Evidian

Web Access Manager

A cornerstone of trustworthy Web accesses

By offering a coherent infrastructure that secures your Web applications, Evidian Web Access Manager makes your organization's security policy more consistent, reduces management costs and accelerates your e-business activities.

Simplify and reinforce access to your applications

With Evidian Web Access Manager, you can easily manage the security of your Web applications from a single control point. Evidian Web Access Manager not only reinforces security thanks to strong authentication, multi-factor authentication and fine-grained access control, but it also increases user productivity with its customization and Single Sign-On (SSO) features. Evidian Web Access Manager provides proof of Authentication and enables access to Cloud applications (Office365™, GoogleApps™, SalesForce™, ...).

SSO for Web applications and dynamic authorization

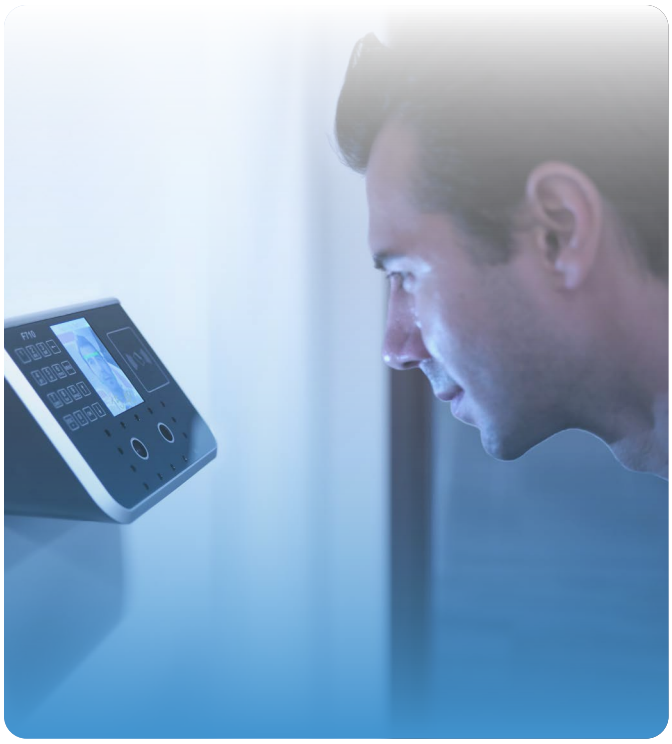
Once the user is connected to Evidian Web Access Manager, connections to multiple websites or applications are transparent. Passwords and authorizations are dynamically provided by Evidian Web Access Manager for each application. Single Sign-On eliminates user frustration inherent to multiple logins or password changes, and thus increases user productivity.

Centralized Web access control & strong authentication

Evidian Web Access Manager protects your organization's critical Web applications, by controlling who has access to what. Thanks to an integrated reverse-proxy, it authenticates users centrally using either a single password, an integrated Windows Authentication; a token, RADIUS, X.509 certificates, a smartcard, or a soft-OTP generated and communicated to the user via SMS, email, Grid card or QRentry™, as well as the new Fido 2 standard. Once identified, users have access only to those resources for which they have access rights, according to their specific profiles. Evidian Web Access Manager enables you to chain authentication policies and build your multi-level and multi-factor authentications.

Evidian QRentry™

With Evidian QRentry™, your users authenticate with a QR Code™ and their smartphone. The QRentry™ solution allows a multi-factor authentication to a Web portal based on QR Codes from a browser on private or public tablets or computers (BYOD, non-managed devices ...).



BYOD and non-managed device accesses

With Web Access Manager, multi-factor authentication and Single Sign-On are extended to non-managed devices. This spares you from installing agents on devices and exposing application passwords outside your internal network. Furthermore, it enables PCs, tablets and smartphones to access Cloud applications using identity federation standards.

SAML-based multi-domain management

Evidian Web Access Manager allows distributed communities to interoperate and use a separate administration for different security domains. Using SAML accreditations generated in real time by the user's domain, each entity can dynamically authorize users of a trusted domain to access its services. This approach also enables to manage accesses to the SaaS providers. Users may be federated or auto-provisioned between trusted domains. It supports SAML-based multi-domain management, as well as social authentication: the keys to manage and control the access of partner or client distributed communities.

Atos

Multi-factor authentication and Web access management for the business

Customized user environment

When a user is authenticated and managed by Evidian Web Access Manager, they access a single page interface from which they can navigate through different integrated solutions. A customized navigation menu is dynamically generated to display the right Web resources for their profile.

This customization feature is provided as standard with Evidian Web Access Manager, or can be integrated with any third-party portal software.

Advanced access management and self-service

You can use a single console to manage access rights in your company, interfaced with LDAP directories. Users can thus benefit from the self- service feature, which includes self-registration, social authentication and registration (OAuth, OpenID Connect), password and profile management.

Quick deployment

You can publish your Web applications easier, quicker and with more reliability and thus improve your overall competitiveness. Evidian Web Access Manager can be used immediately without any additional components and without modifying your applications.

Simplified architecture

Evidian Web Access Manager does not require any modification of your existing Web services, or any plug-in on the browser side. It supports an intelligent reverse-proxy-based architecture. Not only does this architecture minimize the impact on your operating costs, but it also gives you full control of the entire extended company. You can manage a unified access to your own applications even for your external partners or service providers.

Load balancing and high availability

Evidian Web Access Manager's servers are based on efficient high-availability and loadbalancing mechanisms. As a result, they can increase their load to support several millions of users.

Integrated and centralized administration

Interfaced directly with LDAP directories, Evidian Web Access Manager supports authentication against multiple user directories, offering full, role-based access management, with secure account-sharing.

It offers extended audit and log tools that alert security managers on any risks and registers all the accesses. Every user and every administrator activity is monitored and audited.

Centralized audit & reporting

Evidian Web Access Manager can archive alerts regarding the activity of Web Single Sign-On in a single location. This is useful when analyzing security alerts and performing audits. Moreover, when Identity & Access Manager is installed, Evidian Web Access Manager's audit events are archived alongside identity and policy management alerts. This enhances analysis and audit features.

Ensure that your information system is compliant with laws and regulations such as Sarbanes-Oxley, decrees on medical confidentiality, PCI DSS or laws on financial integrity. It will help you comply with your legal and regulatory requirements. You can monitor your user's attempts to access applications; this enables you to demonstrate that your access policy fulfills its objectives. Identity & Access manager embeds a reporting module allowing dashboard generation on key indicators. Reports can be uploaded to authorized users.

Integration with Evidian's I&AM Solutions

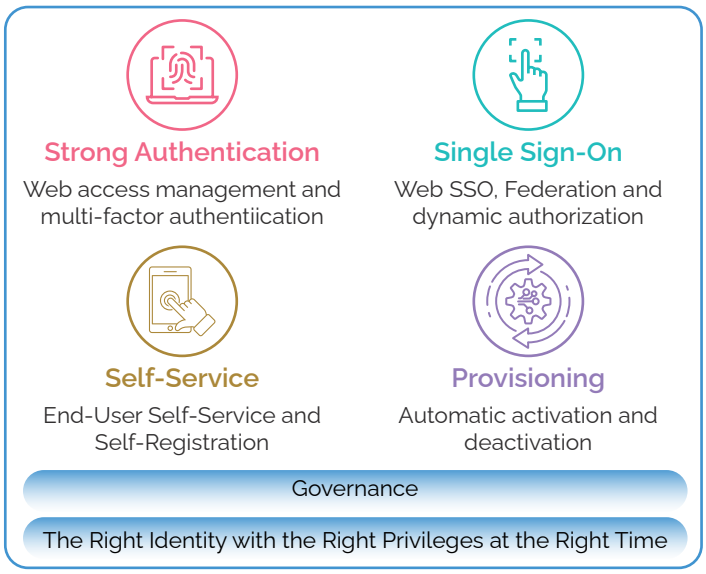
Evidian Web Access Manager is part of Evidian's Identity and Access Management solution.

- With provisioning, you stop distributing passwords to users. Application accounts are automatically synchronized with WAM
- Policy management enables you to determine the actual accounts usage; you can eliminate dormant and obsolete accounts
- 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.

A prerequisite for GDPR*

Identity and Access Management is one element among a range of technical counter-measures to mitigate risks related to data protection. In addition to its access control, strong authentication and identity governance, the Evidian Suite takes into account the requirements for Users' Rights in all its products' roadmaps. Notifications, dedicated personal data reports and self-service functionalities allow users to exercise their rights freely and enable GDPR compliant processes.

* General Data Protection Regulation



For more information: evidian.com

CT-220426-JS-FS-Evidian-Web Access Manager