evidian

Authentication Manager Business oriented ready to use

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

Secure access to your PCs and servers in any situation. Cover all authentication scenarios, whether a user accesses one or several PCs, or several 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.

Dedicated business features

With Evidian Authentication Manager, sales or branch office employees share a PC and access their own environment in a few seconds without having to log on and off to Windows.

Doctors keep their own Windows session when roaming the hospital premises.

From one PC, front desk traders and control room technicians can open, lock, unlock, or close a set of PCs using their multi-factor authentication.

An employee can delegate access to his locked sessions permanently or temporarily (optionally with a read only screen) for one or several PCs.

Simplify multi-factor authentication deployment

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

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

By choosing Evidian Authentication Manager, you are not bound to a technology. You deploy the right authentication in the right place. Your authentication policy is applied from a central point for all methods.

Reduce usage costs

Thanks to Evidian Authentication Manager, from a single console, help desk staff unlock or remove access immediately for any authentication means (password, smart card, RFID, biometrics, One-Time Password (OTP)...).

Moreover, users unlock their Windows access using Self-Service Password Request (SSPR). This eliminates "unlock me" support calls.

Leverage on your existing infrastructure

Evidian Authentication Manager relies on your LDAP or Active Directory where security data is stored encrypted: users are not duplicated and no appliance is needed.

Microsoft smart card logon

Evidian Authentication Manager is fully compatible with smart card logon and can provide you with efficient emergency access procedures.

IGEL thin client integration

Evidian Authentication Manager and IGEL make authentication on thin clients easier, quicker and more secure. Users can access Linux-based thin clients via RFID or smart card.

Already authenticated employees can quickly and securely access their session (Citrix XenApp and Microsoft RDS) on any thin client during the day simply by presenting their RFID badge or inserting their smart card.

Easy deployment

Start with one department and extend Evidian Authentication Manager later to thousands of users. Evidian Authentication Manager runs on Microsoft Windows, Citrix XenApp and Windows Terminal Server environments.

Bull
atos technologies

Business Oriented – Ready to use

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 authentication lifecycle

Evidian Authentication Manager includes card administration features allowing you to manage the devices' lifecycle from a central point. You can issue or lend a card to an employee with stored data and certificates. You can also suspend or blacklist a card.

Delegation initiated by the user

When users plan to be away, Evidian Authentication Manager allows them to delegate access to their PC under the control of the security policy.

Shared account management

Users can securely use generic Windows accounts. They don't even need to know the passwords; audit events contain their authentication information.

ActiveSync integration

Evidian Web Access Manager can control mobile accesses to the e-mailing system, using the ActiveSync protocol without requiring the Windows password on the mobile device. In this case, Evidian Web Access Manager uses the Windows password known by Evidian Authentication Manager to authenticate on the mail server. The combination of Evidian Authentication Manager and Web Access Manager allows you to give users access to mail servers without compromising the Windows passwords.

Strong authentication via QR Code

With Evidian QRentry, users log on to Windows by simply scanning a QR Code with their mobile device. This access is available whether you are connected or not to the corporate network.

Emergency Access from the Windows logon screen

The Evidian Self Service Password Request (SSPR) feature reduces usage costs by allowing users to reset their password by themselves or with a challenge provided by the helpdesk. When this feature is enabled, users answer personal questions. If they forget their means of access, they answer questions, either to reset their password or to access their Windows session.

When users reset their password using SSPR, this password can be:

- A temporary password: allowed for a defined duration
- A password valid only on the PC where the reset has been requested
- The definitive password of the user.

... Even offline!

Mobile users can reset their access from their PC even if they are not connected to the corporate network.

As an alternative solution to questions and answers, QRentry can also be used as an emergency access.

Emergency Access from the web portal

Just as from their workstation, users can connect to the Authentication Manager Web portal to answer questions or activate emergency access.

The Web portal can also be used to reset their password with:

- A confirmation code sent to the user by mail or SMS
- QRentry as an authentication means.

Security of the emergency access procedure can be enforced using a captcha.

Ensure that your information system is compliant with laws and regulations

Signed audit trails related to access and administrative actions are stored into a central database.

Authentication Manager helps you to comply with your legal and regulatory requirements such as Sarbanes - Oxley, decrees on medical confidentiality, PCI DSS or laws on financial integrity.

You can monitor your employees' attempts to access PCs. The audit events contain user identification. This enables you to demonstrate that your access policy is observed and fulfills its objectives.

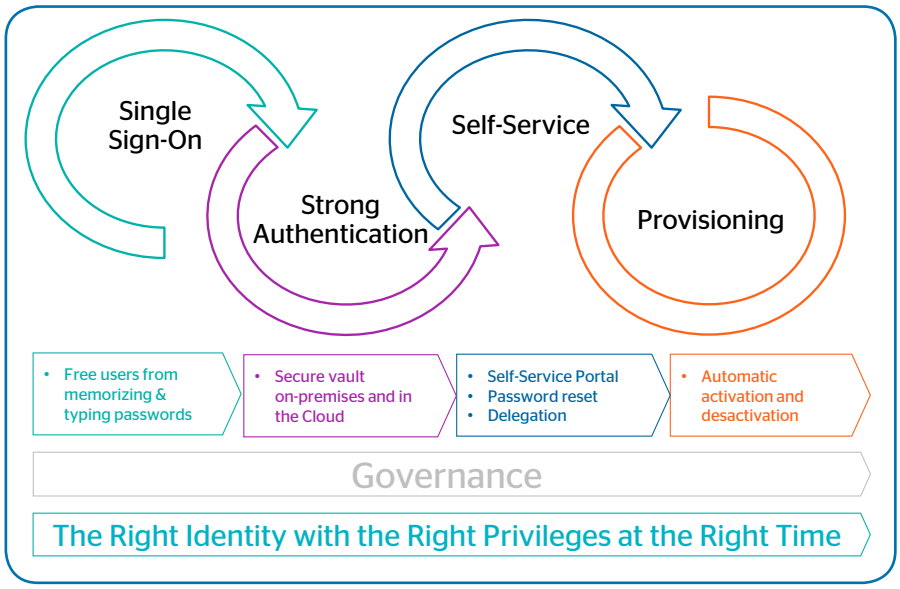
Advanced Reporting Module

Evidian Authentication Manager embeds a reporting module allowing dashboard generation on key indicators such as: activity, snapshot, risk, surveillance and KPIs. Reports can be downloaded by authorized users.

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
- Evidian Identity & Access Manager allows authorization governance and a full lifecycle management of identities and access to services, driven by a security policy combined with approval workflows.



www.evidian.com

CT_170504_LPM_F-Authentication_manager_en1