ADOBE AND MICROSOFT

A strong partnership for secure single sign-on

Local Active Directory or Azure Active Directory enable central user management across different software providers
Management Summary

Register once and then use a wide range of services. This is made possible by Single Sign-On (SSO). Companies can use it to improve user comfort, reduce IT expenditure and increase security. With fewer accounts, management is easier and the risk that access data could be compromised is lowered since separate and possibly insecure passwords aren’t used for countless services. For Adobe Cloud Services, SSO can be implemented in conjunction with the local Microsoft Active Directory or the cloud-based Azure Active Directory. This enables companies to integrate Adobe user management into their existing control center. We will introduce you to both ways and show you how to implement them.

Adobe and Microsoft have had a strategic partnership for years. Both manufacturers are leaders in their field and are increasingly moving their products to the cloud. The Adobe Creative Cloud, Experience Cloud and Document Cloud work perfectly in many areas with Microsoft Azure, Office or Microsoft 365 and Dynamics. For example, customers can create PDF files directly in Office 365 using Adobe Acrobat or Adobe PDF Services and digitally sign using Adobe Sign. The close partnership also provides a great advantage for user administration because it can be handled for Adobe products via the local Microsoft Active Directory (AD) or the cloud-based Azure Active Directory (AAD). Administrators therefore no longer have to log in to the Adobe Management Console to create users and assign licenses.

The more cloud services companies use, the more complex managing users becomes because every service requires its own login. As a result, administrators have to manage a huge number of accounts. They have to make sure that every user has the appropriate access rights and set up corresponding accesses when onboarding and block them again when off boarding.
All of this is done on different management consoles since the individual providers usually provide their own administration tools. This not only creates considerable effort, but also causes IT employees to easily lose track of things and make mistakes. This quickly becomes a security risk. Last but not least, there is a proliferation of usernames and password, which becomes a weak point. If employees constantly have to think up new access data, unsafe combinations arise that hackers can easily crack. With each new account, the number of potential points of attack increases.

**What are the advantages of single sign-on?**

Single sign-on (SSO) is one way to meet these challenges. User authentication takes place via a central service. Users can then automatically log in to many different cloud services with the same login data and no longer have to remember endless variants of access data. The number of accounts to be managed is significantly reduced and management is carried out via a central console. This simplifies the work for administrators and increases security. SSO can be implemented particularly conveniently in conjunction with the local Microsoft Active Directory (AD) or the cloud-based Azure Active Directory (AAD). This will allow administrators to extend the central user login information that they already use in the Microsoft network to the Adobe services. All users of a company, groups and computer information are usually stored in Active Directory. For example, if a user needs access to Photoshop, they are simply added to the corresponding user group in AD. In the future, the user can use his or her Windows username and password to log in to all Adobe services for which he or she is authorized.

**Requirement: Federated ID**

To implement SSO for Adobe services, companies need a so-called Federated ID. What is behind it? With the increasing relocation of its products to the cloud, Adobe has changed the licensing model. Today, licenses are no longer device-based, but user-based. To assign users to the licenses, there are three different ID types: the Adobe ID, the Enterprise ID and the Federated ID.

While the Adobe ID is intended for individual end users, both the Enterprise ID and the Federated ID are suitable for use in organizations. Both are created and managed by the company themselves and offer multiple security levels and password guidelines.

However, there is one crucial difference: With the Enterprise ID, Adobe hosts the password information and performs user authentication. With the Federated ID, on the other hand, this takes place locally in the company or via an appropriate identity provider service. This means that Adobe does not have any access data. The Federated ID is best for implementing an SSO concept. If you are still using the Enterprise ID or even individual Adobe IDs, you should change the ID type first.

**PASSWORD MANAGEMENT COST FACTOR**

According to a study by LastPass, IT security teams spend an average of four hours a week on password-related issues and receive 96 tickets a month. Some IT teams run over 25 requests a day for forgotten passwords. One company even said its IT team spends up to 30 hours a week managing passwords.

*LastPass Study “Guide to Modern Identity Management”*
Two ways to SSO: Active Directory or Azure Active Directory

The next step is to plan the single sign-on concept. There are two ways to go: the connection with the local AD or with the cloud-based AAD. Let’s take a closer look at the differences.

1. Active Directory On-Premises
The Active Directory was first published with the Windows 2000 Server Edition and is used to manage users, applications, devices, file services and other resources in the local Windows network. However, the AD was not designed to manage web-based services.

This is how the connection works
To perform SSO with the AD, two components are required: the Adobe User Sync Tool and an identity provider. The Adobe User Sync Tool connects the AD with the Adobe directory service and synchronizes the two automatically. This makes it possible to create Adobe users directly in the AD and assign them the appropriate licenses. Administrators do not have to log in to the Adobe Management Console to do this.

In this way, Adobe user management can also be integrated into existing user lifecycle processes. If, for example, a new employee comes into the company who needs an Adobe license, it is configured in an identity management system (IDM) and the license is provided automatically.

The identity provider (IDP) is responsible for the actual SSO. It is a service that is either installed locally or can be booked as a cloud service. Adobe works with various IDPs, including NetIQ and Otka.

EASY LICENSE MANAGEMENT WITH THE PYRACLOUD
SoftwareONE will be happy to help you optimize your Adobe licenses and switch to the Federated ID. With our proprietary platform PyraCloud, we also offer you a central platform that you can use to process software licenses and cloud subscriptions from various manufacturers, and to clearly display your on-premises and cloud software inventory. This helps you to identify and realize potential savings.
The Microsoft IDP service, the Active Directory Federation Services (ADFS), is recommended for SSO with AD. Companies that already use an IDP from another manufacturer can also use this. The IDP is connected between the user systems and the Adobe Cloud and takes over the authentication. To do this, a server must be configured that has access to the local AD and on which the users can log in via their systems.

**Advantages and disadvantages**

The advantage of single sign-on with AD and ADFS is that no access data is stored in the cloud. However, the Adobe User Sync Tool requires a firewall or web proxy activation. Large companies sometimes see this as problematic because any local system with direct internet access can be a weak point from a security perspective. Basically, SSO in combination with the local AD is more complex to implement than with the cloud-based AAD.

Administrators must first set up the appropriate infrastructure and then take care of the availability, patching and updating of the local IDP themselves. If it does not work, users cannot log in to their Adobe services.
2. Azure Active Directory

Azure Active Directory is specifically designed for web-based services that use REST API interfaces. It is used for user administration of all Microsoft Cloud Services. Anyone who uses Office 365, SharePoint or Exchange Online therefore uses the AAD anyway. It is usually operated as an additional instance to the local AD.

This is how the connection works

With the AAD, SSO is much easier to implement than with the AD. Customers do not need a sync tool, nor do they need to install an additional IDP. This is because the AAD is usually already automatically synchronized with the local AD via the Microsoft Azure AD Connect and also takes on the role of the IDP itself. The AAD can communicate directly from cloud to cloud with the Adobe Cloud directory service. To establish the connection, all you have to do is set up the Azure AD Connector that Adobe provides. A wizard guides you through the process and automatically performs many steps in the background so that the connection is configured in a few minutes. The connector then synchronizes domains, users and groups from the AAD continuously (every 15 minutes) with the Adobe Cloud directory service. As a result, user administration and license provision for the Adobe services can be carried out entirely in the AAD.
Advantages and disadvantages

Adobe’s cloud services can be connected to the AAD quickly and easily. Since no local software has to be installed and everything is cloud-based, administrators do not have to manage any additional systems even during operation. Microsoft and Adobe take care of patches and updates. Companies also benefit from the high availability of cloud services. By making the SSO independent of the local infrastructure, it works even if a server might fail on-premises. Additionally, users can log in to their Adobe services at any time. However, some companies find it problematic that AAD access data is stored in the cloud. In addition, the setup wizard that connects the AAD to the Adobe console has short-term access rights to the Azure AD instance.

Which way is the right one?

If you mostly have security concerns in the cloud, you should implement SSO with local AD. The access data thus remains on-premises and administrators retain full control. However, it will require a higher technical effort. For companies that already use Microsoft Cloud Services like Office 365 or plan to do so, the AAD connection is the better way. This makes it much easier to implement SSO and reduce IT management efforts in the long term. This variant is also recommended when looking towards the future because AAD can not only act as an IDP for the services of Microsoft and Adobe, but also for the cloud services of many other providers. This enables companies that are increasingly shifting workloads to the cloud to implement a comprehensive SSO concept.
This is how SoftwareONE supports you

Are you unsure which way you should choose to implement SSO? We would be happy to advise you and support you with the implementation if required.

› Consulting
First, we analyze the current situation and work with you to determine what requirements you have. Then we present the advantages and disadvantages of the different options and show which efforts and costs are associated with each. This is how we help make your decision easier.

› Deployment
You don’t have to deal with the technical finesse of the AD connection yourself. We can install and set up the Adobe User Sync Tool and ADFS for you.

› License Management
On request, we support you with services related to Adobe licensing and IDs. We may change your Adobe and Enterprise IDs to the Federated ID and can also take care of the maintenance and optimization of all your Adobe licenses.

› Cloud-Migration
As one of the few Microsoft Azure Expert MSP partners, we also offer suitable service packages and further support in all phases of an Azure migration - from the development of a strategy to implementation and optimization as well as the subsequent administration and cost control.

Conclusion: SSO for Adobe is worth it
Single sign-on for Adobe Cloud Services reduces IT costs, increases security and ensures better user comfort. The most efficient way to do this is in cooperation with AAD. SSO plays an important role, especially in regard to paperless document processes. In this way, companies can also integrate the digital signature with Adobe Sign in workflows without users having to register for the service.

Anyone who uses AAD as a central identity provider can also integrate other cloud services into the SSO concept and is well positioned for the future.