When an employee leaves, their access should leave with them

Accounts still active after an employee leaves: how Single Sign-On keeps access to corporate platforms aligned



An employee leaves the company. Human Resources updates its systems, IT deactivates the email account, and physical access credentials are returned. Everything is in order, or so it seems.

A few weeks later, someone notices that the person is still active on an app used only by certain departments: perhaps HSE, procurement, or research and development.

Why it happens, and why it matters

This is a situation that many organizations recognize, and usually no one is at fault. The reason is organizational: offboarding processes cover the core systems well, but some applications fall outside the scope of centralized credential management. Each has its own users and passwords, and deactivating them requires an extra step, one that someone has to remember to take.

In practice, what does this mean? If the application is accessible via the Internet, **access that has not been revoked remains usable even after employment ends**, from home or anywhere else. And unmanaged access is also access that no one monitors: company information remains within reach of those who are no longer authorized to access it.

Single Sign-On: one badge for all doors

Think of your company badge: it opens the main door, the office, and maybe even the archive. When someone leaves, the badge is deactivated, and all those doors close at once. With keys, on the other hand, you would have to get every single one back: forget just one, and that door stays open.

Single Sign-On (SSO) works in a similar way, but for applications: users log in with the same corporate credentials they already use for email and shared files, instead of having a separate account and password for each platform.

SDS-FullService supports SSO. This means that no separate credentials are needed to use it and that, as a rule, none are issued: access is granted through the corporate identity. The result is simple: **when IT deactivates the corporate account of an employee who leaves the company, access to SDS-FullService is automatically revoked**. There is no second account to remember to deactivate.

An important clarification: SSO does not grant access to everyone. **Having a corporate account does not automatically grant access to SDS-FullService**. Access is granted on a case-by-case basis, depending on each user's role and activities. In short: SSO checks who comes in and shuts out those who leave. Who gets in is up to the company.

Every Software Solutions Srl - Sole-Shareholder Company
Registered and Operative Office: Via Riccardo Lombardi 19/6 - 20153 Milan - Italy
Tel. +39 02 456739.1 – Fax +39 02 456739.88
Fully Paid-Up Share Capital € 80.000,00 - Tax code/VAT number and Company Register 05469330962 - REA Milan n. 1823737
e-mail: info@everysws.com - **Web Site**: www.every-sws.com

A legitimate question: Are passwords shared?

People often ask themselves this question when connecting an external platform to the company's system. The answer is no: **company credentials are not shared**.

When a person logs in, the corporate identity system verifies who they are. It provides the platform with only a temporary "green light," which confirms the identity of the person logging in. The password, however, never reaches the platform; it remains within the corporate identity system.

What do you need to activate it?

For those who manage SDS-FullService within their company, enabling SSO requires no action on their part. The configuration involves only the company's IT team and SDS-FullService customer support; it usually takes just a few hours to complete.

For the IT team: You need a centralized identity management system (Identity Provider) compatible with the SAML 2.0 protocol, such as Microsoft Entra ID, Google Workspace, or Okta. This is the only check you need to perform before deciding whether to proceed.

A check worth doing

If you want to determine whether your infrastructure is already ready to connect SDS-FullService to your company's Single Sign-On system, our team can conduct a preliminary assessment together with your IT team.

Request the assessment: www.sds-fullservice.com/en/contact-us/