DualAuth

Integrated Identity and Access Control for Zero Trust

AutoPassword Access Manager Product Introduction

DualAuth

01 Product Overview	**02** Key Features
03 References	**04** Contact

<div style="text-align:center">

**Integrated ID and Access Management Technology**

</div>

AutoPassword Access Manager, an integrated ID and access management solution, is an access control technology that not only manages integrated accounts for web applications such as email and groupware, but also encompasses business Windows PCs, Linux servers, and wireless networks to establish account issuance and access policies.
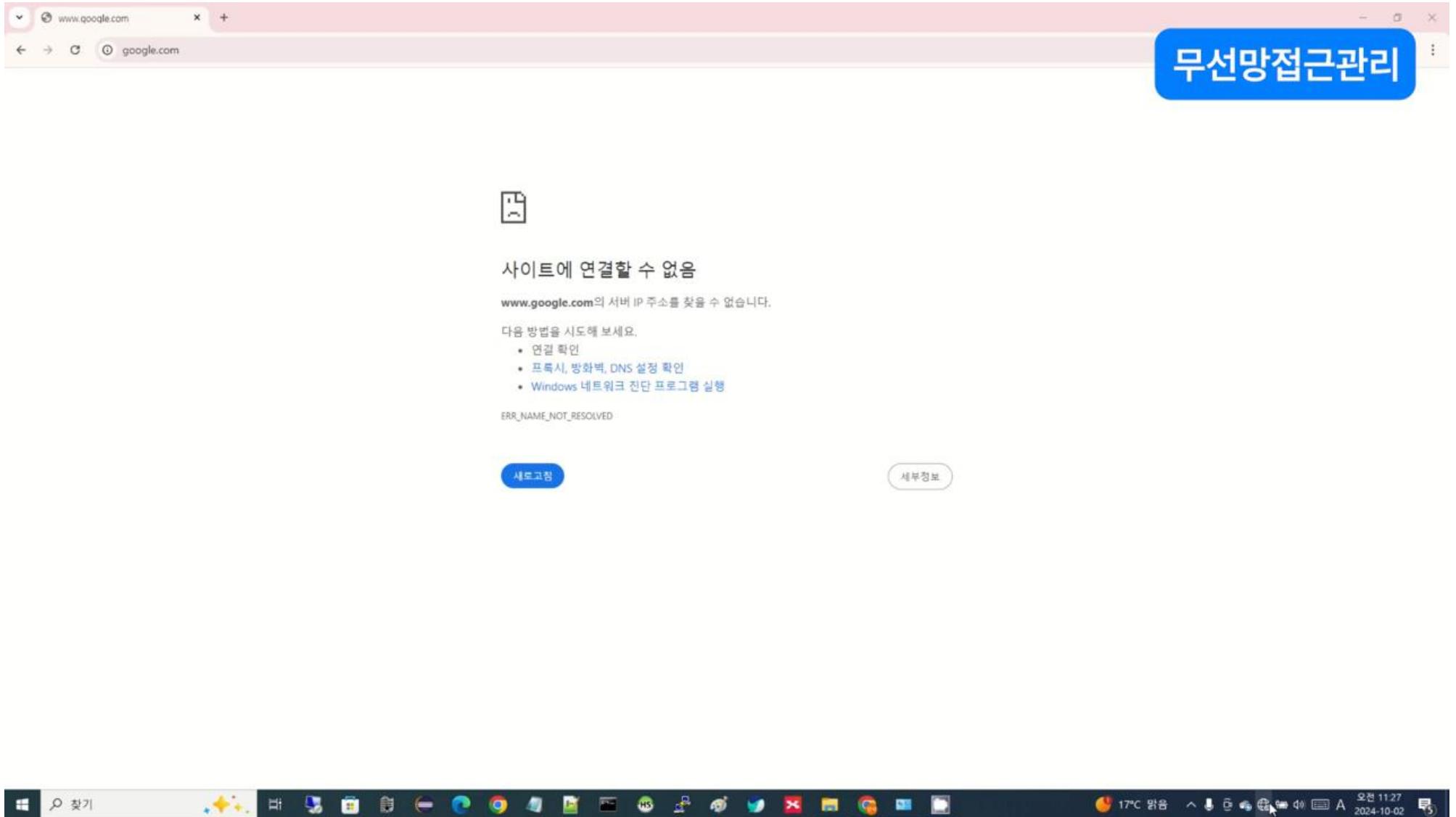
https://youtu.be/l5H1C9gz7tg

https://youtu.be/cjmjBDwgw00
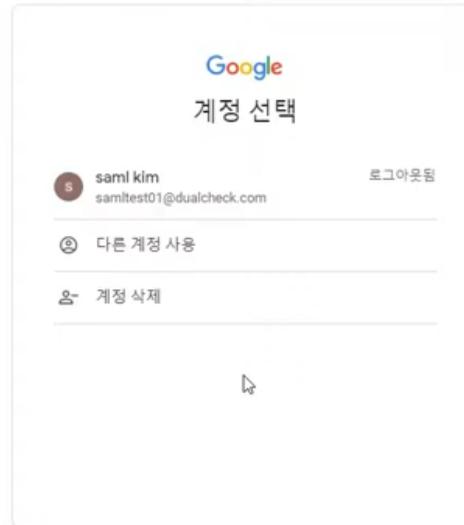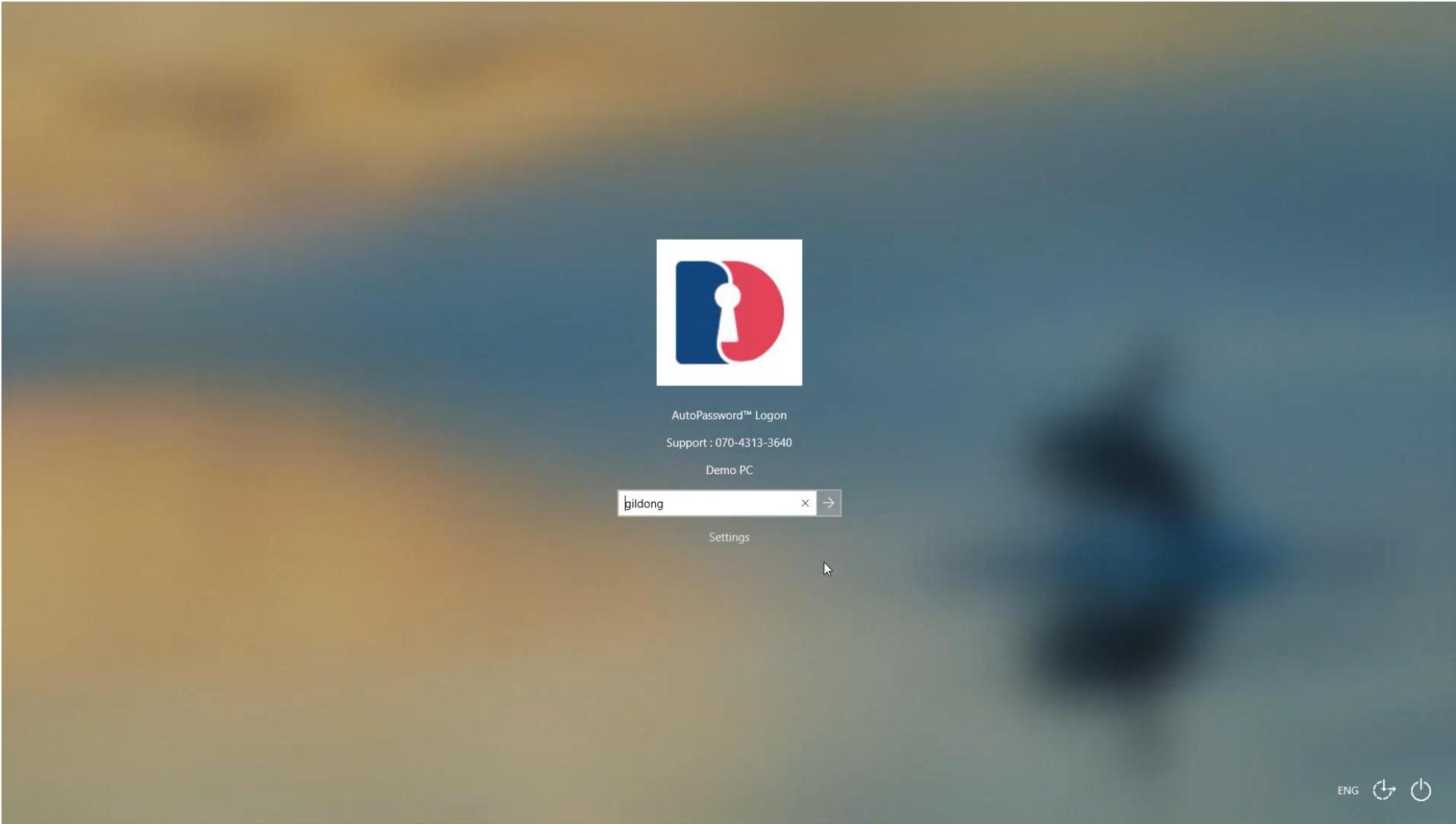
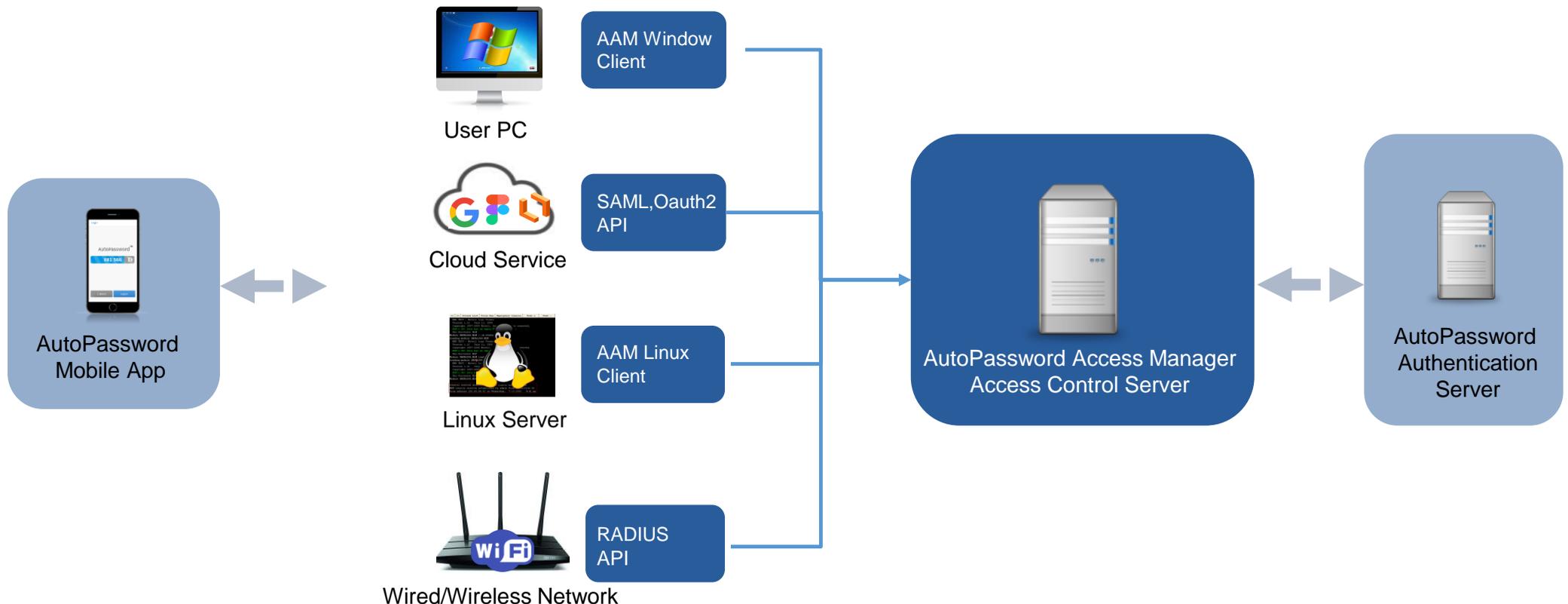**https://youtu.be/SMnv_WHhNe4**

https://youtu.be/FDt0i06otUI
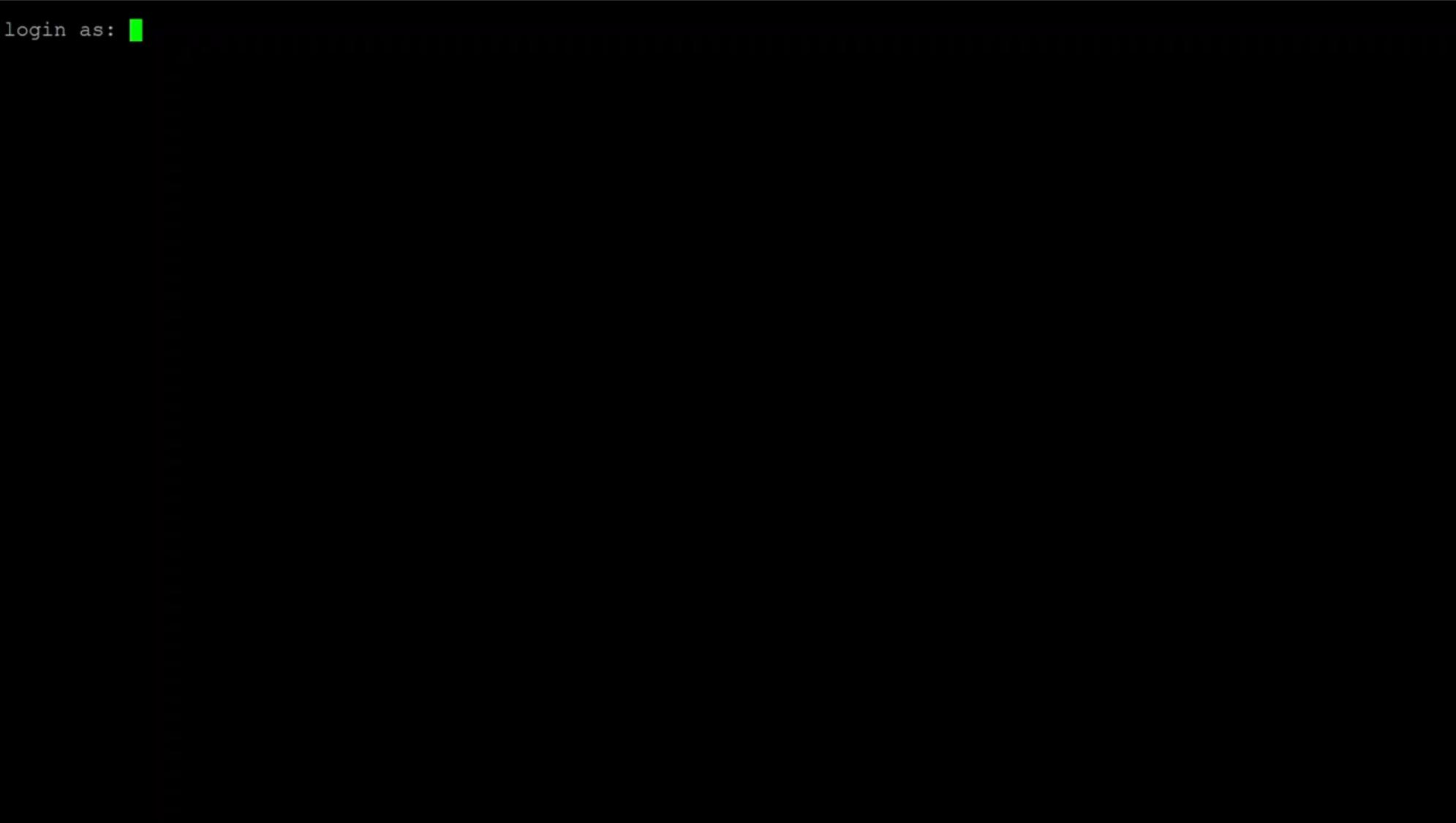
AutoPassword Access Manager Architecture

To switch to AutoPassword Access Manager, all you need is to install the Access Manager server and client on your existing business system and add the AutoPassword authentication server and mobile app. This process enables a secure and convenient authentication environment without significantly changing the existing system structure.

The administrator first installs the Access Manager server, then installs the client program or integrates the API to enable communication between the business system and the server. Additionally, Access Manager supports standard authentication protocols such as SAML, OAuth2, and OpenID Connect, allowing easy integration with various cloud services.

AutoPassword Mobile App

User PC — AAM Window Client

Cloud Service — SAML,Oauth2 API

Linux Server — AAM Linux Client

Wired/Wireless Network — RADIUS API

AutoPassword Access Manager Access Control Server

AutoPassword Authentication Server

DualAuth

01

Product Overview

02

Key Features

03

References

04

Contact

02 Key Features

Feature 1 – Log in to all business systems with a single integrated ID and manage usage history

AutoPassword Access Manager provides an integrated environment in which users can access various business systems—such as PCs, email, cloud services, Linux servers, and wired/wireless networks—with a single ID and authentication method. To achieve this, it integrates with various account management and authentication methods, including Windows AD accounts, local accounts, 802.1X/RADIUS-based wireless networks, SAML, OAuth2, Open ID Connect, and Linux PAM. Administrators can flexibly configure access policies for each user or organization and systematically manage usage history through a single management console.

Log in to all business systems with a single integrated ID and AutoPassword
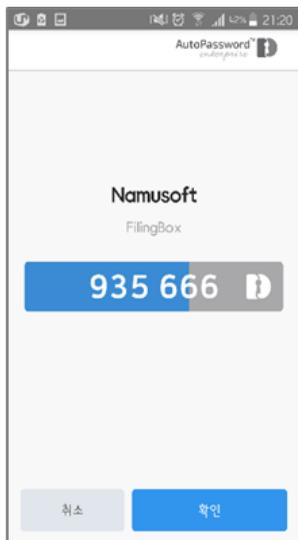
View login history of business systems by integrated ID

Feature 2 – Support for various authentication methods including AutoPassword

AutoPassword Access Manager provides AutoPassword as the default authentication method, enabling out-of-band biometric authentication even on devices without biometric sensors. With this, users can securely log in to business cloud services or Linux servers by verifying the auto password presented by the business system on their smartphone, without manually entering authentication values. In addition, to prepare for situations such as smartphone loss, it supports various alternative authentication methods including FIDO, OTP, one-day temporary passwords, and AAM passwords.

In addition to AutoPassword, supports OTP, FIDO fingerprint authenticators, one-day temporary passwords, etc. for use in case of smartphone loss.

Feature 3 – Integrated login for cloud services and business applications

AutoPassword Access Manager supports standard authentication protocols such as SAML, OAuth2, and OpenID Connect, enabling integrated login with AutoPassword for major cloud services and business web applications. More than 20 major cloud services, including Google Workspace, Figma, LucidChart, Dropbox, GitHub, and WordPress, are already connected, and additional business applications in operation can be integrated using standard protocols. With AutoPassword applied to standard authentication protocols, the most secure federated authentication becomes possible.
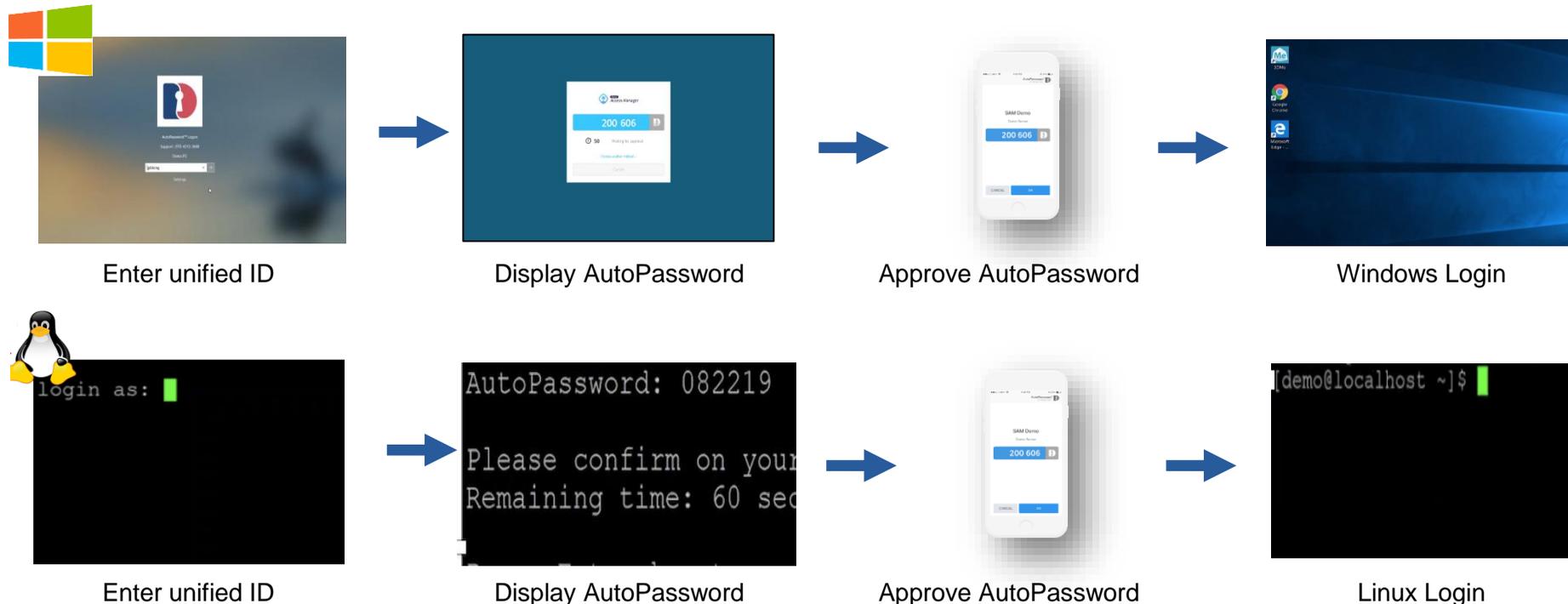
Login to various cloud services with a unified ID and AutoPassword
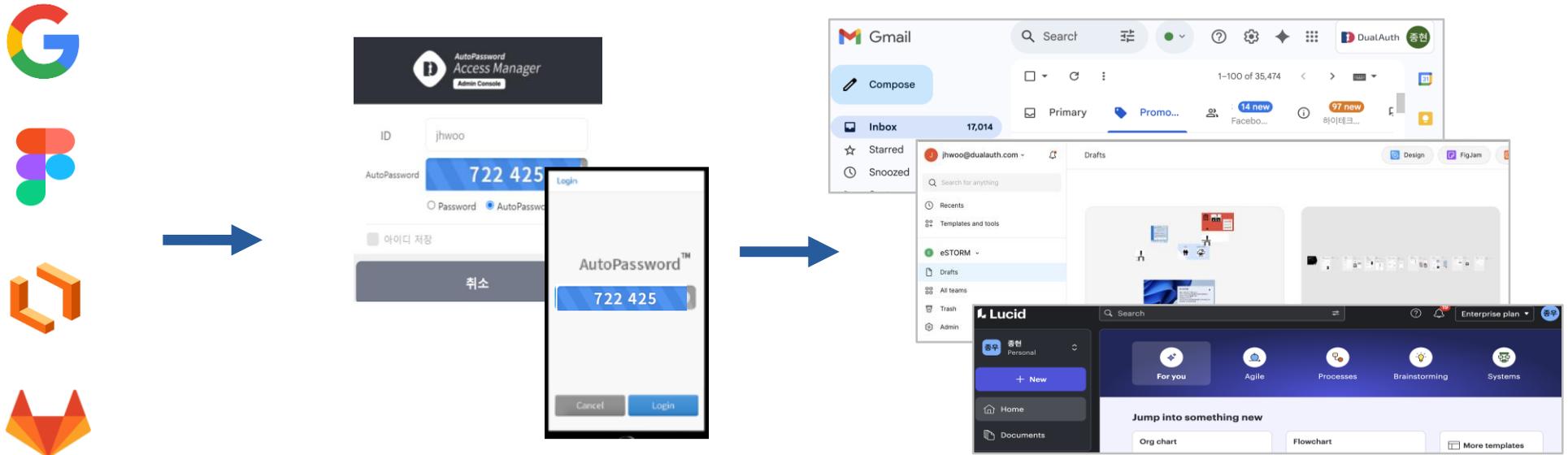
Feature 4 – Integrated login for Windows PCs and Linux servers

AutoPassword Access Manager supports login with AutoPassword on Windows PCs and Linux servers. Even on PCs or Linux servers without biometric sensors, users can securely verify access to PCs or Linux servers through out-of-band biometric authentication. Instead of entering passwords or other authentication values directly on work devices, users can log in by verifying the auto password presented by the Windows or Linux system on their smartphone, achieving both security and convenience. In addition, the operating system password is automatically updated each time the user logs in, freeing them from password change management. (For Windows, both Local Account and AD Account are supported.)

Login to Windows PCs and Linux terminals with AutoPassword

Enter unified ID	Display AutoPassword	Approve AutoPassword	Windows Login

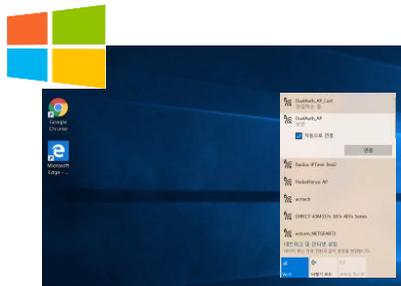| Enter unified ID	Display AutoPassword	Approve AutoPassword	Linux Login

13

Feature 5 – Unified Login for Wired and Wireless Networks

AutoPassword Access Manager supports logins on wired and wireless network devices using RADIUS authentication combined with the AutoPassword app. Normally, it is difficult to modify the authentication window for network access, but AAM solves this issue through its SelfPassword feature within the app.
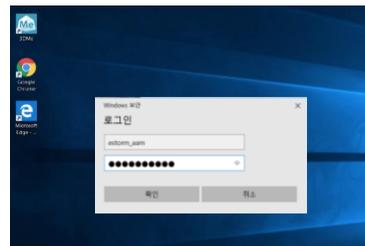
Users simply enter their unified ID in the ID field and any arbitrary SelfPassword in the password field. The same SelfPassword will then appear in the AutoPassword app on the user's smartphone. Once the user approves it through smartphone biometric authentication, the network connection is completed.

This allows users to connect securely to wired and wireless networks using their smartphone, even on PCs without biometric sensors and where the authentication window cannot be modified.

Login to wired/wireless networks where the authentication window cannot be modified using SelfPassword

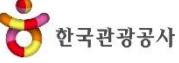| Select wireless network | Enter unified ID and SelfPassword | Approve SelfPassword in AutoPassword app | Connect to wireless network |

DualAuth

|	
01 Product Overview	**02** Key Features
03 References	**04** Contact

03 References

KB 국민은행	KB Kookmin Bank - Establishing and applying a mutual authentication-based enhanced user authentication system through the Zero Trust Adoption Pilot Project
우리은행	Woori Bank - Passwordless PC access management and application access management for Woori Bank employees
유안타증권	Yuanta Securities - Passwordless PC access management and application access management for Yuanta Securities employees
통계청	National Library of Korea - Controlling login rights for statistical information viewing PCs installed in the library introduced by Statistics Korea
KORAIL	Korea Railroad Corporation - Implemented passwordless authentication to strengthen user terminal authentication security for the next-generation Nara Market System
KOMSA 한국해양교통안전공단	Korea Maritime Transportation Safety Authority - Enhanced user login security using passwordless authentication for external webmail login
한국관광공사	Korea Tourism Organization - Enhanced authentication security for managers and partners for system development operations in every corner of Korea
KIAT	Korea Advanced Institute of Industrial Technology - Introduced to internal work system for employees to control individual access to internal and external networks
구리시	Guri City Hall - Responding to security compliance through login security and automatic password change when accessing important servers
CW 건설근로자공제회	Construction Workers' Mutual Aid Society - Strengthened login security of server system to improve internal system operation

03 References

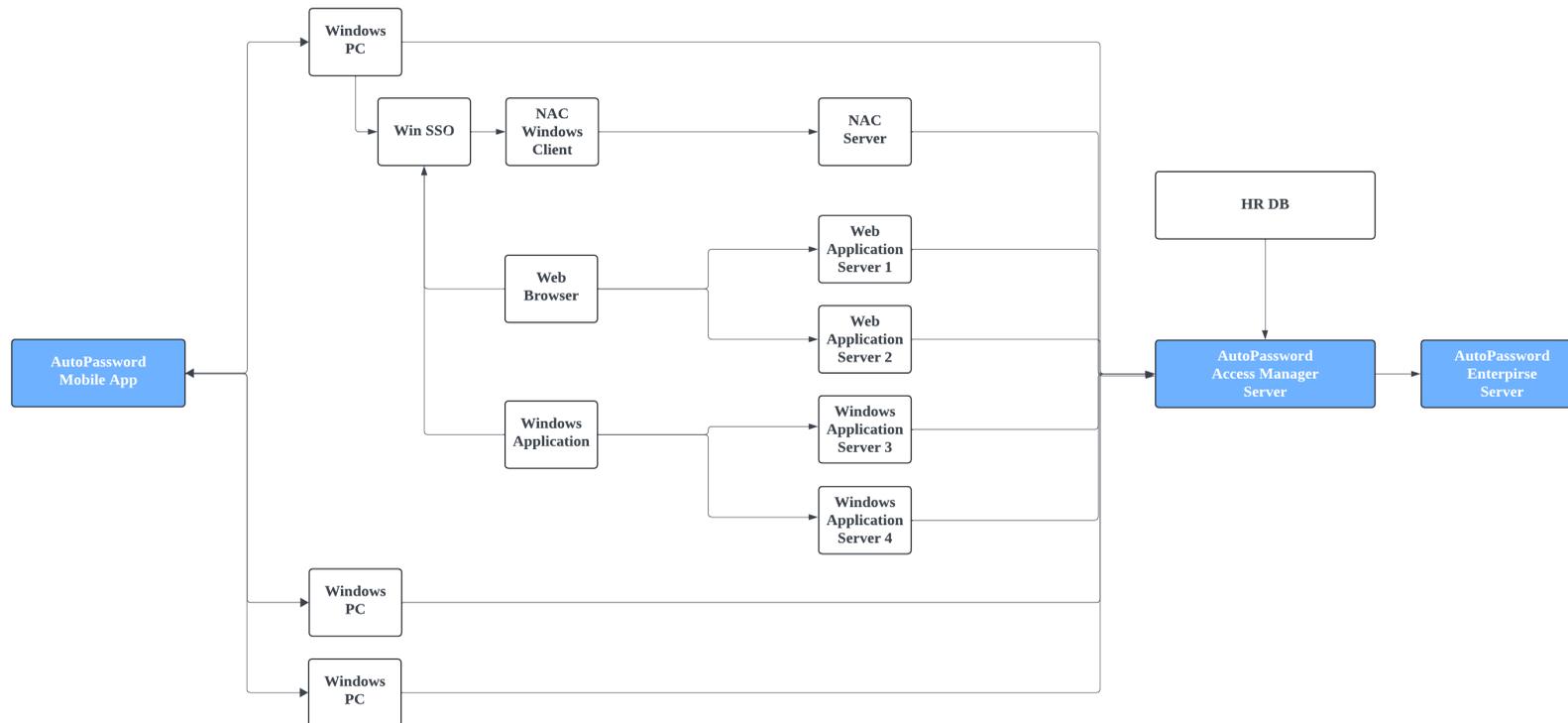## Case 1. Unified identity authentication and access control for employees

- **Background:** Solved the inconvenience of managing more than 3 IDs/PWs for employees' Windows PCs and 7 business applications, partially applied 2FA, and established an integrated authentication system and establish an integrated authentication system for management

- **Business scope:** 50,000 Windows PCs, existing SSO server, and more than 10 web applications

- **Effects**

  - Improved user convenience by reducing the complexity of authentication by integrating PW and 2FA for SSO of the web portal in use as a password service.

  - Established an integrated access management system for numerous Windows PCs deployed at various locations and business applications for each user
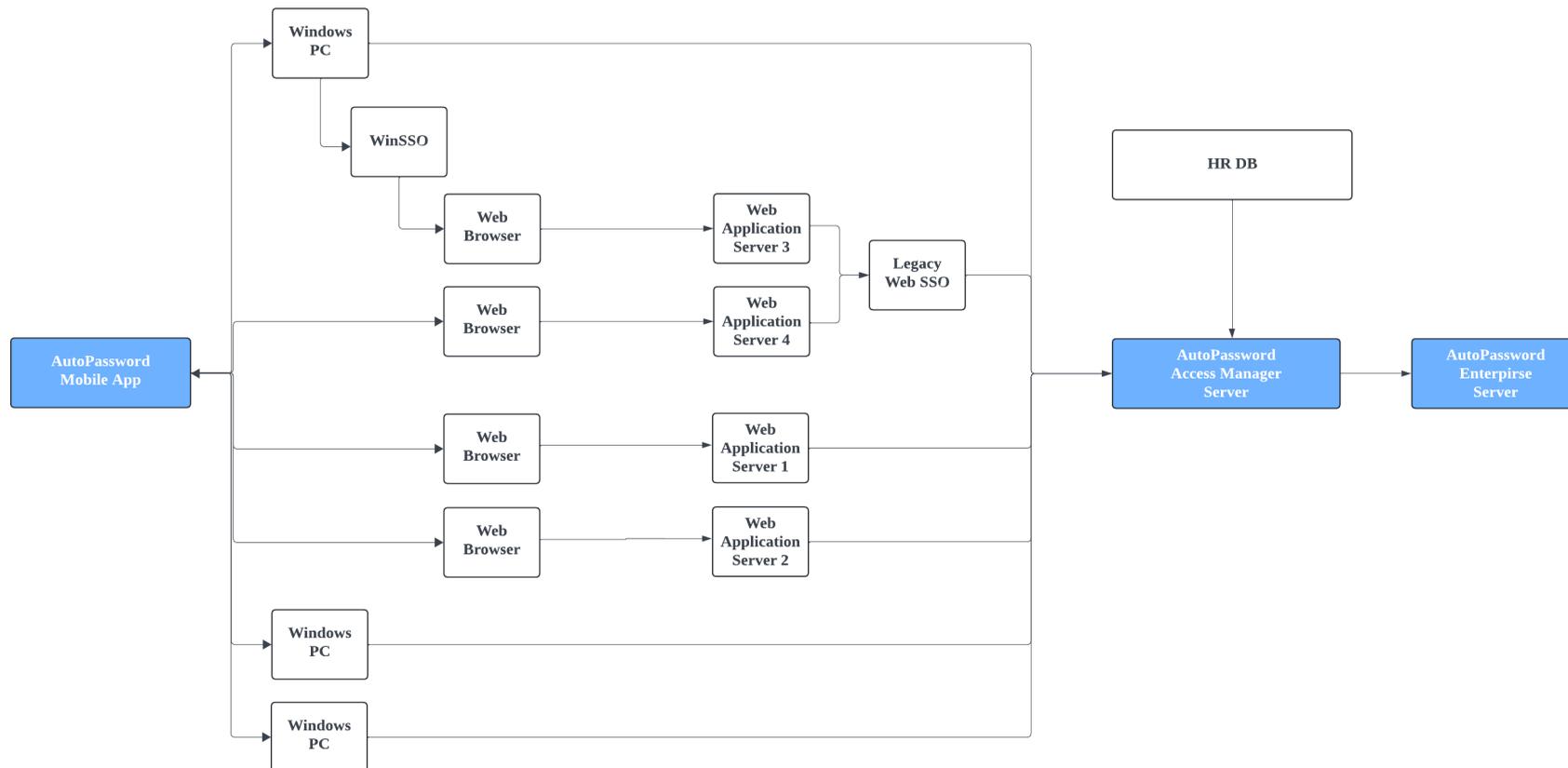
Case 2. Integrated ID authentication and access control management for employees

- **Background:** To solve the inconvenience of managing two or more IDs and PWs for Windows PCs and 10 business applications, it is necessary to improve the user authentication environment for PCs and business applications by switching to an integrated ID and passwordless authentication system.
- **Business scope:** 5,000 Windows PCs, wired network user authentication, around 10 Windows/web applications
- **Effect**
  - Improved accessibility of current users to Windows login and work applications through continuous authentication for NAC, work applications, and individual web applications within the effective time by establishing a continuous authentication system after Windows authentication.
  - Implemented a differentiated authentication process to distinguish security levels, requiring biometric authentication for initial access to the PC when entering the workplace and simple smartphone authentication when the screen is locked during work.

18

03 References

## Case 3. Integrated ID authentication and access control for employees

- **Background:** Solving the inconvenience of managing Windows PCs and two or more ID/PWs for employees and improving accessibility of PC use to the in-house wireless network authentication environment
- **Business scope:** Windows PCs, wireless network, existing Web SSO server, 10+ web applications
- **Effects**
  - Transitioned to a system that authenticates not only Windows PCs but also business applications at once with integrated ID and passwordless method.
  - Significantly improved the accessibility of users' laptop usage by continuously authenticating to the wireless network within the effective time through continuous authentication after Windows authentication.
  - Significantly improved the usability of existing PCs and web portal SSO by connecting the authentication method for existing web SSO in a passwordless manner.
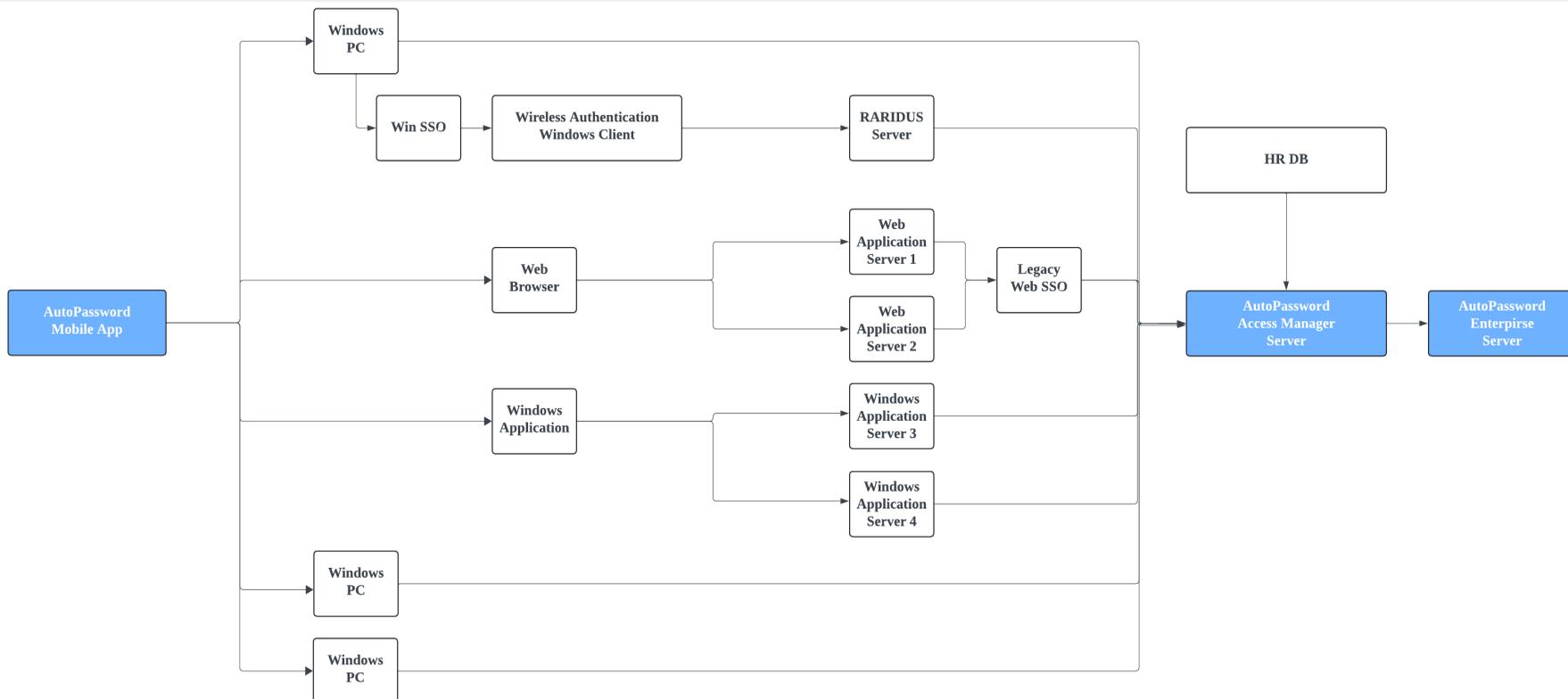
03 References

Case 4. Integrated Identity Authentication and Access Control for IT and Outsourcing

- **Background:** A small computer team needed to improve the efficiency of account and password management for dozens of servers.
- **Business scope:** OO Windows servers and OO Linux servers
- **Effect**
  - Established a systematic integrated account and access management environment for server system
  - Strengthened access control for outsourced personnel and improved work efficiency by switching authentication to passwordless for server access by outsourcing companies
  - Improved administrator work efficiency by automating password change management for OO Women's University servers under operational management

03 References
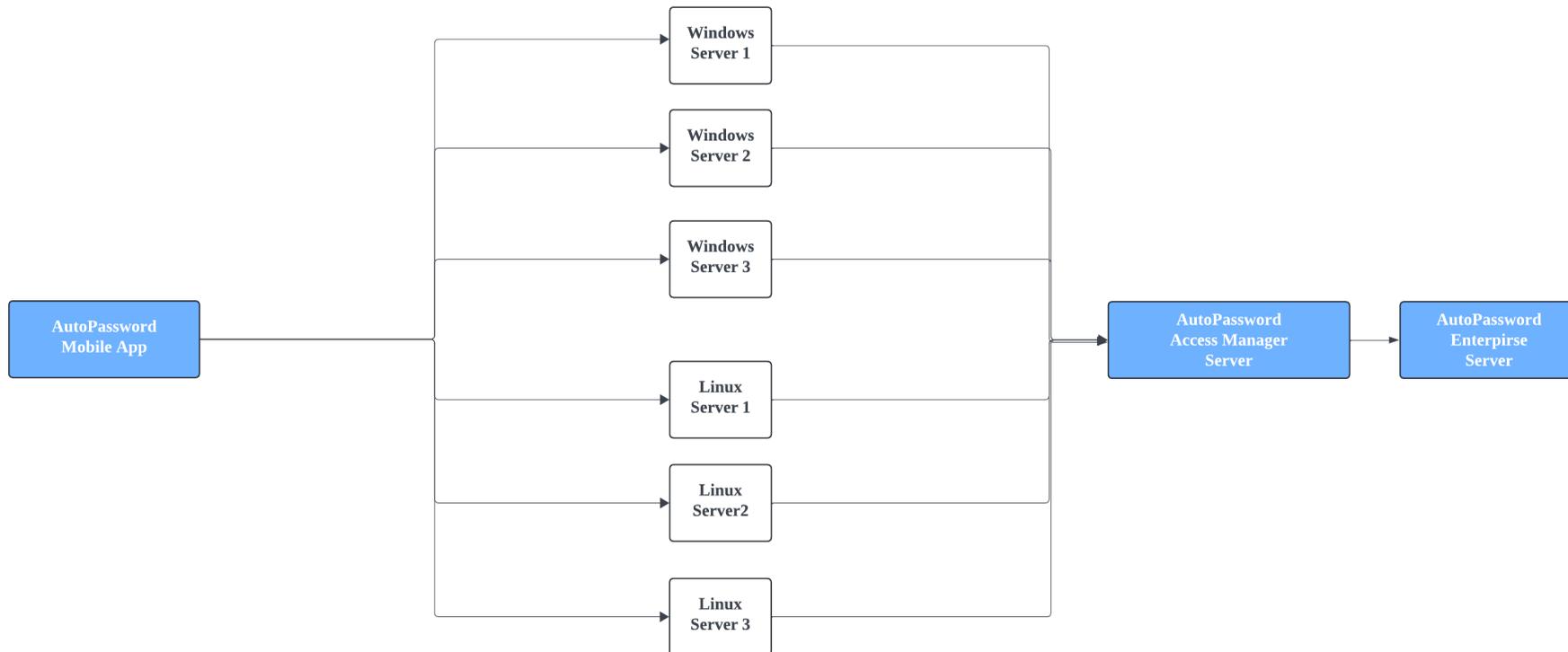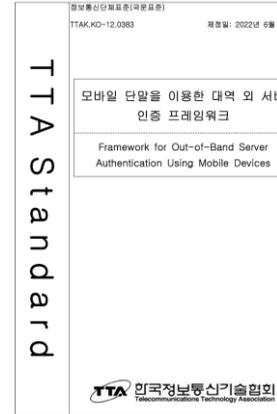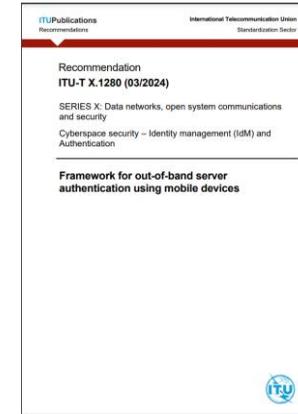
Awards

The Korea Internet Awards

The Commissioner's Award

Standard Technologies

TTAK.KO-12.0383

ITU X.1280

Presentations

FinovateFall 2016 Presenter

https://youtu.be/w2NtbPVaHSk

https://youtu.be/rBUK45fdBtY?t=838

FinovateFall 2018 Presenter

https://youtu.be/-DG-LYmRVfk

https://youtu.be/nF72E24BCec

Certificates

fido CERTIFIED UAF

GOOD Software

ISO/IEC 25023, 25051, 25041

oath — initiative for open authentication

IBM Security

DualAuth

01

Product Overview

02

Key Features

03

References

04

Contact

Specialists in passwordless identity and access management

DualAuth is a technology company providing passwordless identity authentication and access management solutions. Its primary solutions include passwordless authentication solutions, integrated ID and access management, mobile ID solutions, and physical facility access management. These technologies possess outstanding usability and security, as evidenced by their adoption as ITU standards X.1280 and X.oob-pacs under the UN's International Telecommunication Union. They are gaining attention as core technologies in the Zero Trust era. DualAuth is promoting its free Passwordless X1280 solution globally through the Passwordless Alliance based in Geneva, Switzerland, to solve password problems for B2C online services worldwide and advance ESG implementation.

Passwordless Identity Authentication and Access Management for Zero Trust Implementation

Passwordless Authentication Technology	Integrated ID and Access Management Technology	Mobile ID Technology	Physical Facility Access Management Technology

AutoOTP

AutoPassword

AutoPassword
Access Manager

AutoPassword
ID Card

AutoPassword
ID Card Reader

AutoPassword
ID Card

AutoPassword
IoT Controller

AutoPassword

DualAuth

- Company   :   DualAuth
- Website   :   www.dualauth.com
- General Inquiry :   support@dualauth.com

Request Implementation

- Address   :   130 Digtal-ro,Suite 1311,Gumchon-gu Seoul 08589
- Telephone   :   +82-2-6925-1305
- Business Inquiry :   sales@dualauth.com

DualAuth

Thank you