PrinterLogic SaaS Security: A Technical Overview

An operational summary of design and secure communication protocols in PrinterLogic SaaS

PrinterLogic

PrinterLogic Overview and Scope of This Paper

PrinterLogic earned its reputation by providing a serverless printing infrastructure that is feature-rich, secure, and easy to use. There are two versions: a true SaaS implementation that eliminates the need for server resources, licensing, or maintenance, and a self-contained Virtual Appliance for on-prem use.

Due in part to widespread migration to the cloud, PrinterLogic SaaS is fast becoming the preferred solution among customers. It is a completely serverless, multi-tenant, print management platform for organizations that want a secure and efficient way to manage printers and drivers across the organization.

PrinterLogic converts your printing environment into a highly available, centrally managed direct-IP printing system. There is no need for Group Policy Objects (GPOs) or scripting to deploy and manage printers and drivers. And, because print jobs go straight to the printer via direct IP, your confidential data remains local and WAN traffic is minimized.

Key components of PrinterLogic SaaS include a cloud instance (hosted in AWS), a small app that's installed on every workstation (a client), and an enhanced client for additional services that's a shared resource. The third piece is installed on any workstation that stays on.

This paper provides security and operational details about PrinterLogic SaaS. All references to PrinterLogic in this paper apply to the SaaS solution. While there are similarities, the information below does not necessarily apply to the on-prem version.

PrinterLogic Instance and Client Communications

PrinterLogic is an APN Advanced Technology Partner that has passed the AWS Well-Architected review. It inherits all of the benefits of AWS Cloud Security.

PrinterLogic uses an instance-client model to manage and deploy printer drivers and default printing preferences. The client is a small app that's installed on end-user workstations and uses an MSI installer file for Windows, a PKG file for macOS, DEB and RPM files for Linux, and an Extension for Chromebooks. It communicates with the PrinterLogic instance over HTTPS using TLS and an OAuth2 security token that is granted when the client is installed.

Upon logging into the workstation (and on a scheduled interval), the workstation client uses the OAuth2 secure token to broker requests made to the PrinterLogic instance. The client sends an HTTPS request to the PrinterLogic instance to see if any activities are assigned to the

workstation or the user. If the workstation client does not have a valid OAuth2 security token, it is denied communication with the PrinterLogic instance, and the user is told to contact their administrator for a new code.

Once the workstation client has a valid OAuth2 security token, all communication including driver and profile installs/updates, client updates, metadata reporting, and client check-ins is secured over HTTPS and TLS. This eliminates the need for additional open ports in the firewall.

Expiration lengths are assigned to authorization codes for OAuth2 security tokens. Authorization codes that are not used within the allotted time become invalid and a new one must be generated. If needed, the administrator can revoke an OAuth2 security token for any workstation. In this case, the workstation client asks for a new code. Once a new code is entered, the client is then granted a new token, and the expiration timer for the authorization code begins again.

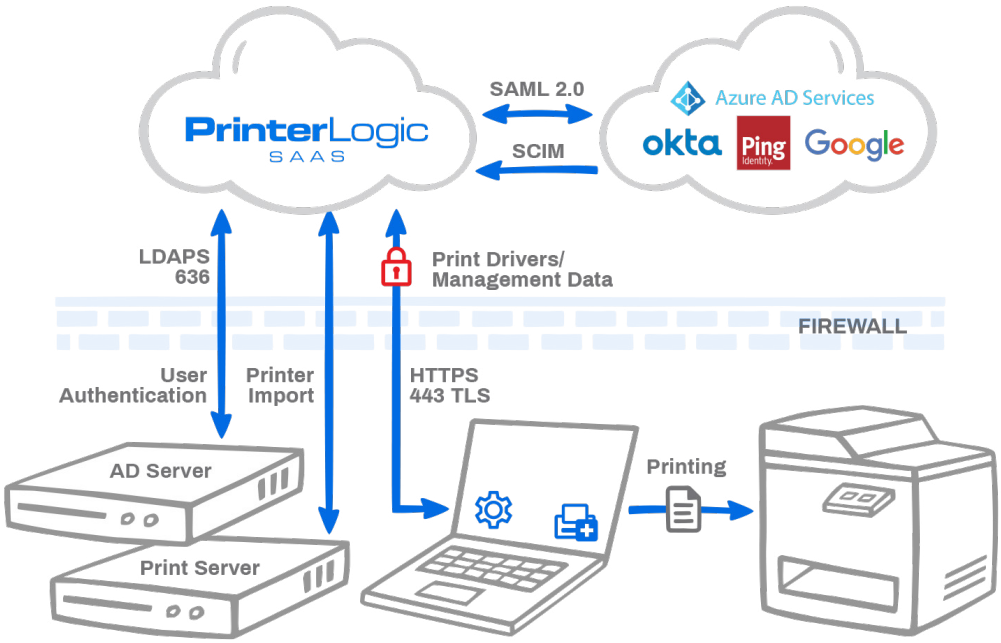

Figure 1: PrinterLogic communication pathways for SaaS instance, workstation client, and identity providers (IdPs).

The PrinterLogic Admin Console and Driver Deployment

Printer drivers are uploaded to the PrinterLogic instance using a manual upload process or via an automatic method that's set up when PrinterLogic is configured. At start-up, PrinterLogic can

import drivers and profile settings from one or more print servers that will be decommissioned later. In order for this to work, an OAuth2 security token is obtained using the authorization code for the workstation that's running the PrinterLogic import tool.

The PrinterLogic Admin Console is used to specify that a driver needs to be installed by the workstation client, aside from the Chrome OS Extension which uses driverless IPP technology. When a client checks in and receives this instruction, it scans the local workstation first for the specified driver. If it's not available, the client downloads the driver from the PrinterLogic instance or a designated driver cache. The driver is then installed using system-service privileges on the workstation. Only drivers that are signed by a trusted certificate authority (typically the printer manufacturer) can be installed by PrinterLogic. The workstation client configures the driver according to the profile defined in the Admin Console.

When printer drivers are downloaded from the PrinterLogic instance, they are sent over an encrypted port (443) using HTTPS and are confirmed with hash verification. Drivers can also be stored in a local cache using a distributed file system (DFS), a file share, or a workstation that's always available. The client installed on a designated cache manager must first receive an OAuth2 security token to enable communication. Once the token is received, obscured printer drivers are copied from the PrinterLogic instance over port 443 to the file share. Other workstation clients in the environment retrieve printer drivers from the file share using port 445, which is a standard means of communication on a Microsoft-based LAN.

Print Jobs Remain on the Local Network

Print jobs are sent from Windows, Mac and Linux workstations directly to the printer via direct IP using port 9100 by default, or as defined in the PrinterLogic instance. PrinterLogic's Chrome OS Client Extension sends print jobs over IPP using port 631.[1]

For reporting purposes, **only metadata** for print jobs is sent via HTTPS to the PrinterLogic instance, and a valid OAuth2 security token is required for this communication. This metadata includes print job date, time, user, originating workstation, printer name, document title, page size, and page count. Transfer of document titles can be disabled in the Admin Console.

Communication with Microsoft Active Directory

PrinterLogic employs identity provider (IdP) services to authenticate and authorize users, groups, and computers for a variety of optional features. These include Admin Console login access, pull printing, and mobile printing.

Configuring PrinterLogic for Active Directory (AD) integration involves several steps. First, because the PrinterLogic instance is outside the firewall, the IT admin must ensure that firewall rules allow access to Active Directory using the encrypted LDAPS protocol port (636) using PrinterLogic AWS static IP addresses.

Second, when PrinterLogic communicates with the AD server, it routes the request from within the PrinterLogic SaaS Virtual Private Cloud (VPC) through a NAT gateway. Communication is initiated from the PrinterLogic instance over LDAPS using TLS encryption through the customer's firewall and goes directly to the LDAPS endpoint.

These transactions utilize two levels of security: First, the traffic is restricted to static IPs for the hosted AWS instance (these vary by geographic region). Second, all traffic is encrypted using TLS. Security is ensured because communication is encrypted over port 636 and is restricted to static IP address(es).

The PrinterLogic instance uses read-only permissions to access the AD server. Each time an authentication or AD membership is required (e.g., by Google Cloud Print, iOS Printing, Email Printing, Control Panel Platform AD Sync, or Badge ID if stored in AD), PrinterLogic requests the AD using a BIND service account. The BIND account information is encrypted and stored in the PrinterLogic database. For added security, the administrator can use a BIND service account with read-only permissions.

When using PrinterLogic pull printing, some secure-release mechanisms require use of the LDAP Sync function. These include username/password, user ID/PIN, and badge release. A PrinterLogic utility synchronizes AD user names, badge IDs, PIN codes, and email addresses within the PrinterLogic user microservice. This data is synchronized using the BIND account and is accessed over port 443 by the Service Client or printer control panel application during user authentication at the printer.

The client installed on the end-user workstation does not connect directly to the PrinterLogic instance for user authentication. Instead, the client authenticates against Active Directory using Active Directory Service Interfaces (ADSI) from a Windows workstation. From a Mac or Linux workstation, it uses Kerberos tickets.

Communication with Cloud-based Identity Providers (IdPs)

If PrinterLogic is configured to integrate with a cloud-based identity provider such as Okta or Azure AD, user-identity information managed in the IdP console is synchronized with PrinterLogic.

This is done using either SCIM or JIT (when a user is logging in for the first time). If the cloud-based IdP provider does not offer native support for SCIM, PrinterLogic has a similar Identity Sync Service that runs on a Service Client and will synchronize the IdP users and Groups with the user microservice. Updates flowing from the IdP to PrinterLogic occur in real-time or every six minutes, depending on the mechanism employed.

In addition, logins to the PrinterLogic instance are facilitated through the IdP using the Security Assertion Markup Language 2.0 (SAML 2.0) or OpenID Connect (OIDC). Synchronized identity information provided by the IdP is used to authorize the following:

- Access to the PrinterLogic Self-service Portal
- Access to the PrinterLogic Admin Console
- Print job release authentication
- The PrinterLogic Client with the IdP user
- Printer deployments

Enhanced security features such as multi-factor authentication (MFA) and single sign-on (SSO), if enabled, are handled by the identify provider. These capabilities improve authentication security and offer productivity advantages for end users.

More information about how PrinterLogic integrates with leading cloud-based identity providers, including operational details and security standards, is available in this white paper.

Zero Trust Off-Network Printing

Off-network Printing allows users to print from any location with internet access to printers behind the company firewall. Print traffic is encrypted using TLS, and any print jobs held on the service client for pull or secure release will be encrypted while at rest inside the network. There are two parts of this solution, the External Gateway and Internal Routing services.

External Gateway Service: The External Gateway is used to receive off-network print jobs from remote workstations over HTTPS (port 443) using TLS encryption. The External Gateway is hosted as a service in AWS by PrinterLogic, though this can also be hosted by the customer, or a hybrid model can be used. If the External Gateway is hosted by the customer, it will run on a Service Client and requires an SSL certificate.

Internal Routing Service: The Internal Routing Service runs on a Service Client inside the customer's network and watches the External Gateway for incoming print jobs via port 443 using Websockets. When a print job is sent to the External Gateway, the Internal Routing Service will immediately download the print job over port 443, and deliver it to the printer over port 9100 or over 631 for Chromebooks. If the print job is sent using the secure or pull print feature, it will be held by default on the end user's workstation.

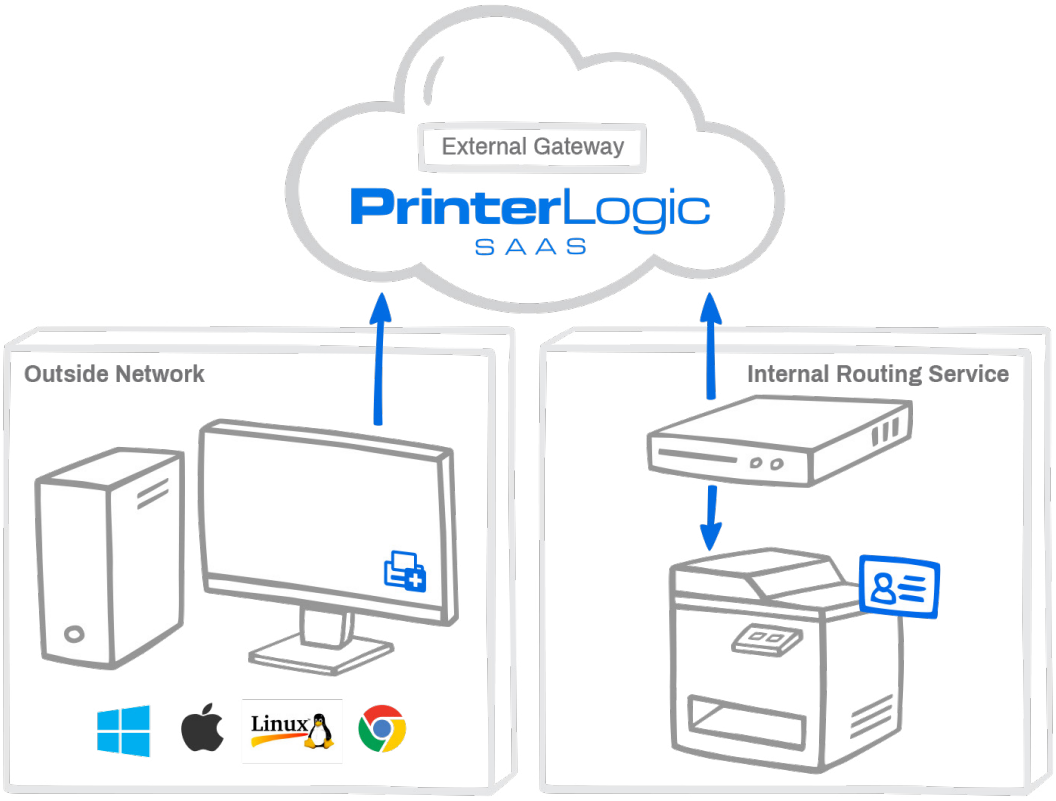

Figure 2: Off-network Printing where the External Gateway is hosted by PrinterLogic in AWS, and the Internal Routing Service is hosted on-prem by the customer.

Pull Printing, Secure Printing, and Offline Secure-release Printing

PrinterLogic offers three secure printing methods:

1. Pull printing (a virtual printer queue where user decides later where to receive the job)
2. Secure printing (a specific printer is configured to receive confidential print jobs)
3. Offline secure-release printing (a job is initiated, workstation goes offline, job is printed later)

In the pull-printing scenario, the user prints to a secure virtual pull printer that holds the job until the user is ready to authenticate at the printer of their choice and receive their output.

The secure printing method allows the administrator to designate a physical printer as a secure device. When a user prints to one of these printers, they get a prompt asking if they would like to have their job held, or if they want it released immediately. If they opt to have the job held, they go to the designated printer and authenticate to receive their output.

In either scenario, the print job is rendered by the print driver and stored in a raw or binary format on the user's workstation in *C:\Windows\System32\spool\PRINTERS\held\local*, a secure folder location that only administrators have access to, until the user goes to the printer and releases the job.

Offline secure-release printing is different. The end user initiates the print job and then has the option to shut down their laptop or workstation and receive the print job later. First, a copy of the print job is held on their workstation. In addition, a copy of the raw print job is sent to the PrinterLogic Service Client over port 31989, where it is encrypted using an open SSL AES-256 algorithm. It remains encrypted on the Service Client, at rest, in the *C:\Program Files (x86)\Printer Properties Pro\Printer Installer Client\service-offline-print\jobs\held* folder.

When the end user goes to a printer to release the job, PrinterLogic attempts to release the job that's held on their workstation. If the workstation is offline, PrinterLogic contacts the Service Client to release its encrypted copy. In the latter scenario, the print job is decrypted on the Service Client using Open SSL and sent to the target printer.

Once the secure print job is released, the extra copy of the print job is deleted from either the user's workstation (once the computer is back online), or from the Service Client, depending on how the job was executed.

Methods for Secure Release Authentication

PrinterLogic SaaS supports five mechanisms for releasing secure and pull print jobs:

1. **Mobile Release App (Android/iOS).** On an Android or iOS smartphone, the PrinterLogic Print Release App can be installed from the Google Play Store or the Apple App Store. In the app, the user enters their PrinterLogic instance URL and Active Directory username and password. Once they authenticate, they will see all secure and pull print jobs available for release, and available printers for each. Communication between the app and the PrinterLogic instance is over HTTPS using port 443.

   Secure print jobs must be received at a specific printer, while pull print jobs allow the user to select from any printer that's been configured as a pull printer. After initiating release from the app, PrinterLogic instructs the user's workstation client, using port 443, to release the job.

2. **Web-based Release Portal.** From any web-enabled device (i.e., phone, tablet, laptop, or PC), a user can use their AD or IdP credentials to log in to the PrinterLogic Release Portal. The portal shows their submitted pull/secure print jobs and lets them release one or more to the designated secure printer. Alternatively, they can select a destination printer from a list they are authorized to use. The PrinterLogic Release Portal authenticates the user over LDAPS port 636 with the Active Directory server. If IdP is used, the user is redirected to their IdP portal for authentication, where their credentials are entered and verified.

3. **Control Panel Application (CPA).** Once the IT admin installs the PrinterLogic application on a compatible network printer, end users can log in at the printer using their AD credentials or a User ID and PIN code. They are then shown any secure print jobs they sent to that printer as well as any pull print jobs waiting for release. When AD credentials are used for authentication, they are obfuscated and encrypted over port 443 to the PrinterLogic instance, and over port 636 to the AD server.

4. **CPA with Badge/Card Reader.** When a supported printer has a built-in badge reader or is equipped with an optional badge reader, the user can swipe their badge for automatic authentication and skip entering AD credentials manually. End-user badge IDs are stored in the PrinterLogic database using the CPA badge-registration process or in an AD attribute defined by the system administrator. When the badge is swiped, the badge ID is compared to IDs stored in the PrinterLogic database (over port 443) or in Active Directory (over port 636). Once authenticated, the user can release a single job or all held print jobs to that printer.

5. **Simple Badge Release.** By connecting an ELATEC TCPConv 2 or rf IDEAS® E-241 network

device and compatible badge reader to any network printer, the printer can be configured for fast, easy release of held print jobs. When the user swipes their badge on the reader, their badge ID is sent to the PrinterLogic Service Client over port 31990. The Service Client then relays that information to the PrinterLogic instance via port 443, where the ID is matched with a registered user account. PrinterLogic authorizes that user and sends a release command to the ELATEC or rf IDEAS® device over port 443, and the user's print job(s) are released. The administrator can configure Simple Badge Release to release either the most recent, or all, held print jobs in a single motion.

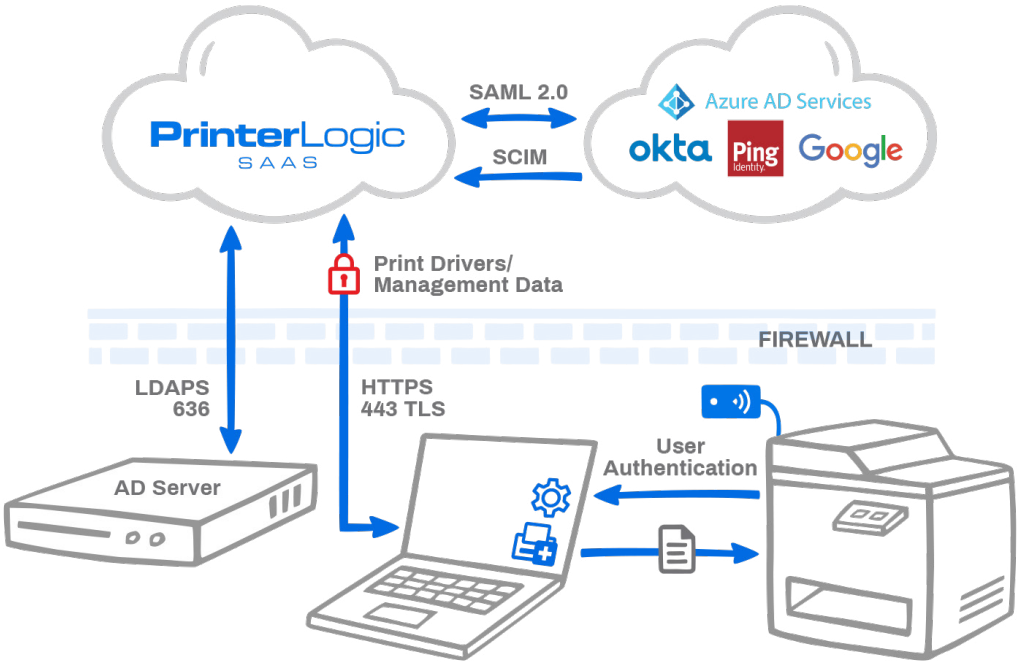

Figure 3: Communications flow for secure-release printing. Users authenticate against Active Directory, the PrinterLogic database, or a cloud-based IdP.

Mobile, BYOD and Email Printing

PrinterLogic's Mobile Printing module is a collection of features that allow native printing from iOS and Android devices. It also provides email printing functionality through the sending of attachements.

A mobile print job can be either (1) routed automatically to the pull-printing queue and held securely until released, or (2) released immediately to a preferred printer. In the first scenario, there are several ways to release the print job. These release options were covered on the previous pages. (See Methods for Secure Release Authentication above.)

Here's a summary of each Mobile Printing feature:

1. **Native iOS Printing.** A PrinterLogic AirPrinter is shared with the iOS device on the network using DNS PTR records. When the user authenticates using AD credentials the PrinterLogic AirPrinter is unlocked and the iOS device begins IPPS communication to the PrinterLogic Service Client over port 631. The mobile print job is converted to a PDF and held until it is released to the target printer. Print release uses the pull-printer driver over port 9100. The print job remains secure on the local network.

Figure 4: iOS AirPrint job flow from an iOS device to a designated printer. Print data remains local and secure, facilitated by the PrinterLogic Service Client.

2. **Android Device Printing.** To configure this feature, the administrator registers the PrinterLogic virtual pull printer as a Google Cloud printer. It's then shared, using the Google Admin console, with end users. The shared printer becomes available on any Android device the user logs into. A print job can be sent from the Android device to the Google Cloud Print service, where it is converted to a PDF. PrinterLogic's Service Client retrieves the job via HTTPS and holds it until it is released by the user at the designated printer.

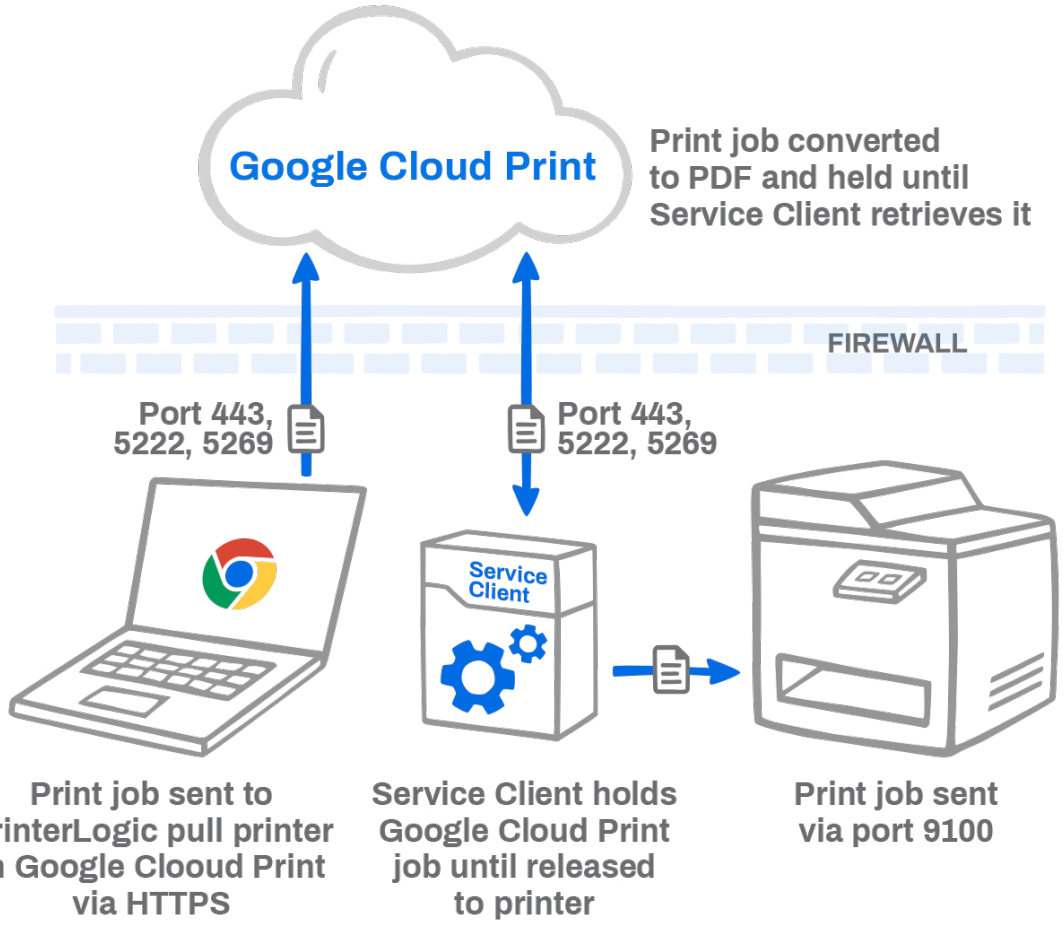

Figure 5: Google Cloud Print job flow from a Chromebook to a network printer, facilitated by the PrinterLogic Service Client.

3. **Email Printing Options.** PrinterLogic offers three email printing options: Email printing, Direct Email printing and Guest Email printing. All three use the same configuration, but they handle print jobs differently. These differences are explained below.

   With **Email Printing,** the admin creates or specifies a dedicated mailbox that is then monitored by the PrinterLogic Service Client. Any email sent to this mailbox is checked against AD using a BIND account to verify that the sender is an authenticated user. Emails that pass this test, including attachments, are retrieved from the dedicated mailbox by the Service Client using IMAP port 993 and converted to a PDF. The print job is held on the Service Client until it's released to the target printer via direct IP over port 9100.

   With **Direct Email Printing**, the admin creates or specifies a dedicated mailbox using a subdomain that is then monitored by the PrinterLogic Service Client. A mail-routing rule is created within the email service provider to route emails sent to the subdomain mailbox to the

primary email printing mailbox. Any email sent directly to a printer's direct print email address is retrieved by the Service Client and checked against AD using a BIND account to verify that the sender is an authenticated user. It's also matched to the destination printer's email address according to its assignment in PrinterLogic's Admin Console. Any emails that pass these tests, including attachments, are converted to a PDF and sent from the Service Client via direct IP over port 9100 to the target printer.

With **Guest Email Printing**, the admin creates or specifies a dedicated mailbox using a subdomain that is then monitored by the PrinterLogic Service Client. A mail-routing rule is then created within the email service provider to route any emails sent to the subdomain mailbox to the primary email printing mailbox. Any email sent directly to the guest printer's direct print email address is retrieved by the Service Client, where the email and attachments are converted to a PDF and sent direct IP over port 9100 to the target printer.

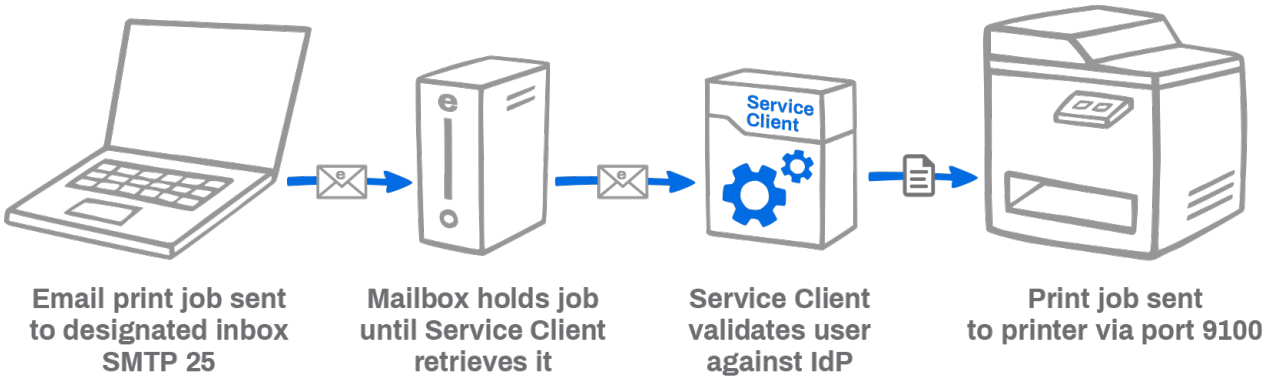

Figure 6: Email printing job flow using a PrinterLogic Service Client, including user-identity validation against Active Directory or a cloud-based IdP.

PrinterLogic Service Client

1. **Service Client functional overview.** The PrinterLogic Service Client is an essential component of PrinterLogic's serverless platform. It is an enhanced (promoted) version of the PrinterLogic Client that's used on every Windows, Mac or Linux workstation. The Service Client facilitates communication between the PrinterLogic instance and advanced PrinterLogic features and helps ensure that confidential print data remains on the local network. Here's a list of features that rely on the Service Client:

    - Email Printing (Standard, Direct, Guest)
    - iOS Printing

- Android Printing (via Google Cloud Print)[2]
- Installing a Control Panel Application on a printer
- Control Panel Application authentication (badge release, User ID/PIN)
- Simple Badge Release (for network printers without a console interface)
- Offline Secure Release
- SNMP monitoring (when Service Client option is enabled)
- Off-network Printing
- Identity Sync Service

2. **How the Service Client is configured.** In the PrinterLogic Admin Console, a Service Client object is created in the tree using the hostname or IP address of any Windows, Mac or Linux workstation that is always on. The PrinterLogic Client is installed on the designated workstation using the same security process described earlier in this document (See PrinterLogic Instance and Client Communications on page 2-3.)

   When the workstation client checks in with the PrinterLogic instance, it detects that it's been designated as a Service Client, and the client OAuth2 secure token is used to retrieve a second OAuth2 secure token from the PrinterLogic instance to facilitate the upgrade.

   The new Service Client then starts up the following processes according to the features that were enabled in the PrinterLogic Admin Console:

   - Email Printing - PrinterLogicServiceEmail
   - iOS Printing - PrinterLogicServiceAirprint
   - Google Cloud Printing - PrinterLogicServiceGoogleCloudPrint
   - Control Panel App - PrinterLogicServicePrinterApp
   - Offline Secure Release - PrinterLogicServiceOfflinePrint
   - SNMP Monitoring - PrinterLogicServiceSNMP
   - Simple Badge Release - PrinterLogicServiceSimpleBadgeRelease

- Off-network Printing - PrinterLogicServiceOffNetworkServer
- Identity Sync Service - PrinterLogicServiceIdentitySync

Conclusion

Any SaaS solution that manages the flow and retrieval of confidential information must be secure. With PrinterLogic, all communication between workstation clients and the AWS-hosted PrinterLogic instance are encrypted over HTTPS and TLS 443 with OAuth2 security tokens. Driver downloads are hash-verified.

PrinterLogic utilizes Amazon Web Services' security features to ensure that PrinterLogic systems and data are secure and take advantage of the AWS ISO 27001 certified platform.

With PrinterLogic's direct-IP architecture, every print job stays local. The only information sent over the WAN to the hosted PrinterLogic instance is print-job metadata. PrinterLogic now integrates with IdP services to authenticate and authorize users, groups, and computers. Multi-factor authentication, when provided by the IdP, is available. Confidential data is also protected through a choice of secure pull-printing capabilities, which are included in the core PrinterLogic SaaS license.

PrinterLogic provides a highly available secure serverless printing platform that empowers IT administrators to completely eliminate print servers. The SaaS solution converts an existing print environment to centrally managed direct-IP printing and offers printer-driver deployment and management, print auditing and reporting, and centralized printer management from a web-based console. In terms of cost-effectiveness, PrinterLogic has a proven track record for high return on investment. Customers report measurable gains resulting from infrastructure reductions, improved IT efficiencies, improved printing uptime/reliability, and lower help-desk costs.

Footnotes

[1] Due to OS security limitations, Chrome OS devices use the PrinterLogic Chrome OS Extension instead of the PrinterLogic Client. It provides similar functionality but cannot be promoted to a Service Client.

[2] Google has announced end-of-life for Google Cloud Print at the end of 2020. PrinterLogic will announce a new Android printing feature in early 2021.