Printix Security and Privacy Guide

Introduction

Printix is a cloud-based print management service especially designed and structured to provide a complete print infrastructure and secure printing environment, that guarantees efficiency, productivity and cost savings. This document describes the components, and architecture of the Printix Cloud system to provide an understanding of the way we handle privacy and security in our solution.

With Printix Cloud Print Management Service you can make printing part of your all-cloud strategy. Say goodbye to print servers and hello to an automated print infrastructure. Printix supports federated Single Sign-On with Microsoft Azure AD and can be deployed with Microsoft Intune. Our powerful cloud technology and innovative client technology is scalable by design and can handle any number of users and printers. Printix gives you flexible and secure printing, and you can automate print driver and queue management and eliminate the need for a print server. Printix is built to work for you and grow with you.

Serverless print infrastructure

Our powerful technology can handle multiple sites and separate networks. You do not have to concern yourself with print server scalability, capacity planning and VPN. There is no manual effort involved in maintaining Printix Client, as it will silently update itself to the latest approved version. Print processing is done locally on the computer, so no additional network traffic is needed to transfer print data to a print server. Printix Client can convert existing print queues.

Driver store

Printix maintains a global driver store with Windows and macOS print drivers. When you start to use Printix Client, it will automatically upload print drivers and put them in your Printix driver store. If there is no dedicated print driver for a particular printer, then an appropriate Universal print driver may be used.

Central web-based management

With Printix Administrator you can configure Printix and centrally manage your printers from a web browser. Minutes after a printer has been unboxed and connected, it can be added to Printix via a smartphone, tablet or computer. You can have print queues automatically added on users' computers.

At a glance

Printix is a multi-tenant cloud print management service. It runs with the Printix Client software installed on users' computers (Windows and Mac) and creates a virtual blueprint of the customers' on-premise print infrastructure, managed in the Printix Cloud service. A Printix installation is therefore, maintained in the cloud but run locally via a network of clients. Each customer is called a tenant or a Printix Home.

Print Driver Management

Any printer discovered in your network is presented to you in our web interface, Printix Administrator. Your configuration data is stored securely in your Printix Home in the cloud, and so are print drivers that Printix Client uploads to your Printix driver store. Your Printix Client is built to only work with your Printix Home and users are required to sign in before use.

- Add, Modify and Delete Print driver configurations to configure:
    - o Device settings (Paper trays, Duplexer, Stapler, Hole punch, and output bins).
    - o Printing defaults (Finishing options, Print 2-sided, and print in black).
- Remotely Add, Update and Delete Printix managed print queues.
  Use Groups to grant exclusive access to printers and deploy printers based on users' group memberships.
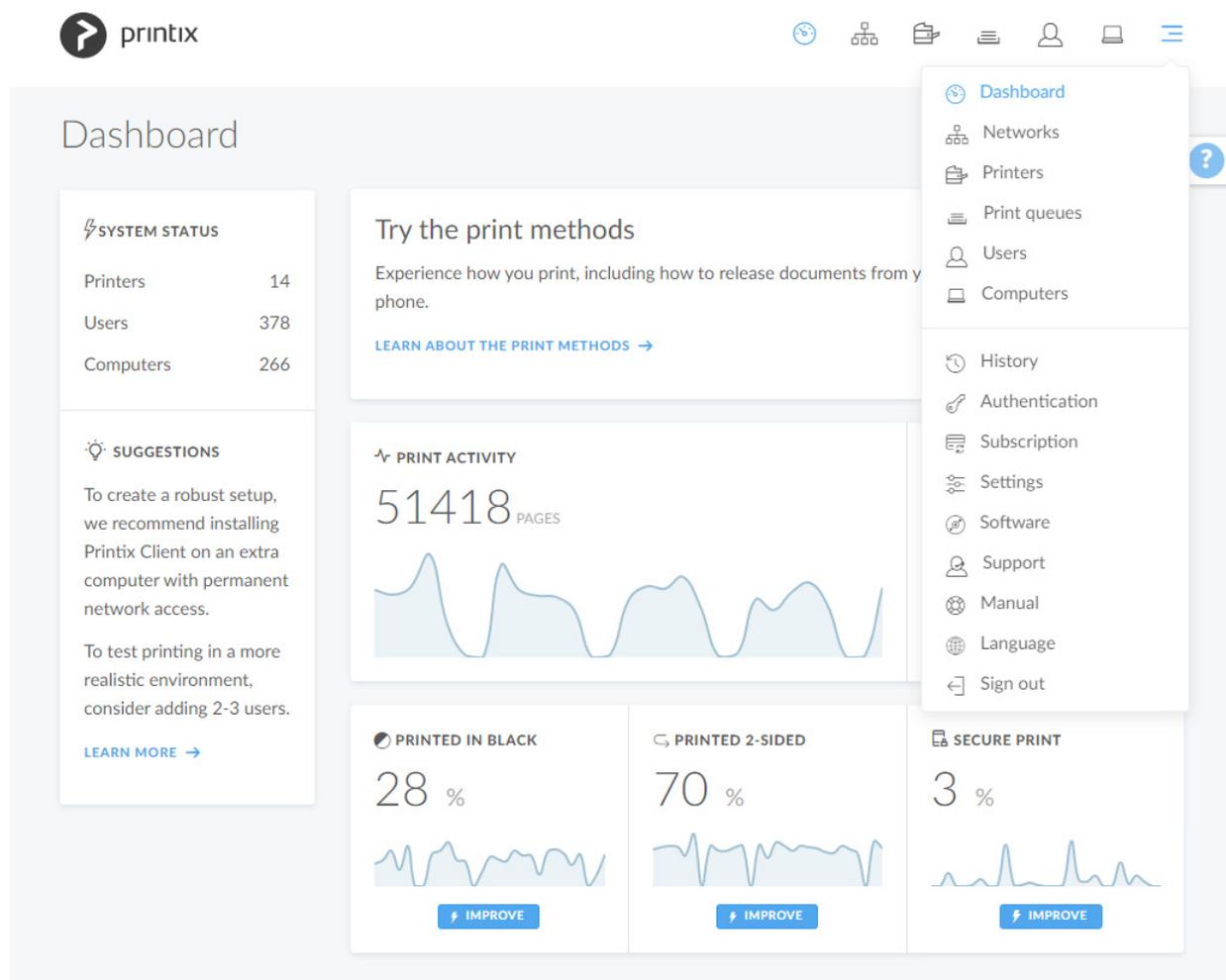
In Printix's multi-tenant architecture, multiple customers' data co-exist in the same infrastructure and run the same shared instance of software. The data is separated logically and secured, but no modifications or customizations may be made to the shared underlying structure. This would be comparable to an apartment building where each tenant has access to only their part of the building, but some resources and services are shared.

Printix Cloud Print Management Service consists of these components:
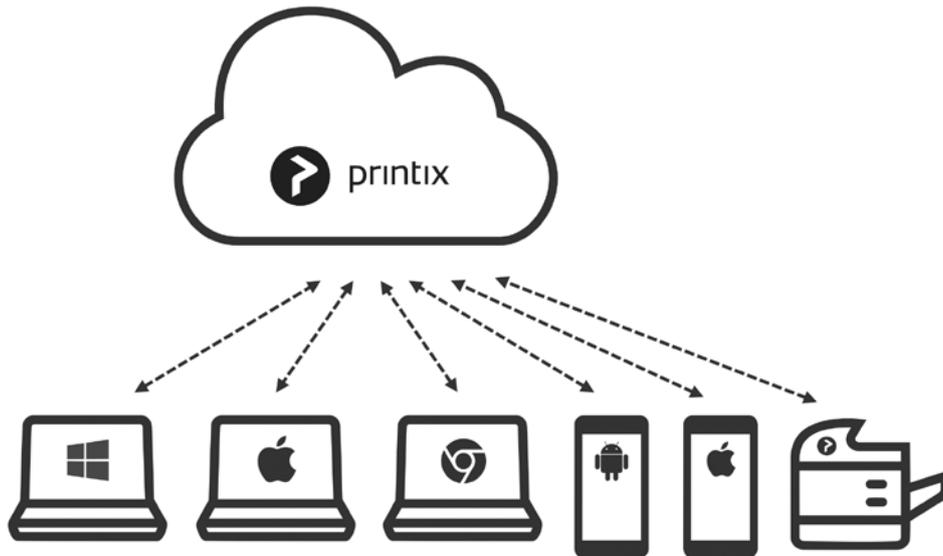
Printix Cloud

Where the customer's print infrastructure is orchestrated by Printix i.e. automated provisioning of the infrastructure services. Handles authorization, configuration data and most of the business logic. Communicates securely with the other components via HTTPS. Printix runs its server infrastructure on Microsoft Azure cloud infrastructure located in the Netherlands. Azure is a Safe Harbor solution and meets a broad set of international and industry-specific compliance standards.
Learn more: https://www.microsoft.com/en-us/trustcenter/security/azure-security

Printix Client

Automates the creation of print queues and installation of print drivers. Runs on users' Windows and Mac computer. The user interface of Printix Client runs under the signed in user's account. The Printix service runs under the Local System account. Both applications write log files that are stored locally. Printix Client communicates with Printix Cloud, to receive context specific configuration details and orchestrate the user's printing. Printix Client is unique for each tenant. Users are required to sign in before use, which can be achieved seamlessly with Printix Single Sign-On support.

Printix for Chromebook

Print to Printix managed printers from Chromebooks and computers with Google Chrome.

Printix Administrator

Web-based interface used to configure Printix and manage your printers, print queues, and print drivers.

Printix App

Used to release, print and delete documents. Used to print confidential documents safely with print release from a smartphone. Runs as a native app on Android and iOS/iPadOS devices and as web app in a web browser.

Printix Redirector

Used to enable printing to a print queue on a Windows computer and enable third party Follow/Pull print queues from PaperCut, SafeCom, Equitrac, PrinterLogic and similar third party Pull Printing solutions and to enable USB printing.

How Printix printing works

The secure and flexible methods of printing with Printix are achieved by allowing Printix Client to temporarily store print data encrypted on the computer and notifying Printix Cloud about the document. Users can print directly (as usual) or they can print securely and release documents from Printix App on their phone, tablet or computer. Pending documents can also be stored in your own secure cloud storage (Azure Blob Storage or Google Cloud Storage).

Behind the scenes the process of releasing the document is as follows:

1. Printix App sends a release-document request to Printix Cloud. The user's record of pending documents is consulted to determine where the document is stored.

2. Printix Cloud sends the release-document request to a Printix Client on the user's computer.

3. The Printix Client on the user's computer decrypts the print data and sends it to the designated printer.
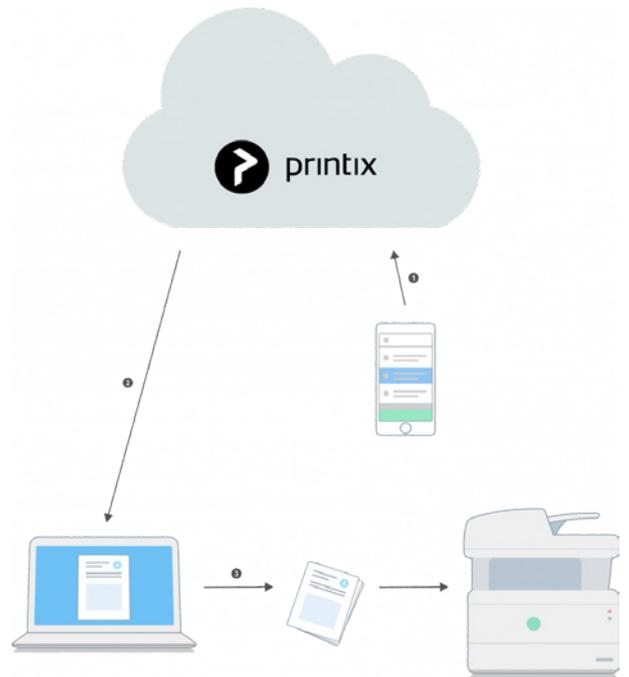

Figure 1: Overview over Printix print scenario

Print via the cloud

To offer the flexibility of being able to print across different networks or geographic locations, like from home to the office or between branch offices, the print jobs can be relayed via the Printix Cloud.

For printing to work, a user's computer (with Printix Client installed) must be on the same company network as the printer. By enabling Printing via the cloud, users can print to this printer from any location like another company network or from home. Printing is achieved via the Printix Cloud and a Printix Client computer on the printer's network. The document remains secure during the transfer over the Internet as the document itself and the communication are both SSL encrypted with Advanced Encryption Standard (AES) with a key length of 256 bits. The document is also encrypted internally when routed and printed internally.

Documents

- Documents are encrypted and stored locally until they expire and/or get deleted.
- Documents do not leave the customer's network, unless using Print via the cloud is enabled.
- Document names can only be seen by the owner of the document.
- Advanced Encryption Standard (AES) with a key length of 256 bits is used to encrypt documents.

Enable printing via the cloud for printer BNM in Berlin.

The user on computer A in Amsterdam can now add the BNM printer and print to this even though it is in Berlin.
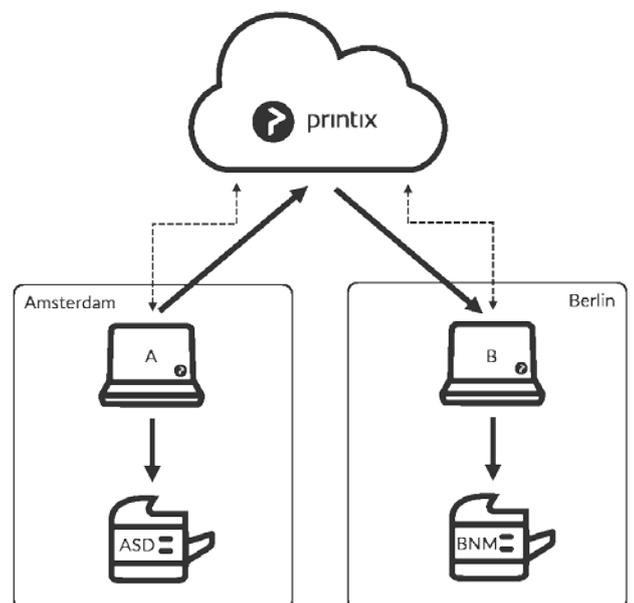
Security and data protection

What data is registered in the Printix Cloud?

To allow customers to manage their print environment via the Printix Cloud and offer its services, Printix registers necessary information. This is typically the information the customer can either see directly or in a processed format in the Printix Administrator interface.

The customer configuration data is stored securely in their Printix Home in the cloud, and so are print drivers that Printix Client uploads to their Printix driver store.

Printers: Address, Vendor, Model name, Name, MAC address, Serial number, Capabilities, Page counters, Consumables data, and statistics.
Computers: Address, Hostname, Type (Laptop, Desktop, Server), System (Windows, Mac).
Networks: Gateway IP and MAC addresses.
Documents: Name, Number of pages, Color, 2-sided, and where and when it was submitted, printed, and deleted. Documents can be stored in the cloud, when cloud print is enabled.
Log Files: System behavior.
Print Drivers: Print Driver program files and configurations.

Users:

Name (as for passwords, please see Authentication below)
Email
Role (User/ System manager)
Department (Azure AD only, and can be used to post data for subsequent departmental billing)
Groups (Only the group membership relevant to Printix functionality is recorded)
As for passwords, please see Authentication below

In addition, data about the customer is stored in the database to run the tenant, such as number of users, last billing period, company address, tokens, logging information and system configurations.

Personally Identifiable Information

• Personally Identifiable Information (PII) in the form of a users' name, email and document names are stored in the Printix Cloud. Here document names are kept as part of job history for 90 days to allow troubleshooting by Printix. In Printix App and Printix Administrator users (and system managers) can only see the document names of their own documents, and only while the document is pending (typically 1 day and maximum 7 days).
• Enabling Cloud storage will for the duration of the pending documents, store the document name and the name of the user as part of the document's metadata.
• Setup of Analytics with an own Azure SQL database will also populate users' name and email into this (but not document names).

	Default setup	Custom setup
Printix Cloud	+ User name and email + Document name (90 days) + Document files, transit only, no storage	+ User name and email + Document name (90 days) − Document files, no transit, no storage
Cloud storage ☁	N/A	+ User name (max 7 days) + Document name (max 7 days) + Document files (max 7 days)
Analytics ▮▮▮ **Own SQL database**	N/A	+ User name and email

How do you separate my data from other customers' data?
Printix uses an authentication/authorization security model based on OAuth, the industry-standard protocol for authorization, which only allows a customer to see their own data.

How do you control the access to customer data by Printix admins/DBAs?
Data access on a DB level is controlled with access rights like DBA. When the application requires access, a user is used to gain access to the database. A user on a tenant can only access data for that tenant. It is only allowed to access the databases from the Printix headquarter and from the Printix cloud.

Data-at-rest protection

How do you separate my data from other customers' data?
Printix is currently hosted in the Microsoft Azure™ data center in The Netherlands. When other data centers open across the globe, this will ensure data sovereignty at all times as customer data remains within the local region.

How strong is your encryption and data integrity?
Printix uses SSL encrypted with Advanced Encryption Standard (AES) with a key length of 256 bits. Databases are backed up daily. The backups are stored encrypted on other locations than the data center. Disaster recovery processes are in place in case of data loss or data corruption. Tenant data gets deleted three months after a tenant stops being a Printix subscriber. As per the terms of service, the 3-month grace period allows a customer to collect data, after the agreement has stopped.

What kind of authentication and access control procedures are in place?
For direct server access to customer systems, Printix uses Secure Shell (SSH). All systems require authentication/ authorization before a user can have access. Access to perform very sensitive tasks, like deleting a tenant, requires Two Factor Authentication.

Documentation for auditors
For audit documentation of Microsoft Azure, where data is stored, please refer to the following:
https://docs.microsoft.com/en-us/azure/security/
https://www.microsoft.com/en-us/trustcenter/security/azure-security

Print data security
The standard setting in Printix sends print jobs unencrypted from the Printix client to the printer. This follows the industry standard for network printing with print servers - TCP/IP and IPP printing – which addresses modern printing requirements including security, job status and printer feature capability.

If a higher level of internal security is required, Printix supports encryption of the print jobs between the Printix Client and the printer. However, this requires that the printer supports enhanced security and not all do.

With Printix' secure document release features like **Print later** and **Print anywhere**, users have the option to hold a print job until they arrive at the printer, and only then release the documents via their smartphone.

Data-in-motion protection

How do you get data from me to you?
Data between the Printix Client and the Cloud is always transported SSL encrypted.

How do you transfer data from one place to another?
Customer data is always transported encrypted.

Can any third party (your service providers) access my data, and if so, how?
Third parties can only access Printix data in encrypted form. For instance, Azure is not able to bypass Printix security and has no access to Printix data, despite owning the data center from which Printix runs.

What about management of encryption key?
Part of key management takes place with Azure Key Vault. Additionally, when an employee leaves the company, their key is revoked from relevant servers.

Can you ensure that all my data is wiped at the end of service?
Normal procedure for an "end of service", is that Printix automatically deletes the tenant data three months after the subscription has run out.

Which data is deleted?
Print data is not stored, unless the customer uses Printix's Print Via the Cloud feature, where data is encrypted and stored for 1-3 days. Otherwise, print data does not leave the company's network. With Print Via the Cloud, the data stored pertains to user print behavior e.g. when a given document was printed, number of pages etc. Printix does not have access to the document itself as it is either encrypted or not transported to the cloud.

Can you ensure that all backup and tapes are erased at the end of service?
Data backups are stored for 30 days, thereafter the customer data is purged from the Printix system.

Data portability

Are there documented procedures and APIs for exporting data from the cloud?
Printer meter readings and user print data can be downloaded via the Printix API and saved as .json files.

Do you provide interoperable export formats for all data stored within the cloud?
CSV file export for all data stored in the Printix Cloud.

Are the API interfaces used standardized?
Yes. System integration is possible with our RESTful API.

What assurance can you provide to your customer regarding the physical security of your location?
All data centers are Azure data center certified.

Secure Communication and network ports

All Printix communication inside and outside the network is secured with encryption and the use of HTTPS (SSL/TLS). Documents are stored encrypted until they expire and get deleted. Documents do not need to leave the customer network.

Secure browser communication between the components and Identity Providers, such as Microsoft Azure AD, Google and others is done with HTTPS on TCP port 443.

Printix does not need any open inbound ports in the firewall. The Printix Clients initiate the communication with the cloud. The Printix client requires access to communicate with the external cloud. SNMP v1 or SNMP v3 can be used to collect information from printers. The default setting is SNMP v1.

The Printix clients communicate internally on the customers' network using port 21335. This traffic is encrypted.
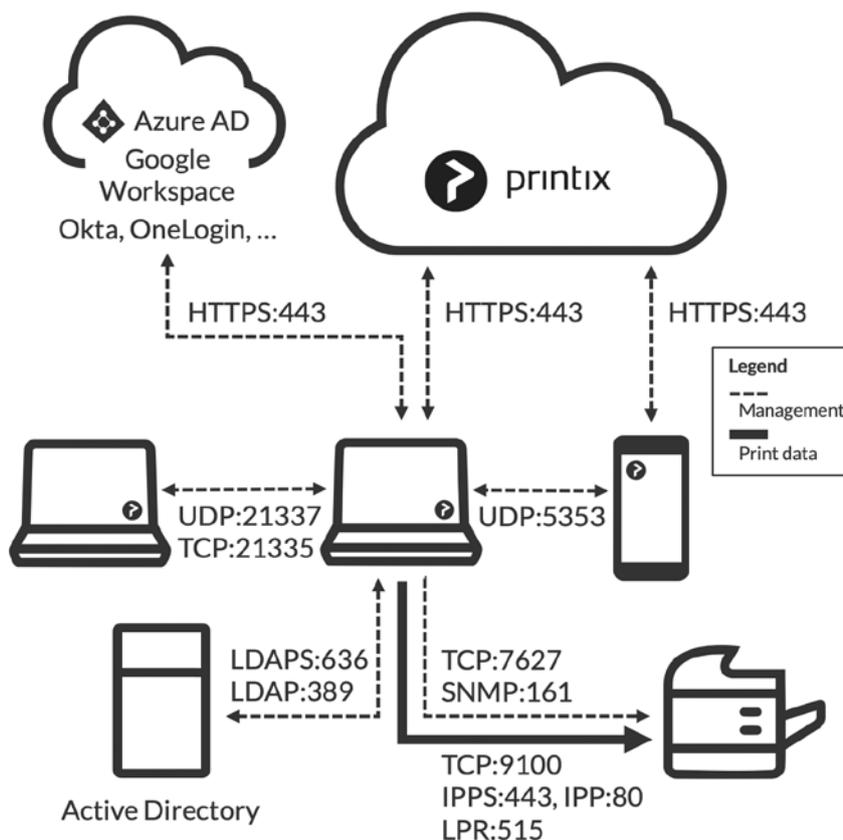

Figure 2: Overview over ports and network protocols used in Printix.

Ports Printix uses to communicate and print

These ports must be open within the network:

SNMP on UDP port 161 for access and to collect information from printers via SNMP v1 or SNMP v3. If the customer requires a Community name, which is different from: "Public", please inform Printix. ICMP message requests and replies must be allowed on the local network, as the ping command is used to discover printers.

RAW print on TCP port 9100 to transfer print data to the printers. The computer with a Printix Client installed must be able to reach the printer on the network to allow printing. Print data can also be sent via LPR and TCP port 515. Use of other port numbers is also supported.

TCP port 21335 to forward print data to another computer running Printix Client. Encrypted.
TCP port 21336 for communication to Printix Redirector, if that is installed, on a Windows Server.
UDP port 21337 for Printix Discovery Protocol used to find computers running Printix Client. Not encrypted.

If Active Directory authentication is enabled, one of these ports must also be open within the network:

Secure LDAPS on TCP 636 for authentication of users via secure LDAPS.
LDAP on TCP port 389 for authentication of users via LDAP.

The Printix Client requires two ports to be open on the local computer, which is done automatically during installation:

TCP port 21338 and 21339 for secure local communication. TCP port 21338 is used for communication between the two processes: PrintixClient.exe and PrintixService.exe. TCP port 21339 is used for listening by the Printix Client built-in web server for sign in and printing (Windows print spooler and CUPS).

Web proxy and SSL inspection
Use of a web proxy and/or SSL inspection may for example prevent Sign in to Printix Client. The customer <u>must</u> add the printix.net domain and subdomains as exceptions so traffic is not blocked.

URLs that must be exempt from SSL inspection:

Required
assets.printix.net
api.printix.net
auth.printix.net
sign-in.printix.net
drivers.printix.net
software.printix.net
* websocket.proxyendpoint.printix.net
acme.printix.net
(replace acme with your Printix home)

Required, if you enable print via the cloud
https://printix-jobs-file-upload.s3-eu-west-1.amazonaws.com
https://printix-jobs.s3-eu-west-1.amazonaws.com

Required, if you enable mobile print (Apple AirPrint)
https://airprint.printix.net

Required for optional data extraction
https://*.blob.core.windows.net

Authentication

With Azure authentication enabled, users' passwords are handled entirely by Azure. Printix never collects passwords.

With Google authentication enabled, users' passwords are handled entirely by Google.

With Active Directory authentication enabled, users' passwords are not stored by Printix, but can be transferred securely via LDAPS to the local Active Directory server for authentication.

For users who authenticate directly with Printix, passwords are protected through salted password hashing. Users can reset a password themselves with a required email address. Passwords must be minimum 6 characters in length and contain uppercase letters, lowercase letters, and digits.

Printix supports Single Sign-On with Azure AD, Google Authentication, Okta, OneLogin, Active Directory and LDAP. With Azure AD, the system administrator can pre-authorize users, so they are automatically signed in to Printix when logging into the computer, without being prompted by Printix.

Printix uses role-based access control to determine what operations a user can and cannot perform.
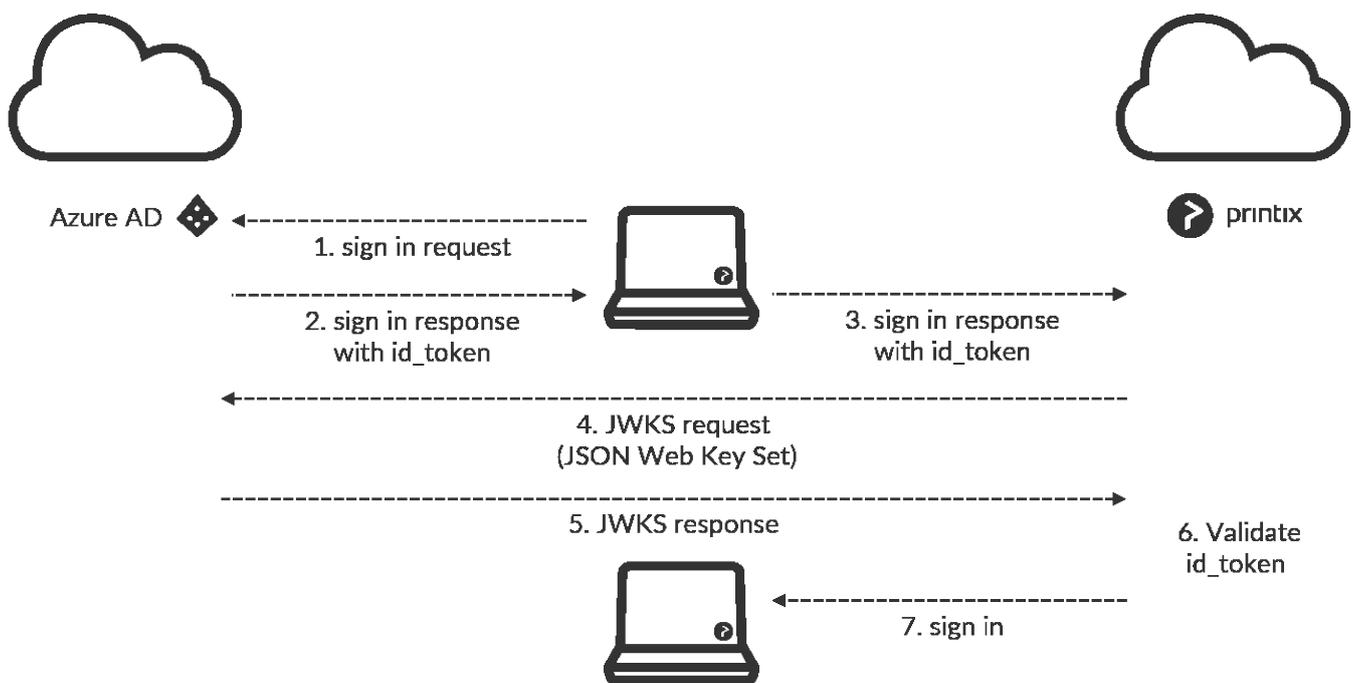
Authentication flow for Azure Active Directory (HTTPS:443)

Client upgrade and maintenance
The Printix Cloud orchestrates the Printix Client software maintenance, upgrades and patching automatically. The client is always patched and run on the newest and most stable version of Printix. The Printix Cloud is maintained, patched, administrated daily.

System monitoring and Service Level Agreement
Printix Service Level Agreement is available online. Printix offers a cloud uptime of minimum 99,9 %. Cloud uptime is the amount of time that cloud systems and cloud services hosted by Printix are up and accessible by end users. The high uptime and performance is achieved with an auto-scaling, load balanced multi-server environment with failover and 24/7 system monitoring. Most upgrades of the Printix Cloud and releases of new features are achieved while the Printix environment is in operation.

Approximately once per quarter, 30-minute service windows may occur during weekends, for larger maintenance releases or updates. The service windows are announced in advance.

What if the cloud is not available?

If the Printix Cloud is not available, due to Printix Cloud downtime, Internet outage or customer network difficulties, it is still possible for users to print. Advanced printing features (print anywhere, print later) are not possible without an internet connection, however if users have access to a printer, they can still print.

How do you overcome the traffic load of local printing assets?

Printix uses client technology in combination with a public cloud solution on Azure. Printix Client software is installed on users' computers (either deployed centrally via for example Microsoft Intune or downloaded through a link).

Print jobs never leave the local environment (unless using Print via the cloud is enabled) and in this way, utilize merely half the network bandwidth compared to a print server scenario. Print data traffic is routed directly from the client to the printer, also called direct IP printing.

With direct IP printing via locally managed drivers (not via print server), how do you handle security?

The first step in print security is keeping the print jobs on the local network and HTTPS encryption. Users can authenticate themselves either via the Printix account, Active Directory, LDAP, Office 365 or many other authentication provider technologies.

As we do not need to install any software on printers, security updates are not necessary and thus, potential leaks avoided. Finally, with secure pull printing, print jobs are safeguarded until release via user authentication at the printer. Print jobs are released from the Printix web app from any web-enabled device.

What is your downtime plan (e.g., service upgrade, patch, etc.)?

The system runs 24/7. New releases and patches are committed to the production environment without any downtime. The cloud and micro services setup make sure that upgrades are done while the system keeps running. A maintenance window is on average announced once per quarter. Remember, even when the Printix cloud is down, the customer can still perform basic print.

Do you have DDoS protection, and if so, how?

Azure does by standard, see documentation: Distributed denial-of-service defenses protect Microsoft's cloud services from network-layer high-volume attacks that choke network pipes and packet-processing capabilities by flooding the network with packets. Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of the Azure continuous monitoring and penetration-testing processes. The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. The Azure DDoS defense technology provides detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to help ensure that network-layer high-volume attacks on the platform itself do not impact customer environments. Application-layer attacks, on the other hand, are direct attacks launched against a customer deployment. The Azure DDoS defense system doesn't provide mitigation or actively block network traffic affecting individual customer deployments, as it's not possible for the system to interpret the expected behavior of customer applications.

Disclaimer: This guide is not legal advice and cannot be interpreted as such. Ensure the requirements of GDPR , HIPPA and other privacy regulations are accurately interpreted for your company's specific use by a legal professional.