PrinterLogic
a VASION solution

PrinterLogic's Virtual Appliance

A white paper explaining the benefits, architecture, and the operational details of PrinterLogic's latest customer-hosted solution

Table of Contents

PrinterLogic Overview

PrinterLogic earned its reputation by providing a serverless printing infrastructure that is feature rich, secure, and easy to use. The platform converts legacy print environments into highly available, centrally managed direct-IP printing systems.

With PrinterLogic, there is no need for Group Policy Objects (GPOs) or time-consuming scripting to deploy and manage printers and drivers. And because print jobs go straight to the printer via direct IP, confidential data remains local and WAN traffic is minimized.

There are two versions of PrinterLogic. One is a true SaaS implementation that eliminates the need for traditional print-server infrastructure, hardware resources, licensing, or maintenance. The other is an easily updated virtual appliance for on-premises use that has equivalent functionality.

This paper describes the benefits, architecture, and security details of the new PrinterLogic Virtual Appliance, which has replaced the company's traditional on-premises version known as Web Stack.

What is the PrinterLogic Virtual Appliance?

The PrinterLogic Virtual Appliance (the VA) is the latest generation of PrinterLogic's on-premises platform.

Typical use cases include:

- Companies that want the benefits of PrinterLogic's serverless printing infrastructure but need tighter control over their print environment.

- Current PrinterLogic Web Stack customers who want to get the latest features PrinterLogic has to offer. This is a track change, but it offers the latest functionality and ongoing support.[1]

PrinterLogic VA is a fully integrated solution that supports:

VMware (OVA, VMDK)
Hyper-V (VHD)
AWS (AMI)
Google Cloud Platform (VMDK)
Azure

This solution helps customers maximize their investment in virtual infrastructure designed to reduce unnecessary hardware, software, and ongoing maintenance costs.

The VA has been called "SaaS in a box" because it is a parallel delivery system for the same application. It installs and spins up much faster than Web Stack, which is the previous on-

[1] PrinterLogic Web Stack will continue to receive engineering support through August 31, 2022. Live product support will continue for an additional six months, through February 28, 2023.

prem implementation. The VA is a complete, unitized solution that's ready to install, including a server OS, web services, network environment, and the PrinterLogic application.

The VA includes a timely and easy update system that allows the customer to get the latest features and improvements. Features become available soon after they are pushed to PrinterLogic SaaS.

Key components include: (1) a self-contained management server, (2) a small app that's installed on every workstation (known as "the Client"), and (3) an enhanced client for additional services that's a shared resource (known as the "Service Client"). The latter is installed on a workstation that remains powered on.

Virtual Appliance: A Closer Look

Moving to a VA provides a number of important benefits. These are derived from new technologies, the architecture itself, and a more timely updating process.

- As preconfigured, pretested solutions, VAs are easier to evaluate, quicker to deploy, and less expensive to maintain. They reduce the costs and complexities associated with OS and hardware configuration, easing the burden on IT.

- New features are available more frequently and updates are easier. Application updates are available soon after they are pushed to the corresponding SaaS platform. Once the update is downloaded, the old a version is detached from persistent storage, and the new one is then attached.

- VAs are more secure on several fronts. Their low-profile operating environment is less exposed as an attack surface. The OS and platform elements are updated more regularly, reducing vulnerabilities. Developers gain tighter control because VAs provide content verification and integrity checking based on public-key infrastructure.

- VAs free up IT resources for more customer-oriented tasks such as training, support, and continuity of service. And, if something goes wrong, a VA is a single-vendor solution with one point of accountability.

The PrinterLogic Virtual Appliance Architecture

The PrinterLogic VA consists of the elements in Figure 1. These elements are explained in detail in the following paragraphs below the diagram.

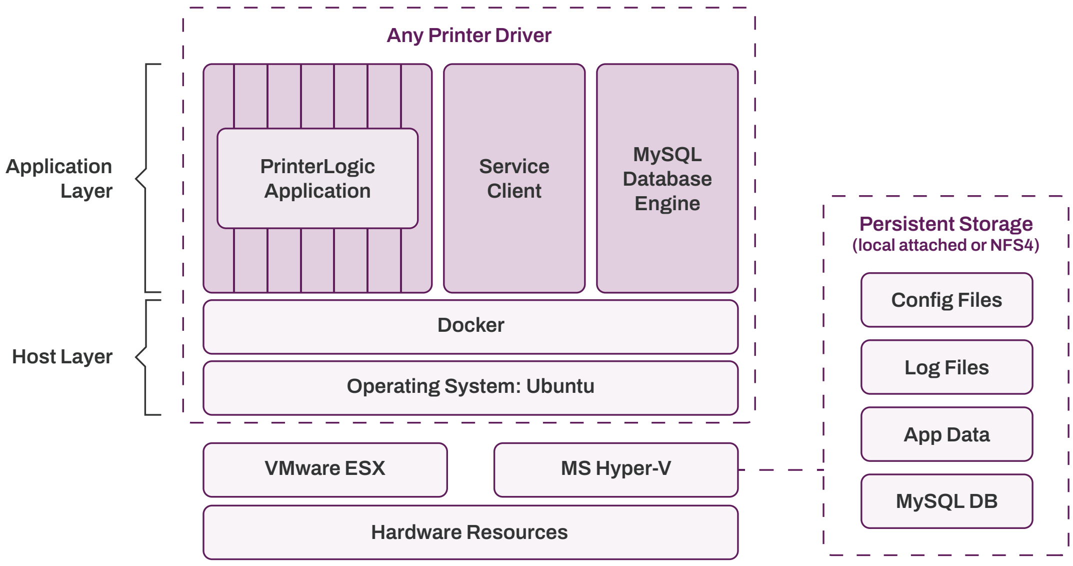

FIGURE 1: *The PrinterLogic Virtual Appliance contains an application layer and a host layer. In this (default) configureation, the MySQL database engine is inside the VA.*

The Application Layer

The application layer, shown above, contains three parts: (1) the core PrinterLogic application, which consists of microservices; (2) the Service Client; and (3) the MySQL database engine. If upgrades and/or bug fixes are available, a new application version is displayed in the Admin Console. These components are explained below.

The PrinterLogic Application

The PrinterLogic application is the heart of the product. The app provides users with a serverless printing infrastructure.

A single shared “code train” between the company’s SaaS and VA solutions uses a series of discrete microservices. For example, the user microservice manages users and the authentication information received from an identity provider (IdP), whereas the queue microservice manages print queues.

Each microservice is self-contained, maintains its own data store, and can be updated independently. These services communicate with each other in well-defined and prescribed ways. Software designed this way speeds up application development and makes it easier to implement new features and functionality.

An app that uses microservices runs more efficiently on multiple servers, where load balancing demands adjustments for transient spikes as well as steady increases over time. This approach also reduces downtime caused by hardware or software problems.

PrinterLogic Service Client

The Service Client is an enhanced version of the PrinterLogic Workstation Client. It facilitates communication between the PrinterLogic Instance and user endpoints, enables advanced features, and ensures that confidential print data is kept local and secure. This is explained more in the PrinterLogic VA Security section below.

MySQL Database Engine

MySQL is the database used by the PrinterLogic Virtual Appliance. The MySQL engine is separate from the data store. It is containerized and installed on Docker, with the physical storage separated and outside the Virtual Appliance.

This allows the Virtual Appliance to be immutable. This means it cannot be changed but can be “destroyed” to make room for a new Virtual Appliance that is then spun up to replace it. The database is configured in one of two ways as discussed in the Host Layer section below.

The Host Layer

This layer consists of Docker, a containerization solution, and Ubuntu, the operating system.

Docker

Docker is a container tool that uses OS-level virtualization and makes it easier to create, deploy, and run applications. It packages up the application along with its associated parts such as libraries and other dependencies. Containers are run by a single operating system kernel and use fewer resources than virtual machines.

Within the VA, Docker is configured to act as a single-node swarm, which increases manageable container traffic.

The Hypervisor

A hypervisor is server-virtualization software that creates and runs virtual machines by allowing multiple operating systems to run independently on a single machine in a data center. Hypervisors encapsulate a guest version of the operating system and emulate hardware resources. They improve resource utilization and lower server costs.

PrinterLogic VA supports the following hypervisors and cloud Platforms:

VMware ESXi
Microsoft Hyper-V
Google Cloud Platform
AWS
Azure

Persistent Storage—Option 1

In a default installation of the VA, the MySQL engine is containerized and installed on Docker within the appliance. The physical database resides outside the VA in persistent storage. Also stored there are the configuration, log, and app data files required by PrinterLogic.

Persistent Storage—Option 2

As shown in Figure 2 below, a second option affords the PrinterLogic customer more control over the database provisioning. Here we see the VA configured so the MySQL engine and database are held outside the VA. Along with local storage, the VA will support NFS4.

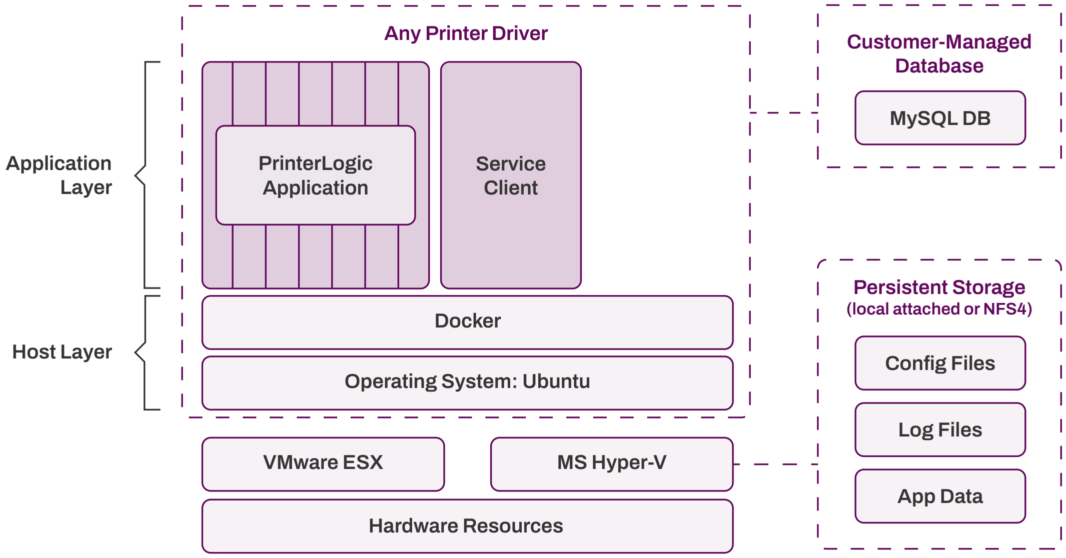

FIGURE 2: *The PrinterLogic Virtual Appliance with customer-managed MySQL database engine and data store outside the VA.*

Upgrading the Virtual Appliance

As with all software systems, PrinterLogic is updated to introduce new functionality and/or fixes. Because the Virtual Appliance includes an operating system, vulnerabilities that crop up in the OS must be addressed. This requires an upgrade to the host layer.

The architecture of the VA allows for the following upgrade scenarios:

1. Update button in the Admin Console: The application layer is updated, including the PrinterLogic application, Service Client, and the MySQL database engine.

2. The entire Virtual Appliance is replaced: This includes the application layer, the host layer, OS, etc.

Based on PrinterLogic's continuous delivery model and the number of changes pushed to the SaaS product, consolidated updates for the VA will occur at least monthly. The ability to download a new VA quickly, load it, spin it up, and then attach it to the persistent storage minimizes down-time and ensures business disruption is minimal.

Upgrades are exucuted at the administrator's discretion. An update button within the PrinterLogic Admin Console will show what updates are available at any given time.

Differences Between PrinterLogic's SaaS and VA

There are three major differences between PrinterLogic's SaaS solution and its on-premise (VA) Solution.

Hosting Location and Admin Control

PrinterLogic SaaS is an AWS well-architected solution that is hosted in several geographic public-cloud regions. No additional servers need to be hosted in your private cloud or data center. Because it is a true SaaS offering, and is secured by AWS, the platform does not offer IT administrators direct access to the database that houses the instance information.

The PrinterLogic VA is a self-contained preconfigured VM image that is hosted on the customer's hypervisor—either in an on-premise datacenter, a private cloud datacenter, or a public-cloud datacenter. Because it's hosted by the customer, they have direct access to their VA instance database and related information.

Multi-tenacy and the MSP/SMB Makretplace

Because PrinterLogic SaaS is built on a scalable AWS platform, the company can offer a solution for multi-tenancy using a single management console. This solution has been designed with managed service providers (MSPs) and smaller business in mind.

The PrinterLogic Virtual Appliance is designed to support one customer instance per VA.

Different Upgrade Systems: Push versus Pull

PrinterLogic SaaS uses a continuous-delivery update methodology. New features and fixes are automatically delivered to SaaS instances.

There are two methods for updating the PrinterLogic Virtual Appliance. First, a full-replacement update method involves detaching the persistant storage disk and replacing the virtual appliance with the updated version. Second, the VA allows partial updates which are accessible via an option in the Tools menu.

Virtual Appliance Operational and Security Details

This section explains the operational and secure-communication protocols that apply to the PrinterLogic Virtual Appliance.

PrinterLogic Instance-Client Communications

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. It communicates with the PrinterLogic instance over HTTP or, with a validated certificate, HTTPS using TLS. Both HTTP and HTTPS communication paths use 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 HTTP/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 HTTP/HTTPs and TLS. This eliminates the need for any 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.

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. 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 or HTTP 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 or 80 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, macOS 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.

For reporting purposes, only metadata for print jobs is sent via HTTP/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. Display of document titles can be disabled in the Admin Console.

Communication with Microsoft Active Directory

PrinterLogic employs identity provider services (IdPs) 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 requires the IP address or hostname of the primary and optional secondary LDAP servers, as well as the port being used 389 or 636.

The PrinterLogic instance uses read-only permissions to access the AD server. Each time an authentication or AD membership is required (e.g., by mobile printing, email printing, control panel platform AD sync, or badge ID if stored in AD), PrinterLogic makes the request to 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 Identity Providers (IdPs)

If PrinterLogic is configured to integrate with a cloud-based identity provider (e.g., Azure AD), user-identity information managed in the IdP console is synchronized with PrinterLogic using SCIM (System for Cross-domain Identity Management). Updates that flow from the IdP to PrinterLogic occur in real-time.

In addition, logins to the PrinterLogic instance are facilitated through the IdP using the Security Assertion Markup Language 2.0 (SAML 2.0). Synchronized identity information provided by the IdP is used to authorize access to the PrinterLogic Self-service Installation Portal, the PrinterLogic Admin Console, and authorized printer deployments. Enhanced security features such as multi-factor authentication (MFA) and single sign-on (SSO), if enabled, are handled by the identity provider. These capabilities improve authentication security and offer productivity advantages for end users.

For more information about how PrinterLogic integrates with leading cloud-based identity providers—and which leading providers are supported—download this white paper.

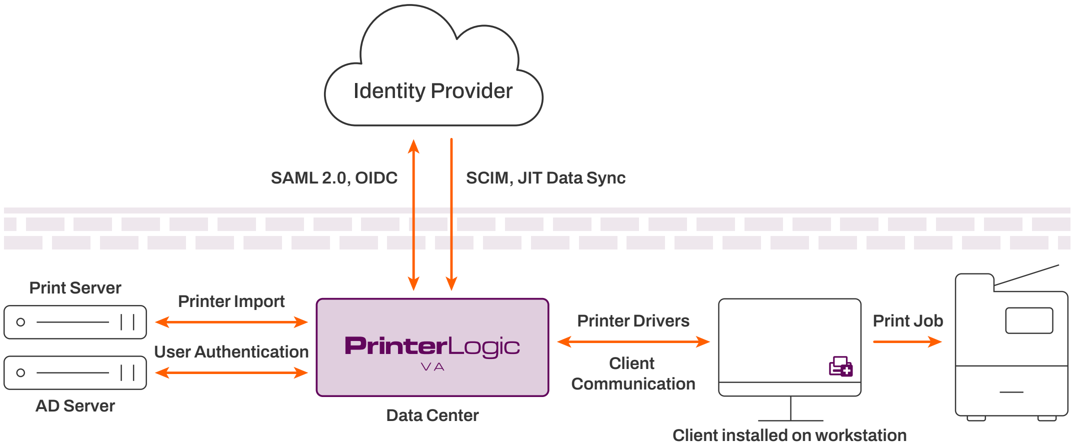

FIGURE 3: *The PrinterLogic communication paths for the Virtual Appliance and workstation client.*

Secure-Release and Pull Printing

Secure and pull printing are available as part of PrinterLogic's Advanced Security Bundle.

PrinterLogic offers three secure printing methods:

1. Pull printing (virtual printer queue; the 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 (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 and 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. Touchless smartphone release with QR code support. Releasing print jobs using our phone apps is convenient and avoids contact with the shared printer. Users can either view and release jobs from within the app, or they can use the app's scanner to read a QR code on the printer. With QR codes, the printer is instantly identified and printing begins, all in one step. Once the user's login credentials are entered into the app, they are stored for improved speed and convenience. What's more, it works with any network printer. PrinterLogic's mobile apps are available on Apple's App Store and the Google Play Store.

2. 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.

3. 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 as defined in the admin console.

4. 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 is released. The administrator can configure Simple Badge Release to release either the most recent, or all, held print jobs in a single motion.

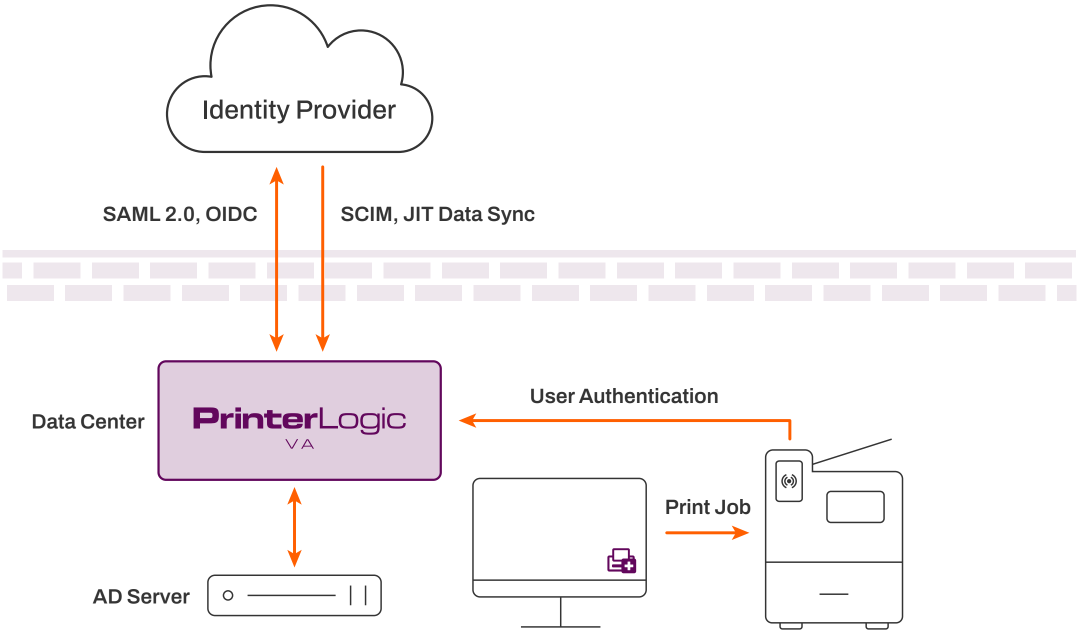

FIGURE 4: *Communications flow for secure-release printing. Users authenticate against either Active Directory or a cloud-based identity provider.*

5. Web-based release portal. From any web-enabled device (e.g., phone, tablet, laptop, 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 secure 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.

Mobile Printing

The PrinterLogic App for iOS and Android devices serves two purposes. First, as we described above, it is used to authenticate and release documents held for secure or pull printing. Second, the app allows users to print from their mobile device directly to virtually any printer on the organization's network. Mobile printing employs driverless printing via the Internet Printing Protocol (IPP).

Traditionally, setting up mobile printing requires network changes and configuring a broker between the mobile device and the printer. With the PrinterLogic App, so long as the user's mobile device can access the same network where printers reside, no additional network changes are required. The mobile app uses the same set of Identity Providers supported by PrinterLogic for any endpoint. The mobile user logs in using the same credential they use on a workstation or laptop.

The app lets IT manage printer deployments for iOS and Android devices the same way they do for other endpoints. MDM deployment is supported, including preconfiguring the customer's PrinterLogic instance URL. This simplifies the sign-in process for the end user and reduces help desk calls.

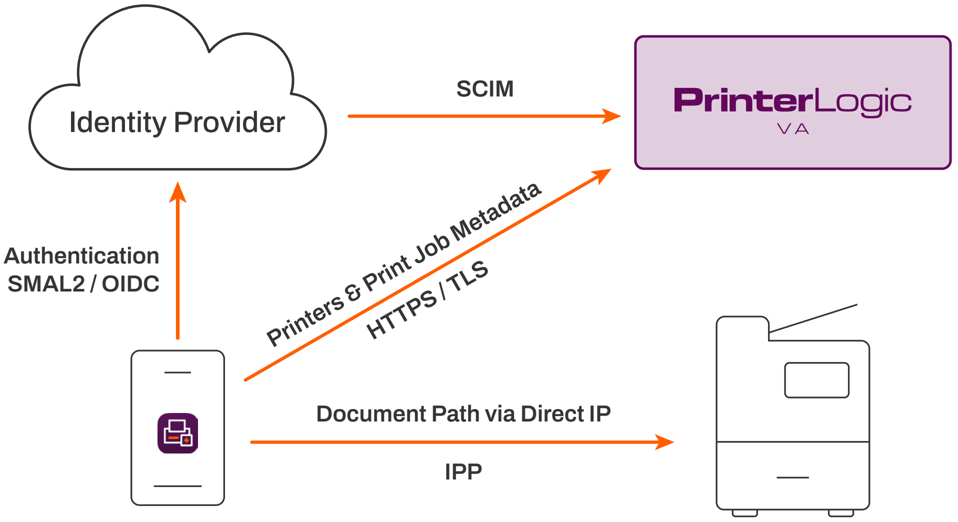

FIGURE 5: *Mobile printing authentication, communication with the PrinterLogic VA instance, and job routing to the network printer.*

The diagram above illustrates the mobile printing process and pathways for authentication, communication with the PrinterLogic instance, and routing for direct IP print jobs.

For direct mobile printing, the phone or tablet must be on the same Wi-Fi network as the printers. Documents are sent via direct IP and remain behind the firewall. With the Virtual Appliance, when using a mobile device to authenticate and release secure print jobs, the device must be on the same Wi-Fi network as the PrinterLogic instance.

The app is available from the Apple App Store and the Google Play Store.

Email Printing

PrinterLogic offers three email printing options: email printing, direct email printing, and guest email printing. All three use the same configuration but 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 PDF. The print job is held on the Service Client until it's released to the target printer via direct IP over port 9100.

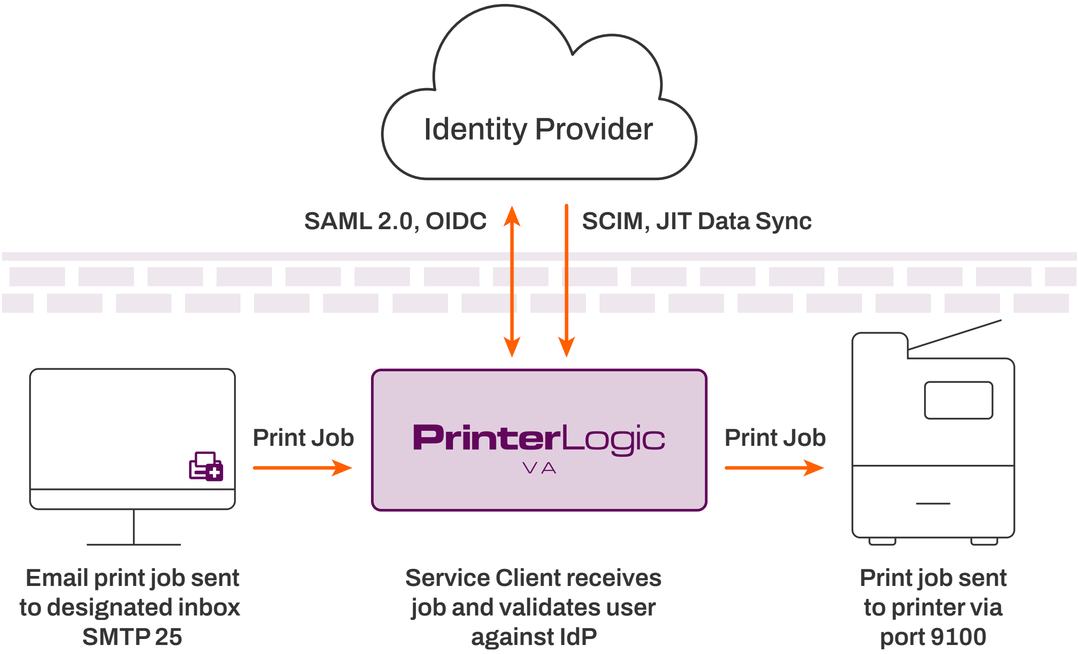
Identity Provider
SAML 2.0, OIDC
SCIM, JIT Data Sync
Print Job
PrinterLogic
VA
Print Job
Email print job sent to designated inbox SMTP 25
Service Client receives job and validates user against IdP
Print job sent to printer via port 9100

FIGURE 6: *Email-printing job flow using a PrinterLogic VA-hosted Service Client and user validation against Active Directory or a cloud-based IdP.*

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 the PrinterLogic Admin Console. Any emails that pass these tests, including attachments, are converted to 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 PDF and sent via direct IP over port 9100 to the target printer.

Off-Network Printing

Off-network printing enables companies to provide convenient and secure printer access to employees, contractors, and partners who reside on different networks. This capability is crucial to organizations adopting a Zero Trust architecture, using onsite contractors, or hosting traveling employees. Off-network printing provides an intuitive, highly available, secure printing experience to visiting parties.

Off-network printing allows users with internet access, from any location, to send print jobs to a printer located behind the company firewall. In addition to PrinterLogic SaaS or VA instance, there are two other components that make this solution work: the External Gateway and the Internal Routing Service.

The External Gateway

The External Gateway receives off-network print jobs from remote workstations. In the PrinterLogic-hosted model, the External Gateway is hosted as a service in AWS by PrinterLogic. In the customer-hosted model, the External Gateway is hosted by the customer with an SSL (Secure Sockets Layer) certificate.

In addition, combined hosting models (known as hybrid models) can be used. The External Gateway uses port 443 to receive print jobs and uses WebSockets to transfer incoming print jobs down to the Internal Routing Service. Print traffic is encrypted using the TLS (Transport Layer Security) cryptographic protocol.

The Internal Routing Service

The Internal Routing Service maintains a constant connection with the External Gateway to watch for print jobs. When the External Gateway receives a print job, the Internal Routing

Service opens a new connection for that print job and downloads and delivers it to the designated printer.

Off-network printing has three configuration options: PrinterLogic-hosted External Gateway with AWS, customer-hosted External Gateway, and a hybrid model. For more information on these three configurations, read our white paper.

PrinterLogic Service Client

Service Client functional overview

The PrinterLogic Service Client is an essential component of PrinterLogic's serverless printing platform. It is an enhanced version of the PrinterLogic Client that's installed on Windows, macOS or Linux workstations. The Service Client facilitates communication between the PrinterLogic instance and advanced PrinterLogic features so 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)
- Installing a Control Panel Application on a printer
- Control Panel Application authentication (badge release, UserID/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 Gateway

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, macOS, 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.)

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
- Control Panel App - PrinterLogicServicePrinterApp
- Offline Secure Release - PrinterLogicServiceOfflinePrint
- SNMP Monitoring - PrinterLogicServiceSNMP
- Simple Badge Release - PrinterLogicServiceSimpleBadgeRelease
- Off-network Printing - PrinterLogicServiceOffNetworkServer
- Identity Sync Service - PrinterLogicServiceIdentitySync

Conclusion

The PrinterLogic Virtual Appliance is the latest generation of PrinterLogic's on-premises platform. The VA can be installed on popular hypervisors and private cloud platforms to meet the requirements of a company's preferred infrastructure.

As a fully integrated solution, the VA offers customers a versatile replacement for the legacy PrinterLogic Web Stack on-premises application, which is scheduled for end of life. It is also an excellent alternative for customers who prefer to host their own infrastructure rather than subscribing to the PrinterLogic SaaS solution.

The VA mirrors all the features and benefits of the SaaS platform with the additional benefits of a simple infrastructure that is easy to install, manage, and update. It is an excellent pathway to true serverless printing in an on-premises environment.

To start a free trial of PrinterLogic SaaS, click here.

For more information, see our FAQ or visit printerlogic.com.

Contact us

+1 435.652.1288

sales@printerlogic.com

PrinterLogic is part of the Vasion® family of products.