PASSLOGY™

Register for the demo

CLICK!

Number of licenses issued

1,330,000 IDs

Confirmed: March 2021

An authentication platform that provides Single Sign-On with tokenless one-time passwords

PassLogic

Reduced Deployment and Operational Costs

Reduce purchasing costs and operating costs. Reduce administrator workload with automated user support.

Increased Security

Implement secure authentication with security policies which can enforce requirements such as two-factor authentication and device authentication.

Improved Operational Efficiency

The platform integrates with a wide range of services in the cloud and on premises to create a single sign-on environment.

Windows Authentication

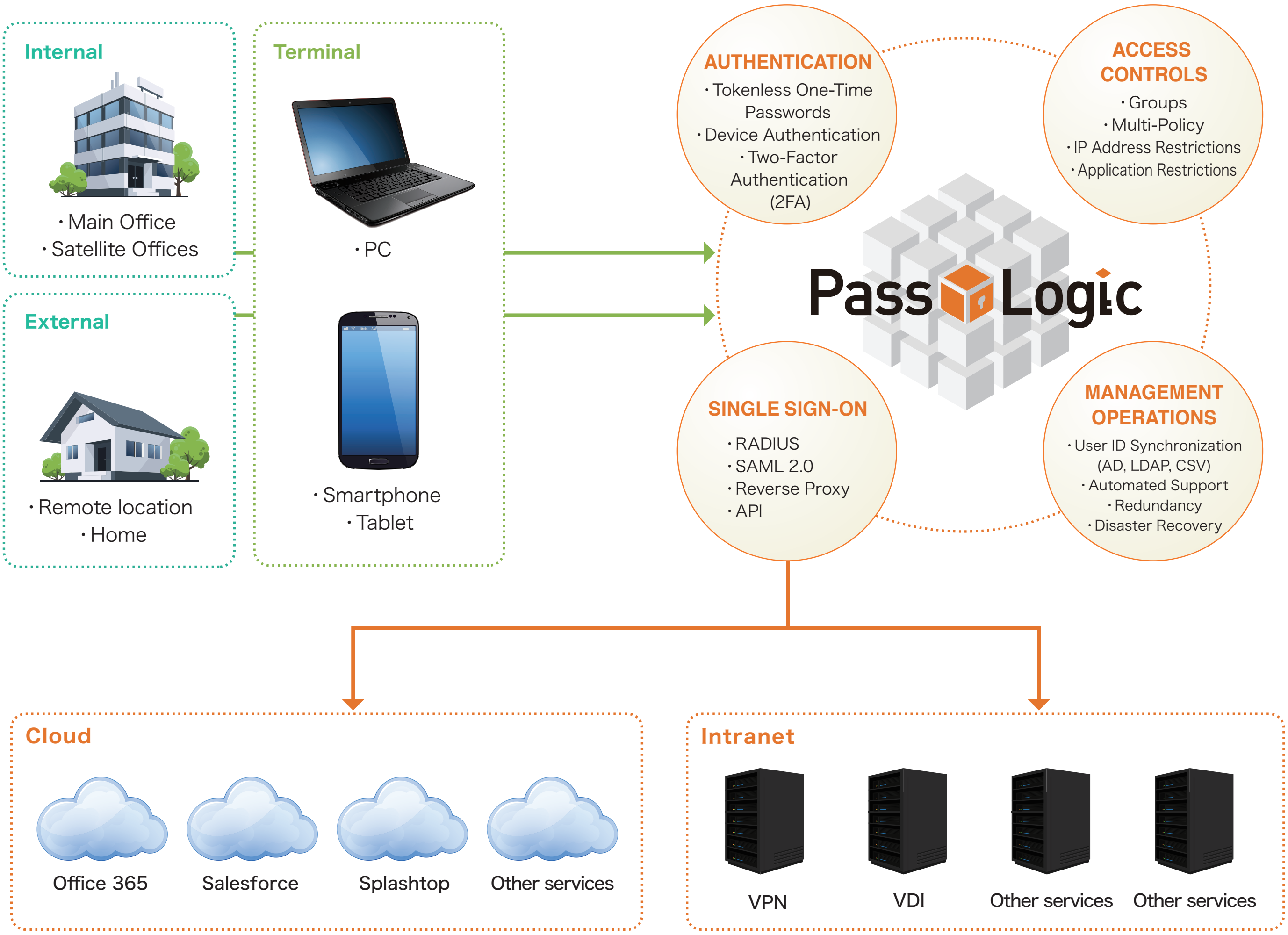
Protect access to Windows desktops by strengthening authentication for Windows Logon.

PassLogic Demo : https://www.passlogy.com/en/passlogic-demo/

Increase both security and operational efficiency with a single solution.

PassLogic provides tokenless one-time password authentication for Single Sign-On to on-permises services and cloud services. ID synchronization with LDAP and Active Directory can be performed. Fine-grained access controls can be implemented to ensure that users' permissions match their job functions and level of authority.

PASSLOGIC: BENEFITS OF USE



Internal
- Main Office
- Satellite Offices

External
- Remote location
- Home

Terminal
- PC
- Smartphone
- Tablet

PassLogic

AUTHENTICATION
- Tokenless One-Time Passwords
- Device Authentication
- Two-Factor Authentication (2FA)

ACCESS CONTROLS
- Groups
- Multi-Policy
- IP Address Restrictions
- Application Restrictions

SINGLE SIGN-ON
- RADIUS
- SAML 2.0
- Reverse Proxy
- API

MANAGEMENT OPERATIONS
- User ID Synchronization (AD, LDAP, CSV)
- Automated Support
- Redundancy
- Disaster Recovery

Cloud

Office 365 / Salesforce / Splashtop / Other services

Intranet

VPN / VDI / Other services / Other services

Customer Comments

The operation is simple; once you understand it, it is easy to use.

Forgotten password requests have been reduced.

Token management tasks have been eliminated.

Our workforce has become more mobile.

No browser setup required - easy operation and maintenance.

We were able to achieve single sign-on for a wide range of resources and services.

*These comments are taken from a survey, which was conducted in January and February of 2015.

● Number of licenses issued: 1,330,000 IDs (Confirmed: March 2021)

● Patent Information
～World-class PassLogic Authentication～

PassLogic is the first authentication system in the world to create a password by extracting it from a random number table. The US patent was obtained in 2000. 101 related patents in 29 countries have been obtained since then (Confirmed: May 2021).

*The product uses the following patents in the United States and Japan: U.S.PAT.6141751 / JP.PAT.5276658 / U.S.PAT.8140854 / JP.PAT.3809441

*Use of the product without the permission of the patent holder constitutes patent infringement; this includes end-user use after purchasing from an unauthorized third party and in-house development uses.

*To date (June 2021), Passlogy has not licensed patents from other companies (this does not include Passlogy's use of services such as cloud services).

Achieve One-Time Password Authentication Without Tokens

What is PassLogic Authentication?

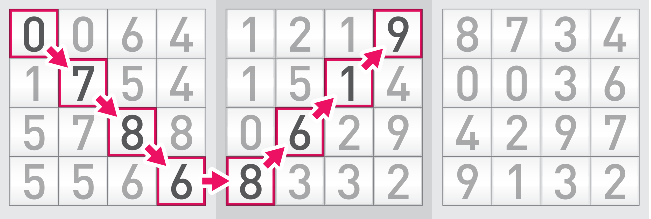
Features

A user only needs to remember one thing: their secret pattern. ▶ The user's password is the sequence of numbers in the random number table that corresponds to their secret pattern. ▶ Since the random number table is refreshed every time a user goes to log in, the password will be new for each login.

PASSLOGIC AUTHENTICATION EXPLAINED

Creating a Secret Pattern

The user creates a secret pattern by selecting a sequence of cells from a grid.



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

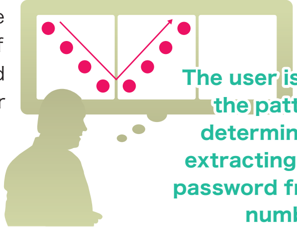
Secured by PassLogic.

Password ******** Login

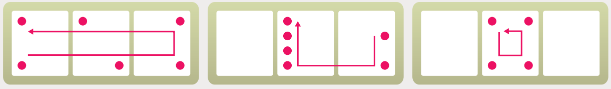
Password 07868619

Password Generation Rules

Users can choose any sequence of cells from the grid when creating their secret patterns.



The user is free to decide the pattern that will determine the rule for extracting their one-time password from the random number table.

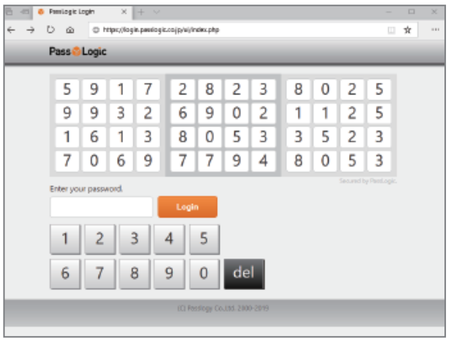


Any sequence of cells can be selected for the pattern.

Authentication Method

The random number table is displayed at login. The user extracts the sequence of numbers from the table that corresponds to his or her secret pattern. The user then enters this sequence into the password field and clicks the Login button.

▶ Random Number Table Screen



PassLogic Login
https://login.passlogic.co.jp/ui/index.php
PassLogic

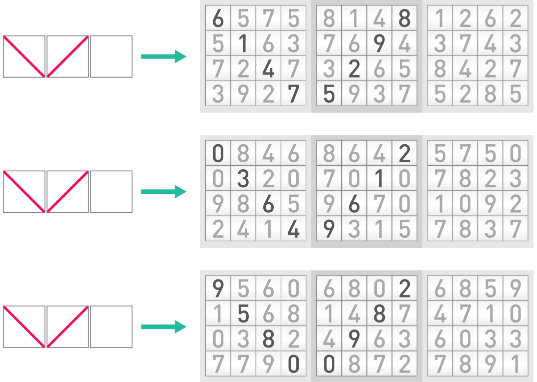
5	9	1	7	2	8	2	3	8	0	2	5
9	9	3	2	6	9	0	2	1	1	2	5
1	6	1	3	8	0	5	3	3	5	2	3
7	0	6	9	7	7	9	4	8	0	5	3

Secured by PassLogic.

Enter your password.

Login
1 2 3 4 5
6 7 8 9 0 del
(C) Passlogy Co.,Ltd. 2000-2019

Since the random number table is refreshed every time a user goes to log in, the password will be new for each login.



1st Time

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

Password 61475298

2nd Time

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

Password 03649612

3rd Time

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

Password 95800982

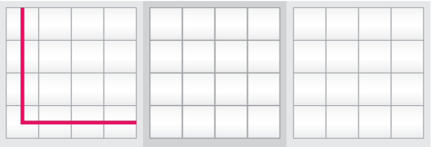
Patent*

*Generate a one-time password by extracting it from a random number table: <U.S.PAT.6141751/JP.PAT.5276658>

Optional Fixed Password Component

The password can be strengthened by prepending or appending a static set of characters to it.

▶ In this example, "PassLogic" is appended to the password that corresponds to the secret pattern.



·Password extracted from the random number table.

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

+

·Fixed Password Component

PassLogic

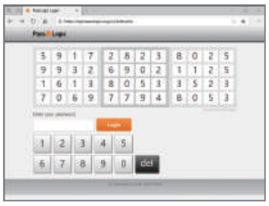
Password 2639247PassLogic

AUTHENTICATION FUNCTIONS

AUTHENTICATION TO THE INTERNAL NETWORK

Irrespective of the location of the service being accessed (internal or external) or the terminal being used (PC, smartphone or tablet) authentication can be performed in a standard browser.

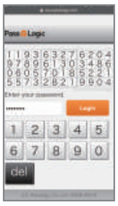
Desktop Browser



Pass Logic

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

Mobile Browser



Pass Logic

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

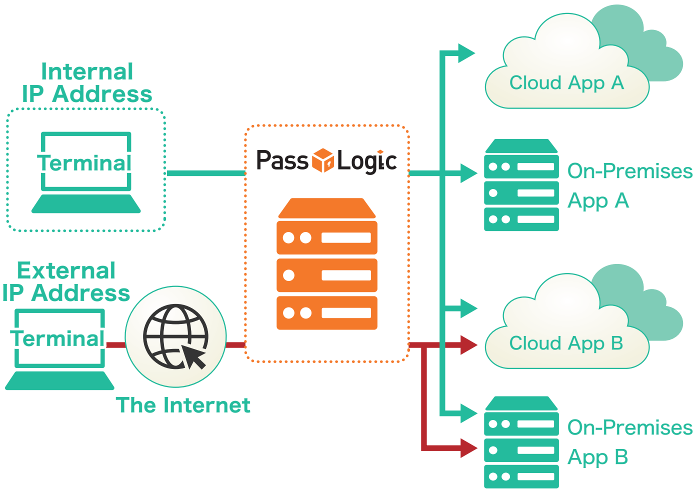
Enter your password

■Supported Browsers

●Internet Explorer 11 ●Edge ●Mozilla Firefox ●Google Chrome
●Safari ●Android Standard browser

IP ADDRESS RESTRICTION

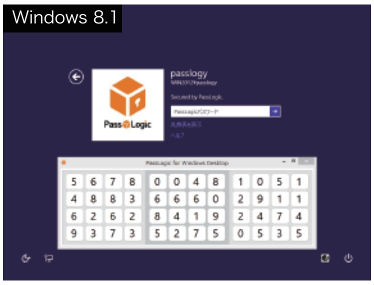
IP access restrictions can be used to control access to applications and systems.



AUTHENTICATION FOR WINDOWS LOGON: PASSLOGIC FOR WINDOWS DESKTOPS

PassLogic can be used as the authentication method for logging on to a Windows computer (starting the device and signing in to a Windows account). The PassLogic method can replace the standard fixed password authentication method for Windows Logon with dynamic passwords.

Windows 8.1



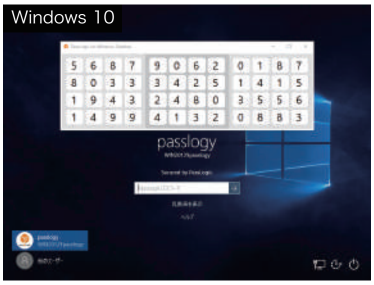
passlogy

Secured by PassLogic

PassLogic for Windows Desktop

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

Windows 10



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

passlogy

•Authentication can be pertorned offline.
•Two-Step Verification can be achieved by combining the Active Directory password with PassLogic's dynamic passwords.

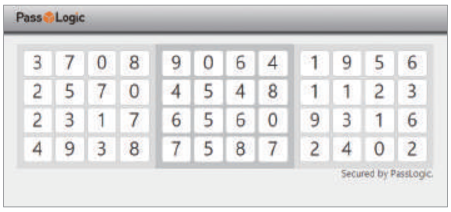
■Supported Windows OS

●Windows 8.1 32bit/64bit ●Windows 10 32bit/64bit
●Windows Server 2016

INTEGRATION WITH CLIENT SOFTWARE

The PassLogic random number table can be displayed in a browser. The user can then extract his or her password from the table and enter it into the authentication screen of the client software.

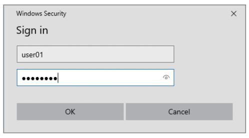
Random Number Table in Browser + Authentication Screen



Pass Logic

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

Secured by PassLogic



Windows Security

Sign in

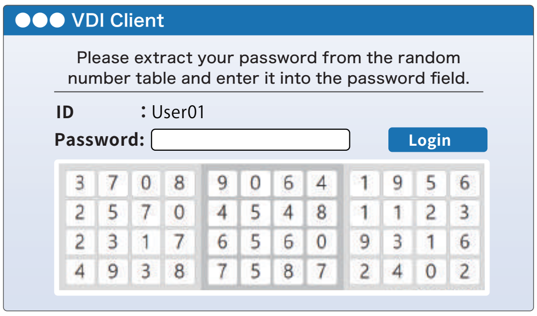
user01

••••••••

Supported Client Software Includes:

- ● Windows Standard Client
- ● VMware Horizon View Client
- ● Cisco ASA AnyConnect ● FortiClient
- ● SonicWall NetExtender ● PaloAlto

Using the Passlogic API to Display the Random Number Table Inside the Authentication Screen



●●● VDI Client

Please extract your password from the random number table and enter it into the password field.

ID : User01

Password:

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

■Overview of the PassLogic API

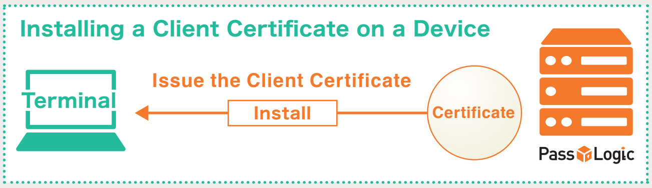
API Type	REST
Data Format	XML、JSON
Authentication API	Tokenless OTP Software Token (PassClip L) Hardware Token *Not compatible with Client Certificate Authentication
Management API	User management (create, edit, delete, search, get user information) Token management (add, delete, search tokens)

DEVICE AUTHENTICATION

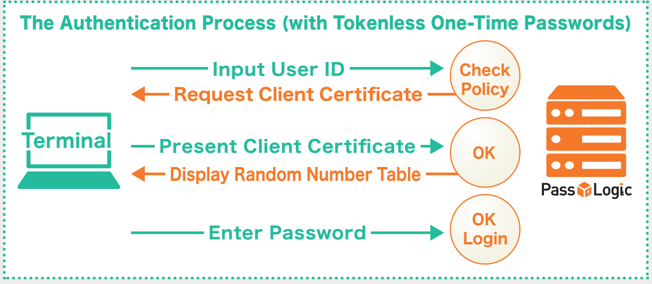
PassLogic can restrict access to a set of devices by performing device authentication.

PKI Client Authentication

PassLogic can issue client certificates to authorized devices and deny access requests from devices that do not have a client certificate installed.



Installing a Client Certificate on a Device

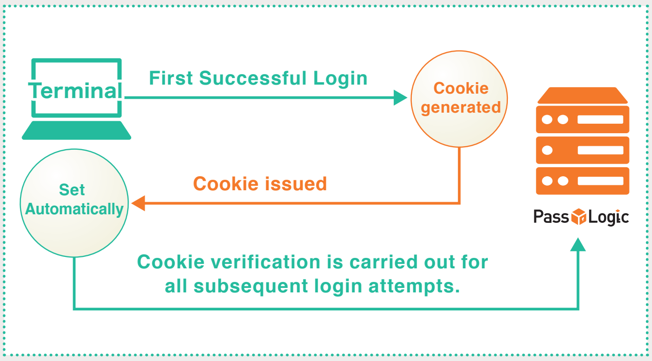


The Authentication Process (with Tokenless One-Time Passwords)

Terminal
Input User ID
Request Client Certificate
Check Policy
Present Client Certificate
Display Random Number Table
OK
Enter Password
OK Login
PassLogic

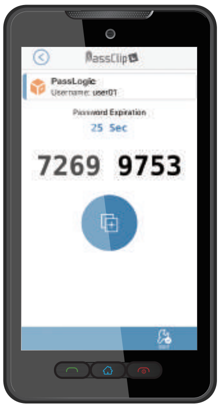
Cookie Authentication

At the first successful login, the device is registered and a cookie is issued to it.
The cookie information is then checked at all subsequent logins.

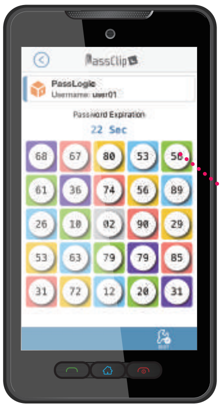


SOFTWARE TOKEN

The 'PassClip L' mobile app is provided, free of charge, as a software token. The app provides two options for displaying one-time passwords: a basic display and a secure grid display. The app can be combined with a fixed password to achieve Two-Factor Authentication.



Basic Display



Secure Grid Display

The PassLogic OTP Mobile App

PassClip L

iOS/Android

Knowledge of a secret pattern is needed to decipher the one-time password dsiplayed in the secure grid display.

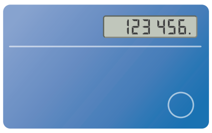
↓

The one-time password can be displayed securely in plain sight.

HARDWARE TOKEN

PassLogic supports the use of OATH-compliant hardware tokens. These tokens can be combined with a PIN in order to achieve Two-Factor Authentication.

Key Fob Type



Card Type

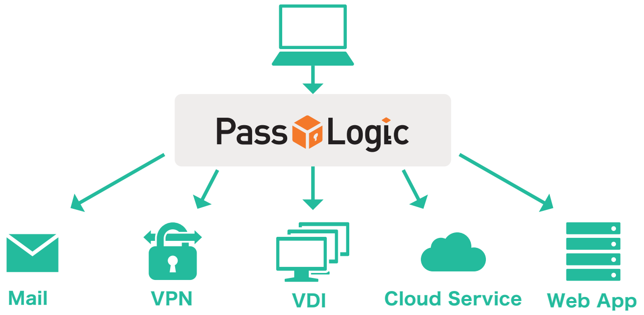
Two-Factor Authnetication Options

PassLogic provides a range of options for achieving Two-Factor Authentication.

Client Certificate or Cookie	+	PassLogic Authentication	→	2FA is achieved without using a specialized authentication device or a fixed password.
PassClip L (Smartphone Possession)	+	PassClip L (Secure Grid Display)	→	2FA is achieved with smartphone possession and knowledge of the secret pattern.
PassClip L (Smartphone Possession)	+	PIN Code (Fixed Password)	→	2FA is achieved with smartphone possession and knowledge of the fixed password.
Hardware Token	+	PIN Code (Fixed Password)	→	2FA is achieved with hardware token possession and knowledge of the PIN.

SINGLE SIGN-ON

After a successful PassLogic authentication, linked services and systems can be accessed without any additional authentication. Password management is simplified and operational effcency is improved.



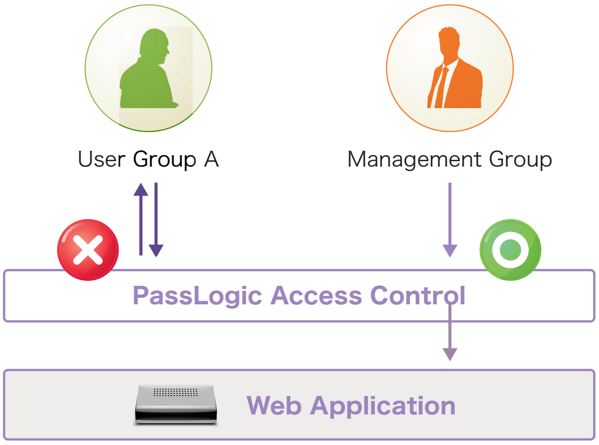
Consolidate logins to mutiple business systems into a single sign-on.

A single authentication provides authorized access to mutiple systems.

Reduce the time wasted on logins and maintain focus on work.

ACCESS CONTROL

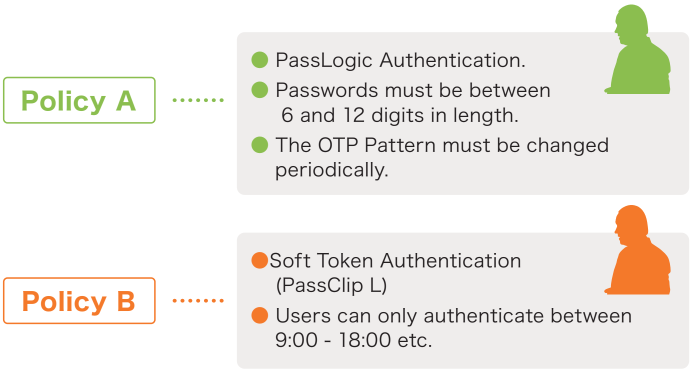
PassLogic also supports group-based access controls; users can be allowed or denied access to a Web application depending on their respective group memberships.



*If a user tries to gain access to a URL that he or she is not authhorized to access, PassLogic will block the access attempt and return a 403 Forbidden message to the user.

MULTI-POLICY

Authentication policies can be tailored to individual services and to individual users.



Policy A

- PassLogic Authentication.
- Passwords must be between 6 and 12 digits in length.
- The OTP Pattern must be changed periodically.

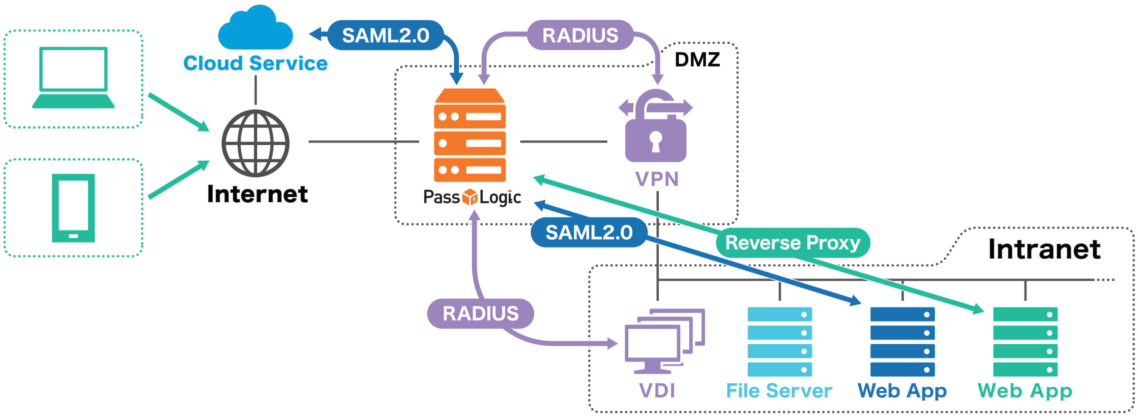
Policy B

- Soft Token Authentication (PassClip L)
- Users can only authenticate between 9:00 - 18:00 etc.

Adjusrable Items and Controls; Authentication Method; Password Length; Time Period When Authentication is Permitted; Pattern History Check; Forced Periodic Password Change; Prohibited Patterns; Account Lockout Threshold etc.

COMPREHENSIVE INTEGRATION

PassLogic integrates with a wide range of services, such as VPN services, VDI environments and Web applications on-premises and in the cloud. A single sign-on environment can be easily created with PassLogic.



Supported Protocols

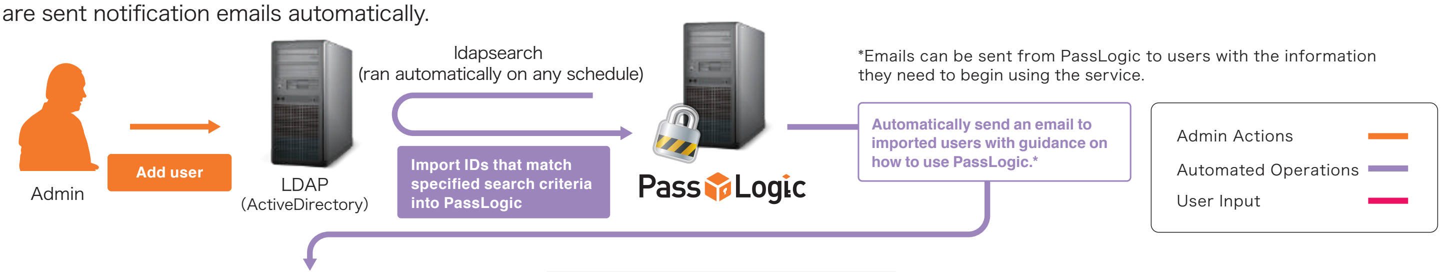
- ● RADIUS
- ● SAML 2.0
- ● REST API
- ● Reverse Proxy

A single policy can be applied to all systems.

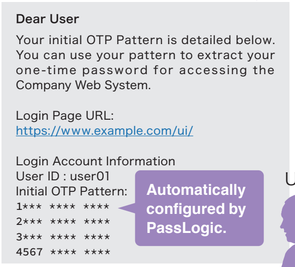
OPERATION AND MANAGEMENT FUNCTIONS

Automatic Registration of Users from LDAP (Active Directory)

PassLogic can be set to check LDAP (Active Directory) periodically and to update its User Information accordingly. Newly registered users are sent notification emails automatically.


Admin
Add user
LDAP
(ActiveDirectory)
ldapsearch
(ran automatically on any schedule)
Import IDs that match specified search criteria into PassLogic
PassLogic
Automatically send an email to imported users with guidance on how to use PassLogic.*
Admin Actions
Automated Operations
User Input

*Emails can be sent from PassLogic to users with the information they need to begin using the service.



Dear User

Your initial OTP Pattern is detailed below. You can use your pattern to extract your one-time password for accessing the Company Web System.

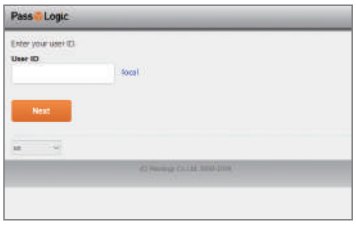
Login Page URL:
https://www.example.com/ui/

Login Account Information
User ID : user01
Initial OTP Pattern:
1*** **** ****
2*** **** ****
3*** **** ****
4567 **** ****

Automatically configured by PassLogic.

User

Follow the instructions and click the link.



PassLogic

Enter your user ID

User ID: local

Next

If the Force Initial Pattern Change function is enabled, the user cannot access any applications or systems until the pattern has been changed.

The following ID registration methods are also available:

- Automatic and Periodic CSV File Import
- Manual Resistraction in the Admin Panel
- Manual bulk registration with a CSV file in the Admin Panel

AUTOMATED USER SUPPORT

The admin workload can be significantly reduced with automated support for tasks such as password resets and user unlocking. These functions can also be controlled manually.

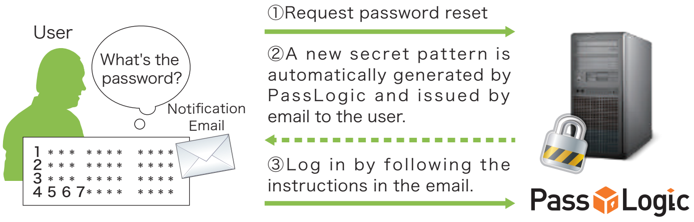
USER SUPPORT ISSUES
- No dedicated support personnel
- No support during nights or holidays

USER SUPPORT AUTOMATION
- Automatic Password Reset
- Automatic unlocking

The support workload can be significantly reduced.

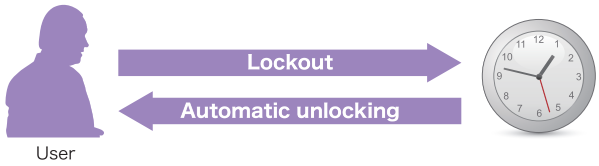
Automatic Password Reset

A Self-Service Password Reset function can be enabled. An administrator password reset function is also provided.



Automatic Unlocking

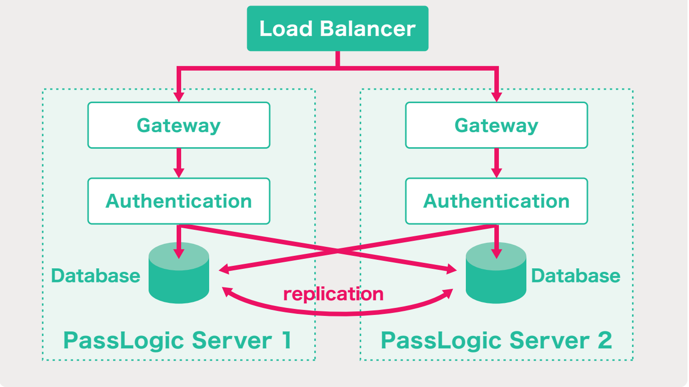
An automatic unlocking function is provided. This can be set to unlock a user who has been locked out due to a number of consecutive failed login attempts after a specifed period of time. A manual unlocking function is also provided for administrators.



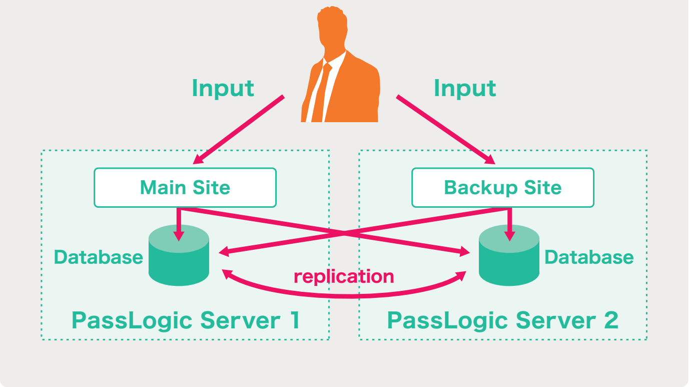
SUPPORT FOR REDUNDANCY AND DISASTER RECOVERY MEASURES

The data replication function

Redundancy Configuration



Disaster Recovery



*The gateway can be separated from the authentication functions with a split-server configuration.

System Requirements

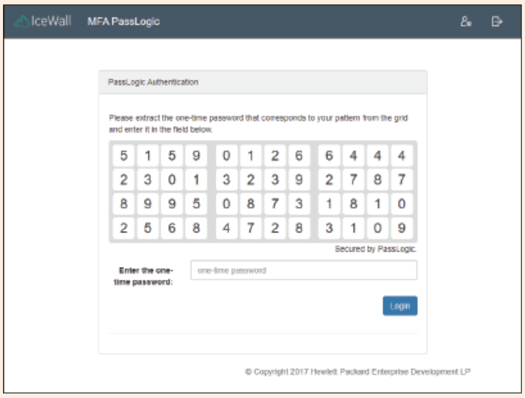
Server OS	Red Hat Enterprise Linux 8.3 or later or CentOS 8.3 or later x86_64 *2
httpd *1	Apache HTTP Server Version : 2.4.37 or later Release : 21.module_el8.2.0
php *1	Version : 7.4.6 or later Release : release: 4.module_el8.3.0

*1 Only OS vendor-supplied modules are supported.
*2 Security-Enhanced Linux (SELinux) is not supported and must be disabled.
※Virtualization is possible where the guest OS is supported.

PASSLOGIC IN THE EDUCATION SECTOR

PassLogic has been widely adopted in the education sector. The institutions which have adopted PassLogic include a number of leading Japanese universities, world-renowned research facilities and governmental education boards.

PassLogic has been successfully integrated with SSO services which work with Shibboleth, such as OpenAM (OSS Tech) and HPE IceWall.



PassLogic Authentication

Please extract the one-time password that corresponds to your pattern from the grid and enter it in the field below.

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

Secured by PassLogic.

Enter the one-time password: one-time password

© Copyright 2017 Hewlett Packard Enterprise Development LP

PassLogic integration with HPE IceWall MFA

Company Profile

Company Name	Passlogy Co., Ltd.
Street Address	Kanda Ogawamachi San-chome Building, 3-26-8, Kanda-Ogawamachi, Chiyoda-ku, Tokyo 101-0052, Japan
Email	global@passlogy.com
Tel.	+81-03-5577-2865 (10:00-17:00 JST) *Closed on Saturdays, Sundays and holidays
URL	www.passlogy.com/en

IS 697637 / ISO 27001

Main Clients

ITOCHU Techno-Solutions Corporation
Internet Initiative Japan Inc.
NTT PC Communications Inc.
Serverworks Inc.
CTC System Management Corporation
NS Solutions Corporation
SoftBank Corp.
SB C&S Corp.
TIS Inc.
DIS Solution Co., Ltd.
NEC Corporation
Japan Business Systems Co., Ltd.
Networld Corporation
Fujitsu Limited
Universal Computer System Co., Ltd.

PASSLOGY™

- Any publications which advertise the use of a Passlogy license should include the official license information.
- Unauthorized use or reproduction of the information contained in this brochure is prohibited.
- Company names, organization names, product and service names that feature in the brochure are trademarks or registered trademarks of their respective companies or organizations.
- To facilitate development and improvement, the design and specifications of the product are subject to change without notification.

202106k