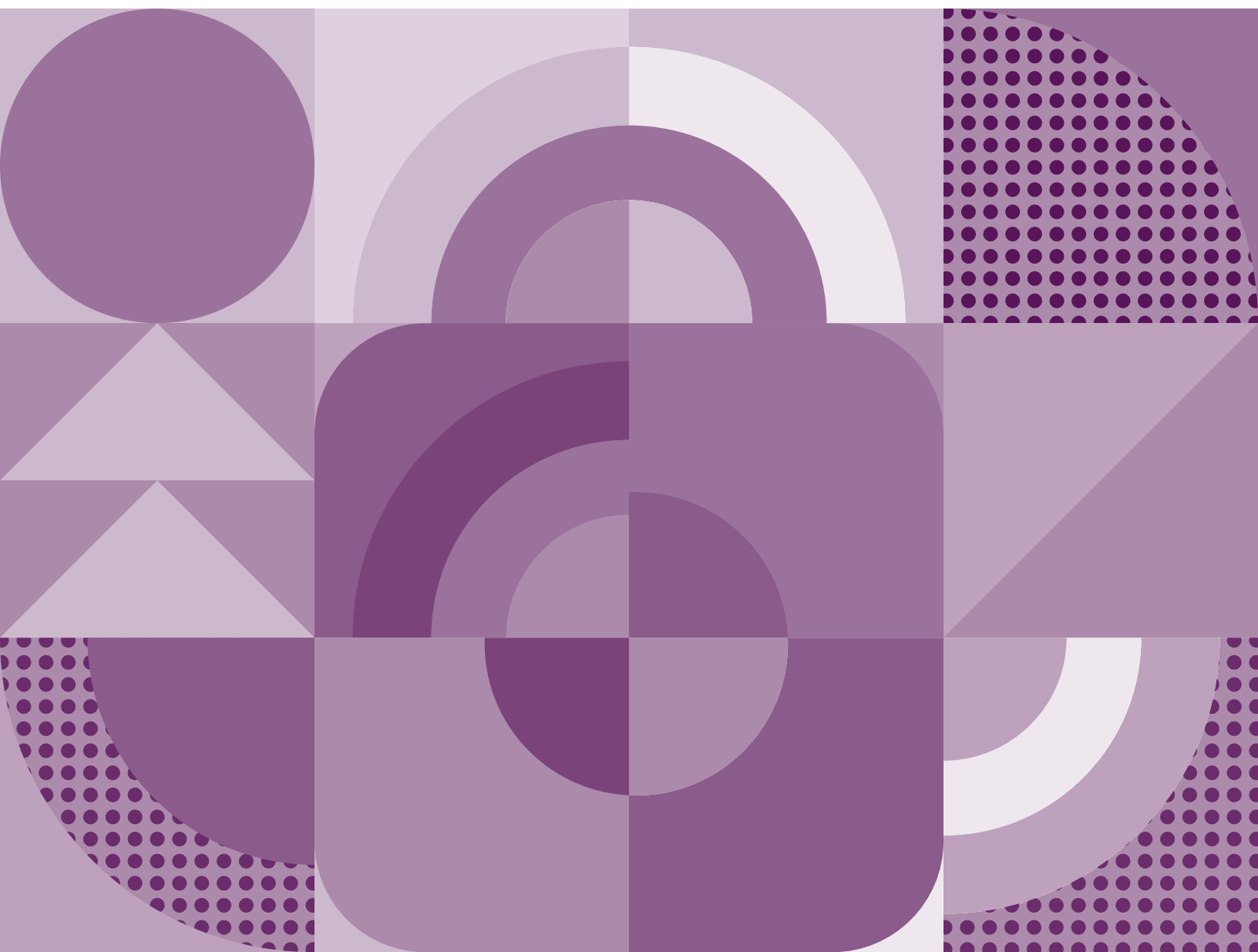**Printer**Logic
a vasion solution

Integration with
Cloud-based IdPs

How PrinterLogic's serverless printing infrastructure integrates with cloud-based Identity Providers to deliver secure access.

An Introduction to Cloud-based Identity Providers (IdPs)

As more organizations move to a cloud-first strategy, they quickly learn that traditional identity management options such as Microsoft's on-premises Active Directory are no longer optimal. The need to centralize administration across applications and improve security, together with the growing infrastructure reduction trend, have made cloud-based IdP companies the natural replacement for on-prem identity services.

An IdP is a trusted third party that securely stores and manages passwords and other authentication data, and grants users access to cloud-based resources when they authenticate. IT teams use IdP services to manage all types of user identities—including employees, contractors, and partners.

Those users are spared the trouble of remembering a dozen or more strong passwords for various applications and services. Instead, they need just one secure set of credentials to log in, a service called Single Sign-on (SSO).

Cloud-based Identity Providers are a subset of a larger market space known as Identity and Access Management (IAM), referred to in Figure 1 below.

Leaders in the rapidly expanding cloud-based IdP space include Okta, Microsoft's Azure Active Directory, Google's Cloud Identity, and Ping Identity, among others. Further information about their relative merits can be found in this Gartner Magic Quadrant report.

Figure 1: Magic Quadrant for Access Management

Source: Gartner (November 2021)

Figure 1. Magic Quadrant for Access Management. *PrinterLogic integrates with IdP leaders including Okta, Ping Identity, and Microsoft's Azure AD.*

Key Benefits of Using an IdP

Below are some widely acknowledged benefits for organizations that standardize on a cloud-based IdP.

Security and data protection—The IdP's management of strong, non-repetitive passwords and Multi-factor Authentication (MFA) helps keep the organization's information assets secure.

Centralized identity management—IT teams can manage user identities through one Administration Console. With access and authentication handled by the IdP, organizations don't need to store identity data in their applications. This saves time and lowers costs.

Login made simple—With SSO, another common vulnerability is eliminated. Users no longer recycle the same easily exploited credentials over and over. Calls to the help desk for password resets also drop. Security is increased, costs reduced, and efficiency improved.

Access visibility—Clearly seeing which users have access to what resources on the network can help eliminate security vulnerabilities. User provisioning and deprovisioning are easier for IT teams.

Immediate data sync—Any change made in the IdP to user credentials is immediately reflected in all applications that support SCIM (the System for Cross-domain Identity Management).[1]

Centralized directory—All users, groups, and devices can be managed in the IdP directory. Group provisioning and deprovisioning are simplified to save IT time and reduce costs.

Cloud-based identity solutions allow IT teams to deliver SaaS applications securely to the right person or team at the right time.
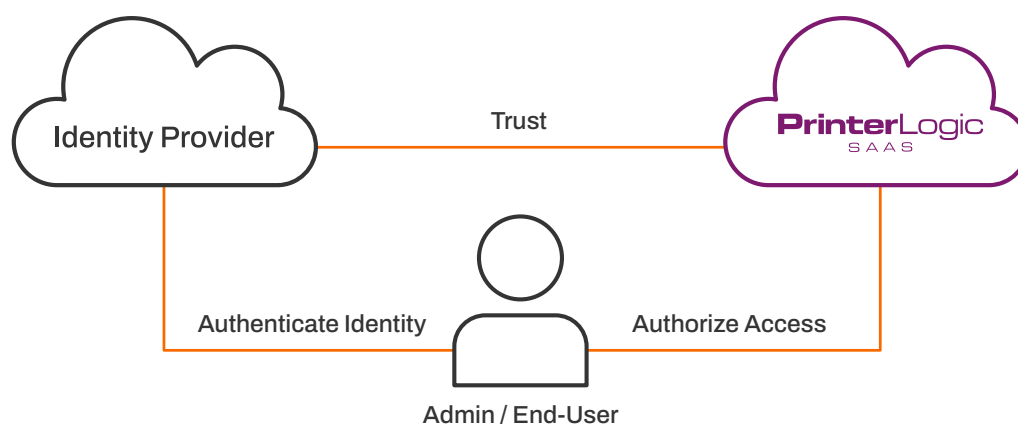
Figure 2. *The IdP is the trusted authority for SaaS applications. User **authenticates** identity through the IdP, then is **authorized** to access PrinterLogic and other cloud-based applications.*

---

[1] Microsoft's Azure AD is the only exception. It has a 40-minute provisioning interval.

# How PrinterLogic Integrates with Leading Cloud-based Identity Providers

PrinterLogic's integration with Identity Providers has grown naturally from the company's focus on eliminating infrastructure. The integration relies upon widely accepted industry standards, such as SCIM, SAML 2.0 (Security Assertion Markup Language), and JIT (Just In Time) provisioning.

SCIM—A Standard for Synchronizing Data

SCIM is an open standard specification used by an IdP for automating the exchange of user identity information. Consider an organization hiring new workers to replace employees who have recently left the company. The organization's directory must be updated to reflect all the changes, ensuring access for the new employees while removing access privileges for those who have gone.

To make a directory update, the IT administrator simply makes the needed change in the IdP, and it is automatically pushed to all SCIM-enabled applications. The "edit once, change all" capability of SCIM makes managing user identities faster and easier for IT teams.

Users authenticated by the IdP are then authorized to access PrinterLogic. They can print needed documents and use other SaaS applications to accomplish their assigned tasks.
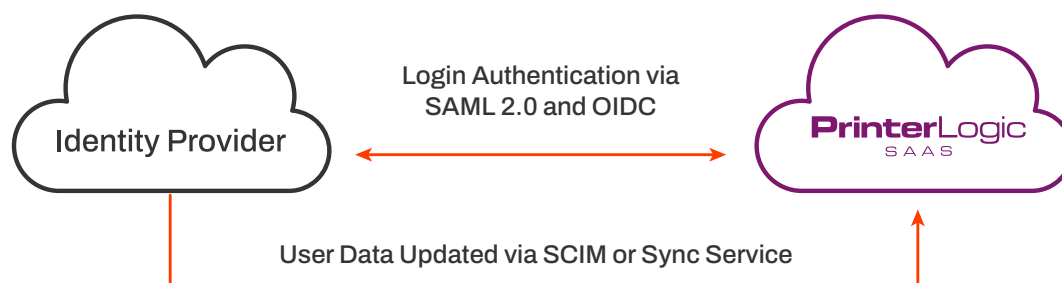
Figure 3. *SCIM, OIDC, and SAML 2.0 in the PrinterLogic integration.*

For IdPs that don't support SCIM, PrinterLogic created an Identity Sync Service. This links the PrinterLogic instance with the IdP via the provider's API, and it checks for data changes every five minutes. This ensures there is no significant latency in data updates between the Identity Provider and PrinterLogic.

JIT—A SCIM Alternative

For many on-prem Virtual Appliance customers, JIT provisioning is preferred to SCIM. PrinterLogic supports an expanded list of user attributes that can be provisioned, including authPin, authPinUser, badge, manager, department, and job title—if they are configured in the

IdP. This means you take advantage of IdP-managed badge and PIN, a feature that was only available in SCIM apps previously.

SAML 2.0—A Standard for Authentication

SAML 2.0 is an open standard specification that an IdP uses to exchange authentication and authorization data. Information is passed between a SAML-compliant Identity Provider, like the employee directory in the above example, and an application such as PrinterLogic.

SAML 2.0 determines whether a specific user is granted or denied access to a cloud-based application like PrinterLogic. This action enables cross-domain SSO, with its previously discussed benefits for end users and for IT teams.

OpenID Connect (OIDC)—An Alternative Authentication Protocol

OpenID Connect (OIDC) is an alternative to SAML 2.0. It uses the OAuth 2.0 protocol and allows clients to verify a user's identity and obtain basic profile information in an interoperable and REST-like manner. PrinterLogic support for the OIDC standard stems from its integration with Google Identity.

PrinterLogic Integrations and Endorsements

PrinterLogic currently integrates with the following leading IdP providers:

- Okta
- Azure AD
- Google Identity
- ForgeRock
- Imprivata

- PingOne
- PingFederate
- OneLogin
- Idaptive
- JumpCloud

In addition, because PrinterLogic complies with SAML and SCIM standards, any identity provider following SAML or SCIM can be easily integrated.

The PrinterLogic implementation has passed rigorous testing by Okta, and is now included in the Okta Integration Network of verified and approved Okta applications. PrinterLogic is also an Okta Embedded Partner. In addition, PrinterLogic is listed in the Azure Marketplace.

Concurrent (Multiple) IdP Support

To address the needs of the enterprise and reduce IT overhead, PrinterLogic supports concurrent IdPs within the same SaaS instance. This makes it easy to support all employees in an organization that uses more than one IdP—either by design or as the result of an acquisition. In some scenarios, the same employee may use more than one IdP. So long as there is a unique matching attribute for these individuals (e.g., e-mail, User ID, etc.), PrinterLogic can be configured so any of their supported credentials can be used to release print jobs and receive printer deployments.

Why Use PrinterLogic?

PrinterLogic is a print management solution available as either a SaaS or on-premises Virtual Appliance (VA) platform. It eliminates the need for print servers and delivers a serverless printing infrastructure in which feature updates are delivered in real-time.

PrinterLogic allows IT administrators to manage all their network printers—across different buildings, different countries, or different continents—from a powerful web-based Admin Console. Customers enjoy a secure, scalable solution with a guaranteed 99.5% uptime service-level agreement (SLA).

PrinterLogic also empowers end users to install printers on their own with a single click, which helps reduce help-desk tickets. The platform supports any network printer and works with Windows, macOS, Linux, Chrome OS, iOS, and Android endpoints.

In addition, the Printerlogic App for mobile devices gives users the ability to print or release print jobs from anywhere. The app integrates seamlessly with major IdPs to give companies the additional security of SSO and MFA from any device.

Conclusion

An IdP is a trusted third party that authenticates users and grants them the correct level of access to cloud-based resources, like PrinterLogic SaaS. Cloud-based IdPs are the natural replacement for on-prem identity services.

Among the benefits an IdP provides are:
- Multi-factor Authentication and management of strong passwords
- One place for IT to manage identities and provision users
- Single Sign-on to reduce password fatigue and help desk tickets
- Real-time sync of identity data changes

PrinterLogic SaaS now integrates with Okta, Azure AD, Ping Identity, and seven other leading cloud-based IdPs - and more integrations are still to come. With PrinterLogic's robust IdP support, customers are assured of secure and appropriate user access to PrinterLogic and other cloud-based applications and resources.

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

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