

Business-aware multi-factor authentication management for the whole organization



Evidian Authentication Manager

Secure access to your workstations and servers in any situation. Cover all authentication scenarios, whether one user accesses one or many PCs, or many users share one PC.

Passwords are a weak point in many authentication policies. Shared or simple Windows passwords are a risk of intrusion, and make it almost impossible to precisely audit Windows account usage.

Strong multi-factor authentication solves these issues by replacing passwords with devices or biometrics. But in the field, strong authentication faces operational constraints. To deploy and manage thousands of users, you must cover all use cases - or risk hindering employees in their daily tasks.

Secure complex authentication scenarios

Evidian Authentication Manager adapts strong authentication usage to the users' business constraints by allowing elaborate scenarios such as:

- Failover access when a device is lost, forgotten or malfunctioning,
- Kiosk mode and fast user switching,
- Authenticating on a cluster of PCs with a single authentication device,
- Individual named access to generic Windows accounts,
- Windows account delegation between users,
- Link with physical access control.

Simplify strong multi-factor authentication

Evidian Authentication Manager simplifies the deployment and day-to-day management of strong authentication:

- Central management of access policy,
- Role-based authentication profiles,
- Integrated card administration (inventory, issuance, black list...),
- Centralized audit of all access attempts to PCs.

With *Evidian Authentication Manager*, you're not locked into a technology. You deploy the right authentication in the right place. Your security policy is defined in a single operation - for all access modes.

Reduce usage costs

Evidian Authentication Manager replaces multiple consoles. Help desk staff unlock or remove access in a few seconds, whether for Windows password, smart card, RFID, biometrics or one-time password (OTP).

With self-service password request (SSPR) and failover access, users unlock their Windows access by themselves. This eliminates "unlock me" support calls.

PRODUCT FEATURES

A wide range of supported authentication methods

Evidian Authentication Manager supports most leading authentication technologies:

- Smart cards and security tokens, with or without certificates,
- Fingerprint and vein biometrics,
- RFID radio tag,
- One-time passwords (OTP),
- Questions and answers sequence,
- Login / password.

Manage the full lifecycle of authentication

Evidian Authentication Manager includes card administration functions, so the devices' lifecycle is managed from a single point. You issue a card to an employee, lend a replacement, blacklist it or store data and certificates.

Specific business functionalities

Sales or branch offices clerks share a common PC kiosk and switch to their own environment in a few seconds without having to log on and off to Window. Doctors keep up their own single session when roaming the hospital premises.

Traders and control rooms technicians can lock, unlock, delegate totally or partially, permanently or temporarily a cluster

of PCs with a single multi-factor authentication.

Delegation by the user

When users go on vacation, *Evidian Authentication Manager* allows them to delegate access to their PC under the control of the security policy.

Shared account management

With *Evidian Authentication Manager*, users can use generic Windows accounts securely. They don't need to know the passwords and are identified by name.

Request a failover access...

When *Evidian Authentication Manager* runs for the first time on a PC, users select personal questions and answers. If they forget their means of access, they answer questions and get a temporary password.

...Even offline!

Mobile users can reset their access even if they are not connected. They answer questions from the login window of their laptop.

Audit all access and administrative actions

Signed audit trails are stored into a central database.

Reports are produced by application, user, access point, smart card, etc. Data can be analyzed via SIEM and report tools.

Integration into Evidian IAM solutions

Evidian Authentication Manager is part of Evidian's identity and access management solutions. This ensures the convergence of authentication and identity lifecycles.

- With *Evidian Enterprise SSO*, launch your applications without any additional password.
- With *Evidian Web Access Manager*, users access their web applications from any browser, securely, without re-authenticating to each application.

Use your existing infrastructure

Evidian Authentication Manager uses your existing LDAP or Active Directory. Users are not duplicated. All security data are encrypted and stored there; appliance is not needed. Start in one department and extend *Evidian Authentication Manager* later to thousands of users.

Evidian Authentication Manager runs on most Microsoft Windows, Citrix XenApp and Windows Terminal Server environments.

"The Evidian solution simplifies users' life, provides a direct return on investment, and enhances security while enabling us to precisely control the use of resources in the company."

Arturo Rivera, Identity Management Project Leader, VALEO

"We have greatly increased security by requiring strong authentication."

The Evidian solution is part of our life: we now use it everywhere."

Marc Jobert, Corporate VP and Chief Technical Officer, PAREXEL

© 2010 Evidian

Evidian is a registered trademark owned by Evidian, a limited company registered in Versailles, France, RCS B422 689 208. All product names, trademarks and other elements mentioned herein belong to their respective owners and may be protected under laws and regulations governing intellectual property. Evidian reserves the right to change specifications of products without prior notice.

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

Evidian - rue Jean Jaurès B.P.68 - 78340 Les Clayes sous Bois - France - Tél. : +33 (0)1 30 80 37 00 - Fax : +33 (0)1 30 80 37 10.

This brochure is printed on paper with 40% fiber eco-certified from a sustainable forest management, and 60% recycled, under environmental rules (ISO 14001).