Evidian

Enterprise Single Sign-On, featuring mobility, security and simplicity

Trusted partner for your **Digital Journey**

Contents

This white paper is an overview of the main functions of Enterprise Single Sign-On. It also presents Evidian's Enterprise SSO solution.

What is Single Sign-On?

With Single Sign-On (SSO), a user only has to log in once using a single authentication method to access all his applications. To log in, you can use for instance, a password, a contactless badge, a certificate on an ID card, an encrypted USB stick, a One Time Password (OTP) or your finger if you have a biometric reader at your disposal.

The benefits of SSO

To use SSO, you generally install a piece of software on your PC, tablet or smartphone that enters application passwords on your behalf. This piece of software is not necessary if you are just running Web applications or working in "thin-client" mode. In this case, the SSO software is hosted on a server and enters passwords remotely.

SSO makes life easier for users, sparing them time and the anxiety of having to enter, change or even know their passwords. Evidian has seen companies in which employees had to remember about thirty different passwords: today, none or just one password is enough. SSO also reinforces security and reduces costs. These concerns are described hereunder in the Three reasons of investing in SSO section.

Individual SSO and enterprise SSO

Many individual SSO tools do exist, for instance the auto-complete functions of Web browsers. However, providing SSO to hundreds – or even thousands – of employees in a company requires an entirely different approach. This is due to the need to manage, control and offer strong authentication means and other key features such as: administration, delegation, mobility, use of tablets, business continuity and audit, which are essential in large organizations.

Therefore, you should choose an SSO tool that can fulfill these functions adequately: this is an enterprise-level decision.

Evidian's Enterprise SSO solution is the result of over fifteen years' experience in identity and access management. More than 5 million users worldwide access their applications every day with Evidian's solution. For instance, Evidian has a customer equipped with 120,000 PCs spread across several continents, covering a wide variety of use cases. Based on this expertise, this white paper provides an overview of state of the art SSO functions.

What are the alternatives to SSO?

Other solutions reduce the number of passwords entered by users.

- Password synchronization allows you to use the same password for all your applications. If the password for your messaging service is "abcd", then the password for the financial application will also be "abcd". With this approach, the user continues to enter his password each time he connects to an application: the user has a single password but not a Single Sign-On. Moreover, a password-change module that synchronizes the users' single passwords must be developed for each application.
- This type of single password seems easy to use but it compromises security instead. Indeed, the Password Format Control Policy (PFCP) is greatly weakened. If password "abcd" is hacked or stolen on a poorly protected application, then all the applications are compromised.
- Therefore you can understand the General Management's concerns regarding mobile employees requesting access to the information system outside the enterprise. Its transformation plans are sometimes delayed because of security constraints due to this type of solution.

- Some organizations try to synchronize passwords according to different policies, depending on the applications' ability to manage more or less long passwords and contain more or less special characters. However, in practice, the user has a complex situation to manage with more than 2 passwords to use for a great number of applications with mandatory password changes. Faced with this situation where passwords are written down on a piece of paper or in a file, providing the user with SSO software becomes a necessity.
- With access tokens (such as Kerberos or SAML), applications delegate authentication to an external module. However, in most cases, the application must be modified and access delegation between colleagues is impossible. Moreover, re-authentication functions to access critical applications and kiosk workstation management are often not present either.

To illustrate this, here are some examples of frequently encountered situations:

Operational Risk	Frequent situations	Evidian Single Sign-On
Passwords used for each application	All identical to the Windows password	All different and complex
Revealing or stealing an application's password	Provides access to all the user's authorized applications	Provides access to this application only
Internal access for users to critical applications These applications require a high privilege level and must not be accessed if the Windows password is forced by support or the administrator	The Windows password provides access to the applications To manage this risk, the critical applications must be excluded from the synchronization **The critical situation is not managed**	Authentication level configurable per critical application and per user If an administrator resets the Windows password, then access to the application through SSO is denied and the owner of the application is warned **The critical situation is managed globally**
External access for users with a mobile device using e-mails, calendar, contacts, notes and instant messaging	Windows domain Internal password stored locally on the device **The critical situation is not managed**	Password different than the Windows password stored locally on the device **The critical situation is managed globally**
External access via a mobile device (PC, tablet…) in thin client mode via VDI farms to manage mobility situations The user can authenticate with his password or with a One Time Password (OTP)	Windows domain Internal password entered by the user during the connection process, single or combined with an OTP This is a very high risk situation as the Windows domain Internal password is exposed on the terminal and on the external network of the enterprise **Mobility induces a high risk situation that slows down its adoption**	Windows domain Internal password not entered by the user during the connection process, only the OTP is required The risk of Windows domain Internal passwords exposed on the terminal and on the external network of the enterprise is eliminated **Mobility does not induce any high risk situation**

Note: to reinforce as effectively as possible the security of external accesses for special users, the Evidian solution enables to combine the OTP with a password different than the Windows one thanks to the multi-factor authentication.

Three reasons for investing in an Enterprise SSO

There are three main factors that motivate companies in their decision to buy an SSO solution.

1 Reinforce security and satisfy regulatory constraints

By creating a mandatory crossing point between a user and his applications, an organization can control the accesses efficiently. For more information, go to section "Reinforcing security: strong authentication".

2 Reduce operating costs

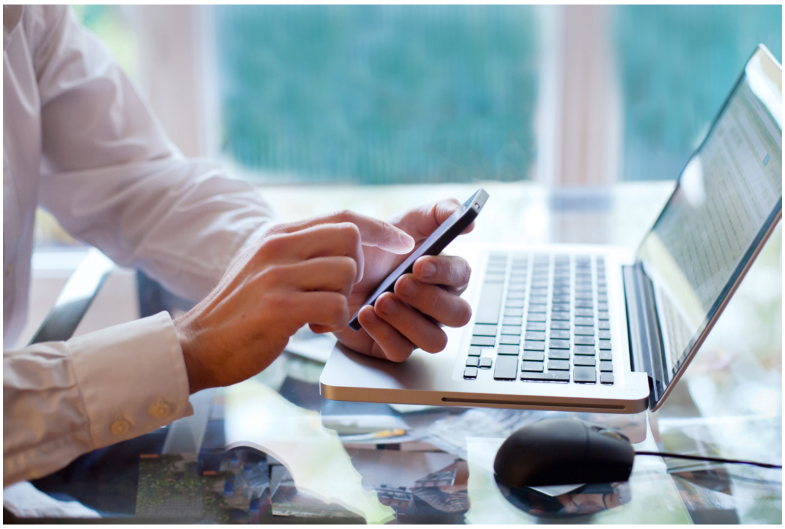
Multiplying passwords, often for excellent reasons, reduces users' productivity and quality of their work. Moreover, these "hidden costs" often have a visible side: up to 30% of helpdesk costs are due to lost passwords. This will be considerably reduced with an SSO solution, with a return on investment that is easy to evaluate. For more information, go to section "Reinforcing security: strong authentication".

3 Open an information system without any risk to the world

This request is getting increasingly frequent: access to the Web has become easy, yet employees still have problems accessing intranet applications from the outside. For more information, go to section "Your information system opens up without risk".

The way to implement the SSO tool may vary depending on these factors, although this tool is the same in all three cases. Of course, some enterprises may choose to kill 2 birds with one stone and meet several needs at the same time!

Security, cost reduction, scalability: Evidian Enterprise SSO meets these needs thanks to a modular architecture. The functional modules can be implemented gradually, providing useful and visible functions in each phase. Moreover, it is possible to first equip one department and then extend SSO to the rest of the company.



A simple Architecture

The three architectures of Enterprise SSO

The SSO software installed on a user's PC, tablet or smartphone enters logins and passwords on the user's behalf. But where does the software find this information? With an individual SSO, the SSO data is stored on the user's workstation. Whatever the data encryption type used, the enterprise gives up individual SSO for enterprise SSO for the following reasons:

- Control: you must be able to remove or assign remote access.
- Audit: you must be able to analyze access to optimize costs related to the use of applications.
- Traceability and user mobility: changing workstations, using workstations in kiosk mode, presentation servers, mobile devices outside the enterprise.

On the Enterprise SSO market, you can find **three architectures** to make SSO information available such as logins, passwords and access rights.

1 **SSO server**: the information is stored on a server, generally dedicated to this task. The PC client queries the server when necessary. The server is often duplicated for high availability and capacity, although cache mechanisms on the PC can compensate for temporary unavailability. Therefore, start-up and operational costs must be taken into account: servers, software installation and periodic synchronization of the user account database with the enterprise directory. In a distributed architecture, the number of these servers may be high; the synchronizations of complex accounts can induce a consistency risk for access right management.

2 **SSO appliance**: it is just a variation of the latter solution. Software and hardware are packaged together. Software-deployment costs are thus reduced. However, it is not possible to install the software on an existing server, which may increase the deployment costs. Finally, it is often impossible to add memory and disk on an appliance, unlike a server. The appliance solution has a limited capacity. Indeed several appliance instances are required for each environment (production, integration, backup site). It introduces a new operating system and a new directory to synchronize. As in the case above, the synchronization of complex accounts induces a consistency risk for access right management. As for the service continuity, this type of solution can induce a risk of SPOF (Single Point Of Failure).

3 **Enterprise directory**: SSO data is simply stored encrypted in the directory that already exists in most companies, ensuring a high level of privacy with a non-reversible encryption of type AES256. For instance, the Active Directory where users are declared and through which they access Windows, or Microsoft AD LDS in which is stored application data associated with the users declared in the Active Directory.

In the Microsoft Active Directory case, you do not need to install any server or appliance. In the Microsoft AD LDS case you can easily use or map servers with the existing Microsoft Active Directory servers. Your PCs are already configured to access the information, since they already access the directory.

The deployment, high availability and service continuity costs for this architecture are reduced significantly. Thus, the solution can also evolve over time and follow the evolution of the components from the Active Directory infrastructure.

In such an architecture, the directory is usually completed with some administration stations and a database in which the activity logs are stored (for audit and reports). This can be a relational database that is already available in the information system. Administration workstations and the database are not used during authentication or user access to applications and therefore are not a mandatory and critical crossing point for the entire system. Therefore, there is no SPOF in this "directory" architecture, unlike "server" and "appliance" architectures.

Evidian Enterprise SSO uses an enterprise-directory-based architecture, enabling scalability without interruption. Experience has shown that this simpler solution is easier and quicker to deploy, while maintaining the highest security level.

Multiple enterprise directories

All companies have created a user directory - but some have more than one! The reasons may be historical (a recently acquired company, an independent subsidiary) or functional (partners are managed in a separate relational database). This may be a problem if a user moves from one domain to another.

In this case, Evidian offers a directory synchronization solution: the most reliable information is obtained in the right place, thus it is possible to create a central directory. This way, a user declared in the human resources databases will be rapidly operational in the entire company.

Therefore, an architecture based on the existing enterprise directory is simple, easy to maintain and rapidly deployable.

MY CRITERIA

- Does the SSO solution require deploying new servers or appliances in my company?
- Is it a problem if my users are listed in several databases, files and directories?

For a large company managing several services or operational companies, each one with its own directory and with no approval system. The global shared SSO service common to all services or operational companies can be deployed without reconsidering this governance principle. This architecture is based on the implementation of a common directory easily deployed. Each user logs on to the local Windows domain of his own company and benefits from the SSO service available from the common directory.

MY CRITERIA

- Does the SSO solution require deploying approval solutions between the domains of my company?
- To benefit from an SSO shared by all my services, is it a problem if my users log on to their domain and if these domains have no approval relations?

Managing becomes a natural task

Managing security with SSO becomes natural

With a well-designed enterprise SSO solution, your security policy is no longer a constraint for your users. They run the applications they are entitled to, without having to remember or manage their passwords. Your employees thus naturally comply with your security policy.

The SSO solution handles all password-related operations. It can even change them automatically, without the user's intervention. You can even prevent the user from knowing the password for a critical application: the user therefore can neither reveal this password, nor provide it to a third party nor use it fraudulently outside the company.

SSO enables you to require a new authentication from the user to authorize access to a specific application.

Use case: Bank BK has Single Sign-On. After logging on to his Windows session with his Smart Card (certificate + PIN), thanks to SSO, the user accesses his applications "BK-Intranet", "BK-Agenda", "BK-Travel", "BK-Presence", "BK-iSeries" without entering his login or password for each application. During this session, the user opens the "BK-SWIFT" application. This application needs a high-level accreditation requiring a One Time Password (OTP) authentication. The SSO queries the access policy, detects that OTP authentication is mandatory and asks the user to enter it. If it is validated, the SSO starts the SWIFT application and transfers the authentication data to the SWIFT application without the user knowing.

From a central management console, you can decide who has access to which application.

Of course, with thousands of employees and hundreds of applications, it is out of question to grant accesses one by one! The administrator simply decides which group of users has access to which group of applications, and from which PCs if needed.

For example:

- Back-office applications must never be used from a trading PC
- R&D PCs must always be accessed through biometrics
- The General Ledger application must be used by the finance service only.

MY CRITERIA

- Can we restrict application access based on the user's job position, but also from where the application is opened?

Managing passwords naturally

With Evidian Enterprise SSO, you can enforce a strict password policy (for instance at least two digits including one in front, more than ten characters, etc.). This policy is different for each application, even if the application itself is more permissive. This is possible since all password operations are under the SSO's control. Therefore, passwords can be different for each application. Exceptions can be made and some applications can be easily declared using the password of the user's Windows session.

But what happens if an employee wishes to be replaced by a colleague while he is away? Before, he used to reveal his login and password, with all the inherent risks in terms of security and audit.

Evidian Enterprise SSO, on the contrary, allows an employee to temporarily delegate access to a colleague. Of course, he can only do so if your security policy authorizes it. Moreover, an access record is kept, so you know which operations have been performed by which user.

MY CRITERIA

- Does the SSO solution allow an employee to personally delegate access temporarily to an application, for instance before going on leave?

Reinforcing security: strong authentication

The login/password combination is the most common access method, especially in Microsoft environments. However, this universal “open sesame” is often not enough to protect critical resources. Does a password prove that the person connecting is actually the password owner?

This is why people sometimes choose to reinforce SSO with strong authentication methods.

These can be deployed on all or part of the workstations; it is a common practice to protect some workstations and sensitive applications.

For example:

- Top management PCs
- Customer adviser PCs in a bank
- Doctors’ access to patient records
- Nurses opening sessions on kiosk stations
- R&D and salesperson sensitive laptops
- Mobile audit firm laptops
- Kiosk stations with certificate cards on the production line
- Video surveillance desk with access to personal data
- Operator with access rights to bills and call tickets in a telecommunications company
- Medical staff moving from one kiosk PC to another by presenting their smart card and retrieving their work session in the same state
- Front office trader opening simultaneously all the Windows sessions on his workstations with a single authentication device on the cluster of workstations.

Here are some common types of strong authentication methods:

TYPE	ORGANIZATIONS	EXAMPLE OF SOLUTIONS
Smartcard or USB token with digital certificates relying on a national, regional, local Public Key Infrastructure (PKI)	‣ Health ‣ Hospitals ‣ Manufacturing ‣ Finances ‣ Public	Carte Santé CPS (FR) NHS Connecting For Health Card (UK) UZI-pas (NL), Corporate ID National Identity Card e-ID (BE, ...)
Biometrics Biometrics and FIDO	‣ Health ‣ Hospitals ‣ Finances	Finger Print Reader on PC Vein ID Captor on PC Finger Print Reader on Smartphone
One Time Password (OTP)	‣ Manufacturing ‣ Bank ‣ Insurances	OTP on Smartphone OTP via SMS OTP token
PIV, CIV Smartcard	‣ Government Defense	Multi-service Smartcard Derived credential on Smart device
RFID Card Radio Badge Bluetooth	‣ Health ‣ Hospitals ‣ Retail	Proximity Card with RFID Wearable device with RFID Smartphone
Dual Smartcard combining physical and logical access	‣ Health ‣ Hospitals ‣ Government	Carte Santé CPS (FR) NHS Connecting For Health Card (UK) UZI-pas (NL), Corporate ID National Identity Card e-ID (BE, ...)
Connected object	‣ Manufacturing	Bluetooth Band

Evidian Enterprise SSO is compatible with the large variety of strong authentication methods presented above. Evidian solutions can manage these devices in an entire company: assignment of smart cards and USB tokens, lending operations, blacklisting, badge customization etc. Access security is thus reinforced for certain categories of users.

MY CRITERIA

- Is the SSO solution compatible with the strong authentication method I have chosen?
- Can I prevent an application from being run on a PC that is not protected through strong authentication?
- Is it possible to support several authentication methods at the same time, based on user or PC profiles?
- Does the SSO solution cover all use cases specific to my business?

Your operating costs are reduced thanks to service continuity

A well-designed SSO tool reduces operating costs. Some of these costs are hard to evaluate since they affect user productivity. However, other savings are easier to measure: they concern helpdesk workload.

Evidian Enterprise SSO handles application password constraints, therefore avoiding forgotten passwords or blocked accounts. Helpdesk calls fall by up to 30%, because users no longer need to remember application passwords.

However, you need to handle forgotten primary passwords or lost access cards. For example, what happens if a salesperson notices in a hotel that his smart card no longer works? Evidian Enterprise SSO, with its **Self-Service Password Request** (SSPR) module will unlock his access. It is not necessary to be connected to the network.

With Evidian's **SSPR** module, the enterprise can choose to use a tailored procedure based on: Questions and Answers, Confirmation code sent via email and SMS, OTP scanning a QRcode with the QRentry Apps. For example, the SSPR module can be configured to request the user to answer three questions the first time SSO is started on his PC. If the user forgets his password or loses his access card, the user will answer the predefined questions and reset his password. This way, the user is not blocked by a lost access.

Evidian also offers **QRentry**, an emergency access without any questions/answers with strong authentication always available.

With **Evidian QRentry,** users connect to their Windows sessions by scanning a QR Code with their smartphone and by entering the code provided by the smartphone. This access is always available online and offline even when the smartphone is not connected to the network. Thus, the user has a one-time password (OTP) generator at his disposal on his smartphone.

Evidian QRentry is the ideal companion for deploying an authentication system, which generates "forgotten password", "lost card" or "broken biometric device" calls. The number of calls to the helpdesk reduces drastically – there is nothing to memorize. A user can unlock his Windows session himself, even if the helpdesk is unreachable.

MY CRITERIA

- Will my users be able to reset their password without calling the helpdesk?
- Is it possible to reset a password offline?
- Does the SSO solution ensure access continuity to users if strong authentication fails?

How to integrate one of your applications into the SSO solution?

SSO replaces the user and enters logins and passwords on his behalf. For this, the SSO software must recognize the software's login window but also the password change window, or the wrong password message window. This is done once for everyone in the company and then distributed to the employees' PCs and mobile stations through the enterprise directory.

This is usually easy for Windows applications that have been developed according to Microsoft standards. However, less classical applications must also be taken into account:

- Internal applications developed many years ago
- Mainframe applications in terminal emulation mode
- Packages with special interface features such as OWA, Office 365, SAP and Lotus Notes
- Java applications or applets
- Web sites and portals through Internet Explorer, Chrome or Firefox.

How to ensure that the SSO software can integrate your applications, even the most 'exotic' ones? It is often wise to ask the vendor to test the solution on premises, and integrate the most critical applications.

Evidian Enterprise SSO allows you to integrate most applications with a few clicks. Start the application and point your mouse to the "login", "password" fields, etc. The application is now recognized everywhere in the company. Some application versions such as Lotus Notes, SAP, or browsers are supported natively and a graphical script tool is available.

MY CRITERIA

- Will the SSO solution allow me to integrate my applications simply, or does it require programming?

Everyday SSO administration

The SSO solution allows you to make real savings. Yet, it should not generate heavy administration costs in return! When you have dozens of users. Instead, it must be extremely easy to manage the rights of a user arriving, changing job position or leaving the company.

Moreover, if some applications are 'discovered' in the company during deployment, you also have to quickly integrate them as well. And since the user may not know the passwords for his critical applications, how do you delegate the user's accesses during holidays without increasing the helpdesk's workload?

To appreciate the daily administrative workload of an SSO tool, it is better to ask for an on-site evaluation. You can test administration scenarios for a few days. You will check whether the profiles of the selected persons are appropriate, and you will estimate their workload.

Evidian has incorporated many administration functions into Enterprise SSO. With over fifteen years' experience, the ergonomics and functions have been refined to make administrators productive.

For example:

- When a user is away, he can delegate his accesses before leaving, without revealing his passwords.
- Local administrators incorporate their own applications and manage their teams' accesses.
- Specific administration roles cover applications, cards, passwords, audit, etc.
- When an administrator changes functions, his rights are easily transferred or delegated. If necessary, the application teams can benefit from a simulation and diagnostics tool to validate the configuration established with their application.

MY CRITERIA

- What will be the daily management workload generated by the SSO solution?

Your information system opens up without risk

Opening to mobile devices

If you must use an iOS or Android mobile device along with or instead of your PC to access intranet or Cloud applications, how can you retrieve your passwords and personal notes?

SSO features must enable access to your applications securely from any other terminal (PC, tablets, smartphone, thin client, virtualized station).

Evidian offers **Enterprise SSO for mobile devices** to its customers. It securely shares the same protected information, passwords or personal notes, whatever the terminal you use.

MY CRITERIA

- If a PC's local SSO changes the password for an application without the user knowing it, will he still be able to access it from his iOS or Android tablet?

Opening to the outside world

When one of your employees is on a business trip, must he use a specially configured PC to use the intranet applications? The better choice is to use SSO functions that allow him to securely access internal Web applications from any browser (cybercafé or client site, for instance).

This can be extremely useful. Some Evidian customers use this function to make their mobile employees really independent: travelling salespersons, police officers on a mission, engineers on a site abroad, etc.

Some other SSO solutions consider Web accesses as a weakly integrated add-on: therefore, the 'Web' and 'intranet' parts do not exchange some pieces of SSO information properly. Unlike these solutions, Evidian Enterprise SSO securely shares the same protected information, regardless of the access mode.

MY CRITERIA

- If a PC's local SSO changes the password for an application without the user knowing it, will the user still access it normally and securely from outside with a browser?
- In that case, how do I avoid propagating internal passwords from my organization between his external browser and the secure access gateway of my information system?
- If my partners have access with a simple browser to my unified service of orders, client accounts and special offers, how can I authenticate them with a one-time password and how can I offer them this unified and secure view?

Scalability

For now, you wish to equip your department or only one site of your company with an SSO solution. But it is wise to anticipate the time when SSO will be extended to the rest of your company, even if it is in the distant future. So, you need to choose a scalable SSO solution or eventually risk changing your solution, with the inherent difficulties of migrating all the passwords.

Scalability is a real issue for certain SSO products that are designed for a few hundred users. How do you share data for mobile users in different countries? Do you need to train an administrator per site or per department? Does the basic technology change? Do you have to install dedicated hardware in many places?

Evidian Enterprise SSO has been deployed in companies with over 200,000 users. The solution is easy to extend: the same simple technology, based on the enterprise directory, is used for clients with one hundred or tens of thousands of users.

MY CRITERIA

- Has the SSO solution shown that it could be deployed for tens of thousands of users?

Integration with identity and access management

Evidian has noticed that SSO is often a prelude to a more ambitious identity and access management project. Indeed, an access policy can be defined rigorously, validated according to a strict process and audited regularly. Employees will naturally comply with it through the existing SSO mechanism.

And that is not the end of it: since SSO provides information on the actual use of applications, it is possible to continuously audit the compliance with the security policy.

Finally, accounts can be updated automatically in the applications; the user is thus immediately operational.

Evidian Enterprise SSO is part of Evidian's IAM suite identity and access management solution. It can be connected to **Evidian Identity & Access Manager** to automate password management or provide actual access data to audit and refine the security policy.

Stop distributing passwords to users: in coordination with your identity management processes, a provisioning module or a workflow can synchronize application accounts with SSO.

MY CRITERIA

- Can the SSO solution be extended later, by integrating role-based access management or provisioning?

Evidian: overview of the access management features

Evidian Enterprise SSO enables you to rapidly deploy an effective Single Sign-On solution. Users access their applications more easily and securely. Building on the SSO features, you can add modules that provide strong authentication and additional administration functions:

- **Quick access to Single Sign-On** with a direct connection to applications, available on PC, tablets and smartphones.

  The Enterprise SSO clients for Windows and for Mobile devices offer Single Sign-On functions such as access and password rules administration, delegation, re-authentication, multi-level authentication, password revealing, digital safe management and audit collection.

  SSO access from the internet with a thin client or a tablet with a standard integrated browser.

  Mobile E-SSO enables users to connect securely through an SSO server to their applications, from any Web browser. In many cases, Mobile E-SSO allows users to authenticate with a One Time Password (OTP) without having to enter the Windows domain password and without having the enterprise internal passwords transit between the user station and the enterprise internal network access point.

  Access to activity continuity procedures.

  If necessary, the Enterprise SSO Web portal enables your organization to provide password delegation and revelation procedures from a Web portal.

- **Access to the emergency plan**

  If necessary, the Enterprise SSO Web portal enables your organization to send the application credentials to your employees by e-mail. Authentication Manager simplifies the use of user authentication methods to access their Windows session with the required security level. These methods are: cryptographic cards with or without PKI in badge or USB format, certificates, active RFID, biometrics and One Time Passwords (OTP) generated by software or hardware mechanisms.

- **Emergency access** to the Windows session and password management

  With Self-Service Password Request, users manage their own emergency access procedures to their session: domain password reset, PIN unblocking, Windows session opening without domain password modification. This procedure is based on a questions/answers mechanism; it can be accessed from the Windows login window on the user's workstation and from the portal's Web page available for domain password modification and account unblocking.

- **Kiosk mode** on a workstation

  The Session Management module enables employees to share a PC in kiosk mode without restarting the Windows session. This module can park one user's running session and start or resume another user's session. A change of users requires only a few seconds.

- **Strong authentication** with **Evidian's QRentry** application

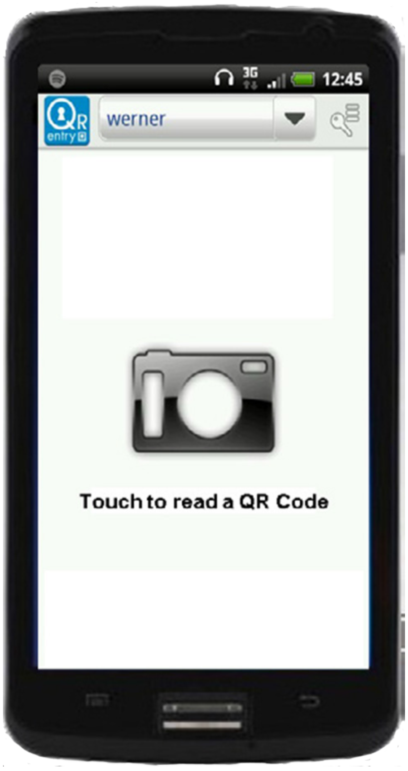
  QRentry enables the user to turn his smartphone into a strong authentication mean protected by the device's PIN. This application allows managing and authenticating the smartphone as an access point protected by a certificate with a private/public key mechanism. It is the ideal way of having an emergency access to the Windows solution without using the questions/answers mechanisms. In online mode, the user just has to validate a notification to authenticate.

- **Cluster mode** to open **n** sessions simultaneously

  With the Cluster Mode, employees can use multiple PCs simultaneously (for instance, traders or plant supervisors). One authentication will unlock all the user's PCs. The PC delegation and detachment mechanisms between users are natively managed by this mode.

- **Reporting**

  Finally, reporting tools generate reports about administration and authentication events, as well as accesses to target applications.



Supported environments

- The SSO client is available for supported versions of iOS, Android, Windows, Mac OS, Citrix, VMware and Terminal Server.
- Most Windows, HTML or Java applications are configured through simple drag and drop. The features of specific applications are supported as standard or through a graphical configuration.
- The directory containing users and the security policy may be supported versions of Active Directory or other LDAP directories.
- Audit events are stored in a relational database.
- Reports are generated in different formats, such as PDF.

Evidian software suite

Our IAM solution is recognized by our customers and analysts as a complete solution. Indeed, it offers the following components that can be deployed independently or natively integrated:

Evidian Identity & Access Manager

enables authorization governance and a complete management of the identity and access to services lifecycle, driven by a security policy and its approval workflows.

Evidian Web Access Manager

federates accesses to Web applications, secures the access of mobile users and replaces all user passwords with a single and strong authentication mode.

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

offers strong authentication on workstations and mobile devices: card or token with certificate, contactless badge, biometrics, One-Time Password.

Evidian SafeKit

brings high availability and load balancing to applications.

16/02/2018 : Visa de sécurité ANSSI (CSPN) pour Evidian Enterprise SSO v. 8.06PL5 b5386.30
(https://www.ssi.gouv.fr/entreprise/certification_cspn/evidian-enterprise-sso-v-8-06pl5-b5386-30/)

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**