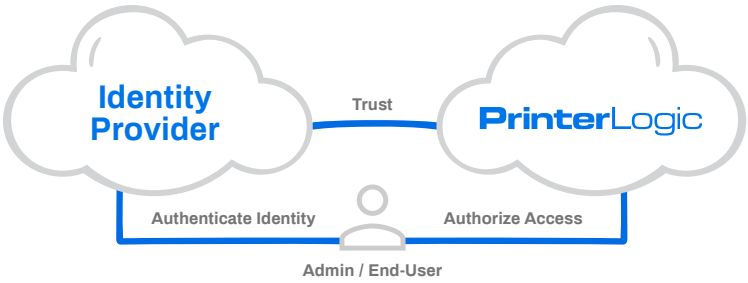
PrinterLogic

Integration with Identity Providers | FAQ

Q What is an IdP and how does it fit within the Identity and Access Management (IAM) market space?

A Identity Providers (IdPs) are a subcategory of IAM and are focused on managing and authenticating user identities. An IdP can be an on-prem solution (e.g., Active Directory), or a cloud-based service (e.g., Okta, Azure AD, Google Identity, etc.). Identity Providers are considered the source of truth for authenticating user identities.



The user authenticates their identity through the IdP, and is then authorized to access PrinterLogic and other cloud-based applications

Q What does it mean for PrinterLogic to integrate with IdPs?

A Integration means PrinterLogic SaaS now works with leading cloud-based IdPs. If an organization uses an IdP in place of Active Directory, it can now integrate with PrinterLogic. PrinterLogic uses protocols like SAML, OIDC, and SCIM to make this work. SAML and OIDC authenticate users, and SCIM channels user provisions from the IdP to the PrinterLogic application.

Q What are the benefits of using a cloud-based Identity Provider?

A An IdP is a trusted third party that securely stores and manages passwords and other authentication data. When users authenticate, the IdP grants the correct level of access to cloud applications and resources. IT admins manage user identities in one place (the IdP console), and changes are pushed out to SCIM-enabled cloud apps automatically. If the IdP supports it, users enjoy the efficiencies of Single Sign-on (SSO), which improves security and reduces helpdesk tickets.

Q Is additional licensing required to use a cloud-based IdP?

A IdP support is included in our SaaS core licensing. The customer is responsible to have a license for the IdP service (e.g., Okta, Azure AD, etc.) A free license for Okta is available by clicking on “Become an Okta Member” in the Identity Provider Settings within the PrinterLogic Admin Console.

Q What PrinterLogic platforms support IdPs?

A Initially, IdP support is included in our SaaS platform. When our Virtual Appliance (the next on-prem release) is released in October 2020, it too will include IdP support.

Q What PrinterLogic features are supported in the first IdP release?

A Our initial release of IdP integration supports the deployment of printers based on IdP users and groups, portal security for users and groups, adding IdP users and groups to PrinterLogic’s database, and releasing print jobs using our web release portal. SSO and Multi-factor Authentication are available if the IdP supports these features. Other PrinterLogic features will be added in subsequent releases.

Q What is SCIM? How does PrinterLogic support this standard?

A SCIM, or System for Cross-domain Identity Management, is an open standard that allows for the automation of user provisioning. It was created in 2011. SCIM communicates user identity data between IdPs and Service Providers (most notably cloud applications) that require user identity information.

Q How does Google Identity work with SCIM?

A At this time, Google ID does not support SCIM. However, PrinterLogic developed a synchronization service for the Google integration that provides essentially the same updating function.

Q If I update user data in PrinterLogic, are changes automatically relayed to my IdP?

A Synchronization of user data goes from the IdP out to all SCIM-enabled apps. Updates that originate in the PrinterLogic console are not sent to the IdP. SCIM data synchronization is not bidirectional.

Q How often is user credential data updated?

A For SCIM-enabled IdPs, the data is updated real-time. In the case of Google Identity, synchronization is done by means of our IdP Sync Service.

Q What is SAML? How does PrinterLogic support this standard?

A The Security Assertion Markup Language (SAML) is an open standard that allows IdPs to pass authorization credentials to Service Providers (e.g., cloud applications). SAML enables Single Sign-on (SSO).

Q What is Single Sign-on (SSO)? How does IdP integration facilitate this?

A Single Sign-on (SSO) is an access-control property of multiple independent software systems. SSO allows users to log in once, and then have their credentials reused transparently for authenticating with other applications. SSO is provided by the IdP, not PrinterLogic.

Q What is Multi-factor Authentication (MFA)?

A Multi-factor Authentication verifies identity by requiring additional credentials. For example, a user enters their username and password, and then is asked for additional proof, such as a code sent to their smartphone, answering a security question, etc. MFA is provided by the IdP, not PrinterLogic.

Q Has the PrinterLogic integration been verified by the IdPs you support?

A Yes. We have been verified by Okta for SAML and SCIM, and we are part of the Okta Integration Network. We have been verified by Microsoft's Azure AD for SAML.

Q Besides Okta, Azure AD,and Google ID, what other cloud-based IdPs will PrinterLogic support?

A Ping Identity, Imprivata, and Idaptive will be added later in 2020.

Q What additional IdP functionality will be added in a future PrinterLogic SaaS release?

A Version 2 of our IdP Integrations will include more robust Secure Release Printing functionality, available in Q3, 2020.

Q Can I use my existing groups in Active Directory?

A Yes. Any AD groups that you bring into the IdP are automatically synchronized with PrinterLogic SaaS.

Q Can I use different IdPs at the same time?

A Not currently. We understand this need and it will be included in a future release. We do not yet have a time projection for this release.

Q What's involved in installing or configuring my IdP within PrinterLogic?

A Configuring PrinterLogic with each IdP is slightly different. Online instructions for setting up **Okta**, **Azure AD**, and **Google Identity** are found in the PrinterLogic SaaS Admin Guide.

Q How many PrinterLogic SaaS admin accounts can be created within the IdP admin console?

A This feature works with an unlimited number of administrators.