Optional finishing information supplied by the job submitter including duplex and paper size. This information helps determine exactly what information is returned.
- Job submission method indicating email, mobile app or web upload.
- Some user information if additional reporting is desired. *Sending this information is optional and can be disabled*.

Identifying Info Sent to the Directory

PrinterOn Enterprise and Express may be easily configured to *block* sending any user identifying information to the Directory. Then the only information sent is:

- The name of the mobile application used to submit the print job
- The version of the mobile application used to submit the print job

In addition, if using the optional Hybrid Cloud deployment option PrinterOn Enterprise and Express may be easily configured to *block* sending *any* document information to the PrinterOn Directory as well.

By configuration, PrinterOn Enterprise and Express may *optionally* send to the Directory:

- The software name that submitted the print job (if third party mobile application)
- The format of the document printed (such as Word or PDF)
- The number of pages printed for the document
- The application used to process the document.

When a job has finished printing some information is sent to the Directory regarding the print job. In most cases the information delivered is about the final state of the job such as whether it succeeded or not. Other information about a print job and its specific details may be minimized as a config option within the software.

Print Release

For each document submitted, a secure release code is generated. The release code is used much like a password for each job. When the user enters the release code, PDS determines whether a job is available for printing. The user is informed whether a job has been found and asks the user to confirm whether they wish to release the print job.

PrinterOn provides a number of solutions for secure document release:

- Remote release from a mobile device
- Print device release (“PrinterOn Embedded Agent”)
- Release using a 3rd party print management system

- PrinterOn PrintValet keypad device

Remote Release from a Mobile Device

Remote Release

Through the integrated remote job release feature of the PrinterOn mobile apps, users can release documents directly from their mobile device. When reviewing a printed job, the user will be presented with a “Release” option to choose to release their job.

Touch ID Support (iOS 8 and later only)

Devices using iOS 8 or later can leverage the additional security of protecting their Release Codes, and release remotely with the help of Apple’s Touch ID. After tapping the “Unlock Release“ button, users will be prompted to provide their Touch ID. As with all Touch ID interfaces, users may also provide their iOS access code.

Print Device Release (“PrinterOn Embedded Agent”)

Through technology partnerships with Brother, Ricoh, and Samsung, PrinterOn Release Agent software is directly embedded on specific printer and MFP models from these manufacturers. This enables users to release documents directly on the print device just as they would if they were using standard network printing. Secure release is done through release codes, or PINs or swipe cards if using an integrated 3rd party print management system.

Release Using a 3rd Party Print Management System

The primary goal of integrating secure mobile print with print management is ensuring a user’s information and identity is correctly linked with their print job throughout the entire print process from submission, to authentication, to job release. PrinterOn Enterprise and Express includes a broad range of techniques to ensure that a user’s identity is properly collected and communicated to the installed print management system.

PrinterOn works best when using the same Active Directory or LDAP server as the print management system. PrinterOn Enterprise and Express will extend traditional authentication and authorization to all its supported printing methods. By providing the print management system with the necessary user information, PrinterOn can extend the existing tracking and auditing capabilities to include new workflows such as:

- User-based auditing and tracking
- Guest print auditing and tracking
- Device-based auditing and tracking
- Mobile app print auditing and tracking
- Email print auditing and tracking

Release via PrintValet Keypad

The network PrintValet keypad network device provides users with the ability to release their documents securely using PrinterOn release codes. The keypad can be connected to any printer or MFP, adding secure release capabilities to any device. A 4-10 digit release code is provided for every document submitted. Only those with the code can access and print their documents.

Using an MDM with PrinterOn

In addition to the standard PrinterOn mobile apps, PrinterOn also provides SDK-integrated applications for industry-leading MDM platforms. This integration involves adding libraries and frameworks to the standard PrinterOn app. By providing an SDK integration, administrators and organizations can benefit from increased security and control including:

- Improved data loss protection through containerization
- User authenticated print job tracking and auditing
- Greater analytics
- Improved compliance

PrinterOn Enterprise and Express and the PrinterOn mobile apps work in conjunction with MDM platforms to provide secure end-to-end mobile printing for users. PrinterOn provides the enterprise with control over print workflows and security from beginning to end, much like an MDM does with mobile devices and the applications on them. PrinterOn and your MDM work as logical extensions of each other with the MDM managing devices on the network and PrinterOn layering secure print workflows on top, connecting networks and enabling mobile users to print securely.

PrinterOn mobile apps offer two levels of MDM integration: Basic MDM Integration with Express and Basic or Advanced MDM Integration with Enterprise. Both Basic and Advanced provide the ability to control the distribution and configuration of the SDK-wrapped PrinterOn mobile apps for iOS and Android. Advanced Integration takes that one step farther by also integrating the PrinterOn secure mobile printing service infrastructure with the MDM vendor’s secure mobile gateway.

FAQ

Q: Who uses PrinterOn Enterprise and Express?

A: PrinterOn Enterprise and Express Editions have been reviewed, validated and approved by many “Fortune 500” security conscious accounts in industries such as financial services, law firms, pharmaceuticals and retail.

Q: Where does my document go between the time it is submitted to when it comes out of the printer?

A: The document is submitted to the PrinterOn software running on one or more servers on your trusted network. Documents are transmitted directly from a user’s device to the on-premise server for processing. That server is responsible for identifying the file type, the driver to be used for rendering and encryption. From there, the document is delivered to an instance of Print Delivery Station (PDS) which also resides on your trusted network. The Print Delivery Station communicates with the printer, Windows shared queue or managed print queue to deliver the job data for output. In other words, the documents never leave your trusted network.

Q: If documents are not released for print, what happens to them?

A: Jobs are retained within Print Delivery Hub (PDH) or Print Delivery Station (PDS) for 72 hours by default. This value is configurable by you, the customer. These components are deployed and managed within the trusted network. Once expired, the jobs are purged from the server and no longer available to print.

Q: How is encryption handled on the mobile device?

A: The PrinterOn mobile apps store all user and account information used within the application in the most secure and safest manner possible. This includes a combination of both OS-specific security capabilities as well as PrinterOn specific enhancements.

Account information is encrypted and stored using vendor recommended secure storage, such as the iOS Keychain. In addition to the OS specific tools, PrinterOn additionally encrypts information prior to saving within the OS secure encrypted services, providing two levels of encryption.

Q: We have policies that prevent certain applications from using ports 443, etc. Can PrinterOn use other ports?

A: Yes, we can modify any port used internally however the Directory service requires access over port 443.

Q: How does our current reverse proxy configuration work with PrinterOn Enterprise and Express?

A: PrinterOn Enterprise and Express have been successfully deployed with many commercially available reverse proxy servers as well as a number of freely available open source solutions and use industry standard HTTPS web services for communication. Through adoption of these standards, PrinterOn Enterprise or Express can easily be integrated with a reverse proxy service to provide increased security.

Q: If the admin credentials to PrinterOn are compromised, what can someone do with them?

A: Compromised credentials provide no security risk. While the PrinterOn credentials are used to perform centralized configuration initially, all print data remains within the control of the corporate network and this cannot be accessed with the admin credentials.

Q: How does the overall end-to-end security of the solution change if certain PrinterOn components are deployed in different places on the network?

A: PrinterOn's solution is designed at its core to provide the highest level of security even across networks distributed in various locations. By using PrinterOn's print data encryption solution, PrinterOn can ensure that print data is encrypted at rest, as well as in transit and provide incremental security by encrypting both the data and the communication channel.

Q: What data is stored in the Directory that is configurable?

A: The Directory stores details like the make/model of the printer, finishing options such as paper size, color support, duplex etc. Also the destination of the job data (which will be an instance of Print Delivery Hub or Print Delivery Station that resides in your secure network).

Trademarks and Service Marks

The following are trademarks or registered trademarks of PrinterOn Corporation in Canada and other countries:

PrinterOn®, PrintAnywhere®, Print Simply Anywhere®, PrintWhere®, PRINTSPOTS®, the PrinterOn Logo, the PrinterOn Symbol, PrintConnect™ and PrintValet™ are trademarks and/or registered trademarks of PrinterOn.

The following are trademarks or registered trademarks of other companies:

Windows, Internet Explorer, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Visio are trademarks or registered trademarks of Microsoft Corporation.

iPad, iPhone and AirPrint and OS X are trademarks or registered trademarks of Apple.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

Android, Chrome OS and Chromebook are trademarks or registered trademarks of Google Inc.

BlackBerry is a registered trademark of BlackBerry, Ltd.

Other brands and their products are trademarks or registered trademarks of their respective holders.

Copyright Notice

Disclaimer:

PrinterOn Inc. makes no warranty with respect to the adequacy of this documentation, programs, or hardware, which it describes for any particular purpose, or with respect to the adequacy to produce any particular result. In no event shall PrinterOn Inc. be held liable for special, direct, indirect, or consequential damages, losses, costs, charges, claims, demands, or claim for lost profits, fees, or expenses of any nature or kind.

Version 2.0.5 | April 2016

PRINTERON®
PRINT SIMPLY ANYWHERE

PrinterOn is the world's leading enterprise-grade Mobile Printing Platform. PrinterOn has been delivering mobile printing solutions since 2001 to three major verticals: enterprise, education, and public printing locations.

PrinterOn was the first to develop a private and public cloud printing solution and today operates the largest public printing NOC (Network Operations Center) in the world. PrinterOn uses cloud technology to enable users to print documents from any smartphone, tablet, or laptop to any PrinterOn-enabled printer in the world. There are over 10,000 PrinterOn printing locations worldwide.

The PrinterOn mobile printing solution is the only patent protected, fully-agnostic solution in the market today with the ability to connect disparate networks into one simple-to-manage enterprise or hosted solution. PrinterOn has been deployed in corporations, hotels, universities, airports, libraries in over 120 countries. Since its inception, users of PrinterOn have printed over 80 million pages.

PrinterOn technology is protected in the U.S. and internationally by issued and pending patents including US Patents 7,007,093, 7,249,188, 6,990,527 and 7,827,293.

www.printeron.com

mobile printing solutions | enterprise | education | public printing locations