evidian

Self-Service password reset

Bull
atos technologies

Because one security measure doesn't fit all situations

One help desk call for a password reset costs around 15 euros and is time-consuming (about 20 minutes). Three to four password resets are performed per employee and year (According to the Gartner Research - Note T-15-6454). A self-service password reset reduces this cost and frees up your IT.

Evidian Self-Service Password Reset offers several different authentication methods. From a web portal or from their workstation, users can securely reset their Windows passwords without having to contact the helpdesk. Evidian Self-Service Password Reset is also available in offline mode.

Evidian Self-Service Password Reset (SSPR) identifies the user with different means: Questions and Answers, Scan of a QR Code, Confirmation code sent via email or SMS, Push notification on mobile and subsequently executes the reset of a new password or generates a temporary password (TPA).

Evidian Self-Service Password Reset features enable users to change their Windows password securely (network login, Windows login), connected or not connected to the network. The solution provides a large range of authentication methods and full audit trails to demonstrate the implementation of the password policy.

Evidian Self-Service password reset

Evidian primary password management features manage the expiration and the reset of the Windows password according to the password policy.

Notification mails are sent before password expiration to help the user manage his Windows password and when the Windows password is changed.

A large range of Self-Service Password Reset authentication methods:

- Answering pre-defined questions with or without an available network and without contacting of the help desk.
- Scanning a QR Code with Evidian QRentry App with or without an available network and without the help desk (no network connectivity is required from the mobile).
- Using a one-time password sent via email without involving the help desk (network required).
- Using a one-time password sent via SMS without involving the help desk (network required).
- Validating a notification received on the user's mobile without involving the help desk (network required).
- Using a challenge response mechanism when the reset password is used.

Strong password policy enforcement with Evidian Self Service Password Reset

Evidian SSPR can enforce a strong password policy for the network login. You can define the network login password format such as the type of characters as well as their position, the minimum and maximum number of characters, etc...

This policy can be different regarding who is resetting the Windows password.

Full audit trail of network login access and password change with Evidian Self Service Password Reset

The solution provides a full audit trail of WHO has access to WHAT, WHEN and from WHERE. Reports can be generated based on these audit trails.

These reports can help demonstrate that your password change policy is effectively implemented. They can also be used to prove the return on investment.

Reporting features can also be used to detect accounts which the Windows password has not been changed for a while (risky/useless Windows account).

Use your company's existing LDAP/Active Directory infrastructure

Evidian SSPR relies on your existing Active Directory. Thus, you do not need to synchronize identities, once installed all employees can benefit from the SSPR feature. All the Evidian security data is encrypted and stored in your company directory: Active Directory or AD LDS.

From the login screen and a web portal

Evidian Self-Service Windows password reset is available from a web portal and from the login screen of the user's workstation.

The solution is easy to deploy and is compatible with managed services.

It fits perfectly into digital workplaces with a large range of terminals as well as on VDI infrastructure (Citrix XenApp, Windows RDS and VMware).

Identity proofing

Questions & Answers mechanism can also be used to identify the user.

From the web portal, users can generate a one-time code that can be verified by an administrator.

By enabling One-Time Password verifications via mobile, SMS and e-mail for identity verification, organizations are able to increase end-user adoption rates of Self-Service Password Reset up to 98%.

3 reasons to manage passwords with Evidian Self-Service Password Reset:

1. Free your IT from "Password reset" time cost
2. Fully integrated to your Microsoft environment, with an intuitive user interface
3. Facilitate your multi-factor authentication deployment by offering a user-friendly fallback.

Evidian Enterprise SSO (E-SSO) main features

Identity proofing

A non-intrusive solution

You will not need to modify any of your applications. Evidian Enterprise SSO activates single sign-on in many types of applications: Windows, web, terminal emulator, etc.

A universal solution

Evidian Enterprise SSO can be run from Windows, Mac OS, Android, iOS, on smartphone, tablet, server, virtual environment such as Citrix, Vmware or Microsoft, from standard and thin client. Password vault, credentials, personal notes and single sign-on are always secure and available for the user and from any terminal.

Password-free access to your mobile applications

With Evidian Enterprise SSO for Mobile device, Evidian delivers an Android SSO and iOS SSO solution that extends its Enterprise Single Sign-On offer. Enterprise SSO for mobile devices automatically enters application passwords for you, stores securely personal notes and passwords in your mobile password vault, this information is securely stored on-premises or in a Cloud and is available from your workstation and your mobile devices.

Turn your mobile device into a strong authentication device

When you activate your mobile device with a QR Code, it becomes a secure access point to your enterprise network. The authentication on your mobile device grants you a secure access to your applications.

Easy deployment in your existing infrastructure

Evidian Enterprise SSO collects user passwords so they do not need to be redefined. It can also be associated with an existing provisioning system. You can start with only one department and then deploy SSO later on thousands of devices. Evidian Enterprise SSO is based on an LDAP, Active Directory or AD LDS directory. No additional hardware is required.

Eliminate use of passwords for remote users.

Users, either internal or external, often have remote access to applications running in virtualized environment. Evidian Enterprise SSO frees these users from memorizing and typing passwords for these virtualized applications. For instance Evidian Enterprise SSO is certified Citrix-Ready. Several other solutions have been certified too, you can find them on the Evidian Web site.

Convergence with remote accesses for BYODs and non- managed devices

With Web Access Manager, Single Sign-On is extended to non-managed devices. This spares you from installing agents on devices and exposing application passwords outside your internal network. Furthermore, it enables PC, tablet, smartphone accessing Cloud applications using identity federation through standard protocols such as OAUTH, OpenID Connect, SAMLv2.

Strong authentication

Evidian Authentication Manager reinforces and manages strong authentication for Windows with smartcards or cryptographic USB tokens, hard or soft OTP, biometrics, RFID badges, smartphone with QRentry, etc.

Self-service Password Reset

A Self-Service Password request (SSPR) function allows users who have forgotten their Windows password, or their access card, to unlock their accesses - even offline, with or without contacting the helpdesk.

Emergency Access for the Windows session

With Self-Service Password Request, users can unlock their access themselves with an emergency procedure, available online and offline, in self-service mode.

Business-oriented functions

With Evidian Authentication Manager, sales teams and branch office employees can share a kiosk PC. They can switch to their own environment in a matter of seconds, without having to close then open a Windows session.

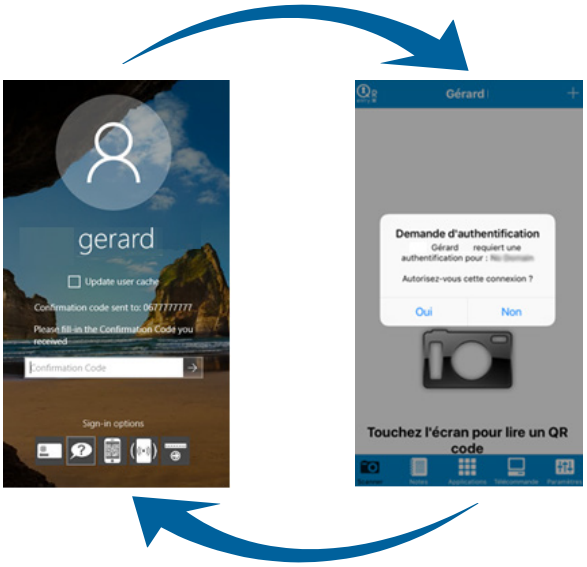
When doctors make rounds in a hospital their session moves with them. They access it by tapping their radio badge or presenting a smart card.

Traders in front office or back office working with a cluster of PCs can with a single authentication, they can lock, unlock, and delegate that cluster – fully or partially, permanently or temporarily.

Ensure that your information system is compliant with your policy and regulations

You can monitor your employees' attempts to access applications and PCs. All accesses will be audited by name, including accesses to Windows accounts and generic applications. This will enable you to demonstrate that your access policy is observed and fulfills its objectives.

Evidian Enterprise SSO embeds a reporting module allowing dashboard generation on key indicators such as: activity, snapshot, risk, surveillance and KPIs. Reports can be uploaded to authorized users.



About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
ascent.atos.net

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.

Bull is the European leader in HPC and its products include Bull sequana, the open exascale-class supercomputers; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; Trustway, the hardware security module and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information, **visit bull.com**

IMPRIM'VERT
This brochure is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001).

CT_171010_LPM_F-SSPR_and_password_management_en1

Trusted partner for your **Digital Journey**

Atos