nevis®

Making security an experience.

Handbook

# Efficient and Secure User Authentication with Single Sign-On

*Companies that enable single sign-on authentication for online resources for their customers or employees are not just making life easier for users. They are also reducing their running costs. This handbook explains what's behind the concept of single sign-on and how you can use it to achieve more than just an improved customer experience.*

# Inhalt

# Foreword

*Customers value convenience. If the login is too complicated and inconvenient, they will go to a competitor instead. However, companies and institutions have it within their power to make their login processes as simple as possible while also making them secure. One effective measure is the single sign-on (SSO), as offered by modern customer identity and access management systems. This makes it possible to grant users access to a variety of different online services through a centralised registration and login. In this context, there are different possible ways in which a company can integrate SSO into its systems. However, one thing is always the same: the providers who do this will simplify the login for users and can guarantee comprehensive security of data. In addition, SSO offers the potential to use customer data to provide a better customer experience without incurring additional costs or adding to the workload of your IT team. This is also why investing in a streamlined login process with a state-of-the-art CIAM will pay off very quickly. How? We explain it all in this handbook.*

*We hope you'll find it an informative read.*

*Stephan Schweizer*
*CEO, Nevis Security AG*

# Introduction

> **Single sign-on**
> *enables users to authenticate themselves for multiple online resources with a one-time login.*

What makes single sign-on solutions (SSO) so attractive for users is already apparent from the name, which explicitly states that users only have to **log in once.** This means that users can use just one set of login details to authenticate themselves for different applications. In this scenario, the providers of the respective platforms or software outsource the verification of the user identity to a third-party provider. This third party acts as a central authentication service, also referred to as an identity provider (IdP) or central authentication service (CAS), and verifies the login data.

Single sign-on solutions can be used in on-premises environments or in the cloud as a SaaS solution. A distinction is made between **three configuration approaches:**

### Local solution

In this case, the login details are stored in a local infrastructure. An SSO client on the workstation that is regularly used then uses this data to automatically log into the respective service.

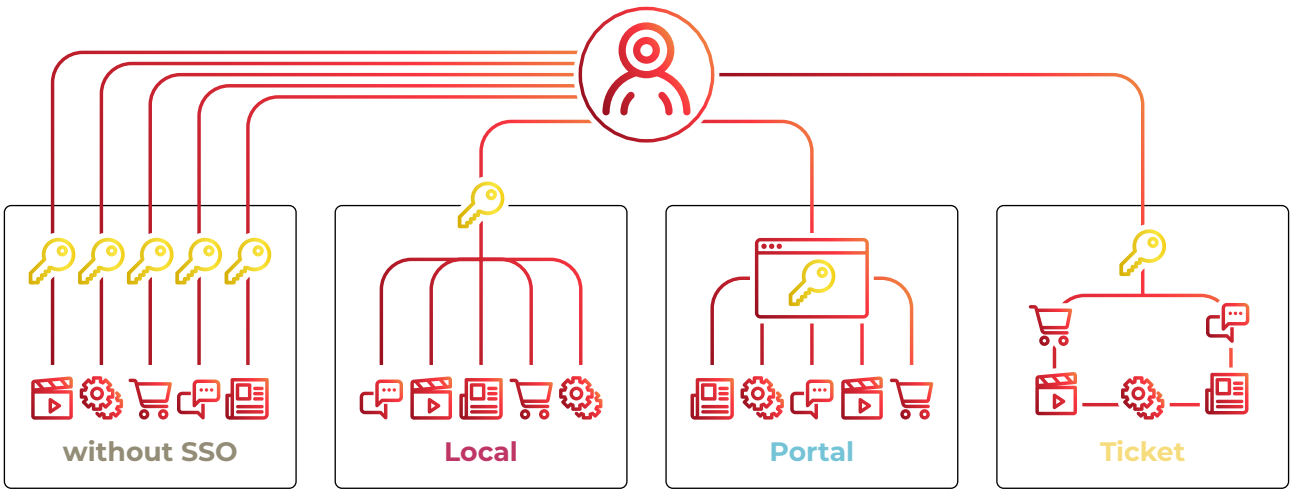
### Portal solution

This is where the role of the identity provider is assigned to a portal such as the Google Account. The portal performs the authorisation and authentication checks so that the user is then granted access to the various integrated applications and services, such as Google Mail.

### Circle of trust or ticketing solution

This configuration is suitable if SSO is to be used to grant access to different products that are connected as part of a network of trusted services. After logging into one of the services, the user receives a ticket that they can use to authenticate themselves with all other applications within the ‘circle of trust’.

**Overview of SSO solutions**




Expand your knowledge with our blog:
What Is Single Sign-On and Why Do I Need It?
Interesting Facts About Advantages and Disadvantages of Single Sign-On

# What are OAuth 2.0, OpenID Connect and SAML?

SSO is based on the concept of federated identity. This means that the attributes of an identity are shared between systems that are independent of one another but that trust one another. In this way, if one system recognises a user's access authorisation, that user is then also able to access the other systems that trust the first system. The use of SSO involves different standards and protocols. We present the most popular of these below.

## OAuth 2.0

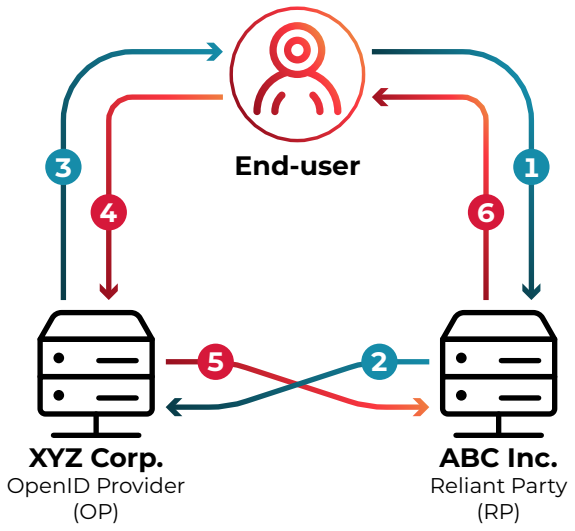
> **OAuth 2.0 (Open Authorisation)** is an authorisation protocol that allows users to make use of the identity from one website to access an application on another website.

Open Authorisation 2.0, or OAuth 2.0, refers to an authentication protocol that is based on an open standard and is widely used nowadays for exchanging encrypted identification data between different applications. It allows users to grant applications permission to access their data on their behalf in another application. The advantage: users no longer need to validate their identity manually for this purpose. The drawback: OAuth 2.0 cannot ensure that the person has identified themselves before granting permission to access the data.

## OpenID Connect

**OpenID Connect**
builds on OAuth 2.0 (Open Authorisation) to ensure that the user has been authenticated prior to the authorisation.

This is why OpenID Connect (OIDC) is used in addition to OAuth 2.0. An application that can access user data with the help of OAuth 2.0 is only aware of the authorisation. It has no information about the user, especially whether and how the user was authenticated. Since OpenID Connect enables the requesting application (client or relying party) to access cryptographically signed proofs of identity, it guarantees with the help of an access and ID token that authentication was performed.




1. The end-user wants to use their XYZ login data to access ABC
2. ABC (RP) forwards the request via OIDC to XYZ (OP)
3. XYZ requests the end-user to enter their login data
4. End-user authenticates themself successfully
5. XYZ (OP) returns signed OIDC response to ABC (RP)
6. ABC grants access to the end-user

The Userinfo endpoint makes it possible to query additional information about the user, such as their first and second name or their date of birth. For this to happen, the user must have consented to the release of this information beforehand.

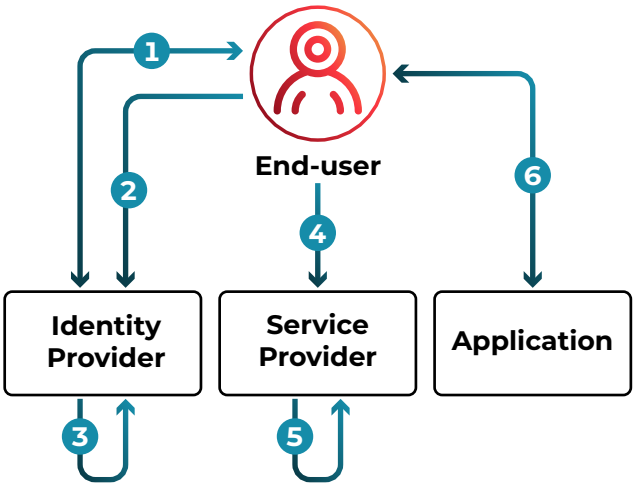
## SAML

**SAML (Security Assertion Markup Language)**
is a standard that is used to exchange authorisation data as well as authentication data between an identity provider and a service provider.

SAML stands for Security Assertion Markup Language and is an open SSO standard that is widely used to transmit identity data between an identity provider (IdP) and a service provider (SP). The IdP performs the authentication requested by the service provider. If this is successful, the SP authorises access to the desired resource. With regard to the application, a distinction is made between IdP-initiated and SP-initiated SSO.

**The SSO process with SAML triggered by the IdP**

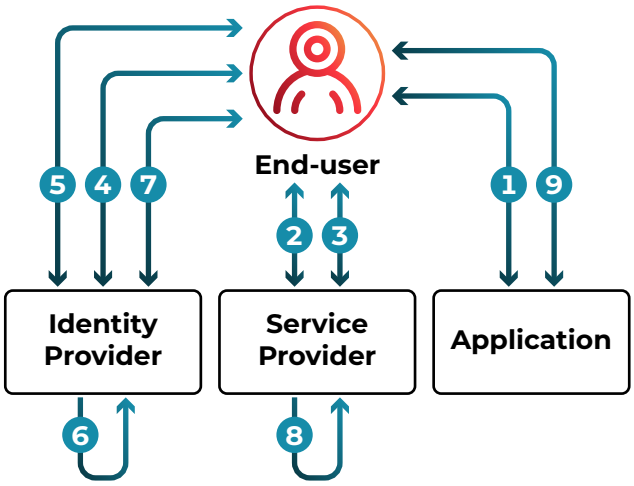
This form of SSO is often found in companies. Here, employees log into the system and can then – depending on their user rights – view a list of all resources for which their employer has granted them SSO access.




1. Authentication of user
2. User chooses service provider application
3. Generation and signing of confirmation
4. Redirection of user to SP with confirmation
5. Validation of confirmation and user identity
6. Transfer user to application

**The SSO process with SAML triggered by the SP**

A different process is used if a user wants to access a service directly without first authenticating themself with the service provider. In this process, the user is first transferred to the identity provider for authentication.




1. User accesses application without session
2. Redirect user to SP
3. Determine which IdP to be used
4. Forward to IdP
5. Authentication of user
6. Generate and sign confirmation
7. Redirect user with confirmation to SP
8. Validate confirmation and user identity
9. Transfer user to application

Expand your knowledge with our blog:
**SAML 2.0 – Secure Login Standard for Single Sign-On**

### Similarities and differences between OAuth 2.0, OpenID Connect and SAML

Whereas all standards are used as part of SSO, OAuth 2.0 differs from OpenID Connect and SAML in that it controls the authorisation. On the other hand, OpenID Connect and SAML are authentication standards. This means that they fulfil different functions but can be used in combination.

Whether OpenID Connect or SAML is the most suitable choice for an SSO solution will depend on which processes a company is trying to secure. Their different functionalities make them suitable for different applications:

- **Open ID Connect** uses OAuth 2.0 as a basis and a JSON Web Token (JWT) as an ID token. **Many consumer websites and mobile apps use this standard for authenticating users.** This allows users who have logged into Google or Facebook, for example, to access another website or application without having to log in again.

- **SAML** is independent of OAuth 2.0 but can be used in combination with it. With this standard, the authorisation and authentication information is sent between identity providers and service providers by means of XML-based SAML assertion. **Particularly in corporate networks, SAML enables users** whose identity and authorisations have been verified to **access different resources** such as software by means of SSO.

## Social login

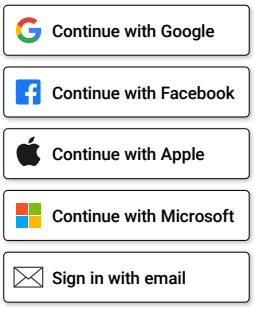
> **Social login**
> lets users log into a third party using their login details for a social network.

One form of SSO is the social login (or social sign-in). It is widely used by online retailers, streaming providers or on internet fora. In many cases, they allow users to log in, for example, with their Facebook, Google or Twitter accounts.

The benefit to users: They can use the respective service without first having to register a separate new account. Instead, the streaming provider acting as the third party relies on information previously stored with the social network and uses this information to perform the login. This means that users do not have to think about new credentials. They can simply use the username/password combination that they already use for the chosen social network. The underlying protocol used here is OAuth2/OIDC.

## How social logins work

**Step 1:** The user visits a third-party website that offers a social login, such as a streaming portal. The user clicks on “Log in” to open a selection menu containing the available login options. It might look like this:




For all the OAuth providers shown, the streaming portal as an OAuth client has already completed the configuration. Users who do not (wish to) use a social network will usually find an option to use their email address to register and authenticate themselves with the respective provider.

**Step 2:** The user selects their preferred social network, and the OAuth client sends a login request.

**Step 3:** If the user has not yet logged into the social network, they are now requested to do so. Once they have done so, the OAuth provider transfers the user back to the client, and the user must then consent in a pop-up window to the data being accessed. The client then receives an access token/ID token in order to access the data of the OAuth provider – the user is then logged in.

## Social login and single sign-on compared

| Social login | SSO |
|---|---|
| ***Functional difference*** | |
| Existing accounts with different social media networks are used to access a website or a mobile application | An authentication method that allows users to log into all networked yet independent applications with a single ID and a single password |
| ***Authentication*** | |
| Via different identity providers in the form of social media platforms such as Facebook | Via an identity provider for multiple networked applications/websites |
| ***In practice*** | |
| Used for a website or a mobile application for which the users can authenticate themselves with their existing social media accounts. There is no need to create a new account for the platform. | Used for a website or a mobile application for which the users frequently require other connected but independent websites/applications. There is no need for separate authentication on the individual platforms. |
| ***User experience*** | |
| Excellent user experience because the (time) expenditure for setting up accounts for specific platforms no longer applies | Excellent user experience because users can use all connected applications without having to log in repeatedly |

## The social login: five advantages for your company

- ☑ **More new user registrations**
  A social login makes it quicker and easier for users to register for a new service. The registration process that often results in the loss of a user is no longer required.

- ☑ **Fewer errors during the login**
  Users who have forgotten their password have two options. They can use the password recovery process – which is time-consuming for them and costly for the provider – or they can simply leave the website there and then. The social login does away with forgotten passwords during the login. Moreover, most users are almost always logged into their social networks on their mobile devices – which means that a social login frequently allows them to log in with just a single click.

- ☑ **Simple implementation**
  Nowadays, companies can incorporate a social login on their websites and web applications without major expense.

- ☑ **The identity provider covers the IT security costs**
  Identity providers such as Facebook, Twitter and so on have IT security resources at their disposal beyond anything that an individual website operator could muster.

- ☑ **Improved customer relationship management**
  Social networks have access to large volumes of user data. Companies that cooperate with them in providing the social login also benefit from this data. For example, they can use this data to provide users with personalised content on their website, in newsletters or on the social networks themselves.

Expand your knowledge with our blog:
**How Secure Is an Identity Check Based on a Social Login?**
**Password Security Fail: Are We Unteachable?**

# Profitable connection: get to know customers even better with user account linking

**User account linking**
allows users to authenticate themselves for an online resource with different accounts – typically from different social login providers. The accounts are linked to a user profile.

## What is user account linking?

User account linking refers to the linking of user accounts with different identity providers with a linked user profile. The requirement for this is the existence of a primary and a secondary user account.

This offers a major advantage for users: They can use each of their accounts with an identity provider to authenticate themselves and are recognised by the provider's application – be it an online retailer, a news platform or a community – and assigned to their user profile.

### How can user account linking be achieved?

There are different ways of achieving user account linking. It can typically be done with customer identity access management (CIAM) systems such as the Nevis Identity Cloud using the standard OAuth 2.0 protocol for authorisation.

In this case, all identities are treated as separate by default. In other words: If the login is completed first using a social login via Google or Facebook and then by the CIAM provided by Nevis, the CIAM detects this as two different users, provided that two different email addresses are used. Modern CIAM solutions provide companies with functionalities that explicitly allow end-users to link different accounts.

### User account linking – a major advantage for customers

Users log into different accounts with the same email address, be it with networks such as Facebook or Twitter, or on individual websites. If a website offers its users multiple login possibilities, such as several social login options, a customer may no longer remember which social network they originally used to log in. They may have used Facebook for the first login but suspect that they subsequently logged in again using their Google account.

In this case, modern CIAM systems will not simply perform the login with the Google account. They draw the user's attention to the fact that they previously logged in using a different account registered to the same email address. The user can then decide whether to link both accounts so that they can choose in future to log into their user profile using their Google account as well as their Facebook account.

It's also not a problem if the user deliberately chooses an account with a different identity provider than the one used for the first login. The user is also given the option to set up a new account with the new identity provider directly.

### Good to know!

User account linking has many benefits for companies, which we will examine in the next section. To profit fully from this, companies must observe the following:

***The primary identity or primary user account covers the user ID and all key attributes of the profile. If the primary account is deleted, then the secondary account is automatically deleted.***

## How to boost revenue with user account linking

Consumers nowadays have access to unprecedented possibilities. They can make purchases everywhere online, on different websites and portals and, more recently, even on social media platforms. They have long since abandoned their desktop computers for these tasks and instead rely increasingly on mobile devices such as tablets or smartphones.

Against this background, companies have a hard time gaining a clear picture of their customers.

However, sales, marketing or support departments need comprehensive information if they are to make their work as efficient as possible. This calls for a 360-degree customer perspective. This offers a comprehensive and up-to-date overview of all the information that is gathered at the various touchpoints.

One of the most important tools for realising the 360-degree customer perspective is a CIAM with functionalities such as user account linking. Ideally, it will also enable – as the Nevis Identity Cloud does – straightforward integration, for instance, of customer relationship management or a customer management system.

### How user account linking simplifies data storage

Thanks to user account linking, a company can use its CIAM as a central storage location for all information about the customer that is gathered from different channels. This involves creating a unique profile for every customer, in which all information – logins, devices used, search and purchase operations or activities on social media accounts – is combined in one location. User account linking also enables information about a user who previously logged in via Google and the next time via Facebook to be allocated and saved to the same profile without difficulty. The only requirement is that the user is registered to the same email address for all these services.

### User account linking supports progressive profiling

By enabling access to the treasure trove of data stored on social networks, user account linking supports the progressive profiling that is so important for marketing executives. In this process, information about a customer is recorded not just once but over an extended period, making it much more comprehensive. The variety of information to which a company has access over a period of time enables it to address its customers in a more focused manner at no additional cost. The possibilities in this regard are diverse: based on social media information, for instance, the content shown on the corporate website such as product recommendations can be better aligned with user interests. In addition, the insights gained from linked user accounts can be used for community management.

### Twin benefits in terms of security

The possibility of SSO alone has a positive impact on corporate security because the number of passwords – which remains a major risk factor – is reduced. If users only need to remember a single password for authentication purposes, this also reduces the risk of them using their password carelessly – typically by using it across multiple accounts. Added to this is the fact that companies can be certain that new users are real people if these users link one or more social media accounts.

## The three biggest advantages of user account linking

- ☑ **Greater user convenience**
  Users can use every identity provider to log into their user profile
- ☑ **Better marketing**
  Based on the stored information collected from the different accounts, companies can offer their customers cost-efficient and targeted marketing
- ☑ **Security bonus**
  When customers link multiple social media accounts, this gives companies greater confidence that they are dealing with real people

# Summary: SSO – three letters with a major impact

Compared with separate login solutions, SSO impresses with key advantages concerning user convenience, security and cost-efficiency. The login process is more convenient for users – thereby creating a better customer experience and boosting brand loyalty. It also increases the productivity of employees.
When it comes to security, SSO pays off in several ways. Users no longer need to remember numerous, possibly insecure, passwords. What's more, companies can outsource the security problem associated with logins to their SSO partner. This saves time and money for the in-house IT team, which also benefits from the fact that all changes for a user profile only have to be made once. The need to modify multiple profiles across different databases is eliminated, which makes administration and the addition of new users much easier and creates greater transparency regarding user data.

### SSO helps cut IT costs – easily

SSO supports companies in all aspects of the login not only with security but also in terms of cost. Since fewer passwords are required, this also means fewer reset requests as a result. Since requests for support due to forgotten passwords entail substantial costs, SSO helps save money. For those who rely on finding out as much as possible about their customers to ensure the success of their business, SSO makes it easier to conduct more targeted marketing activities. After all, in combination with the social login, SSO helps collect and use data about user activities and interests.

In this context, SSO functionality is extremely easy to integrate into the existing IT infrastructure of companies, especially as part of innovative CIAM systems such as the Nevis Identity Cloud.

However, it is important to remember: if hackers gain access to SSO credentials, they will then be able to access all resources for which the user has authorisations. For this reason, additional security measures are a must. In this context, the Nevis Identity Cloud offers the possibility of two-factor authentication, FIDO2 as well as biometric authentication. This keeps companies safely protected against unauthorised access by cybercriminals and allows them to reap all the competitive advantages of an SSO solution.

**→ Read more**

nevis®

Making security an experience.

## About Nevis

Nevis develops security solutions for the digital world of tomorrow. Its portfolio includes passwordless logins that are intuitive to use and optimally protect user data. Nevis is the market leader in Switzerland for customer identity and access management services and secures over 80 per cent of all online banking transactions. Government agencies and leading service and industrial companies around the world rely on Nevis solutions. The authentication specialist has locations in Switzerland, Germany, the UK and Hungary.



www.nevis.net