

제로트러스트를 위한 통합 ID 및 접근제어 솔루션

복잡한 계정·인증·권한 관리를 AutoPassword Access Manager로 한 번에 해결하세요!

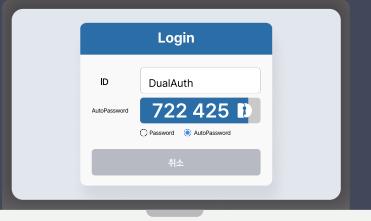


업무 시스템마다 다른 사용자 계정, 상이한 인증 수단, 단절된 권한 설정으로 인해 보안과 운영 관리에 어려움을 겪고 있습니까? AutoPassword Access Manager는 이러한 문제를 해결하기 위해 개발된 AutoPassword 기반의 통합 ID 및 접근 관리 솔루션입니다. 이메일·그룹웨어 등 웹 애플리케이션 뿐 아니라, Windows PC, Linux 서버, 무선 네트워크 까지 한 번에 관리할 수 있으며, 중앙에서 계정·인증·접근 관리 정책을 통합적으로 설정하고 운영할 수 있습니다.



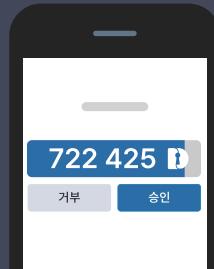
AutoPassword Access Manager 특징

생체인증 센서가 없는 PC나 서버에서 대역외 생체인증



PC나 서버의
자동패스워드를 확인

스마트폰 생체인증으로
사용자를 확인



- 생체인증 센서가 없는 PC나 서버에서 스마트폰 생체인증을 대역외로 사용할 수 있는 국제표준 기술(X.1280)
- PC나 서버가 자동패스워드를 사용자에게 제출하면 사용자가 스마트폰 앱에서 자동패스워드를 확인
- 사용자가 자동패스워드를 승인할 때 스마트폰의 생체인증으로 사용자를 확인하고 PC나 서버에 로그인

사용자 로그인 시점마다 자동으로 OS의 암호를 변경



Windows 또는
Linux 로그인



OS 패스워드
자동 갱신



- AutoPassword Access Manager로 사용자가 윈도우즈나 리눅스에 로그인할 때마다 자동으로 기존의 OS 패스워드를 변경
- AutoPassword Access Manager가 보안 규정에 맞게 PC나 서버 내부의 사용자 패스워드를 복잡한 값으로 자동 갱신
- 관리자의 설정에 따라 사용자별 접근 가능한 PC와 서버 설정

스마트폰을 분실했거나 네트워크가 안 되는 상황을 대비한 다양한 인증 방식 지원

AutoPassword

SelfPassword

AAM 패스워드

당일 임시 패스워드

FIDO 지문인증기

카드 OTP

모바일 OTP

오프라인 OTP

■ 사용자가 스마트폰을 분실한 경우에도 항상 PC에 로그인 할 수 있도록 다양한 대체 인증 수단을 지원 (AutoPassword, FIDO 지문인증기, 카드 OTP, 모바일 OTP, 오프라인 OTP, SelfPassword, AAM 패스워드, 당일 임시 패스워드 등)

■ PC의 네트워크가 지원되지 않는 상황에서도 PC에 로그온 할 수 있도록 오프라인 OTP 기반 윈도우 로그온을 지원

■ 관리자가 사용자의 인증 수단을 직접 변경할 수도 있으며, 사용자가 인증 수단 변경을 요청하고 관리자가 승인할 수도 있음