Evidian

7 rules for a successful SSO

Trusted partner for your **Digital Journey**

Summary

Based on 20 years of experience in Single Sign-On (SSO), this white paper describes the good practices and the traps to avoid in order to achieve a successful deployment.

Deploy SSO in your organization

Single Sign-On (SSO) enhances user productivity, increases security, reduces helpdesk costs and helps an organization comply with legal constraints.

An SSO project cannot be implemented just like that. It must be well prepared to ensure a quick deployment, to meet project objectives and obtain users' approval for the project.

Since 1999, Evidian and its partners have implemented hundreds of SSO projects. The main lessons learnt from these projects are described in this document. As you will notice, most of these "golden rules" concern project organization, beyond the purely technical aspects:

1. Clearly define and share the project objectives
2. Demonstrate that the project improves regulatory compliance
3. Involve users actively in the project
4. Observe the existing procedures and policies
5. Keep a simple architecture
6. Publish figure indicators regularly
7. Prepare the implementation of identity management

What is Single Sign-On?

Single Sign-On enables you to access all your applications using only one authentication method. For example, a password, a company badge, or your fingerprint.

Application passwords are automatically filled-in by the SSO tool.

Clearly define and share the project objectives

In summary

The objectives of a successful SSO project are always very concrete

- Reducing helpdesk costs
- Improving users' productivity: doctors, salespersons, traders, etc.
- Reinforcing security of access to critical applications
- Complying with laws and regulations: medical secret, PCI DSS, etc.
- Prepare the implementation of identity management

In general, each SSO project has one or two main objectives, with precise sub-objectives. It is important to define in writing the expected concrete results.

This SSO target plan may be open to formal comments by project participants. It can even be subject to collegial decision-making, for instance, by external participants such as the system integrator and internal participants: finance, internal control or operations departments.

Why is this important?

A well-defined objective, with cost estimates and a realistic target, help you to obtain the support of your management in the course of the project. It will serve as reference for project participants. Indeed, the goal of SSO is not to eliminate 100% of the passwords, but rather to eliminate the input of the most frequently used passwords.

To help the implementation and the involvement of users in the project, you insure management support, either operational or not; by working with it to evaluate the expected benefits.

Practical case

An important bank wished to replace an SSO on 80,000 stations. Its concrete objective: replace an SSO provider that was not supported anymore with an innovative solution providing all the features of the previous one.

This bank also had compliance pre-requisites with tier products and customization needs for the SSO.

Evidian and the integration-service provider rapidly deployed a complete enterprise SSO solution for most of the applications. Then, additional developments were required for specific applications as well as for the customization of the solution for the bank.

Demonstrate that the project improves regulatory compliance

In summary

Even if the main objective of the SSO project is operational - productivity or cost reduction for example - it may be useful to contact the internal control unit. An SSO solution can enable the company to achieve its regulatory compliance objectives, to simplify existing control procedures and to simplify audits.

Most laws and regulations aim to improve the integrity, confidentiality or availability of IT systems.

- **Integrity**: SSO limits access to critical resources, financial resources for instance, to persons whose role requires such access. It can also detect unused accounts.
- **Confidentiality**: the applications that manage personal data (medical information, payment cards) are protected by SSO. Access logs are stored in a central point.
- **Availability**: if a password is forgotten, the PCs and applications remain available thanks to an emergency access with question and answer or with an OTP provided to the user by email, SMS or through the dedicated application QRentry. Moreover, if the SSO solution uses existing directories, it is easily included in an emergency plan.

Why is this important?

The internal control unit must be included in the project, even for consultation reasons, as it can lend additional credibility to this effort and add value to the SSO.

Moreover, by expressing their opinion on the deployment project at a very early stage, the internal control unit may make some recommendations that will be useful later. The way you deploy SSO can help them perform their audit tasks better. This will also allow finding sponsors.

Regulatory compliance is therefore an essential objective that must be put forward by the management team, as its consequences are important for the enterprise.

Practical case

A big telecom company wished to deploy SSO so its users could be more productive and to comply with Sarbanes-Oxley. The purpose of this US law is to ensure the integrity of financial reporting.

While preparing this project, Evidian and its local partner consulted the client's internal control department, as well as external auditors. This consultation revealed other needs that had not been initially identified. For example, auditors verify control procedures by viewing consolidated access data. The auditors, therefore, asked for this SSO data to remain unchanged, and that its origin be systematically documented and logged.

Finally, the project team wrote procedures to verify the gathered information. This made it possible to accelerate by several days the annual audits of access procedures.

Involve users actively in the project

In summary

Employees are the main persons concerned by SSO. So, it is very important to seek their opinion and to take it into consideration in the deployment process. It is not enough to seek the opinion of their managers!

Therefore, you have to identify the most influential employee categories. They may be wary of a novelty like SSO, but will become its driving force once convinced. All their observations will enable you to anticipate user reactions during deployment.

- Identify the profiles and persons who will benefit most from SSO.
- Hold regular meetings of 'pilot' users, with demonstrations.
- Offer them to test the SSO solution and some features prior to its release, such as the delegation of shared accounts.
- Prove them that their work habits will not change.
- Show them the business - and not technical - advantages.

Why is this important?

Once they become supporters of SSO, users will realize the use comfort it provides. They will no longer have to remember any password and will then become promoters of the project.

Moreover, users' remarks help to detect and correct some hitches in advance. For example, you will identify a critical application to be taken into account, local requirements, or some overlooked needs.

Practical case

A hospital group of 100,000 users wished to deploy Single Sign-On for its healthcare staff. In a hospital, the time lost entering passwords has an impact on the quality of healthcare services. Therefore, Single Sign-On based on the healthcare staff's smart card allows them to devote more time to patient care.

The project team made several demonstrations to healthcare staff representatives and performed a test in a department. It noticed that some doctors, who regarded information systems as a constraint, wanted the system to be as discreet as possible. However, doctors appreciated the quick launch of applications and the fact that accesses were logged. Moreover, nurses quickly adapted to SSO access on a shared PC.

However, doctors at the emergency department rejected the systematic use of a smart card for authentication. This impeded access speed. The solution was to adopt a specific security policy in the emergency unit, based on a grace period and session roaming. As access to this unit is physically controlled by a smart card, it was possible to combine speed with security.

Observe the existing procedures and policies

In summary

SSO is not just a "technical project": it improves the day-to-day life of users and organization processes.

Users must be involved in the SSO project to anticipate necessary changes and prevent managers from discovering that they must modify their procedures to take SSO into account. For instance, the manner in which they grant users with access rights to applications may change.

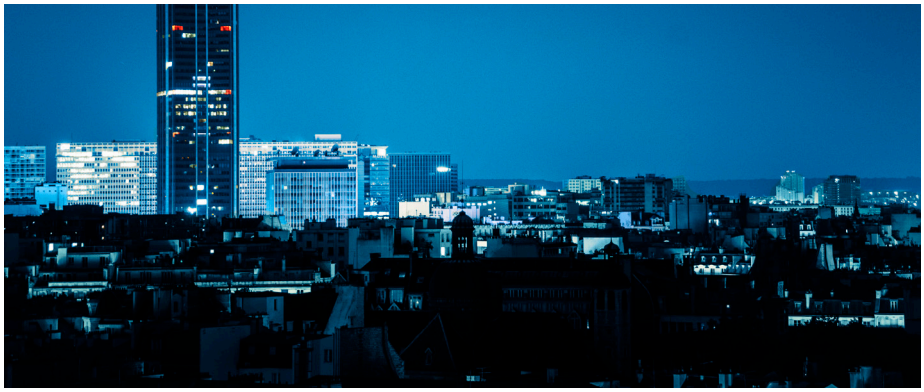
Therefore, you must ensure that these changes are reduced to a minimum and anticipate them when they are unavoidable. Better still; allow each organization to plan some phases gradually according to their needs.

Why is this important?

A well prepared deployment, with the involvement of site or division managers, has an excellent probability of success.

In general, reluctance on the part of managers is not a question of inertia: they do not all have the same priorities and calendar. For example, finance or sales departments avoid installing new tools towards the end of a fiscal year.

Even if SSO simplifies procedures – one can manage access to all the applications from just one screen – local administrators need to be trained. Indeed, when a procedure exists for legal reasons, it is certainly documented and audited; changing it is costly.



Practical case

An industrial company wished to deploy SSO on over 70,000 PCs. The division and site managers supported the SSO project. However, it soon became clear that each of them had different priorities and specific implementation requirements.

Only a few managers agreed to change their application access management methods right away. Some applications like mySAP had to be subject to tests before being included in the SSO – in compliance with financial security laws.

The solution: defining, for each site and organization, 10 to 20 basic applications to be integrated immediately into SSO. Applications such as mySAP were initially excluded from that list, to respect the organizations' pace. The decision to "switch to SSO mode" was taken by each division.

In the same way, SSO does not necessarily change the way accesses are managed. It can just automate access to already existing accounts in a first step. Therefore, SSO was deployed smoothly. Each organization remained free in its choice of calendar and options: which applications to integrate, when to integrate them and how to manage access rights.

Keep a simple architecture

In summary

A project stands a better chance to succeed if its cost is low and if it adapts well to the existing IT environment. Therefore, the architecture should be as simple as possible. Note that the SSO solution itself is only a part of the equation. You also need to have a reliable – and up-to-date – list of users. Moreover, for each user to work unimpeded, the SSO information stored under the identity of each user (encrypted passwords, list of authorized applications, etc.) must be available on each main site.

However, these requirements do not necessarily imply a complex solution. By using already existing directories, servers and network resources, the project can make considerable savings during installation and use.

Why is this important?

Controlling the cost and complexity of a project contributes to its success. You will demonstrate a quick return on investment more easily.

Your company already has a user identity repository: your LDAP directory. You might as well use this resource, and benefit from existing user update procedures.

In the same way, "appliances" can allow a quick deployment for some hundreds of users. However, if your company is organized into several sites, you may have to multiply these appliances and the associated support. By using existing local databases, you will take advantage of resident logistics and skills.

Practical case

A hospital group wished to deploy SSO for its 5000-strong healthcare and administrative staff. Its objectives: reducing helpdesk costs and securing access based on the healthcare staff card. Of course, service continuity of clinical applications is essential in a hospital environment.

An appliance-based SSO solution was being deployed. However, in view of the volume and complexity of its organization, the hospital had noticed some performance and reliability issues. It realized that, if maintenance and replacement were taken into account, operational costs would be higher than planned, and high availability was not guaranteed.

The hospital, therefore, chose to change the architecture and use the existing Active Directory. This directory can host SSO data itself: no new hardware was necessary. The SSO data was thus available on each site, close to the users, making SSO faster. The high availability of the SSO solution is that of the directory. Moreover, emergency plans and backup procedures already exist: they are the ones used for the directory.

Publish figure indicators regularly

In summary

Throughout your project, SSO publishes deployment and operating reports. Since the visibility of SSO goes beyond the IT world, these reports are understandable for non-technicians, and contain indicators that make sense:

- Number of PCs on which the SSO solution is installed, number of users concerned
- Volume of calls to the helpdesk, problems solved
- Size and range of collected audit data, activated security functions
- User satisfaction indicators (through surveys.)
- Number of application accounts declared, total and per user
- Number of applications covered by SSO
- Number of automated logins, with an estimate of saved time

More technical points are of course important, but reports are both communication and management tools. In a number of cases, an automated audit tool collects the required indicators. This facilitates analysis and optimization work. Thus, it is generally easy to demonstrate the quick return on investment of SSO.

Why is this important?

These reports give a view of the project status. As we have seen, you need to win the trust of operations and financial managers, auditors, etc. They expect objective results: provide them clearly.

Do not forget that deployments are easier when the departments concerned participate actively. Once the solution is installed in the first sites and departments, the resulting facts and figures will convince the others. When SSO deployment is finished, you will have gained enough credibility to accelerate some future phases or other projects.

Practical case

In the French subsidiary of an international bank, the security department had noticed that the multiplication of passwords was creating security loopholes and irritated the 1200 employees. So, it launched an SSO project, with biometric authentication. To get the green light, an important argument was the expected decrease in the helpdesk cost.

Reports regarding biometrics use enabled to identify the good and bad pupils. For good pupils, those who activated biometrics, the report enabled to check that there was a low false rejection rate. For bad pupils, those who had not activated biometrics, the report enabled to send reminder emails regarding the new authentication policy.

Thanks to this follow-up, the new authentication policy was implemented quickly and successfully. The practical lessons learned also helped to convince the parent company to generalize the new policy abroad.

Prepare the implementation of identity management

In summary

At the end of an SSO project, it is useful to assess whether objectives were met. Some pending points, such as strong authentication and integration of new applications, may result in future projects.

Evidian has noticed that SSO is an excellent first step towards more ambitious identity management projects. For after a few months, you will have a useful information source: you know which application accounts are actually used, and by whom.

This state also enables you to detect dormant accounts (accounts declared in the application that are not associated with any user). Therefore, these accounts can be deleted or deactivated and thus reduce license costs.

Why is this important?

A successful SSO project is an opportunity to propose an extension to identity and access management (IAM). The reason for this is simple. Since you now know how applications are used, you can define a realistic security policy. Moreover, before enforcing it, you can predict its results.

In the same way, you will be able to implement account "provisioning", namely their automated update under the control of an approval workflow. Account passwords will be sent to the SSO solution.

Users will, thus, naturally comply with your security policy. Their accounts will be created and deleted automatically according to their employee status in the company.

Practical case

A big European railway company wished to implement a security policy to manage more than 150,000 users over 80 applications, i.e. over one million application accounts.

It started taking an inventory of all accounts, but this turned out to be both utopian and costly. On the one hand, getting these accounts was more difficult than expected, on the other hand: how do you know who is using account "sch002": one employee, an entire team, nobody? The company quickly realized that working along this line would cost thousands of man hours.

Instead, the company decided to take an automatic inventory of the accounts that were actually used. Evidian's SSO client performed that task. For three months, it effortlessly gathered information on the actual use of the information system. Each time a user accessed an account, this information was logged in a central database. In a second phase, the company compared this database with the list of all accounts declared in the applications. This enabled it to eliminate obsolete accounts, and to build its security policy on a concrete foundation. It is on these foundations that a future identity and access management project can be built.

Implement your SSO project

Each SSO project is different, but they all follow the same general pattern. Note that for deployment on over a hundred PCs, you are advised to use the services of a system integrator.

1. Model

Before choosing a supplier, ask him to install and test its product on some of your PCs with representative applications. Take notes: is the SSO tool easy to install, can it integrate applications easily, will it scale well when deployed on all your PCs?

2. Planning

Define the functional objectives and inherent costs in writing. Draw a list of internal representatives with the system integrator and select some user representatives. Make an inventory of sites, applications to be integrated and specific requirements. This will help you to work out a projected schedule.

3. Pilot phase

This phase is important; the pilot phase should be implemented in a representative department. For example, test the product on 100 users for 30 days. Use this phase as an opportunity to configure the SSO solution on the most common applications. Do not forget to make a detailed assessment and to learn some lessons from it for the general deployment.

4. Deployment

First of all, check that you have a complete and reliable user directory. If this is not the case, there are tools that can create and keep this source of information up-to-date.

Secondly, the SSO client will be installed on PCs on a phase-by-phase basis, for example from one department to the other. Clearly notify the users in advance, or even offer some training sessions to some of them. Give the helpdesk some time to answer the unavoidable questions before moving to the next department.

During deployment, regularly provide managers with factual reports. They must notice the progress of the project and the results achieved.

5. Assessment

Assess the deployment operation at the end of the project. The remaining points to be handled must be identified and described in action plans.

This will be an opportunity to plan the next phases, such as access policy management or application account provisioning.

Evidian software suite

We offer our clients a complete, integrated and modular solution for digital identity management and access governance compatible with their security policies and the new regulatory requirements.

Our vertical approach provides organizations from all sectors with an implementation of our solutions that are adapted to each profession.

Our software solution is recognized by customers and analysts as a complete solution. It offers the following components, either deployed independently or combined:

- **Evidian Identity Governance & Administration (IGA)** enables authorization governance and a complete management of the identity and access to services lifecycle, driven by a security policy and its approval workflows. IGA manages the four pillars of the Identity and Access Governance market: Identities, Policy, Process & Access. With IGA, only the right people access the right resources with the required rights for the right business reasons. Dynamic audit reports are provided to analyze and detect irregularities in order to fix and improve the security policy.
- **Evidian Web Access Manager (WAM)** is designed to manage access federation to Web applications, secure user access. Indeed, mobile users and partners want to access their messages or company applications securely. WAM allows you to manage access to web applications and replace all user passwords with a single mean of authentication without modifying the applications.
- **Evidian Enterprise SSO** manages access to enterprise and personal applications on workstations as well as mobile devices, preventing the user from memorizing and entering passwords.
- **Evidian Authentication Manager** provides strong authentication on workstations and mobile devices: smartcard or token with certificate, contactless RFID cards, biometrics, One Time Password.
- **Evidian SafeKit** brings high availability and load balancing to applications.

For more information,
please consult our website: **evidian.com**

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

For more information : **Evidian.com**

CT_180622_EM_WP-7RULES-SUCCESSFUL-SSO-EN