Systancia Access

Access Management (AM) and Authentication

Your concerns are our concerns

As a **CISO** you must meet increasing **regulatory compliance** obligations (PGSSI-S, privacy decree...). You must manage the **traceability** of access to information systems and avoid any identity **theft** or access to confidential information.

As a **CIO**, you must increase the **security level** of your information system and strengthen access to the various physical or application resources with no impact on their productivity. You need to **simplify** user self-help procedures and **reduce the cost** of managing associated incidents.

As an **End-user representative**, you need to ensure that the security solutions provided are **user-friendly** and improve access to the IS while remaining **as transparent as possible, without compromising users' productivity.**

The continuous increase of your application assets and of the number of users in your information system makes it more difficult to ensure the respect of a **strong** and **easy to implement password management policy.** It is important to provide solutions that can cover your entire application park, leaving no application behind.

Phone: +33 (0)**3 89 33 58 20**
www.**systancia**.com

Systancia Access: Transparent authentication, in all its forms, to all your applications, on premise or cloud

Systancia Access is an access management (AM) and authentication solution. It is designed to secure IS access and single sign-on mechanisms. Its various modules meet specific needs and allow for a progressive implementation, while capitalizing on the initial infrastructure.

The combination of different modules provides different features:

Centralized and secure password management

- Create a centralized and secure password repository.
- Check the compliance of the user's password with the company's security policy.
- Strengthen password security by automating password lifecycle management (creation, renewal).

Single sign-on

- Provide transparent and secure access to users accessing local or published applications from nominative workstations, kiosks, published environments or workstations outside the domain.
- Federate the authentication of applications supporting SAML.
- Support tools for application enrolment (ESSO, Web SSO) covering a wide range of use cases.

Strong primary authentication

- Perform a strong authentication of users during the primary connection (Windows login) via different medias such as cards with certificates (CPS, IASECC), contactless cards (Mifare Classic, Mifare Desfire EV1/EV2), One Time Passwords (OTP) or via push notifications (Out of Band).

Continuity of service for mobile users

- Guarantee the continuity of service for mobile users accessing applications from controlled or uncontrolled workstations.
- Provide users with a mobile application allowing them to benefit from SSO features and generate OTPs or receive push notifications for login or access to applications.
- Allow users who forgot their Windows password to continue accessing their email from mobile devices (smartphone/tablet).

Self-service

- Provide tools that will offer users a controlled autonomy to unlock their authentication media (password, card).

Audit and reporting

- Benefit from audit features and continuous access traceability in compliance with regulations.

Systancia Access

Access Management (AM) and Authentication

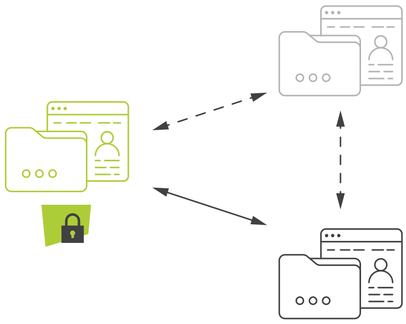
Why you should choose Systancia Access?

- Guarantee a natural integration of our solution into your infrastructure without disrupting the way your information system works.
- Benefit from a solution that has proven itself in our client environments with a small or large number of users without any impact on access or user productivity.
- Provide a strong configuration tool capable of integrating all applications regardless of their architecture and without requiring any adaptation of them.
- Guarantee full mobility for employees by providing an SSO solution for any type of terminal (controlled or uncontrolled workstation, computer, smartphone or tablet) or any application (eSSO, Web SSO, Federation, mobile SSO).
- Reduce user support costs with self-service unlocking. The self-service features provided allow users to access their session or unlock their authentication media autonomously, in connected or disconnected mode.

A deployment offer adapted to your needs

Systancia Access

Software product with a simple and fast deployment:



ADLDS directory independent from the Enterprise directory which will store product and user information (vaults and configurations)

Mandatory approval relationship between the different directories for multi-entities

Part of the service is hosted by Systancia for the push notification authentication feature (Out of Band)

"Systancia Access allowed us to carry out our project, to simplify access and define a stronger password policy. It was a success in relation to the initial challenges! "

M. Ernest Sossavi
Architecture and security manager

SEINE & MARNE 77 LE DÉPARTEMENT

Deployed in a third of French university hospitals, Systancia Access is the most widely used access management and authentication solution in the French hospital sector.

AGENCE DU NUMÉRIQUE EN SANTÉ — AXEL — IDEMIA — Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE Agence Nationale des Titres Sécurisés

Systancia Access perfectly integrates with other solutions on the market to manage strong user authentication