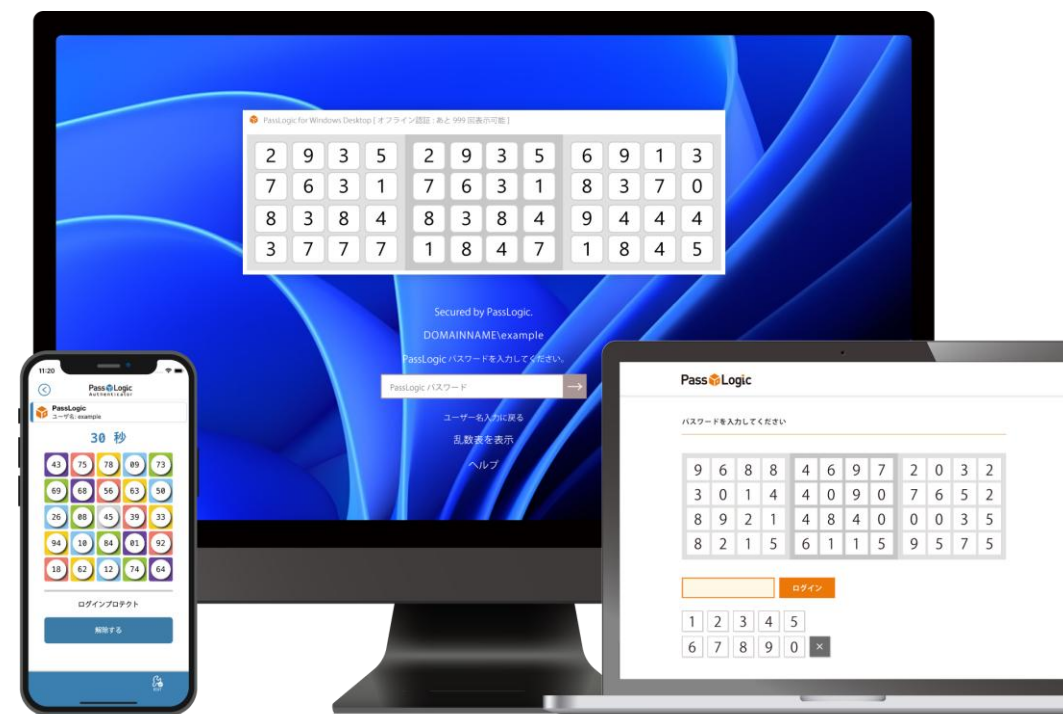


Multi-Factor Authentication Solution

PassLogic



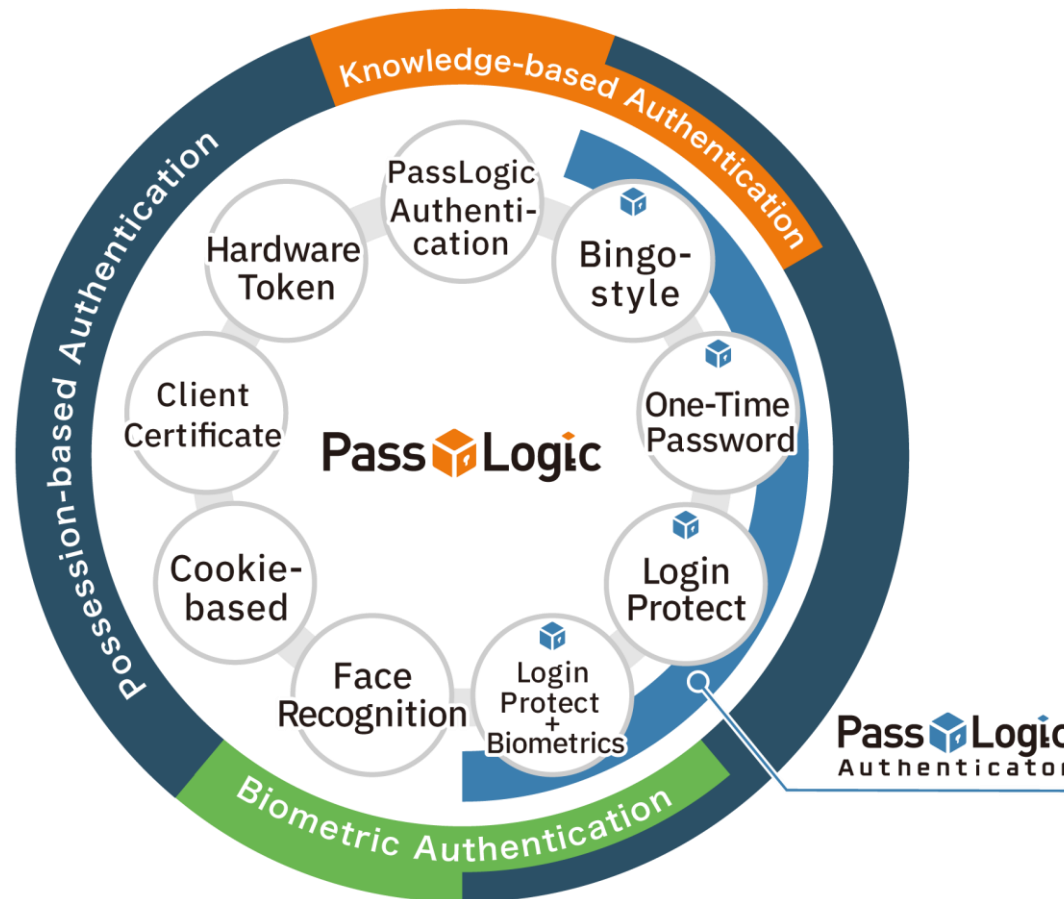
Passlogy Co., Ltd.
TAKII TOKYO BLD.7F 1-6-1 Kandajimbocho Chiyoda Tokyo

© Passlogy Co., Ltd. All rights reserved.

The Perfect Multi-Factor Authentication for Your Needs.

Nine Types Of Authentication Methods

Supports All Three
Authentication Factors:
Knowledge, Possession,
and Biometrics



Versatile MFA

Versatile Multi-Factor Authentication That Solves Every Security Challenge

Knowledge

Possession

Biometrics

Main Challenges and Use Cases

Enable MFA Without Devices
— Even in a Closed Network

PassLogic
Authntication

Client
Authentication
Certificate

- ✓ Enhance Authentication in Device-Restricted Environments
— No Smartphone Needed

Achieve MFA That Balances Ease of Use
and High Security with Face Recognition

PassLogic
Authntication

Facial
Recognition

- ✓ Browser-Based Authentication
— No Devices, No Passwords.
- ✓ Utilize Advanced Facial Recognition Technology.

Enhance Device Authentication on
Windows OS

PassLogic
Authntication

 Login Protect

- ✓ Enhance authentication for portable (off-site) devices
- ✓ Enhance authentication when accessing via remote desktop

Simplify Operations with Passwordless
Authentication

Bingo-style
Authentication

- ✓ Eliminate the risk of password leaks
- ✓ Avoid the use of weak or easily guessed passwords



Diverse Authentication Methods

Even if business environments or infrastructure change in the future, PassLogic allows flexible switching among nine different authentication methods to suit various situations, enabling long-term use as a multi-factor authentication solution.



Grid Authentication Method

As a knowledge-based authentication method replacing passwords, PassLogic adopts a grid authentication system ("PassLogic Authentication"). It generates one-time passwords directly in the browser, eliminating the need for dedicated devices or fixed passwords, thereby achieving both high convenience and strong security.



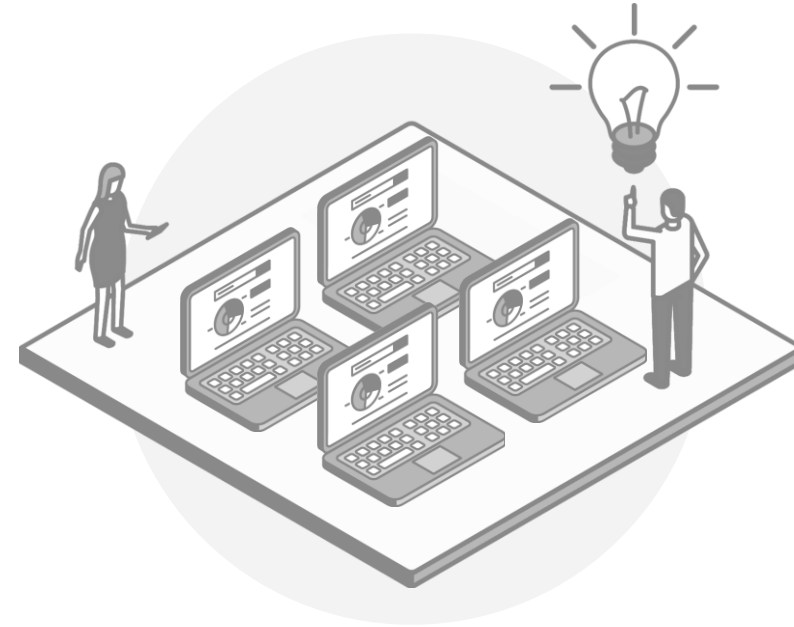
High Adaptability

PassLogic supports SSO integration with a wide range of systems, including cloud services such as Microsoft 365 and on-premises internal web applications. It also works with SASE, SSE, and VPN environments, and enhances authentication for Windows OS devices, enabling multi-factor authentication even for remote access.



Access Control

Access to business systems can be controlled based on each user's role, department, or IP address, with detailed configuration of authentication conditions such as device type and access time.



Single Sign-On (SSO)

Supports standard integration protocols (SAML, RADIUS, and Reverse Proxy), enabling connectivity with a wide range of business systems across both cloud and on-premises environments.

Enhance Windows OS sign-in security with multi-factor authentication



Official Name

PassLogic for Windows Desktop(Ver. 3.1.0)

Supported OS

Windows Server 2022 / 2019 / 2016、Windows 11/ Windows 10 Pro / Enterprise
※64bit exclusive support

- ※ Implemented using the Credential Provider framework.
- ※ OTP input for Remote Desktop connection client applications is not supported.

✓ Compatible with all accounts

- Active Directory (AD) account
- Microsoft account
- Local account

Note: An AD server is not required.

✓ Seamless Sign-On

Seamless single sign-on to web apps after Windows sign-in

✓ Offline Authentication

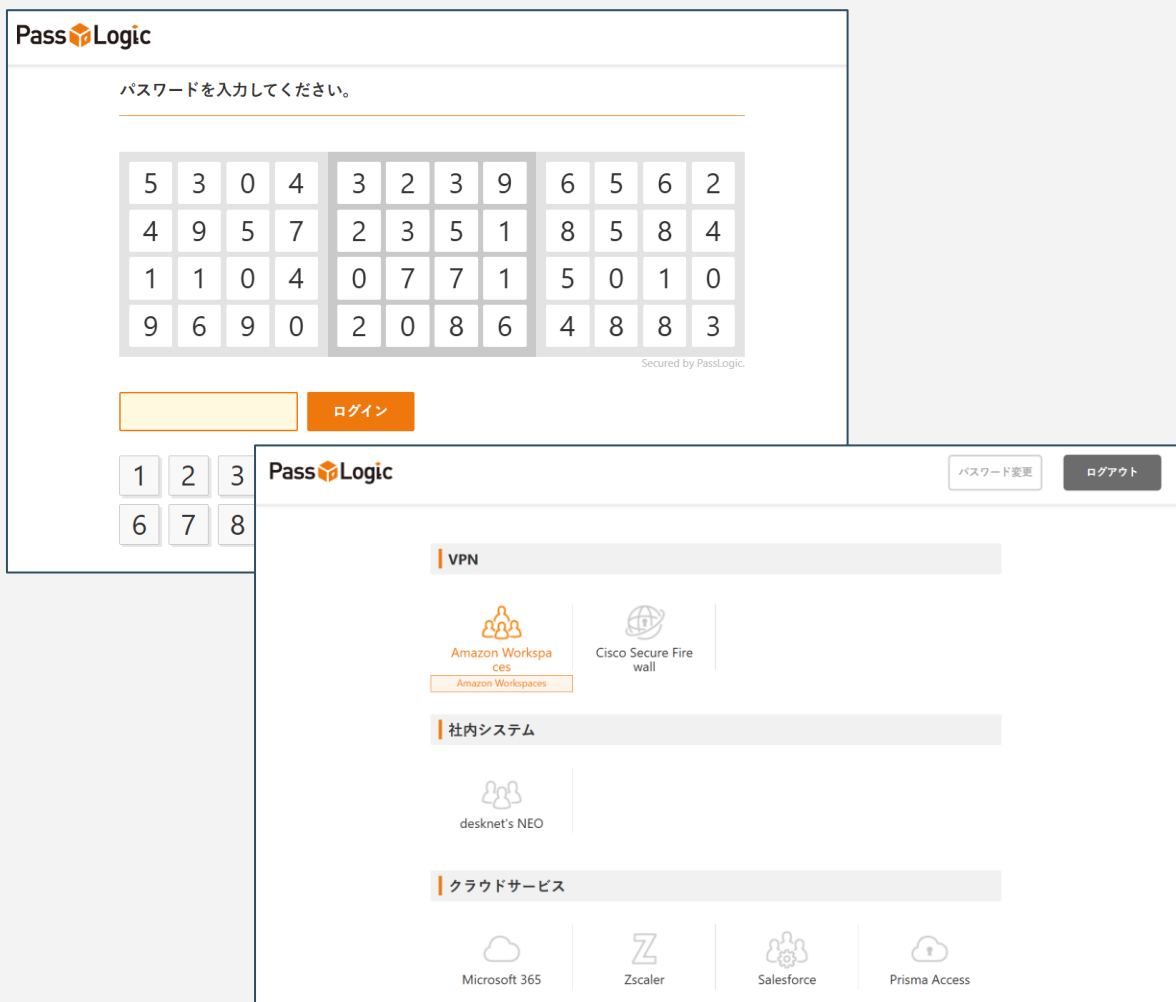
Login possible even when the Windows OS device is offline

- Up to 10,000 random number tables and their correct values are stored while online. During offline operation, authentication is performed using these stored random number tables and correct values.
- Authentication is also possible offline when using software or hardware tokens.

✓ Easy Configuration

Supports silent installation for client app deployment

Intuitive, user-friendly design



Improved usability, clarity, and convenience UI everyone can enjoy

Design excellence

- A simple, clean, white-based interface that provides a safe and comfortable experience for all users.
- Color schemes designed with consideration for color vision characteristics, accommodating a diverse range of users.

Operability

- Optimized navigation flow for an intuitive, easy-to-operate UI
- Centralized menus in the header for smooth, effortless access without confusion

Visibility • Usability

- Introduced icons that allow users to instantly recognize linked services at a glance
- Optimized display for smartphones and tablets

Functionality Efficiency

- Organized the information on the password change screen to streamline user operations
- Clarified operation steps with easy-to-understand instructions

PassLogic Authentication Methods

Simple Operation: Just Remember a Pattern

Access with Just a Browser

Enter your password

..... Login

Secured by PassLogic.

Password 480958

PassLogic Authentication(Grid method)

Read numbers from a randomized grid using your own predefined pattern to generate a one-time password.

Pattern = position and sequence

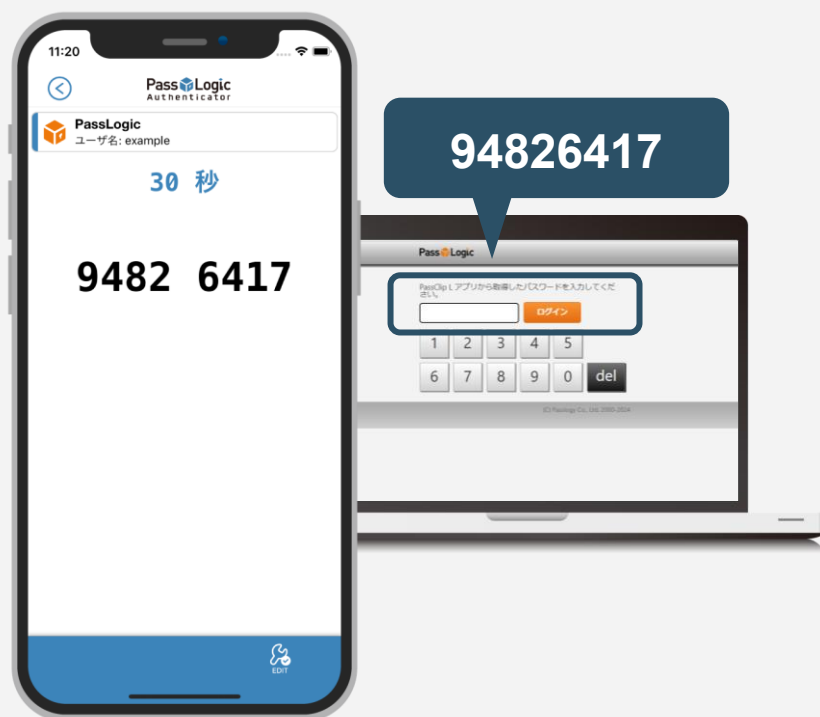
- On the login screen, a randomized grid is displayed.
- By following your predefined pattern and reading the numbers, you can generate a one-time password.
- All you need to remember is the grid positions and sequence, enabling strong one-time password login without the worry of forgetting static passwords.

Not Just Numbers! Letters and Symbols Can Also Be Used

It is also possible to add a fixed string — such as letters or symbols — before, after, or within the one-time password as an additional phrase.

[Watch the 30-Second Explainer Video >>](#)

Generates time-based one-time passwords (TOTP)



Simple and user-friendly interface

Uses the dedicated mobile app “PassLogic Authenticator”, which includes a function that generates one-time passwords changing at fixed intervals.

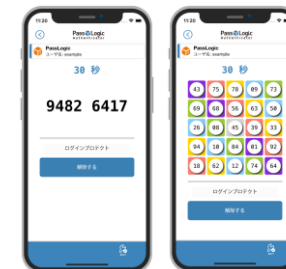
You simply enter the displayed one-time password — a straightforward and simple authentication method.

Since communication is not required to generate the one-time password, it can also be used in offline environments.

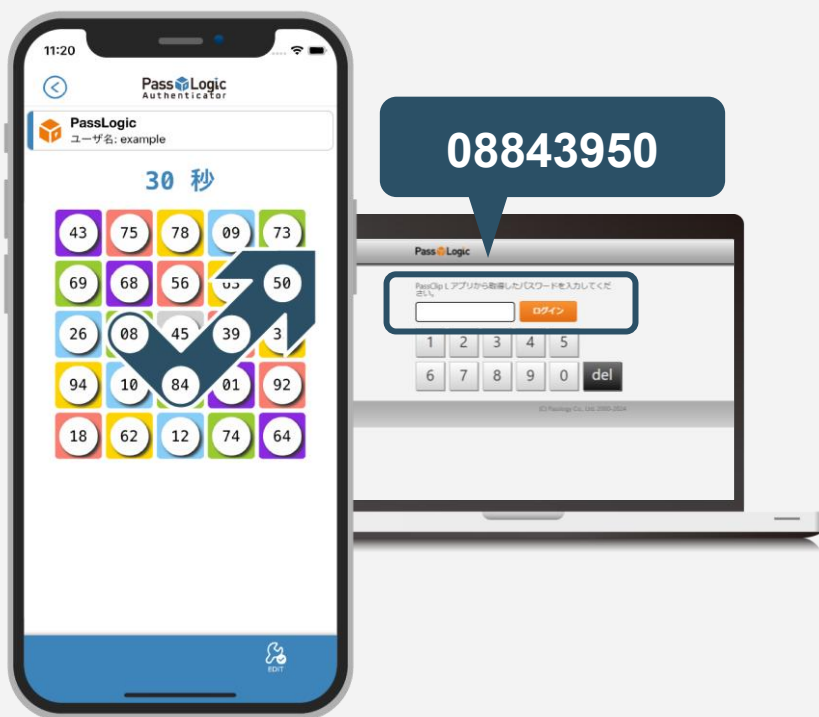
Utilizes the dedicated mobile app “PassLogic Authenticator”

PassLogic
Authenticator

for iOS/ Android



Displays time-based one-time passwords securely in hidden view



Bingo-style display that keeps your password hidden from others

Uses the dedicated mobile app “PassLogic Authenticator”, equipped with a function that generates one-time passwords which change at fixed intervals.

The one-time password is hidden within a 5×5 grid, and the user reads it by following a predefined pattern they have set in advance.

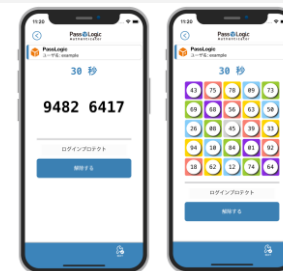
Even if someone else sees the screen due to loss or theft, the password cannot be read — this is PassLogic’s unique “Bingo-style display” method.

Since communication is not required to generate the one-time password, it can also be used in offline environments.

Utilizes the dedicated mobile app “PassLogic Authenticator”

PassLogic
Authenticator

for iOS/ Android



Just press a button — simple to use

■ Feitian Japan-made token



Keyholder Type



Card Type

■ Thales-made token



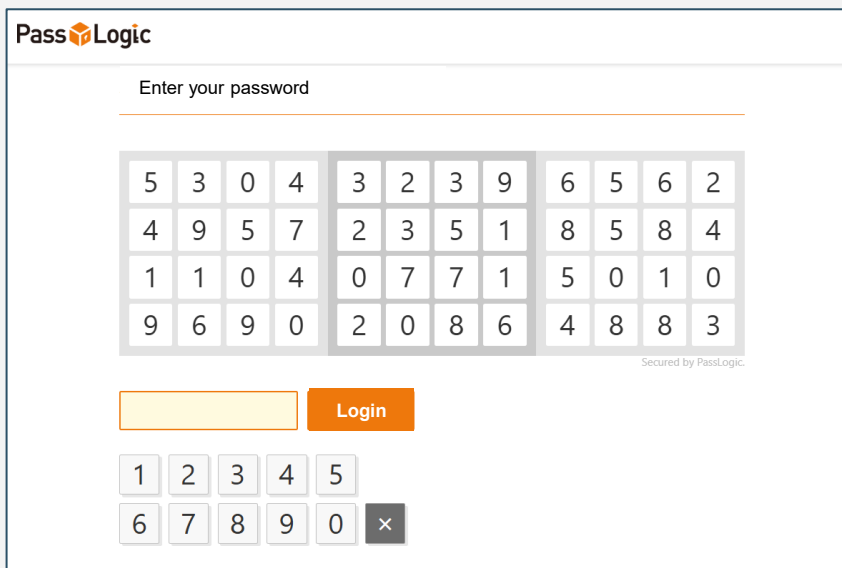
One-time password generation method usable offline

This method generates one-time passwords based on time, allowing use even in offline environments.

Available in keyholder-type and card-type models for convenient portability. Operation is simple — just press a button to generate a one-time password, making it easy and user-friendly.

A PIN code can also be set, enabling multi-factor authentication that combines knowledge and possession.

PassLogic Authentication

The image shows a web-based authentication interface for PassLogic. At the top left is the PassLogic logo. Below it is a text input field labeled "Enter your password". Underneath the password field is a large grid of numbers arranged in three columns and four rows. The first column contains 5, 4, 1, 9; the second contains 3, 2, 0, 2; the third contains 3, 2, 7, 0; the fourth contains 9, 1, 7, 8; the fifth contains 6, 5, 5, 4; the sixth contains 6, 8, 0, 8; the seventh contains 2, 4, 1, 8; and the eighth contains 2, 4, 0, 3. Below the grid is a "Login" button. At the bottom is a numeric keypad with digits 1-9, 0, and a delete key (X).

PassLogic

Enter your password

5	3	0	4	3	2	3	9	6	5	6	2
4	9	5	7	2	3	5	1	8	5	8	4
1	1	0	4	0	7	7	1	5	0	1	0
9	6	9	0	2	0	8	6	4	8	8	3

Secured by PassLogic.

Login

1	2	3	4	5
6	7	8	9	0

X

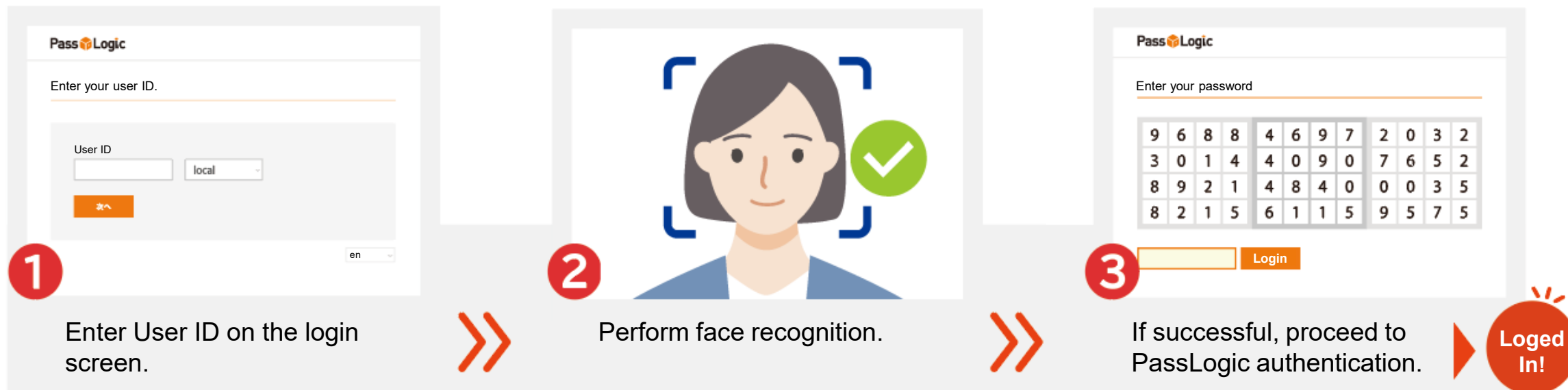
Facial Recognition



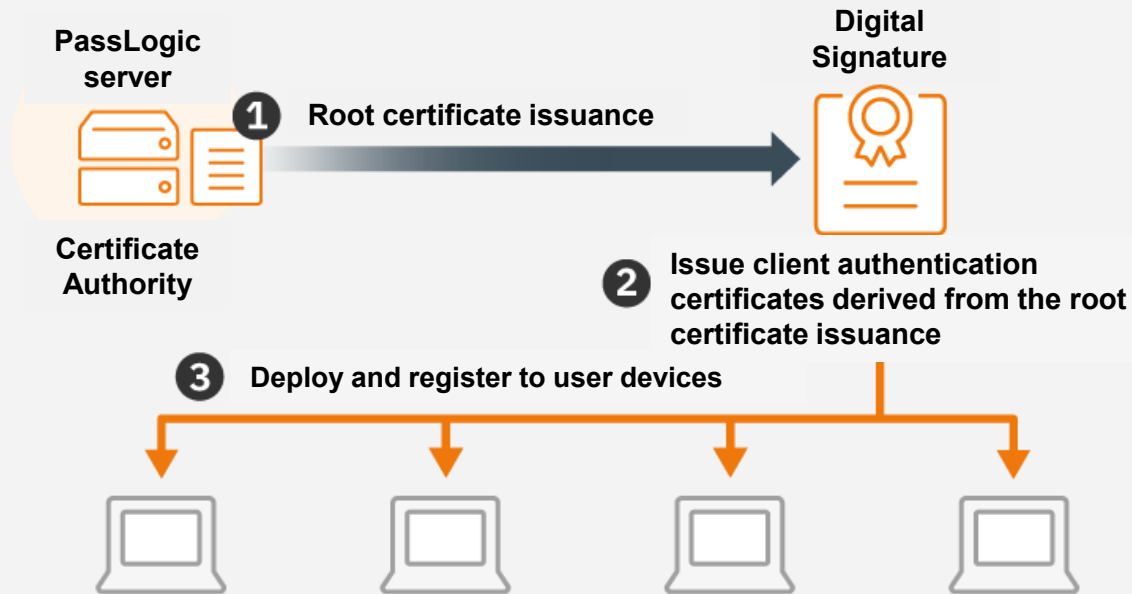
Facial recognition is available in Japan only,
with overseas deployment in progress.

- Traditionally, multi-factor authentication with facial recognition was combined with static passwords.
- In this solution, facial recognition is integrated with PassLogic Authentication (Grid method), enabling advanced multi-factor authentication directly in the browser—without tokens or dedicated devices.

Advanced multi-factor authentication using only a browser — no tokens or dedicated devices required.



Standard-equipped with a private certification authority(CA)



Blocks logins from unregistered devices and issues Client Authentication Certificates via a built-in private CA

Client Authentication Certificates are issued using the root certificate from the built-in private CA.

These certificates can be distributed and installed on user devices through methods suited to each organization's operational requirements.

Selectable Methods for Client Authentication Certificate

Choose from flexible distribution methods, including convenient automatic issuance, to match your operational needs.

- ✓ Automatic issuance on first login
- ✓ Distribution via email
- ✓ Printable option
- ✓ Downloadable from the admin console

Smooth implementation and lightweight device authentication for both admins and users



Blocks logins from unregistered devices and automatically registers a Cookie value on the first login device

When a user logs in for the first time, a Cookie value is automatically registered on that device.

From the second login onward, logins from any device other than the one registered during the first login will be rejected.

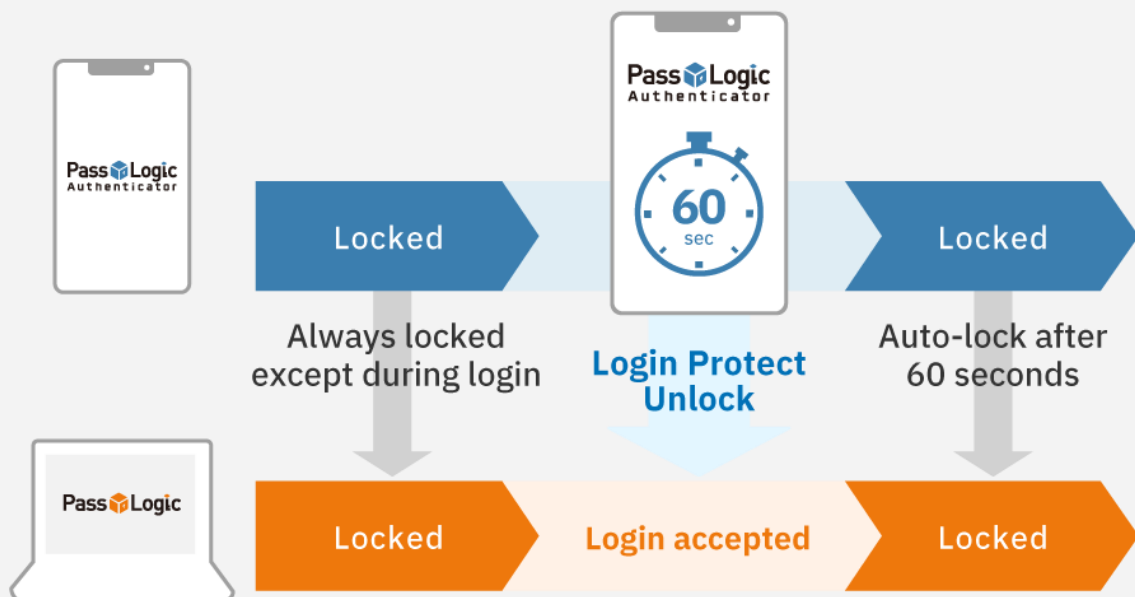
No complex configuration is required, reducing the operational load for both administrators and users.

Register up to five devices

Administrators can permit registration of up to five devices.

Users can register multiple terminals — including office, remote access, and portable devices — under the same account.

Maximum security with time-based access control



Access available for only 60 seconds!

The dedicated mobile app “**PassLogic Authenticator Login Protect**” provides a secure environment that accepts logins for only 60 seconds.

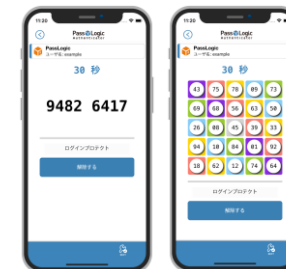
Outside this 60-second, login is blocked even with the correct one-time password, and the system automatically locks to prevent any further access.

By minimizing the time for potential attacks, security strength is dramatically enhanced.

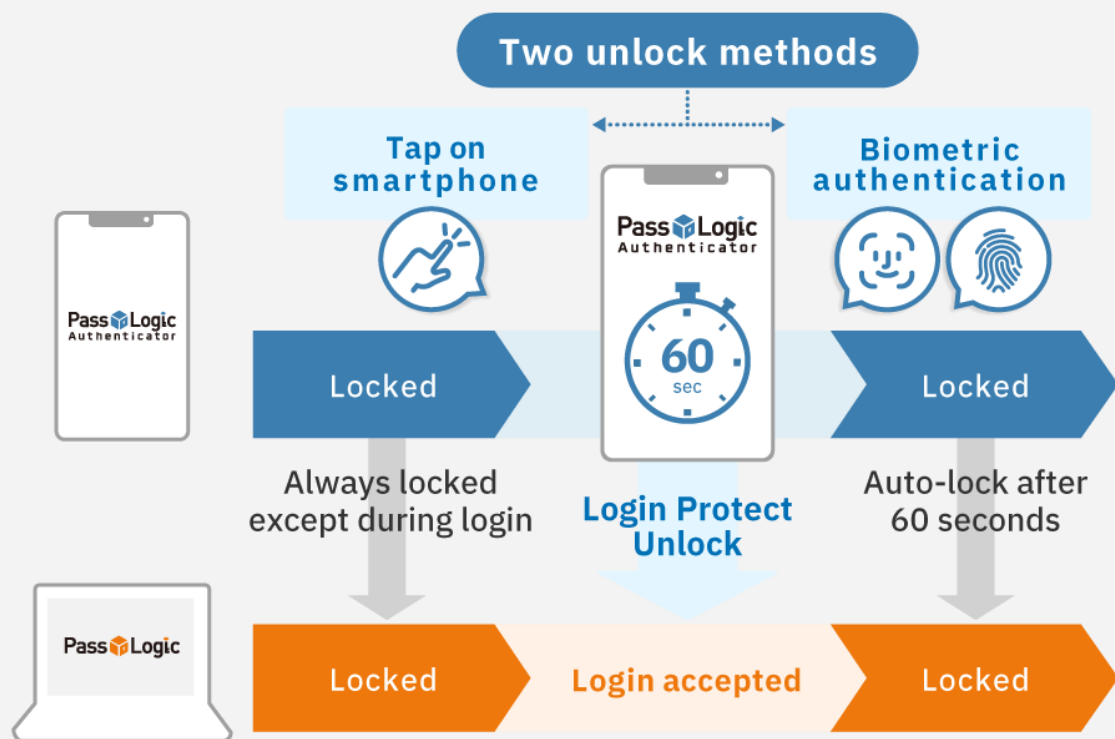
Utilizes the dedicated mobile app “PassLogic Authenticator”

PassLogic
Authenticator

for iOS/ Android



Seamless and comfortable experience using your smartphone



Enable 60-second secure access with smartphone biometrics — powered by “Login Protect” in PassLogic Authenticator.

Utilizes the dedicated mobile app “PassLogic Authenticator”

PassLogic Authenticator
for iOS/ Android

