

Password Management

EVIDIAN
A Groupe Bull Company



Trust
in an open world

Manage your passwords

Evidian Enterprise SSO's password management capabilities enable users to create and change both primary passwords (network login) and the passwords to all applications. They provide a full audit trail to demonstrate the implementation of the password policy.

Password life cycle

Evidian Enterprise SSO password management capabilities cover the main domain of the password life cycle: creation, modification, reset...

Automation of password change for all applications, based on their password policy

Evidian Enterprise SSO manages password change by reacting to a prompt from the application or forcing a password change on a regular basis.

Self-service password change for all applications

In addition to the automated approach above you can enable users to define and submit a new password for all applications on a regular basis

Self-service primary password reset for users' network login, whilst connected or disconnected from the domain.

Users who have forgotten their network login can reset this password by answering pre-defined questions whether they are working online or offline.

Enforcing strong password policy for all applications

Evidian Enterprise SSO can enforce a different strong password policy for all applications.

You can define for each application different password attributes such as the type of characters as well as their position, the minimum and maximum number of characters, etc...

Full audit trail of application access and password change

The solution provides a full audit trail of WHO has access to WHAT, WHEN and from WHERE in addition to a full audit trail of password changes events and locations. This type of report can help to demonstrate that your password change policy is effectively implemented.

Use your company's existing LDAP infrastructure

Evidian Enterprise SSO works with your existing LDAP directory. So, you do not need to deploy any additional servers. All the Evidian Enterprise SSO security data is encrypted and stored in your company directory.

3 reasons to manage password with Evidian Enterprise SSO

- 1 Enforce your password policy effectively.
- 2 Hide to end users the complexity of the password management.
- 3 Reduce helpdesk "password reset" related costs.



Password Management

Evidian Enterprise SSO Enterprise SSO Main Features

Make life easier for your users

Evidian Enterprise SSO offers self-learning and self-administration functions for initializing passwords. When users are absent, they can delegate their accesses without revealing their passwords.

Excellent SSO policy management

With Evidian Enterprise SSO, your administrator may decide, for example, that call center PCs must only be used with smart cards. He or she may also decide that corporate applications (messaging system, time or invoice management) will only be accessible through Windows Terminal Server.

Delegate your administrative tasks

Evidian Enterprise SSO allows you to define administrator roles for applications, cards, password management, audit, etc. When an administrator leaves an organization, you can easily transfer his or her rights to another person.

Integrated connection-analysis and administration tools

Event audits are stored in a relational database. A console allows contextual analyses (by application, user, access point, and smart card), or criteria-based analyses using filters.

Reinforce your user authentications

With Evidian Enterprise SSO, you can deploy strong authentication methods with the help of smartcards (or USB keys), one-time passwords (OTP), biometrics or proximity cards (RFID, HID, MIFARE). A secure login client is installed on the PC to control initial access to the company's network. The user is thus robustly authenticated on the company's LDAP directory and can then access all his or her applications.

Emergency access when a user forgets his or her password or smartcard PIN

Employees or mobile users can reset their password after answering some personal questions. They can securely access their PC even if it is not connected to the company network.

Manage the entire lifecycle of your smart cards

Evidian Enterprise SSO offers a smart card and USB-key administration system. This solution allows you to personalize the card, assign it to a user, lend a card if lost or forgotten, unlock it, blacklist it, and store SSO data and certificates.

Enhance the mobility of your users in order to accelerate your business

Mobile users can connect to your company's web applications from any web browser, without re-authenticating with a password.

With the most appropriate authentication method (password, OTP, smartcard, etc.), the mobile user is authenticated to the company directory through a security gateway.

Fast user switching

Thanks to a fast-user-switching solution, users can securely share a PC without having to close then re-open a Windows session.

User profiles are managed with a dedicated console. Evidian Enterprise SSO authenticates the user, provides him or her with his or her personal SSO data, and controls user changes through a smartcard or proximity smartcard.

Reset your primary password

When Evidian Enterprise SSO is first started on a workstation, the user provides three questions/answers.

If users forget their primary password, they connect to a web address. They enter their login, answer some predefined questions, and is then allowed to reset their primary password.

You no longer need to distribute passwords to users

A provisioning function, perfectly coordinated with the company's identity management system, synchronizes the SSO data with the creation and deletion of application accounts.

Through web services, such as SOAP or C/C++ APIs, this function enables you to create, modify, invalidate and delete SSO data stored by Evidian Enterprise SSO in the company's directory.

Supported environments

The user-management and security-policy-storage LDAP directory can be Active Directory or ADAM in Windows 2000/2003, Sun Java System Directory Server, Novell eDirectory, IBM Directory Server or OpenLDAP.

Audit events can be stored in Microsoft SQL Server, MySQL, IBM DB2 or Oracle databases.

Evidian Enterprise SSO components are available in Windows 2000, 2003, XP and Vista. Pre-provisioning will be available in Red Hat Linux and Sun Solaris.

From workstations or thin clients, Evidian Enterprise SSO supports Citrix and Windows Terminal Server environments.

For further information, visit our website: www.evidian.com or contact us: info@evidian.com

Evidian Enterprise SSO is a registered trademark of Evidian. All the cited products and brand names are trademarks of their respective owners. Evidian reserves the right to modify the characteristics of its products without prior notice