PrinterOn Security Discussion Paper

Enterprise Edition

PrinterOn Enterprise security framework-in depth

PRINTERON
print simply anywhere

Contents

Executive Summary

PrinterOn's cloud software development experience started in 2001. As a result, today PrinterOn offers the broadest range of printing solutions to address any type of secure cloud printing scenario. PrinterOn also has significant experience with private cloud deployment—behind the organization's firewall. Today PrinterOn refers to *all* these PrinterOn deployment options under the banner *True Cloud Printing*™.

This paper discusses the security of the PrinterOn Enterprise Edition in its three deployment options:

- PrinterOn Managed Cloud
- Third-Party Cloud
- Private Cloud (traditional on-premise 100% behind the firewall)

Security measures of the technical solution are the same, no matter which method of deployment is chosen. What changes is the responsibility for the underlying infrastructure. In this paper, callouts are made to specific measures as it relates to Enterprise deployed in the PrinterOn Managed Cloud.

The intended audience for this document is enterprise, cloud, and solution architects, or IT groups or sales engineers who require deeper knowledge of the PrinterOn technology platform and how it delivers secure printing workflows. PrinterOn provides multiple levels of security at every point of the print workflow from submission to release.

Glossary

Term	Description	Resides Where?
PrinterOn Managed Cloud	Secure cloud printing managed service enabling printing from any device, any platform on any network. Underlying cloud service is provisioned, managed and monitored by PrinterOn.	PrinterOn Cloud
Print Delivery Gateway (PDG)	Protocol gateway to PrinterOn printers allowing jobs to be submitted using various methods including native iOS print, Google Cloud Print and Windows	PrinterOn Cloud OR Customer Trusted Network
Central Print Service (CPS)	Entry point for all print requests submitted to PrinterOn	PrinterOn Cloud OR Customer Trusted Network
PrintAnywhere® Service (PAS)	Facilitates receiving and printing of documents. Delivers the processed documents to a specified printer or PDH	PrinterOn Cloud OR Customer Trusted Network
Print Delivery Hub (PDH)	Transfers print jobs to PDS through firewalls and across disparate networks. Uses Internet Printing Protocol (IPP) over TLS	PrinterOn Cloud OR Customer Trusted Network
Print Delivery Station (PDS)	Bridges PrinterOn with the physical printer or print queue. Pulls print jobs from PDH and releases them to enabled printers	Printer's LAN
PrintWhere®	Enables submitting print jobs to PrinterOn using the traditional File>Print workflow on Windows laptops, desktops and Surface® tablets	Windows PC or Surface tablet

PrinterOn Overview

PrinterOn is a secure solution designed for organizations that want to unburden themselves of print infrastructure and reduce their IT costs. It is a solution that truly aligns with your cloud-centric IT strategy. PrinterOn can also be deployed traditionally on premise "behind the firewall" as a private cloud solution.

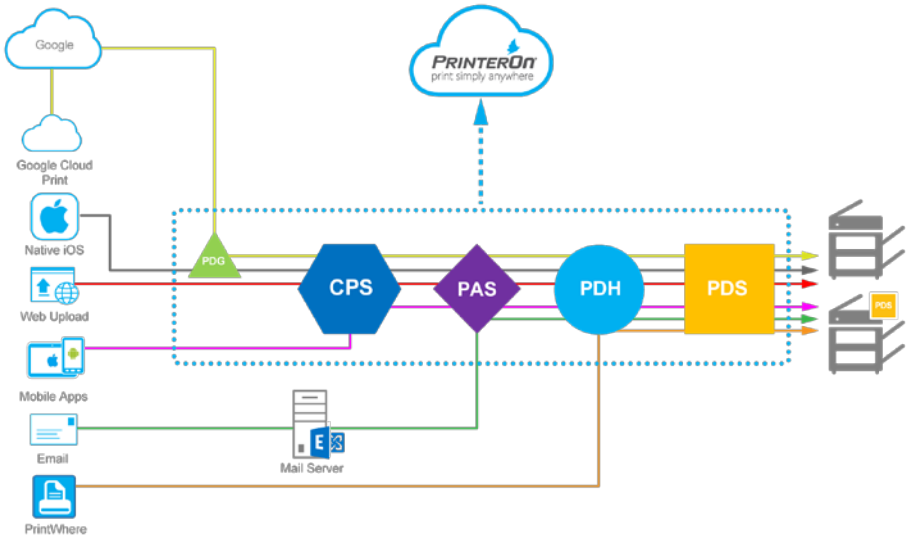
With PrinterOn managed cloud deployment, your entire print infrastructure is managed in the cloud so you can focus on more important business. Even more, the managed cloud deployment option takes care of the details such as deployment, management, scaling, upgrading, support and maintenance so you don't have to.

The benefits of PrinterOn's managed cloud deployment option are:

- Reduced server cost – With a print solution in the cloud, you no longer require all of those print servers. No maintenance, no hardware failures, no headaches.
- Lower IT operations costs – Dramatic reductions in hours spent maintaining cumbersome enterprise solutions and configuring networks and firewalls. Those resources can be freed up to IT activities that actually advance your organization's mission.
- Elastic processing - Processing power can expand and contract on demand as needed. As your requirements increase, more processing servers are brought online in a matter of minutes. When needs decrease, the extra capacity is removed, saving you money.
- Predictable and consistent operating costs - Subscription services enable you to plan costs with greater accuracy. Costs are paid as the service is used instead of all up front. Print can now be an operating expense rather than a capital expense.

PrinterOn Architecture

To understand PrinterOn 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. All services operate the same in all deployment modes. The diagram below depicts a high level overview of the components that constitute PrinterOn. Most externally facing services are port-configurable (except for Directory communications via TLS on port 443).



Central Print Services (CPS)

Central Print Services is the primary entry point for all requests submitted to PrinterOn. 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 using PrinterOn APIs.

In addition to providing print service access, CPS management is integrated into a centralized, 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 document processing as part of PrinterOn print services. The PrintAnywhere service includes a number of software services that facilitate the receiving and printing of 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 TLS and based on the industry standard IPP protocol which itself is based on HTTPS. In addition to using IPP over TLS, optional job data encryption using PrinterOn extensions is available. PDS communicates to the PrinterOn services by default on ports 443. This is configurable.

Print Delivery Gateway (PDG)

The Print Delivery Gateway software serves as a protocol gateway to PrinterOn services, allowing the PrinterOn service to support additional print protocols such as native iOS printing (AirPrint®), Google Cloud Print and Windows printing. It acts as a bridge supporting multiple print workflows using the native printing experience of each platform. The Print Delivery Gateway uses industry standard IPP protocol for iOS print and XMPP protocol for Google Cloud Print. The Print Delivery Gateway may be installed on the local network to facilitate traditional Windows print. In this scenario, the Print Delivery Gateway uses standard Windows APIs to collect print jobs, and then establishes a secure connection from the local network to the PrinterOn services over TLS.

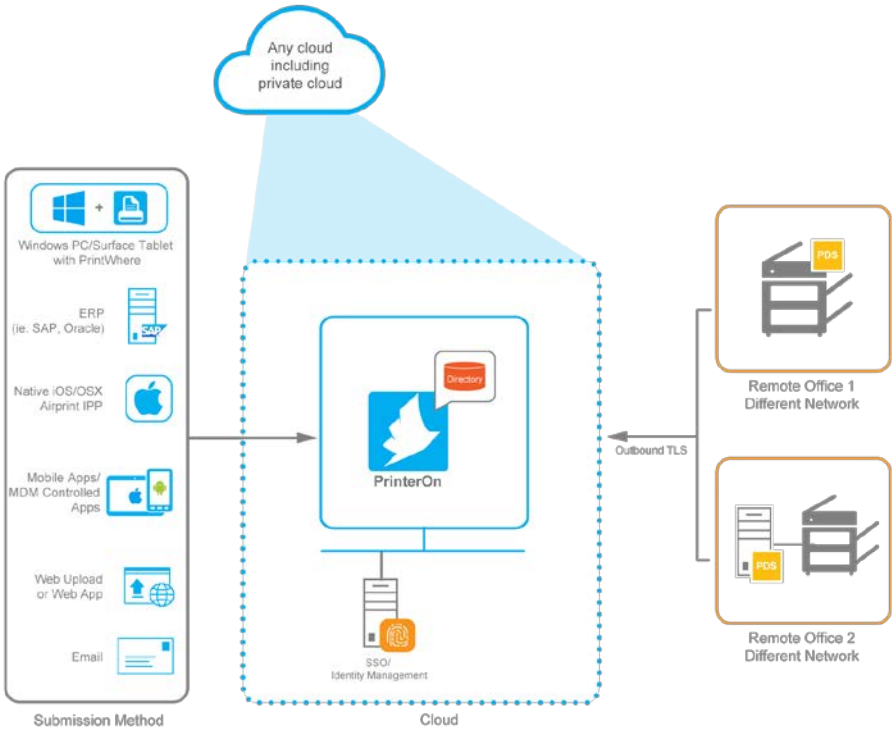
PDG secured communications for receiving client print jobs are over TLS and by default on ports 631 for native iOS Print and 5222 for Google Cloud Print. This is configurable.

Print Delivery Hub (PDH)

The Print Delivery Hub (PDH) acts as a centralized distribution server, delivering print jobs when printers and MFPs are distributed across disparate networks. In most cloud print deployments, delivering print jobs directly from PrinterOn to desired printers on disparate networks may not be possible due to network configuration. In this arrangement, print jobs are delivered to the PDH. The PDS services communicate with PDH to detect and download the print jobs from the cloud print services. Additionally, leveraging a simple and rapid deployment of print devices will benefit from the centralized installation of PDH. PDH communicates by default on ports 443/631. This is configurable.

Architectural Flexibility

PrinterOn has ultimate flexibility allowing its main components to be placed literally in any cloud infrastructure, in any specific datacenter. Each component can be scaled out horizontally for volume or set up in a redundant configuration. This means that no matter the existing cloud deployment configuration or the enterprise network architecture, PrinterOn can be deployed without local trusted network infrastructure changes.



Summary of Port Configuration for PrinterOn

PrinterOn Component	Port Configuration
PrintWhere Driver	443 (default), 631 (optional)
PDG (Print Delivery Gateway)	631 (default) using IPP protocol
PAS (PrintAnywhere Server)	443/631 (default) 5200,5400 for internal clustering*
PDH (Print Delivery Hub)	443/631 (default)
PDS (Print Delivery Station)	443/631 (default)
CPS (Central Print Services)	443 (default)

*This is not externally accessible by any client application. This is to listen only to internal components like CPS. Applies only to private cloud deployments

PrinterOn uses the latest versions of TLS for communications and can implement virtually any certificate management scheme the end customer desires.

Service Design, Management and Security

Multitenancy

"Multitenancy" is the fundamental technology that clouds use to share resources cost-efficiently and securely among multiple subscribers. PrinterOn is a modern Software as a Service ("SaaS") architecture that is built with multitenancy inherent in its design. PrinterOn employs industry-standard techniques and security methods to deliver multitenancy.

The PrinterOn multi-tenant design reflects separation of service data from the service components that manipulate and process subscriber requests and subscriber data. PrinterOn also uses an abstracted data model. The overall benefit of this multi-tenant design is the data processing components can be shared across all tenants safely and securely, eliminating the security concern regarding persistent subscriber data storage within these components. Within PrinterOn, these components include services such as document converters, or data delivery components where the data is typically transient.

PrinterOn subscriber tenant data is logically organized such that each tenant is uniquely managed and has a globally unique organization ID representing the tenant within the multi-tenant data store. These obfuscated data IDs facilitate anonymized access and references to data that may be used across the shared services. This ensures that unnecessary data sharing is avoided and at the same time maximizes the efficient use of the shared components.

PrinterOn's service model is based on a microservice design. Microservice architecture enables delegation of duties to purpose-built components. This minimizes the need for information access by any one component. An individual shared service can perform complex and/or commonly-requested operations on tenant data without sharing tenant-specific information with other components. Components are provided the minimal information necessary to perform an operation. References to tenant data are obfuscated whenever possible so that a wide range of shared services can be used safely and securely across all tenants without sharing tenant-specific information.

Tenant-specific information is not accessible to users outside the tenant's scope. Access to tenant-identifying information is strictly controlled using industry-standard authentication and authorization. This ensures that only authorized users within a single tenant can access the unique organization's IDs which are used to retrieve the information needed to carry out the requested service action.

PrinterOn Managed Cloud Print Service Personnel Access

An integral part of the overall security of a managed cloud solution relates to how the service is managed from an operational standpoint. PrinterOn has taken measures to ensure that access to the underlying infrastructure of its managed cloud service is limited to those authorized to actually manage the service.

PrinterOn's managed cloud service is managed by a dedicated team who monitors the service 24 hours a day. This team is responsible for coordinating the initial deployments and configurations with customers, and for monitoring the service to ensure it continues operate as expected.

Access to all services are managed using an audited series of tools that provide tiered access. The management team accesses all infrastructure services through a centralized console where each service

is isolated and managed independently. From this console, the management team can review and monitor the status of the services.

Should additional access be required, such as direct access to the managed cloud servers, a series of security measures are in place to review authorization:

- Access to managed cloud instances is only accessible from within a dedicated managed PrinterOn network. Access is authorized only from a small number of IP addresses.
- The team must create a temporary secure tunnel to connect to the cloud instance. The tunnel is limited to a maximum of a few hours at a time.
- Team members must re-authenticate at the instance prior to accessing the instance itself, further validating the team members identity.

Change Management and Auditing

To ensure limited access to the cloud instances, other measures are in place to ensure that any access is monitored and audited. Additionally, all changes made to the cloud services are recorded and regularly reviewed.

Log on attempts and activities performed on the cloud services are tracked and stored in an auditable backup that can be used to identify which user logged into the cloud services, as well as identifying what operations were performed. This auditable record can be used during regular security audits as well if any specific incidents occur to identify which team members were engaged.

All changes to the cloud service must be entered into an incident management system. This system allows the team to track historical changes to the services and identify any changes that may potentially affect the service. The incident management system requires that all information is logged including the team member responsible for the change, the purpose for the change, the date and time the change was made, as well as a detailed account of the changes.

PrinterOn Document Submission

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

PrintWhere® for Windows

Windows-based desktop PCs, laptops or Microsoft Surface® tablet users can securely submit print jobs using PrinterOn PrintWhere. PrintWhere is like a Windows driver that enables users to print using the standard (File>Print) workflow and enables them to securely deliver their print job to any remote print destination set up within PrinterOn, even if the destination printer is on a completely different network. PrintWhere also supports the ability to intelligently detect if a printer is available via the local network. It will then adjust the communication path to use the local network instead of the cloud delivery path. This is an optional configuration enabled the administrator.

PrintWhere 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. PrintWhere communicates on ports 443/631 and may optionally communicate on other ports for direct print. This is configurable.

Native macOS

PrinterOn provides a secure method for users to print on or off the secure network using the native print functionality of macOS. IPP (Internet Printing Protocol) is the native protocol used by the macOS platform and is also used by AirPrint. PrinterOn supports IPP printing enabling macOS users to print securely without the need to install drivers. PrinterOn also supports standard macOS authentication in addition to supporting native macOS print authentication with LDAP/AD or OpenID Connect-compatible identity management solutions. IPP-secured communications are over TLS and by default on ports 443/631.

iOS Mobile App

Users can search for printers and securely submit print jobs using the PrinterOn mobile application for iOS. There are also versions of this application available which are specifically "wrapped" to be deployed through popular Mobile Device Management (MDM) providers' platforms (please refer to the section later in this document). PrinterOn mobile apps also integrate authentication with LDAP/AD or OpenID Connect-compatible identity management solutions, role-based access control, and guest print rules. Since PrinterOn Central Print Services uses TLS, the mobile applications benefit from the same security. Mobile apps communicate on ports 443. This is configurable.

Native iOS

PrinterOn Enterprise provides a secure way for users to print on or off the trusted corporate network using the native print functionality of iOS devices, with or without Apple Bonjour service discovery protocol. With the Print Delivery Gateway (PDG) installed in the deployment configuration, PrinterOn integrates the native iOS print authentication with LDAP/AD or OpenID Connect-compatible identity management solutions, role-based access control, and guest printing rules to inform the iOS devices how and where to find printers on a network.

While some deployments may be well suited to using Apple's Bonjour, in many cases Bonjour is not a viable option for administrators to connect users to printers, even in simple network configurations. There are basic limitations of Bonjour that come into play in environments with large user and/or printer counts, and/or complex networks. The end result in many situations is an unmanageable deployment.

To provide the ability to print from an iOS device without Bonjour, you need to "push" printer profiles to an iOS device using any supported MDM/MAM service or Apple's own configuration tools.

IPP-secured communications are over TLS and by default on ports 443/631.

Android Mobile App

Users can search for printers and securely submit print jobs to Central Print Services (CPS) using the PrinterOn mobile application for Android. There are also versions of these applications available which are specifically "wrapped" to be deployed through popular Mobile Device Management (MDM) providers' platforms (please refer to the section later in this document). PrinterOn mobile apps also integrate authentication with LDAP/AD or Open ID Connect-compatible identity management solutions, role-based access control, and guest print rules. Since CPS uses TLS, the mobile applications benefit from the same security. Mobile apps communicate on ports 443 by default. This is configurable on the server.

Google Cloud Print

For those wanting to bridge the gap between existing Google Cloud Print (GCP) workflows and PrinterOn Enterprise, the PDG service allows users to print seamlessly from any of the GCP client applications (ChromeOS, Chrome Browser etc.) to PrinterOn-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 a connection to the Google Cloud Print services to print.*

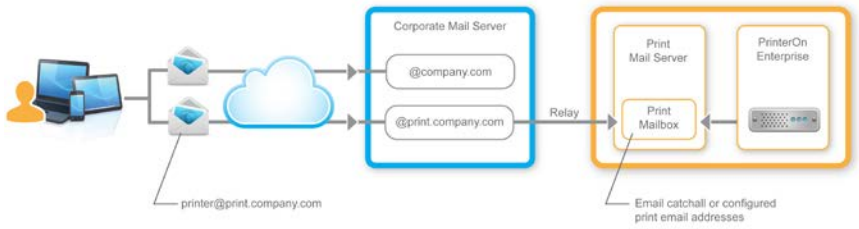
The combination of PrinterOn Enterprise and Google Cloud Print enables management of BYOD environments where devices do not connect exclusively to the existing print infrastructure. Google Cloud Print communicates using HTTPS/XMPP over ports 443/5222.

Email Printing

Users can 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 dedicated email service just for print jobs. PrinterOn leverages trusted and proven third-party email security services such as TLS, virus and spam filters. The PrinterOn service uses secure SMTP to generate email responses to print requests.

Users continue to use their existing email accounts and services, such as Office365, Google, iCloud or a company-managed mail service for receiving their messages and forward from their existing mail server to the PrinterOn email print service.



Web Print

Documents can be submitted by uploading through a 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 TLS to provide additional security. From CPS, documents are forwarded to PAS on the trusted network to be rendered and printed. Web submission communicates on Port 443.

Web App

The PrinterOn web app uses the same underlying technology as Web Print and is designed for smartphones and tablets. It enables users to submit and release documents through the mobile web browser on their device. In addition to Android and iOS devices, the Web App is optimized for Windows Phone and BlackBerry® device screens. Similar to Web Print, the users authenticate themselves before selecting the desired printer and uploading the document they would like to print. The Web App leverages the Document Picker feature to allow the users to select the documents to be uploaded for printing.

The Web App printing service is provided as part of CPS, which uses TLS, so it benefits from the same security. From CPS, documents are forwarded to PAS on the trusted network to be rendered and printed. Web submission communicates on Port 443.

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 infrastructure, thereby bridging the gap between existing Windows print queues and PrinterOn. It enables users to submit jobs using standard Windows workflows (File>Print) leveraging the capabilities of PrinterOn to deliver the pre-rendered data content to printers located anywhere in the world. PQMS communications are part of PDG. When PDG is installed, print jobs are retrieved using a standard Windows Printer Port installed on a PC or server. After retrieving the print job, the Print Delivery Gateway uses a TLS-secured connection to submit the job from the on-premise server to the PrinterOn services using port 443.

Authentication

PrinterOn provides a number of authentication options. The power in the architecture is that PrinterOn can leverage *cloud-based user authentication.* Any OpenID Connect-compatible identify management solution, such as Microsoft Azure AD, can be used. This flexible, standards-based authentication support enables even more flexibility to deploy a pure cloud secure printing solution.

PrinterOn also supports independent user management without the need for third-party integration. This independent user management follows the same security principles as Azure AD and other identity management providers using OpenID Connect.

In addition, PrinterOn supports traditional LDAP or Active Directory configurations to authenticate users when printing, although these methods are typically used for on-premise deployments, rather than deployments in the cloud.

Authentication services are managed centrally by CPS, which is configured to communicate with the existing cloud-based identity management solution (or LDAP or AD server) and authenticate users accessing the print services. This approach provides a central location for integrating authentication for all print methods and also enables print jobs to be associated with a user's existing credentials. PrinterOn is a flexible and modular system that can adapt to situation-specific requirements through the use of authentication APIs available for the service.

Active Directory Support

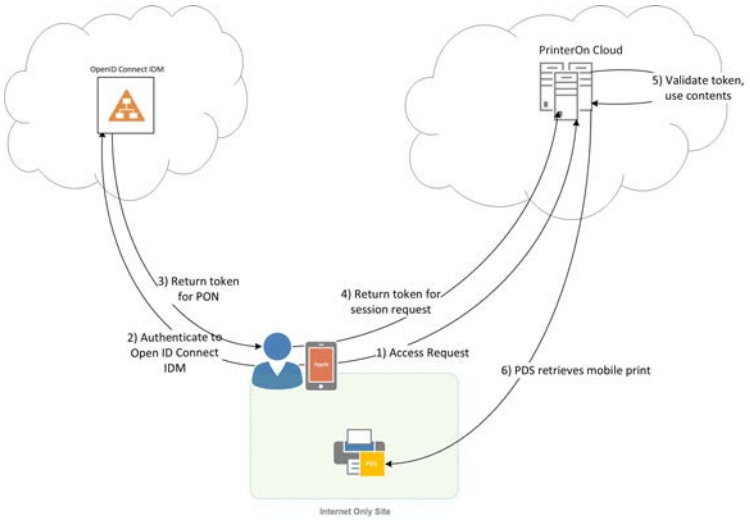
PrinterOn supports traditional LDAP or Active Directory configurations to authenticate users when printing. Typically, most organizations will already be leveraging Microsoft® Active Directory, but for the ones that do not, PrinterOn also supports user authentication against LDAP user database servers. Authentication services are managed centrally by the Central Print Services allowing print jobs to be associated with a user's existing credentials irrespective of the submission method.

In addition to authenticating the user at the time of submission, the PrinterOn service can also be configured to request credentials when the user releases the print job to the printer. The credentials supplied by the print user are sent CPS, which uses TLS to ensure the security of sensitive information. From CPS, the credentials are forwarded to the LDAP/AD server on the trusted network to be authenticated.

Typically LDAP/AD servers use TCP or UDP as the transport protocol. The default TCP and UDP port for LDAP traffic is 389. LDAP/AD communications can also be tunneled through TLS-encrypted connections. The default LDAP TCP port for SSL is 636. The ports are configurable.

Azure AD Identity Management Support

PrinterOn supports cloud-based user authentication and identity management solutions (IDM). Any OpenID Connect-compatible identity management solution (such as Microsoft Azure AD), can be used.



While the authentication services are managed centrally by CPS, client applications (such as mobile apps and PrintWhere desktop clients), perform the authentication process with the cloud-based identity management solution. Upon authentication, the IDM solution returns an access token to the client which it uses to retrieve printers and submit print jobs. In addition, the token enables PrinterOn to ensure the user is still authorized to use the service without requiring the user to re-authenticate. This method also ensures print jobs are associated with the proper user.

In addition to authenticating the user at the time of submission, PrinterOn can also be configured to request credentials when the user releases the job to the printer. The release client application will either redirect the user to a secure web page form provided by the IDM solution to ask for user credentials or use other OpenID Connect-certified methods to authenticate the user. After the initial successful authentication, the token information returned by the IDM solution is forwarded to the CPS service by the client application over TLS to protect the identity of the print user. CPS also connects to the IDM solution over TLS to verify the validity of the tokens and retrieve user information. The default port for all these communication exchanges is 443.

NOTE: Some print submission methods, such as Apple AirPrint, do not yet support form-based authentication. To work around this, administrators can optionally enable these workflows to utilize the standard Resource Owner Credentials Flow that is approved as part of OpenID Connect and is supported by all major IDM solutions. This method uses a user-approved TLS connection from the AirPrint client device to PrinterOn for authentication. PrinterOn then redirects the request to the identity management solution using the OpenID Connect flow to receive an access token. In this scenario no user credentials are stored or managed by PrinterOn; PrinterOn only relays them on behalf of the user. When services such as AirPrint support form-based authentication, PrinterOn will consider adding support.

PrintWhere® Authentication

When the user submits a print job, PrintWhere for Windows will automatically present the user with an authentication page, most commonly using an OpenID Connect-compatible cloud-based authentication solution such as AzureAD or a traditional on-premise Active Directory. When using a cloud-based identity management solution, PrintWhere will redirect the user to a secure form provided by that solution to collect the user credentials for authentication.

Once authenticated, the PrintWhere client will store the user's tokens but not store the user's password. Subsequent print requests made from PrintWhere will include these tokens, as opposed to the credentials, and the PrinterOn service will validate the user's access with the identity management solution provider each time the user accesses the service to ensure they remain authorized to use it.

Native macOS Authentication

PrinterOn supports native Apple macOS print authentication with OpenID Connect-compatible solutions or LDAP/AD. Upon print submission, the macOS will authenticate against the cloud-based user authentication service (or LDAP/AD server) using CPS as the intermediary.

Native macOS print is based on IPP and does not yet support form-based authentication and administrators can optionally enable these workflows to utilize the standard Resource Owner Credentials Flow that is approved as part of OpenID Connect and supported by all major iDMs. This method uses a user-approved TLS connection from the macOS device to the PrinterOn service to authenticate. The PrinterOn service then redirects the request to the identity management provider using the OpenID Connect flow to receive an access token. In this scenario, no user credentials are stored or managed by PrinterOn; PrinterOn relays them on behalf of the user.

iOS Mobile App Authentication

PrinterOn iOS mobile applications are able to leverage the same cloud-based user authentication services (or LDAP/AD services) as for all other authentication purposes. The user will be authenticated prior to submitting their print jobs. Prior to completing the print request, the user will authenticate themselves using the identity management service using OpenID Connect.

Like macOS, iOS does not yet support form-based authentication. However administrators can optionally enable these workflows to utilize the standard Resource Owner Credentials Flow that is approved as part of OpenID Connect and supported by all major iDMs. This method uses a user-approved TLS connection from the iOS device to the PrinterOn service to authenticate. The PrinterOn service then redirects the request to the identity management provider using the OpenID Connect flow to receive an access token. In this scenario, no user credentials are stored or managed by PrinterOn; PrinterOn only relays them on behalf of the user.

Once authenticated, the iOS Mobile Apps will store the user's tokens but not store the user's password. Subsequent print requests made from the app will include these tokens, as opposed to the credentials, and the PrinterOn service will validate the user's access with the identity management provider each time the user accesses the service to ensure they remain authorized.

iOS Extensions Authentication

The iOS extension allows many iOS applications to access the PrinterOn app's printing capabilities from within the application itself. Using the "Open in" function. Most iOS applications support iOS Extensions

(since iOS 8). PrinterOn's iOS Extensions are used to start the print process with the rest of the print workflow managed by the iOS App. Regardless of whether you print using iOS Extensions, or leverage the iOS Mobile App, the user authentication process remains the same.

Native iOS Authentication

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. However, by deploying PrinterOn Enterprise with PDG, user authentication against cloud-based users (or traditional AD or LDAP) becomes possible within the native iOS print workflow. Prior to completing the print request, the user will authenticate themselves against the cloud-based user authentication service (or LDAP/AD server) using CPS as the intermediary.

Note, however, that just as with macOS and PrinterOn's iOS app, native iOS print does not yet support form-based authentication. Administrators can optionally enable these workflows to utilize the standard Resource Owner Credentials Flow that is approved as part of OpenID Connect and supported by all major IDMs. This method uses a user-approved TLS connection from the iOS device to the PrinterOn service to authenticate. The PrinterOn service then redirects the request to the identity management provider using the OpenID Connect flow to receive an access token. In this scenario, no user credentials are stored or managed by PrinterOn; PrinterOn only relays them on behalf of the user.

Android Mobile App Authentication

PrinterOn mobile applications for Android are able to leverage the same cloud-based user authentication services (or LDAP/AD services) as other users. The user will be authenticated prior to submitting their print jobs. Prior to completing the print request, the user will authenticate themselves using the identity management service using OpenID Connect. If the service is configured for cloud-based user authentication such as Azure AD, then the PrinterOn mobile application will redirect the print user to a secure web page provided by the identity service to collect the user credentials for authentication.

Once authenticated, the Android Mobile Apps will store the user's tokens but not store the user's password. Subsequent print requests made from the Apps will include these tokens, as opposed to the credentials, and the PrinterOn service will validate the user's access with the identity management provider each time the user access the service to ensure they remain authorized.

Android Print Service Plug-In Authentication

The PrinterOn Print Service Plugin for Android enables printing from any application that supports Android's native printing without the need for an intermediate app. This plug-in conforms to the specifications written by Google to enable adding in third-party print services to the Android operating Android application itself. The Print Service Plugin uses the same implementation as the Android Mobile App. Regardless of whether you print using the Android Print Service Plug-in or Android Mobile App, the user authentication process remains the same.

Google Cloud Print Authentication

After submitting a document for print, the user is authenticated in Google using Gmail or Google Business accounts. When submitting jobs via Google Cloud Print, the PrinterOn service is configured to allow Google to perform the authentication process. PrinterOn trusts that authentication is completed successfully.

That user info is then delivered to PrinterOn. Optionally, authentication can take place against the cloud-based user authentication service (local AD or LDAP) where email addresses are matched with internal users. PrinterOn Enterprise then processes the job and delivers it to the printer, print queue or print management server providing secure release. To take advantage of the user email verification, users must log into the PrinterOn service using another method, such the web site, to create their identity in PrinterOn.

Email Print Authentication

There are two options to authenticate 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. PrinterOn will use its existing LDAP/AD configuration to locate a user based on their email address. The user's network login will be returned by the authentication server and included with print jobs.

To take advantage of the user email verification, users must log into the PrinterOn service using another method, such the web site, to create their identity in PrinterOn.

Web Print Authentication

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

Users printing using Web Print will automatically be presented with an authentication page for their print jobs. Prior to completing the print request, the user will authenticate themselves using the identity management service using OpenID Connect. If the service is configured for cloud-based user authentication such as Azure AD, then the Web Submission will redirect the user to a secure web page provided by the identity management service to collect the user credentials for authentication.

PQMS (Print Queue Monitoring Service) Authentication

Since the native 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 PrinterOn 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 (Internet Printing Protocol)

IPP allows the same behavior as native iOS and native macOS print. Most IPP clients do not yet support form-based authentication however administrators can optionally enable these workflows to utilize the standard Resource Owner Credentials Flow that is approved as part of OpenID Connect and supported by all major IDMs. This method uses a user-approved TLS connection from the IPP client to the PrinterOn service to authenticate. The PrinterOn service then redirects the request to the identity management provider using the OpenID Connect flow to receive an access token. In this scenario, no user credentials are stored or managed by PrinterOn; PrinterOn only relays them on behalf of the user.

Using an MDM/MAM with PrinterOn

In addition to the standard PrinterOn mobile apps, PrinterOn also provides SDK-integrated applications for industry-leading MDM/MAM 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 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.

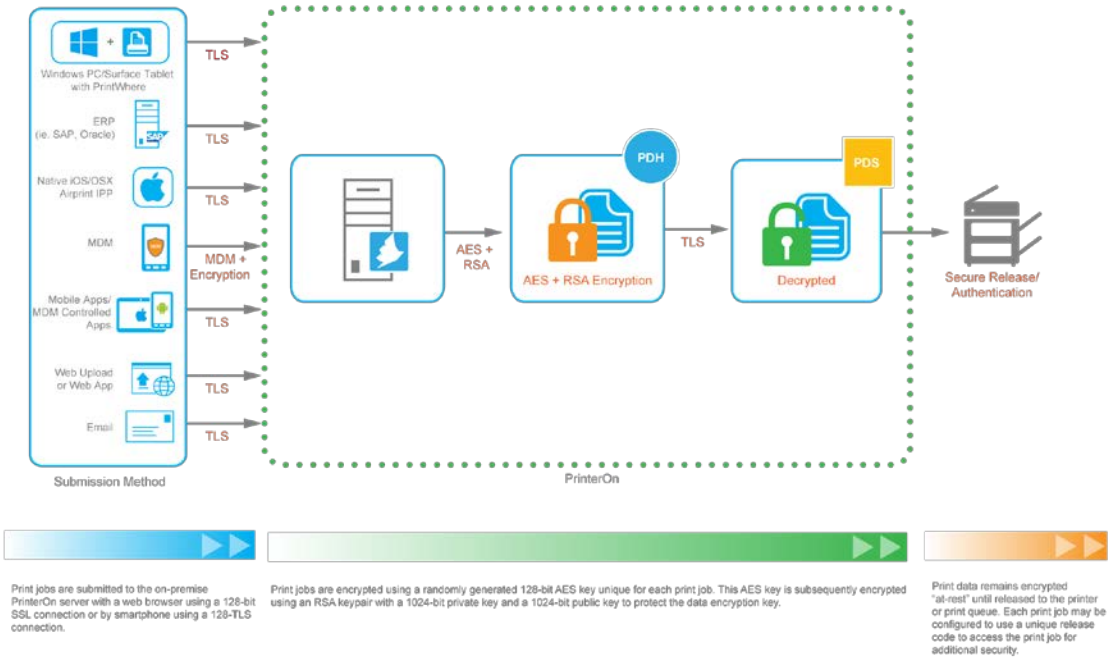
PrinterOn mobile apps with MDM integration provide the ability to control the configuration and distribution of the SDK-wrapped PrinterOn mobile apps for iOS and Android. PrinterOn MDM integration is also able to connect the PrinterOn secure mobile printing service infrastructure with the MDM vendor's secure mobile gateway, if desired.

PrinterOn supports the most popular MDM/MAM solutions to enhance its overall security. Currently PrinterOn provides support for:

- VMWare AirWatch
- BlackBerry (formerly Good) MDM/MAM
- MobileIron
- Citrix Worx

Although not an MDM in the purest sense, PrinterOn has recently added support for Microsoft Intune and the ability to deliver PrintWhere complete with auto-configuration.

Print Job Processing and Encryption



User 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.

On both iOS and Android, PrinterOn specific device information is first encoded using a complex algorithm to obfuscate the information before saving it to OS-specific storage. On iOS, the information is stored using the Apple designed Keychain where all sensitive information is stored. The Keychain uses highly secure algorithms to encrypt the data.

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

PrinterOn applies industry-standard best practices for all network communications and security. All PrinterOn services are protected by fully signed and verifiable certificates that ensure connections are encrypted and that their authenticity can be confirmed.

Additionally, clients such as the PrinterOn mobile application ensure that all communication is done securely at the client level. Users will be notified whenever attempting to connect to any discovered

services using a self-signed certificate to ensure that users are aware of the service identity prior to a connection being established.

Email Security

PrinterOn Enterprise only performs 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. PrinterOn email printing 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.

Print Data Encryption

PrinterOn 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 the print service. The job is securely delivered to the service using TLS. Once documents are received by CPS, they are rendered and converted to a printable form.

To encrypt print data at rest outside the secure PrinterOn service environment, every PDS service instance generates a unique RSA 1024-bit public and private key pair and publishes the public key to the PrinterOn Service. A unique, one time use 128-bit AES encryption key is then generated. The print data is then compressed and encrypted using 128-bit AES encryption and the 128-bit AES key is encrypted using the asymmetric RSA key before being included with the print metadata. Finally, the Print Delivery Station (PDS) downloads the data over a secure TLS connection and stores the print job securely on a PC or server. This scheme effectively creates two levels of encryption for every print job.

Print Data Security

At its core, PrinterOn relies on the directory service. 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 that is unique within an organization as well as a globally unique identifier that is unique across all of PrinterOn. When configuring PDS, this printer identifier is used to associate the physical printer with a PrinterOn "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.

The PrinterOn service uses industry-accepted secure cloud storage best practices. Each customer's data is stored in a dedicated and isolated storage container. The container is protected with access control rules limiting access to the customer connected services. Security can be increased by reducing the number of components interacting with the data and allowing the PDS to directly download the print jobs from the cloud storage on demand. The PrinterOn PDS may be configured to request a short-lived reference to the print data and download it directly from the cloud storage service, as opposed to using PDH. This option is available for modern release stations capable of interacting with the cloud storage.

The reference to the print data is generated at the time the user requests the job with a unique and secure URL that expires after a short period of time ensuring the information is not available to other software or users.

Data Deletion

Fundamentally, the PrinterOn architecture considers all print job data to be transient and not persistent. This means that the solution minimizes the amount of time print data is stored in it. This includes both the submitted documents and the print data destined for the printer.

Input documents are deleted as soon as they have been converted to a printable format and completely processed. Depending on the stage of the processing, different APIs may be used to delete the data. In all cases, standard APIs are used and made available by the specified programming language.

When the service is deleted and/or retired, the instance the software is running on is destroyed, and the information wiped from the services using approved cloud provider techniques to protect the data and ensure it is not re-used in the future.

When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. PrinterOn's cloud supports U.S. DoD Wipe Standards and NIST Guidelines for Media Sanitization. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Database Security

PrinterOn uses modern "cloud-aware" databases to store and manage an organization's data. The specific database technology used depends on use case, but includes both SQL and NoSQL databases. In all cases, the same high level of security is applied. Databases are deployed in facilities with comprehensive control environments that includes the necessary policies, processes and control activities for the delivery of each of the cloud service offerings.

Each organization has an isolated and unique database instance to store their data. The database itself is not exposed to the Internet and is managed beneath multiple layers of firewalls to ensure that there is no external access to the data. In addition, the database instances use security policies that limit connectivity to specific logical services that make up the larger PrinterOn service ensuring that only those services requiring access can interact with the data. Access control is comprised of both network access control (limiting specific inbound connections), as well as user access control, by providing credentials to connect to the instance if allowed by the network.

PrinterOn manages a wide range of information to enable administrators to customize the service. The organization's isolated directory contains information including:

- Printers and printer configurations connected to PrinterOn
- Print activity details including document names, formats and sizes. (Neither the documents themselves, nor their contents are persisted in PrinterOn).
- User information required to track print activity including the user first name, last name and PrinterOn account credentials.

Print Release

Secure Release Anywhere™ - PrinterOn Pull Printing

PrinterOn supports pull printing through the *Secure Release Anywhere*™ feature. Pull printing simplifies printing for users. Rather than requiring users to know the physical location of the specific printer they print to, users simply print. They *then* go to the nearest printer, enter their credentials or release code, and *pull* the job to that location to be printed. PrinterOn's *Secure Release Anywhere* supports a variety of printers, MFPs, and release stations, and can be configured to work with built-in browsers, keypads, or with a PrinterOn's PrintValet™ connected to single function printers.

PrinterOn's *Secure Release Anywhere* provides the same level of security as non-pull print delivery flows yet provides the flexibility to release a print job anywhere. Administrators can choose from various options to customize their pull print experience. In all cases, data retention options are provided to determine how un-released data should be managed. In most configurations, jobs that are not released after 72 hours will be purged automatically from the central server. This setting is configurable.

There are two primary configurations for *Secure Release Anywhere*, Central Store and Local Download. These options are configured for each release station individually to allow for different behavior depending on the type of facility and/or security profile of the facility and organization as a whole.

The Central Store configuration leaves all print jobs on the central PDH server. Jobs are not downloaded until the user requests to release the print job at the release station. This allows an administrator to centrally store and manage all jobs and reduce the number of print jobs and time a job is outside the central service.

The Local Download configuration allows jobs to be downloaded to a release station in advance of the user requesting to release their print jobs. This mode allows an administrator to determine which locations are eligible for this option. This mode is beneficial when performance and minimum time to release is paramount. In some scenarios, PDS may be deployed on-site to service a number of print devices. Configuration allows jobs to be pre-downloaded to the PDS location and then locally delivered to the printer at the time of release, reducing the time to print. In this mode, the administrator can configure both the time unreleased jobs are held centrally, as well as at the release station.

If the service is configured for Local Download, multiple copies of the print job are stored securely across the devices that are part of the pull group. If the job is printed from a device, the job will be purged from the local device. Optionally, the administrator can choose whether to delete the job from the central storage automatically after releasing the print job and also from all release stations after printing, or to allow the user to walk up to any device and print the job again.

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.

Walk-up Print Job Release

PrinterOn Printer Agent Software ("PrinterOn Release Agent")

Through technology partnerships with HP Inc., Ricoh, and Samsung, the PrinterOn Release Agent resides directly on specific printer and MFP models from these manufacturers. This enables users to release documents directly from the print device panel. Secure release is done through several different methods depending on the printer manufacturer and the exact user interface of the printer or MFP model.

Release via PrintValet Keypad

For those printers that do not have built-in agent release capability, the PrintValet keypad network device provides users with the ability to release their documents securely using PrinterOn unique, per job release codes. The keypad can be connected to any printer or MFP, adding secure release capabilities to any device. A 4 to 10 digit unique release code is provided for every document submitted. Only those with the code can access and print their documents.

Release Using PDS on a Windows PC

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 running on a Windows PC enables users to release their documents securely using either PrinterOn release codes or through cloud-based user authentication services (or LDAP/AD services). When configured for user authentication, the user will authenticate themselves against the cloud-based user authentication service (or LDAP/AD server)—using CPS as the intermediary—before being allowed to access the print jobs. The communication between PDS and CPS are over TLS.

Release Using a Third-Party Print Management System

PrinterOn can be deployed in conjunction with a variety of queue-based, third-party print management solutions. In these cases, PrinterOn hands off a print job to these systems for processing, delivery, and secure release.

The primary requirement of integrating PrinterOn with an existing print management solution is ensuring a user's identity is correctly linked with their print job throughout the entire print process from submission, to authentication, to job release. PrinterOn 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 user credentials as the existing print management system. PrinterOn will extend authentication and authorization to all its supported printing methods. By providing the print management system with the necessary user information, PrinterOn effectively extends the existing tracking and auditing capabilities to include:

- 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

Geographical Considerations in the Cloud

For PrinterOn managed cloud deployments, PrinterOn adopts a shared responsibility approach to data security. This means PrinterOn works with customers to ensure that it meets the security requirements specific to the customer. PrinterOn will be transparent and provide the information necessary for the customer to make an informed decision. It is then the customer's responsibility to determine if their specific security needs and requirements have been met. This shared responsibility is critical as each organization's requirements are different and are impacted by regional jurisdiction that varies based on their business, location and size.

PrinterOn Enterprise Managed Cloud runs in the PrinterOn Cloud. PrinterOn Enterprise can also be deployed in a private cloud behind an organization's firewall or in any third-party datacenter in the world. Based on customer requirements, the service allows for selection of the appropriate data center that complies with the security and legal requirements of the client. PrinterOn's preferred hosting datacenter locations are in the U.S. and Germany to service European customers.

PrinterOn's underlying cloud infrastructure service provider is in compliance with current EU Privacy Guidelines and GDPR requirements. The service provider is also a member of the Association of Cloud Infrastructure Services Providers in Europe (CISPE). Services used by the PrinterOn are all compliant with the CISPE code.

PrinterOn's service is designed to allow for each client to access the appropriate regional datacenters using location-based DNS resolution. This ensures clients in one geographic region access services in the region desired.

Standards Compliance

PrinterOn Enterprise managed cloud service operates in a facility that complies with all key standards and ensures a high degree of accountability and security. Internationally recognized certifications and accreditations include compliance with ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1 and others. PrinterOn's infrastructure provider also helps its customers meet local security standards such as BSI's Common Cloud Computing Controls Catalogue (C5), which is important in Germany.

Of course if a customer chooses to deploy in their own private cloud, whether behind their firewall or with a third party, compliance with these standards is the customer's responsibility.

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, True Cloud Printing™ , Secure Release Anywhere™, 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, Azure AD, Active Directory, and Microsoft Visio are trademarks or registered trademarks of Microsoft Corporation.

iPad, iPhone, AirPrint and macOS 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, Google Cloud Print, 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

Version 3.0 | December 2017

PrinterOn is the premier cloud printing solution that enables users to securely print from any smartphone, tablet, laptop or desktop, to any printer, no matter the networks in between. With PrinterOn you can "Print Simply Anywhere®".

Today PrinterOn has the broadest and deepest secure mobile print offering available for cloud or on premise deployment. This is a direct result of cumulative product innovation and evolution since 2001 when PrinterOn pioneered secure mobile printing.

Today PrinterOn is an HP, Inc company. PrinterOn has both the strength and wherewithal of a global technology leader and the agility of a smaller independent company to advance the state of secure cloud printing, tracking, and management. This unique combination enables PrinterOn to continue to both innovate and support its customer base around the world. www.printeron.com

PRINTERON®
print simply anywhere