PassLogic Enterprise Edition

Ver.2.4.0

Installation and Management Guide

PASSLOGY™

Introduction

This manual describes installation and management of the PassLogic authentication server software.

Display screens

Because display screens shown in this manual are used as examples, they might be different from actually displayed screens.

Patents

Passlogy's product "PassLogic" is protected by one or more of the United States patents or applications listed below. This information is provided in satisfaction of the virtual patent marking provisions pursuant to United States patent laws (35 U.S.C. §287, as amended). This list may not be exhaustive:

7206850
8140854
8812862
7814331
6141751
8312538
8281380
8959603
14/322,577
14/404,759
13/820,075

Trademarks and disclaimers

- PassLogic and Passlogy are registered trademarks of Passlogy Co., Ltd.
- All other company names and product names shown in this manual are trademarks or registered trademarks of their respective companies.
- This product is not intended for a high level of safety use as medical equipment, nuclear facilities, aviation related equipment, military equipment, transfer facilities, and other facilities and equipment that directly affect people's lives. Do not use on such applicable facilities and equipment.

Copyright/cautions

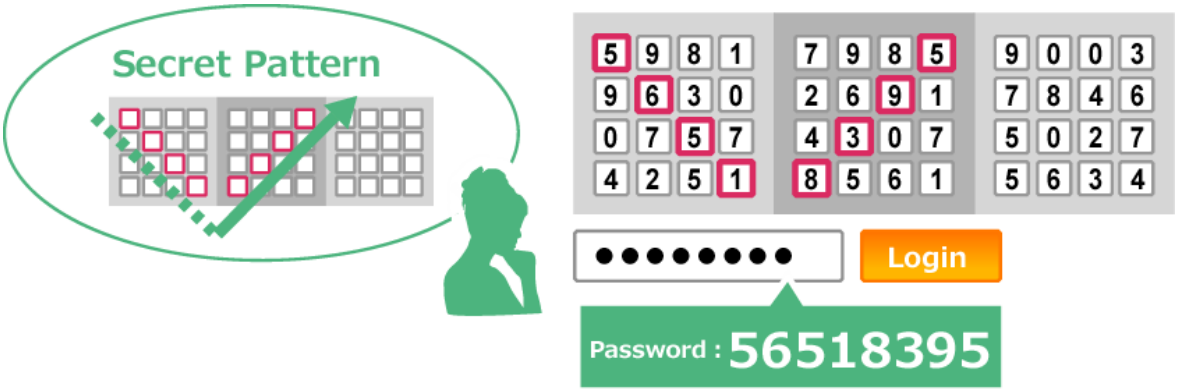
- Partial or total copying of the contents of this manual without prior consent is prohibited.
- The contents of this manual and the specification of the product may be changed without prior notice.

The contents of this document are prepared with extreme care, however, if you have found any obscure points, errors, omissions, disarranged pages, or missing pages, please contact us.

Contents

What is PassLogic authentication method?

The PassLogic authentication method uses "position" and "order" on a random number grid displayed during logging in as the password generation rule, which is a secure authentication method that generates a valid password for each login.



The password generation rule is called a "secret pattern" which can be changed by users. In addition, a "static password (fixed password)" can be combined with a one-time password. The following example describes a method to set a V-shaped pattern and static password.

How to change the secret pattern with static password

First, please determine any secret pattern and static password.

*In view of the uniqueness and easy to remember, determine the pattern and password.

<< Example of secret pattern and static password >>

The following secret pattern (“position” and “order”) and static password are the new password.

Secret pattern:

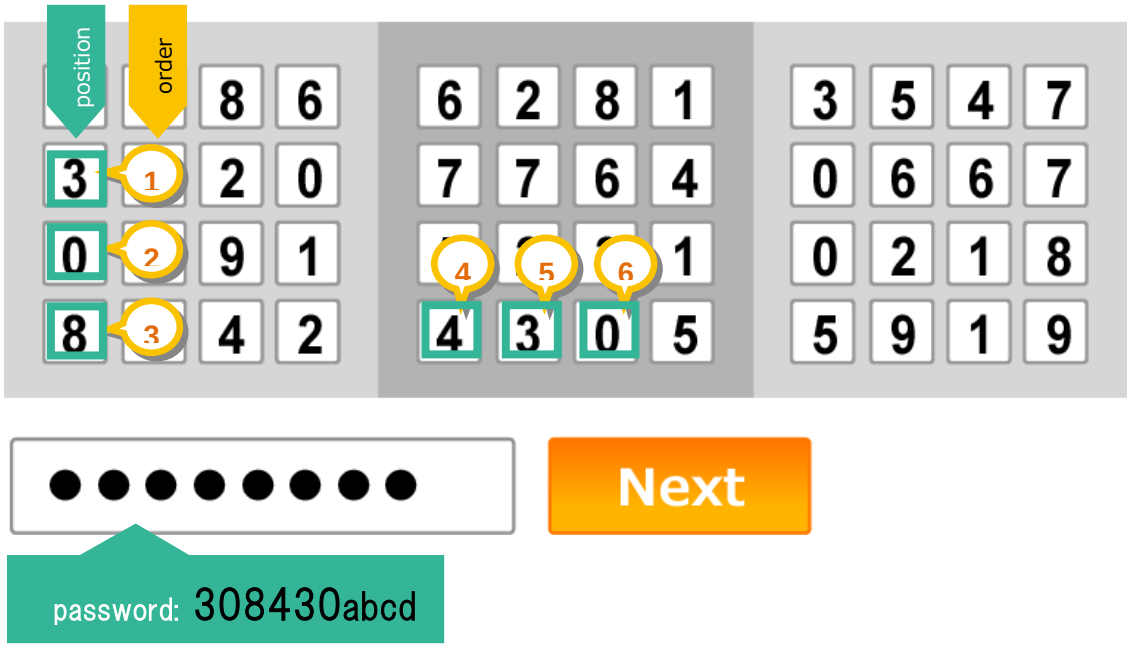
■■■■ ■■■■ ■■■■
1■■■ ■■■■ ■■■■
2■■■ ■■■■ ■■■■
3■■■ 4 5 6■ ■■■■

Static password ： abcd

STEP 1.

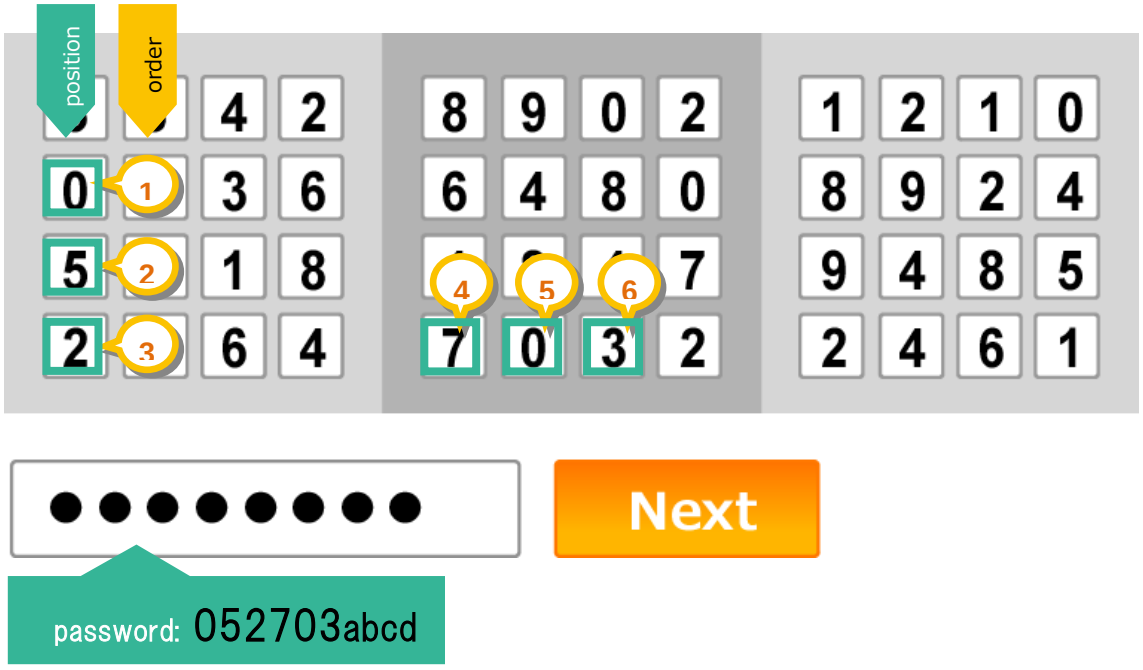
Enter six numbers according to the secret pattern (position and order) and the static password. Then click [Next] button.

*Enter the number using the keyboard. Grid cannot be clicked.



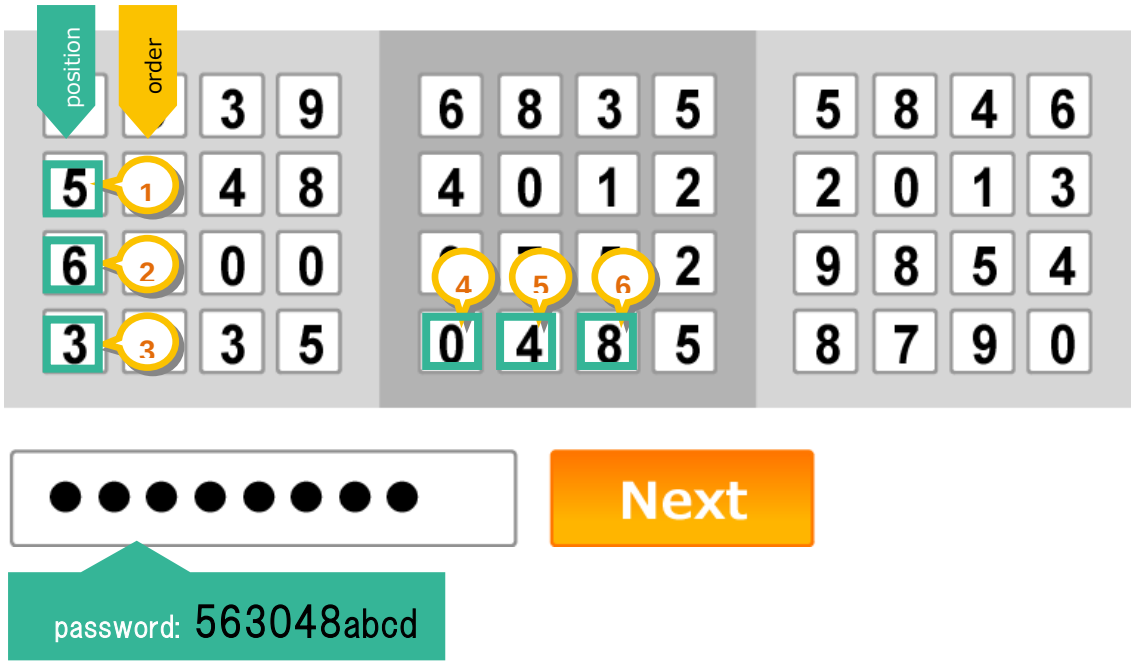
STEP 2.

Click [Next] in STEP 1 to display a new random number grid. Enter the secret pattern numbers and the static password. Then click [Next] button.



STEP 3.

Again display a new random number grid. Enter the secret pattern numbers and the static password. After these three entries in total, password change completes.



1 Installation guide

1.1 System Requirements

System requirements for the PassLogic authentication server is shown next.

	Red Hat Enterprise Linux 6.1 or later x86_64/ CentOS 6.1 or later x86_64
httpd	Apache HTTP Server version:2.2.15 release: 9.EL6 or later
php	version:5.3.3 release: 3.EL6 or later

	Red Hat Enterprise Linux 7.1 or later / CentOS 7.1 or later
httpd	Apache HTTP Server version:2.4.6 release: 31.EL7 or later
php	version:5.4.16 release: 36.EL7_1 or later

*Contact our support about operating systems and distributions not shown above.

*For each module, only the packages provided by OS vendor are supported. Uniquely compiled ones are not eligible for support, and therefore, please inquire separately.

*Because the environment where NSA Security-Enhanced Linux (SELinux) is set to [enforcing] is not supported, set to [permissive / disabled] during OS installation.

*This product is tested on CentOS; however, please be cautious that if any issues are generated resulting from the OS when using CentOS, support from Red Hat, Inc. is not possible.

1.2 Installing SSL certificate

Follow the manual provided by the SSL server certificate authority, and install it on Apache of PassLogic server.

1.3 Using anti-virus software

Remove the following directories of the PassLogic authentication server from scanning targets.

/var/lib/php/session

1.4 Recommended browsers

The PassLogic user interface is developed with HTML5, CSS3, and JavaScript. In addition, cookie is used to maintain session information.

	Browser	Character code
Management tool	[PC] Internet Explorer11	UTF-8
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
User interface	[PC] Internet Explorer9, 10, 11	
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
	[iPhone / iPad] Safari (iOS7, 8, 9)	
	[Android] standard browser (Android4, 5, 6)	

*SSO to non-trusted certificate site does not work on Edge browser.

*When to use legacy document modes (Internet Explorer), PassLogic screen does not appear correctly. It can be prevented by customizing the template file.

1.5 Ports

User interface	443	tcp	https
Management tool	8443	tcp	https
RADIUS	1812	udp	radius
Database	5439 9915 9925	tcp	postgresql pgpool pgpool

*When using firewalls such as iptables, perform settings as necessary so that the PassLogic authentication server software can access the port to be used.

1.6 Required packages

Install package software necessary to operate the PassLogic server software.

```
(Execute with root privileges)
# yum -y install sed
# yum -y install sudo
# yum -y install gnupg2
# yum -y install rpm
# yum -y install perl
# yum -y install openssl
# yum -y install openssh-clients
# yum -y install tmpwatch
# yum -y install httpd
# yum -y install mod_ssl
# yum -y install ntp              (only RHEL6/CentOS6)
# yum -y install chrony           (only RHEL7/CentOS7)
# yum -y install zip
# yum -y install unzip
# yum -y install crontabs
# yum -y install postfix
# yum -y install php
# yum -y install php-gd
# yum -y install php-ldap
# yum -y install php-pgsql
# yum -y install php-mbstring     (RHEL6/7 is required to enable optional repository.)
# yum -y install php-process      (RHEL6/7 is required to enable optional repository.)
# yum -y install php-pecl-apc     (only RHEL6/CentOS6)
# yum -y install net-snmp-utils
# yum -y install curl
# yum -y install libtool-ltdl
# yum -y install libxslt
# yum -y install rsync
# yum -y install mailx
# yum -y install apr-util-pgsql   (RHEL6/7 is required to enable optional repository.)
# yum -y install xmlsec1
# yum -y install xmlsec1-openssl
# yum –y install freeradius       (only RHEL7/CentOS7)
```

```
# yum –y install tncfhh-libs                    (only RHEL7/CentOS7)
```

*When installing php-mbstring, php-process and apr-util-pgsql packages in using yum, [Optional] needs to be enabled with SoftwareChannels of RedHat Network.

Command that enable Optional repository:

```
(RHEL6) # subscription-manager repos --enable=rhel-6-server-optional-rpms
(RHEL7) # subscription-manager repos --enable=rhel-7-server-optional-rpms
```

1.7 Installing PassLogic

Install the PassLogic authentication server software.

```
 (Execute with root privileges)
# cp /cdrom/PassLogic-ent-x.x.x-el6.tar.gz /usr/local/src/        (RHEL/CentOS 6)
# cp /cdrom/PassLogic-ent-x.x.x-el7.tar.gz /usr/local/src/        (RHEL/CentOS 7)
# cd /usr/local/src/
# tar zxvf PassLogic-ent-x.x.x.tar.gz
# cd passlogic-ent-x.x.x/
# ./install.sh install
```

*Please unzip the installer to a directory that "other users" can access.

*install.sh outputs install.log to the same directory.

During installation, the following settings are automatically added and changed.

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
LoadModule filter_module modules/mod_filter.so	Remove the comment out to enable. (RHEL/CentOS 6)
#AddDefaultCharset	Comment out to disable the setting value.
ServerSignature	Off
TraceEnable	Off

/etc/php.ini

post_max_size	16M
upload_max_filesize	16M
memory_limit	256M
session.cookie_secure	1
expose_php	Off
error_reporting	E_ALL & ~E_NOTICE
session.cookie_httponly	On
short_open_tag	On

/etc/yum.conf （only RHEL6/CentOS6）

exclude=freeradius*	Add

*If freeradius is updated, PassLogic becomes not usable; therefore, exclude it from the update targets in the yum command.

/etc/sudoers （RHEL6/CentOS6）

apache ALL=NOPASSWD: /sbin/service httpd status apache ALL=NOPASSWD: /sbin/service postfix status apache ALL=NOPASSWD: /sbin/service radiusd status apache ALL=NOPASSWD: /sbin/service ntpd status apache ALL=NOPASSWD: /opt/passlogic/apps/tools/httpd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/radiusd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/restore.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_info.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_recovery.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/recovery_tar.sh	Add
#Defaults requiretty	Disable

/etc/sudoers (RHEL7/CentOS7)

apache ALL=NOPASSWD: /bin/systemctl status httpd apache ALL=NOPASSWD: /bin/systemctl status postfix apache ALL=NOPASSWD: /bin/systemctl status radiusd apache ALL=NOPASSWD: /bin/systemctl status chronyd apache ALL=NOPASSWD: /opt/passlogic/apps/tools/httpd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/radiusd_restart.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/restore.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_info.sh apache ALL=NOPASSWD: /opt/passlogic/apps/tools/support_recovery.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/recovery_tar.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgpool-start.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgpool-stop.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgsql-start.sh passlogic ALL=NOPASSWD: /opt/passlogic/apps/tools/pgsql-stop.sh Cmnd_Alias PASSLOGIC_SERVICE = /bin/systemctl * passlogic-pgpool, /bin/systemctl * passlogic-pgsql, /bin/systemctl * radiusd, /bin/systemctl * httpd passlogic ALL=NOPASSWD: PASSLOGIC_SERVICE	Add
#Defaults requiretty	Disable

*Above settings are necessary to enable setting changes with the management tool.

/etc/ssh/ssh_config

StrictHostKeyChecking no	Add

*Disable the ssh connection confirmation between PassLogic servers.

Automatic start with the chkconfig or systemctl command.

httpd ntpd (only RHEL6/CentOS6) chronyd (only RHEL7/CentOS7) crond postfix passlogic-pgsql passlogic-pgpool radiusd

1.8 Apache recommended settings

To mitigate web server vulnerability, it is recommended that you change Apache default settings as followings.

To prevent directory listings
/etc/httpd/conf/httpd.conf
(Before) Options Indexes FollowSymLinks
(After of RHEL6) Options -Indexes FollowSymLinks
(After of RHEL7) Options FollowSymLinks
Disable TRACE method
/etc/httpd/conf/httpd.conf
(Addition) TraceEnable Off
Remove unnecessary directories
/var/www/icons/ (RHEL6 only)
/var/www/error/ (RHEL6 only)
/var/www/cgi-bin/
Disable SSL version 3
/etc/httpd/conf.d/ssl.conf
(Before) SSLProtocol all -SSLv2
(After) SSLProtocol all -SSLv2 -SSLv3
Rename unnecessary setting files (RHEL7 のみ)
- Disable directory listing
(Before) /etc/httpd/conf.d/autoindex.conf
(After) /etc/httpd/conf.d/autoindex.conf.org
- Disable settings of mod_userdir
(Before) /etc/httpd/conf.d/userdir.conf
(After) /etc/httpd/conf.d/userdir.conf.org
- Disable Apache default top page
(Before) /etc/httpd/conf.d/welcome.conf
(After) /etc/httpd/conf.d/welcome.conf.org

*After settings changes, require a restart of Apache.

1.9 Accessing the management tool

Create an initial administrator (User ID: admin) with the following command.

```
(Execute with root privileges)
# /opt/passlogic/apps/tools/modify_admin_passwd.php
-------------------------------------------
(Example of a command execution result)
modified admin password: 3nEG0uUY
```

*"3nEG0uUY" in the above example of a command execution result changes for each command execution. This part is an initial password of the administrator (User ID: admin).

Access the management tool of the PassLogic authentication server software with a web browser.

```
https://[hostname of PassLogic authentication server]:8443/passlogic-admin/
```

* When firewalls such as iptables are launched, open TCP port 8443 to allow access to the PassLogic management tool.

Enter "admin" in the user ID input field of the management tool, and then go to the next page to display a random number grid, and enter the initial password generated previously.

* The initial administrator user cannot be deleted.

1.10 Registering license

Register the license file (license-ent.asc). Click [Maintenance] > [License Settings] from the left menu on the management tool. Register the license file, and verify the license information is reflected correctly.

*Operated with the maximum number of users = 1 after initial installation.

*Any services will not restart when registering new license file.

*Register license file to PassLogic authentication server, not to PassLogic gateway server.

*In the case of server replication configuration, register license to all authentication servers.

*Do not edit license file.

1.11 Updating

Update the PassLogic authentication server software. Updating from other edition is not supported.

*Before updating, please make sure to perform a backup using the management tool and stop users access to PassLogic servers.

*Run the update when scheduled automatic task is not working.

```
(Execute with root privileges)
# cp PassLogic-ent-x.x.x.tar.gz /usr/local/src/
# tar zxvf PassLogic-ent-x.x.x.tar.gz
# cd passlogic-ent-x.x.x/
# ./install.sh update
PassLogic Authentication Server Software をアップデートします。よろしいですか？- start update
PassLogic Authentication Server Software [yes or no]
(Enter yes.)
```

The PassLogic authentication server software is automatically updated, and httpd restarts.

Recovering method in case of problems

```
(Execute with root privileges)
(Uninstall PassLogic after updating)
# cd passlogic-ent-x.x.x/ (x.x.x is the version after updating)
# ./install.sh uninstall
(Reinstall PassLogic before updating)
# cd ../passlogic-ent-y.y.y/ (y.y.y is the version before updating)
# ./install.sh install
# /opt/passlogic/apps/tools/modify_admin_passwd.php
(Access the management tool, and restore the backup file.)
```

The PassLogic authentication server software is automatically installed, and httpd restarts.

Notes update from ver.2.0.0

After update, delete “MAIL_CC” and “MAIL_BCC” on /opt/passlogic/data/conf/settings.conf.

Notes update from ver.2.1.0

LDAP Synchronization Mode [Add / Update / Inactive] is replaced to [Add / Update / Delete]. If you don’t want to delete PassLogic users automatically, Please change the Synchronization Mode to [Add / Update].

Notes update from ver.2.2.1

"Fixing" was added to the cookie value which is Device restriction.
version 2.2.0 previous cookie value is moving in setting of "Change".
Please change from Config > Policy Settings > Edit > Device restriction.

"attribute and parameter" please register the following setting about the function.
Phrase setting [Config] > [UI Settings] > [Edit] from the left menu on the management tool.

```
【ja】
Back：
  戻る
Register：
  登録
Change passparam：
  設定
Setpass Form：
  パラメータを入力してください。
Setpass Confirm：
  下記内容でパラメータ登録します。
Setting Completed：
  設定が完了しました。

【en】
Back：
  Back
Register：
  Register
Change passparam：
  Config
Setpass Form：
  Please set the parameters.
Setpass Confirm：
  Parameter registration in the following contents.
Setting Completed：
  Setting has been completed.
```

Setting of "Setting AD" "LDAP synchronization" will be aggregated into a "Domains".
Setting of "LDAP synchronization" of the old version is forcibly treated as "LDAP ID Sync" settings of the local domain, not inherited bind password.
After the update, please re-register the bind password from "Domains" of left menu links, and then click the "Edit" in the line of the "local" domain.

When doing users import on the command line, it was change as follows.

```
# /usr/bin/php /opt/passlogic/apps/admin/cgi/userimport.php {CSV file path} {Config file path}
```

Notes update from ver.2.3.2

Add new item to settings.conf file.

＊Please refer to [settings.conf] of this manual for more information.

Phrase setting [Config] > [UI Settings] > [Edit] from the left menu on the management tool.

【ja】
Account expiration:
　アカウント有効期限
Password expiration:
　パスワード有効期限
Last login:
　前回ログイン日時
Day:
　日
Indefinite:
　無期限

【en】
Account expiration:
　Account expiration
Password expiration:
　Password expiration
Last login:
　Last login
Day:
　day(s)
Indefinite:
　Indefinite.

A few setting items have been added in "Cloud > SP Settings" and the format of SAML response has been changed.

After the update, please test the operation of the SAML authentication in advance.

*If an error what is related with "Audience" is occured, please set the value of "Audience" as "RelayStateURL".

There are differences shown following wording between ver.2.3.2 and 2.4.0. These are not updated automatically by PassLogic version-up installer.

Phrase setting [Config] > [UI Settings] > [Edit] from the left menu on the management tool.

【ja】
Instruction1:
　2.3.2 以前:ユーザー名を入力してください。
　2.4.0 以降:ユーザ ID を入力してください。
Username:
　2.3.2 以前:ユーザー名
　2.4.0 以降:ユーザ ID
Change password required:
　2.3.2 以前:パスワード変更が必要なユーザです。
　2.4.0 以降:パスワード変更が必要です。
Change password message1:

2.3.2 以前:STEP.1 パスワード(パスワード位置情報の数字)を入力してください。
STEP.2 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。
2.4.0 以降:<script type="text/javascript">$(function(){ $("#detail").css("display", "none");
$("#detail_disp").click(function(){ $("#detail").toggle(); }); });</script>
<style type="text/css">.PLHelpPasschg {background-color:#fff; padding:1em;
margin-bottom:1em;}</style>

■パスワード変更:入力 1/3 回目
【ヘルプ:手順を表示】

※この説明の表記はサンプルです。必ず設定したポリシー条件に合わせて変更してください!(管理ツール > 設定 > UI 設定 > Change password message1)
【はじめに】当システムのパスワード変更手順を説明します。
はじめてご利用になる方は、<a href="http://www.passlogy.com/pattern_staticpass"
target="_blank">認証方式と用語の説明(別ページが開きます)をご参照ください。
<hr>
【STEP1】下記の条件を満たす「シークレットパターン」と「スタティックパスワード(任意の文字列)」を決めてください。

シークレットパターンの設定条件

・6~12 マス分を選択
・左、中央、右の各 16 マス(4×4)のブロックから、最低 1 マスずつ選択
・一筆書き(すべてのマスがつながっている)のパターンは禁止

スタティックパスワードの設定条件

・6~12 桁
・半角英数(大文字小文字を区別)
・記号(_ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < >)

【STEP2】STEP1 で決めたシークレットパターンに沿ってマス内の数字をパスワード欄に入力し、つづけてスタティックパスワードを入力してください。その後、「次へ」を押してください。

Change password message2:
2.3.2 以前:STEP.1 パスワード(パスワード位置情報の数字)を入力してください。
STEP.2 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。
2.4.0 以降:■パスワード変更:入力 2/3 回目
マス内の数字が変わりました。
もう一度、あなたが設定したいシークレットパターンに沿ってマス内の数字を入力し、つづけてスタティックパスワードを入力してください。
入力後、「次へ」を押してください。

Change password message3:
2.3.2 以前:STEP.1 パスワード(パスワード位置情報の数字)を入力してください。
STEP.2 STEP.1 にて選択したパスワード位置情報と同じ位置の数字を入力してください。
STEP.3 確認の為、もう一度パスワード(パスワード位置情報の数字)を入力してください。
2.4.0 以降:■パスワード変更:入力 3/3 回目
再度マス内の数字が変わりました。
1 回目、2 回目の入力と同じように、もう一度、あなたが設定したいシークレットパターンに沿ってマス内の数字を入力し、つづけてスタティックパスワードを入力してください。
入力後、「次へ」を押してください。

Navigation to reset pattern:

2.3.2 以前：ユーザ名と登録されているメールアドレスを入力して[次へ]をクリックしてください。
シークレットパターン再発行のメールを送信します。
2.4.0 以降：ユーザ ID と登録されているメールアドレスを入力して[次へ]をクリックしてください。
シークレットパターン再発行のメールを送信します。

【en】
Instruction1：
2.3.2 以前：Enter your username.
2.4.0 以降：Enter your user ID.
Username：
2.3.2 以前：Username
2.4.0 以降：User ID
Change password message1：
2.3.2 以前：STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.
2.4.0 以降：<script type="text/javascript">$(function(){ $("#detail").css("display", "none");
$("#detail_disp").click(function(){ $("#detail").toggle(); }); });</script>
<style type="text/css">.PLHelpPasschg {background-color:#fff; padding:1em;
margin-bottom:1em;}</style>

[First Input (1/3)]
*Input three times to complete.
Show procedure

*This description is a SAMPLE. Please change to match the policy conditions! (Management Tool > Config > UI Settings > Change password message1)
Introduction:The following section describes the password change procedure of this system.
For first time user, please refer to this link about authentication method and terminology.

STEP1:Make your unique Secret Pattern and Static Password according to the following terms.
<hr>
Regulations on Secret Pattern

-Choose positions from 6 to 12.
-Choose at least one grid from each left, center and right 4 by 4 grid blocks.
-You cannot make a Secret Pattern with a single stroke.

Regulations on Static Password

-Use 6-12 degits.
-Alphanumeric (Uppercase and lowercase are used interchangably.)
-The following symbols are usable.(_ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < >)

STEP2:Enter numbers according to your Secret Pattern made in the STEP1, and enter your Static Password following the numbers. Then press "Next."
*Please make sure that you do not lose your Secret Pattern and Static Password!

Change password message2：
2.3.2 以前：STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.
2.4.0 以降：[Second Input (2/3)]

Enter numbers according to your Secret Pattern. And enter your Static Password following the numbers.
(*Numbers in the matrix are changing every time.)
Then press "Next."

Change password message3:
2.3.2 以前:STEP.1 Please enter the pattern from the matrix.
STEP.2 Please again enter the same pattern from the matrix.
STEP.3 Please again enter the same pattern from the matrix to confirm.
STEP.4 Done.
2.4.0 以降:[Second Input (3/3)]
Enter numbers according to your Secret Pattern. And enter your Static Password following the numbers.
(*Numbers in the matrix are reformed.)
Then press "Next."

Navigation to reset pattern:
2.3.2 以前:Enter your username and registered e-mail address, and click the [next].
Then instructions to reset your secret pattern is sent to you.
2.4.0 以降:Enter your User ID and registered e-mail address, and click the [next].
Then instructions to reset your Secret Pattern is sent to you.

Register the following settings for expiration prior notice of the validity period.

Phrase setting [Config] > [Policy Settings] > (PassLogic Authentication) [Edit] > [Mail to expiration date closer user] from the left menu on the management tool.

Template (Reference values)

【件名】
PassLogic パスワード有効期限のお知らせ
【本文】
<%UNAME%> 様

パスワードの有効期限についてお知らせします。

パスワード有効期限:<%EXPIRE_DATE%>

期限が切れる前にパスワードを再設定してください。

■ログインページの URL
https://[PassLogic サーバ FQDN]/ui/

【PassLogic の利用に関するお問い合わせ先】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

1.12 Uninstalling

Uninstall the PassLogic authentication server software.

```
(Execute with root privileges)
# cd passlogic-ent-x.x.x/
# ./install.sh uninstall
PassLogic Authentication Server Software をアンインストールするとすべてのデータが削除されます。よろしいですか？ - if uninstalling PassLogic Authentication Server Software, all data is gone
[yes or no]
(Enter yes.)
```

*Restart OS after uninstall is done.

*Uninstall rpm package manually.

2 System administrator guide

2.1 Creating administrator account

One of the following management privileges can be assigned to a PassLogic administrator account.

Administrator privileges

	All administrator functions	Create, edit, delete and disable users, and user lock and terminal fixing	Unlock and reissue password
admin	○	○	○
useradmin	×	○	○
operator	×	×	○

<<Registration steps>>

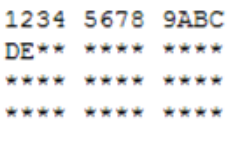
(i) Click [Admins] > [Create New Admin] from the left menu on the management tool.

(ii) Edit as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Save].

<<Item explanation>>

[uid] (required)	Enter a user ID. Alphanumeric (case-sensitive) characters and the following three symbols can be used. (1 to 30 characters) . (period) - (hyphen) and _ (underscore)
[role] (required)	Select an administrator privilege.
[E-mail address]	It is required when notifying user creation results by e-mail. 255 characters maximum
[User Name]	255 characters maximum
[Employee number]	255 characters maximum
[Section]	255 characters maximum
[Phone]	255 characters maximum

[Secret pattern] (one-time password)	Specify initial values of the secret pattern. A notification example is shown below.  1234 5678 9ABC DE** **** **** **** **** **** **** **** **** ＊ Use alphabets [A-Z,a-z] for 10 digits or more. ＊ Random generation is enabled by checking the [Set secret pattern randomly] checkbox.
[Static password]	Specify an initial value of the static password appended after the one-time password. Alphanumeric (case-sensitive) characters and the following three symbols can be used for the static password. _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & ＊ = | ; " < > *Unable to use a comma and a colon *This is not a required field. If not specified, password is only secret pattern.
[Active / Inactive] (required)	Select to enable or disable an account.
[Expiration date]	Set an effective period of an account. *An account is valid until a set date. *Even after the effective period of an account expires, the account remains on the management tool; therefore, if the account needs to be deleted, it must be deleted explicitly. ＊ After the effective period of an account expires, the effective period can be extended with the management tool, and its setting information is maintained.
[Notes]	255 characters maximum

2.2 Setting policy

PassLogic can use multiple security policy. One user is applied to one policy. After installation, the "Default Policy" is only registered. "Default Policy" is a template data of policy to add.

*Administrator accounts are applied to the "Default Policy".

<<Policy additional steps>>

(i) Click [Config] > [Policy Settings] from the left menu on the management tool and click [Add].

(ii) Edit the policy name (alphanumeric, - (hyphen), _ (underscore) only, First letter is required alphabetic character or underscore. , 30 characters maximum), and click [Next].

(iii) Confirm the contents you have entered, and click [Save].

(iv) Click "return" link > "Edit" link on the right of added policy name.

(v) Edit the policy settings as necessary, and click [Next].

(vi) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

Authentication General	
[Authentication Method]	Select PassLogic or PassClip. *"Default Policy" is only PassLogic.
[Maximum Failure]	If a user fails authentication sequentially up to the number set here, the user is locked. 0 indicates no lockout will be performed.
[Lockout Duration]	Automatically release lockout after specified seconds. Check [until unlocked by an administrator] not to automatically release lockout.
[The time of day when users can be authenticated]	Set a time period during which authentication is possible. When the end time is earlier than the start time, the end time is considered as the following day. (Example: When Start time 18:00 and End time 06:00, authentication is possible from 18:00 to 06:00 on the next day)
[Device restriction]	Fix terminals (browsers) for which user authentication is possible. Cookie value specification Fixing (default) : Use the first cookie value persistently. Change : Cookie value changes each time of login. It's possible to set "Fixing" "Change" the cookie value (default Fixing). Please set if necessary. *Up to five terminals can be registered for one user.

[Save AD Password]	When login to Active Directory succeeds, the AD password is saved. An AD user whose AD password is saved, he/she does not have to enter the AD password from the following login.
[Attribute and parameter]	When permitting the user parameter change, please input a check and name. Please refer to "4.1User's parameter setting" for details of parameter change.
[Last login display]	To display last login date to users, please put the check. "No data" is shown to the user logged in for the first time.
[Account expiration display]	To display account expiration date to users, please put the check. "Indefinite" is shown to the user who doesn't have the expiration date. *Config>UI Settings Indefinite
PassLogic Authentication	
[Validity Period of a Random Number Table] *1	Set an effective period of a random number grid. When the set time is exceeded, a correct password on the PassLogic authentication server is deleted. A new random number grid needs to be obtained for authentication.
[History Count] *1	Prohibit a secret pattern setting that is identical with the last n times.
[The validity period of a pattern] *2	Set days to periodically force to change a secret pattern. A periodical change is not necessary, when [unlimite] is checked.
	If the validity period has limited, send email to the user that will be expiring in a specific period. The input form of days is necessary to set a smaller number than the validity period.
[Password expiration display]	To display password expiration date, please change the settings. 'YYYY/MM/DD': It displays the password expiration date in the format. 'CountDown': It displays the remaining number of days that the password is valid. "Indefinite" is shown to the user who doesn't have the expiration date. *Config>UI Settings Indefinite

[Require to change the initial pattern]	Force users to change their passwords after initial access.
[Enable password change]	When permitting the user change password, please input a check. Otherwise, When [Require to change the initial pattern] is checked or [The validity period of a pattern] has expired, the user can change password.
[Require current password to change the initial pattern]	Set whether or not to request current password for confirmation before changing the password,
[Size of Passlogic grid]	Set Row and Col of Passlogic grid size(max value: row 4, col 12)
[Length range of One-Time Password] *1	Specify the length of a one-time password. *Set the minimum and maximum from 0 to 64.
[Length of an Auto Generated Pattern (One-Time Password)] *1	Set the length of a secret pattern, when it is randomly created. **Generated by 2 lines** It generate a simplified random pattern of 2 lines. It can be used when 'Size of Passlogic grid' is '4*12' and 'Length of an Auto Generated Pattern(OTP)' is 8 or less.
[Length range of static password] *1	Specify the length of a static password (fixed password). *Set the minimum and maximum from 0 to 64. *Alphanumeric (case-sensitive) characters and the following symbols can be used for a static password. _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < > (Unable to use a comma and a colon)
[Length of an Auto Generated Pattern (static password)] *1	Set the length of a static password, when it is randomly created. It is generated with number, lower case and upper case. (0, 1, l, I and O are excluded.)
[Restriction of a secret pattern] *1	Disabled a simplistic secret patterns. **Disable a traversable pattern** Prohibit the secret pattern from the start point to the end point can be written one stroke. *3 **One or more numbers have to be selected from each blocks.** requires to select from all three blocks of 4*4. **Forbidden secret pattern(s)** Set a secret pattern that users cannot use. *It is not partial matching, but complete matching.

[Password reminder]	Set whether a user can use the password reissuing function, when a user forgets his/her password.
[Web Token]	Set whether or not to use Web Token.
[Display guide in grid]	Set whether or not to use grid guide.

*1：Applied also to administrator accounts.

*2：Though an administrator account can login the management tool even after the secret pattern's effective time expires, [[!]The validity period of a pattern is expired.] is continually displayed in red on the top part of the screen after login.

*3：The secret pattern that adjacent positions of the eight directions around the specific position (vertical, horizontal and diagonal) is continuous.

2.3 Setting user notification

Set an e-mail template to send to PassLogic users for each policy.

<<Setting steps>>

(i) Click [Config] > [Policy Settings] from the left menu on the management tool.

(ii) Click "Edit" link on the right of the policy name.

(iii) Edit the User Notification Settings, and click [Next].

(iv) Confirm the contents you have entered, and click [Submit].

Configure e-mail addresses of the user notification From, Cc and Bcc that is sent from PassLogic.

Sender e-mail address	It is able to set up only one.
Cc	Carbon copy e-mail address (es). * It is able to set up multiple addresses separated by commas.
Bcc	Blind carbon copy e-mail address (es). * It is able to set up multiple addresses separated by commas.

The following notification templates are available. Select, edit and use a notification template according to your purpose.

1)	PassLogic authentication [Mail to a new user]	E-mail template for new PassLogic authentication user. Please include how to start to use PassLogic for users such as login URL, user ID and initial password.
2)	PassLogic authentication [Mail of password reissue]	E-mail template of password reissue for PassLogic authentication user. Please include how to log in using new password.

3)	PassLogic authentication [Mail of password reminder]	E-mail template of password reminder for PassLogic authentication user. Please include password reset URL.
4)	PassLogic and PassClip [Mail of device restriction activate]	E-mail template for second or more devices to activate. Please include activation key. *First device is registered automatically at the first authentication success.
5)	PassClip authentication [Mail to new user]	E-mail template for new PassClip authentication user. Please include how to log in such as PassClip activate URL, login URL and user ID.
6)	PassClip authentication [Mail of PassClip resetup]	E-mail template for users when reactivating PassClip. Please include PassClip activation URL.
7)	PassLogic authentication [Mail to expiration date closer user]	E-mail template of expiration date closer user for PassLogic authentication user. Please include expiration date.

*1) 2) 3) 7) Authentication method "PassLogic" only.

*5) 6) Authentication method "Passclip" only.

<<Replacement tag definition>>

When embedding variable information for each user on a notification template, use the following items.

<%UNAME%>	Name
<%UID%>	PassLogic user ID
<%DOMAIN%>	Domain name
<%PASSLOGICPATTERN%>	Secret pattern of PassLogic
<%SPASSWORD%>	Static password (fixed password) to append after the one-time password
<%ENTRYKEY%>	URL key for device activation
<%REMINDER_URLKEY%>	URL key when using the password reminder
<%PASSCLIP_URL%>	URL key for PassClip activation
<%EXPIRE_DATE%>	Expiration date of the password

*Replacement tags can be used only in the Body of e-mail. They cannot be used in Subject.

*Change the URL "https://remote.example.com/" for the initial value login page of notification template to an appropriate URL.

2.4 Mail Server Settings

Perform settings for the e-mail server to handle outgoing e-mails from PassLogic.

<<Setting steps>>

(i) Click Management tool left menu [Config] > [Policy Settings] > Default Policy “Edit” link.

(ii) Edit the Mail Server Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[SMTP Server]	IP address or hostname of SMTP server
[SMTP Server port]	Port for SMTP server
[SMTP-AUTH User Name(SMTP-AUTH)]	User ID when using SMTP-AUTH
[SMTP-AUTH Password (SMTP-AUTH)]	Password when using SMTP-AUTH
TLS/SSL	Select when connecting with TLS or SSL

2.5 Setting logs

Perform settings on the management and usage logs of PassLogic.

<<Setting steps>>

(i) Click Management tool left menu [Config] > [Policy Settings] > Default Policy “Edit” link.

(ii) Edit the Log Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[Log Level]	Select a minimum set of log levels. When a particular level is specified, messages from all other levels of higher significance will be reported as well. *Look at the ″Log reference″ section in this manual about each logs. Default value: notice
[Logging with Syslogd]	When set to ON, the same information as /var/log/passlogic/passlogic.log is also output to syslog. Default value: off

2.6 settings.conf

The following parameters are system unique settings.

Edit the /opt/passlogic/data/conf/settings.conf file on PassLogic authentication server.

Item	Settings	Value
PL_SESSION_TIMEOUT *1	Session time out period (seconds)	Default value: 900
URL_HANDLER_SHOW *2	Define a part of User-Agent of web browsers to display links for special URI scheme (such as anyconnect://) on PassLogic user's menu page (This affects only SSL-VPN).	Default value: Android|iPhone|iPad
PASSCLIP_SERVER_URL *2	Activation URL of PassClip server *Please do not edit the default value.	Default value: http://appscheme.passclip.com/?mode=passlogic&query=
MULTI_LOGIN *2	Permit or not multiple login for one user at the same time..	Default value: 1 *3
DOMAIN_PULLDOWN *5	Set whether to display a pull-down to select a domain when a user name input. Enter your user name in the format of "user name @ domain name", If you do not want to display. *4	Default value: 1 Not dislay: 0 Display: Other than 0
DISABLE_SAVED_AD_PASSWORD *6	If the AD password is saved, then the password input field will be in inactivate state.	Default value: 0 Active state: 0 Inactive state: 1

*1 : If change the session time out value, Edit the following file also.
"AuthPasslogicExpire" value in /opt/passlogic/data/conf/xauth_passlogic_00.conf. Set a same value as PL_SESSION_TIMEOUT, and restart httpd.
"PL_SESSION_TIMEOUT" in settings.conf is the session time out period for user interface and management tool. "AuthPasslogicExpire" in xauth_passlogic_00.conf is the session time out period for PassLogic reverse proxy server.

*2 : If updated from PassLogic ver.1.3.0 or lower versions, Add the Item to settings.conf file.

*3 : If set "0", Previous session is forced to logout and latest session is useful.

*4: If you enter only the user name, without entering the "@ domain name", it is treated as a local user.

*5: If updated from PassLogic ver.2.2.1 or lower versions, Add the Item to settings.conf file.
*6: If updated from PassLogic ver.2.3.2 or lower versions, Add the Item to settings.conf file.

2.7 Setting groups

Group is a user group to restrict access to backend services. The number of groups that can be managed is unlimited, however the maximum applying number per user is up to 5 and the number per service is up to ten.

<<Steps to add a group>>
(i) Click Management tool left menu [Config] > [Group Settings] > [Add].
(ii) Enter a group name (alphanumeric, - (hyphen), _ (underscore) only, 20 characters maximum), and click [Next].
(iii) Confirm the contents you have entered, and click [Save].
*About how to apply group to user, please look at the "Createing new user" section in this manual.
*About how to apply group to service, please look at the access group of "SSL-VPN > SSO - Single sign-on", "WebAPP", "Cloud > Registering SP" section in this manual.

<<Steps to delete a group>>
(i) In the [Group list] screen, click [delete] on the line of the group to delete.
(ii) Click [OK] in the confirmation dialog box.
*Groups to which members belong or used in the access group settings cannot be deleted.

<<User search with group name>>
Click the link of a group name, a list of users from the group can be retrieved.

2.8 Setting UI (User Interface)

Edit the logo and the message on the user interface.

<<Steps to edit UI>>

(i) Click Management tool left menu [Config] > [UI Settings] > [Edit].

(ii) Edit the messages as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

*If add other language, Click [Add] button.

*If browser top priority language is “ja”, Japanese is the initial language. In other cases, English is the initial language.

<<Steps to change logo file>>

(i) Click Management tool left menu [Config] > [UI Settings] > [logo upload].

(ii) Select a new logo file, and click [Send].

*If click the delete link, uploaded file is deleted and return to the original logo.

*Specification of logo file

Size:	Width 154 pixel, Height: 22 pixel
Format:	PNG (transparent)

*A logo file cannot be updated with IE9. Use other browsers.

*The user interface is the following URL.

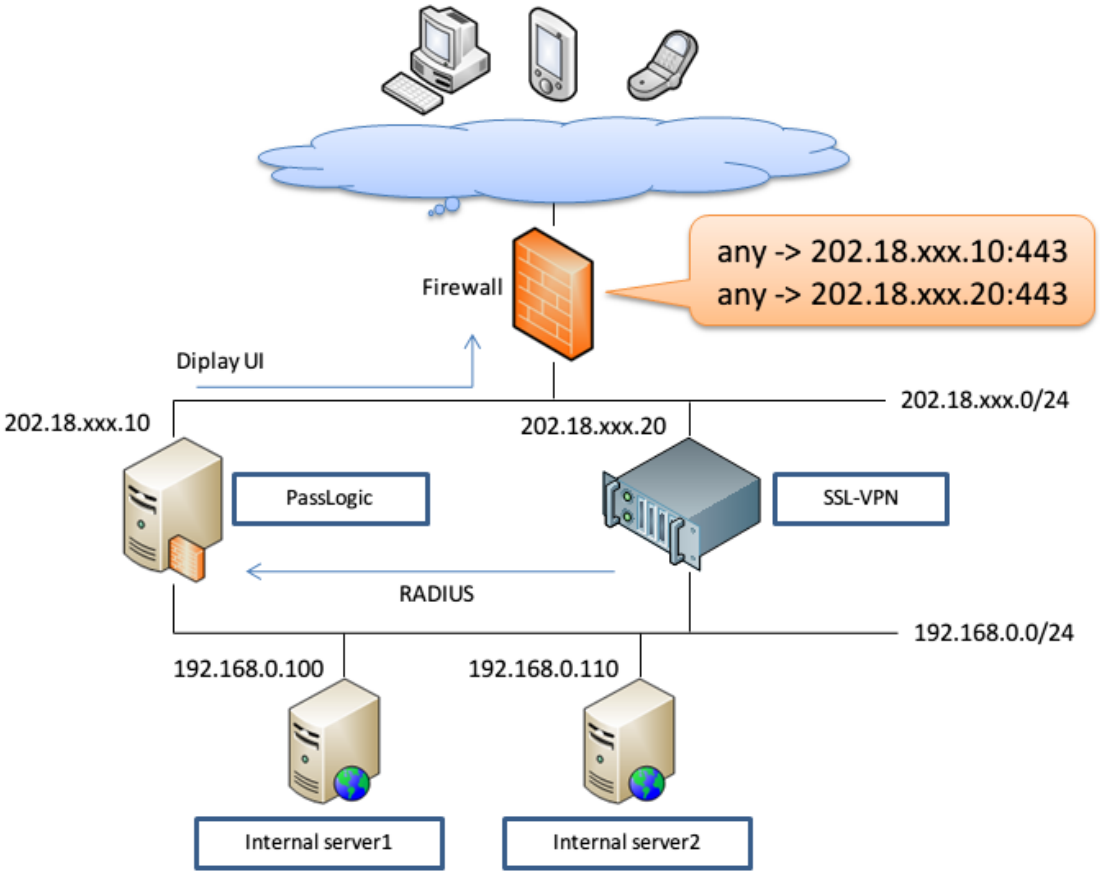
https://[PassLogic Server]/ui/

2.9 SSL-VPN

When the PassLogic authentication server is installed, the RADIUS server extended for PassLogic runs.

Therefore, an authentication linking is possible with RADIUS of a SSL-VPN device.

PAP, CHAP, and MSCHAPv1 and v2 are supported authentication methods.



Client Setting

Register a SSL-VPN device using the PassLogic management tool.

<<Setting steps>>

(i) Click Management tool left menu [SSL-VPN] > [Client Settings] > [Add].

(ii) Edit the Client Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Save].

<<Item explanation>>

[Shortname]	Identifier on PassLogic. Alphanumeric characters,- (hyphen) and _ (underscore) can be used. (1 to 31 characters).

[IP address]	IP address or hostname of a RADIUS client to access.
[Secret]	Shared secret string.
[Attributes for each user]	When an attribute is necessary for each user, enter an attribute name. Refer to RFC2865 (http://freeradius.org/rfc/attributes-rfc2865.html), etc., and enter only the attributes that can be appended to Access Accept packets of RADIUS. * Attribute 1 to 10 of a SSL-VPN device registration during user registration (User information CSV batch loading item attribute 1 to 10) are supported as attribute values.

SSO - Single sign-on

Using Single sign-on, users can skip logging in page on SSL-VPN.

*Contact our technical support about the integration with SSL-VPN.

<<Setting steps>>

(i) Click Management tool left menu [SSL-VPN] > [SSO] > [Add].

(ii) Edit the SSO Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[No.]	Enter the sort number (ascending) of the user's menu after log in to PassLogic. Set 0, not to display on the menu (skip the menu screen is possible).
[Application Name]	Specified name displayed on the menu after login to PassLogic.
[Destination URL where SSO information should be posted] *1	Specify a URL to send login information to SSL-VPN.
[Name of LoginID]	Enter a name of the login ID (User ID) name attribute used for SSL-VPN login. (Example: UserID) *The corresponding attribute value is a "Value of LoginID" formatted strings.

[Value of LoginID]	Select a form of the login ID (User ID) from [Uid Only], [PassLogic Domain (uid@PassLogic Domain)], [ActiveDirectory Domain (uid@AD Domain)] or [NT Domain (NT Domain¥uid)]. *PassLogic Domain refers to "Domain Name" of the Domains list screen. *Active Directory Domain and NT Domain refer to "Active Directory Domain Name or NT Domain Name" of LDAP Settings of Domains. *When the "local" domain user tries SSO, always the form of login ID is treated as [Uid Only]. *When the user without [Active Directory Domain name or NT Domain name] tries SSO, the form of login ID is treated as [Uid Only].
[Name of Password]	Enter the name of the name attribute of the password used for SSL-VPN login. (Example: Password) *This attribute value is a one-time password for PassLogic RADIUS Server. The one-time password is generated automatically by the system.
[AD password]	Check to send the password of Active Directory when logging in to the SSL-VPN (same password that the user entered when logging in to PassLogic). After checked, enter a name of the AD password name attribute. (Example: ADpassword) *This attribute value is the AD Password on PassLogic login.
[Access Group]	Select a group to permit access. *If not specified, all users are available.
[HTTP Method]	Select GET or POST.

[Web application login page URL]	Set the URL of a login page, only when it is necessary to acquire specific HTML entity contained in the login page before sending login information. *Acquired entity is sent to the destination URL of authentication along with login information. [Retrieval data name from login page]*2 Enter a name of an entity, when there is an HTML entity to acquire from a login page. (Example: SESSION_TOKEN)
[Additional parameters]	Set parameters other than a login ID and a password necessary for application login. It is different per application.
[Parameters of each user]	Specify a name attribute of a parameter to POST per user. Single sign-on param1 to 10 during user registration (user information CSV batch loading item sslvpn param1 to 10) are supported as value attributes. will be the price the user after login established from password1 to 5.

*1：Special URI scheme other than http or https can be registered (example: anyconnect://). When using special URI scheme, the following replacement tag is available in the URI.

<%AUTHID%>	Login ID (“Value of LoginID” formatted strings)
<%PASSWORD%>	Authentication Password
<%PARAM1%>	User’s value: sslvpn param1
<%PARAM2%>	User’s value: sslvpn param2
<%PARAM3%>	User’s value: sslvpn param3
<%PARAM4%>	User’s value: sslvpn param4
<%PARAM5%>	User’s value: sslvpn param5
<%PARAM6%>	User’s value: sslvpn param6
<%PARAM7%>	User’s value: sslvpn param7
<%PARAM8%>	User’s value: sslvpn param8
<%PARAM9%>	User’s value: sslvpn param9
<%PARAM10%>	User’s value: sslvpn param10
<%USERPASS1%>	User’s value: password1
<%USERPASS2%>	User’s value: password2
<%USERPASS3%>	User’s value: password3
<%USERPASS4%>	User’s value: password4

<%USERPASS5%>	User's value: password5

*2:Depending on VPN devices, there may be entities with values that are dynamic, which are generated automatically when accessed to a login page.

Example:

```
<form method="post" name="VPNForm" action="login.cgi">
Login name: <input type="text" name="user_id"><br />
Password: <input type="password" name="password"><br />
 <input type="hidden" name="SESSION_TOKEN" value="[Dynamic value]">
<br />
<input type="submit" name="submit" value="Login">
<input type="hidden" name="mode" value="login">
</form>
```

* By specifying "SESSION_TOKEN" in [Retrieval data name from login page] for a login page above, the PassLogic authentication server acquires a dynamic value from the HTML source, and send a name=value pair to a VPN device.

Web Token

Using Web Token enables direct login to SSL-VPN without login to PassLogic menu. The grid of one-time password for SSL-VPN login can be displayed on PC or smart devices.

Web Token URL

```
https://[PassLogic Server]/ui/token.php?uid=[uid]&domain=[domain]
```

*Only user of Web Token available policy.

*If Web Token available user, Web Token link appears on PassLogic menu. This link is same URL as the above URL. By bookmark of the link, user can access the Web Token directly.

*If Authentication Method of the user policy is "PassClip", please use the password which made by PassClip instead of "Web Token" to login to SSL-VPN.

*"@domain" is required as a part of username that you input to SSL-VPN login page. In case that domain is "local", @local can be removed.

RADIUS authentication operation (reference)

Examples for authentication operation by radclient are shown next. Actual operation differs depending on applications or devices.

・PAP

```
# echo "User-Name=test, User-Password=8283" |
radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 44 to 192.168.0.203 port 1812
        User-Name = "test"
        User-Password = "8283"
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=44,
length=20
```

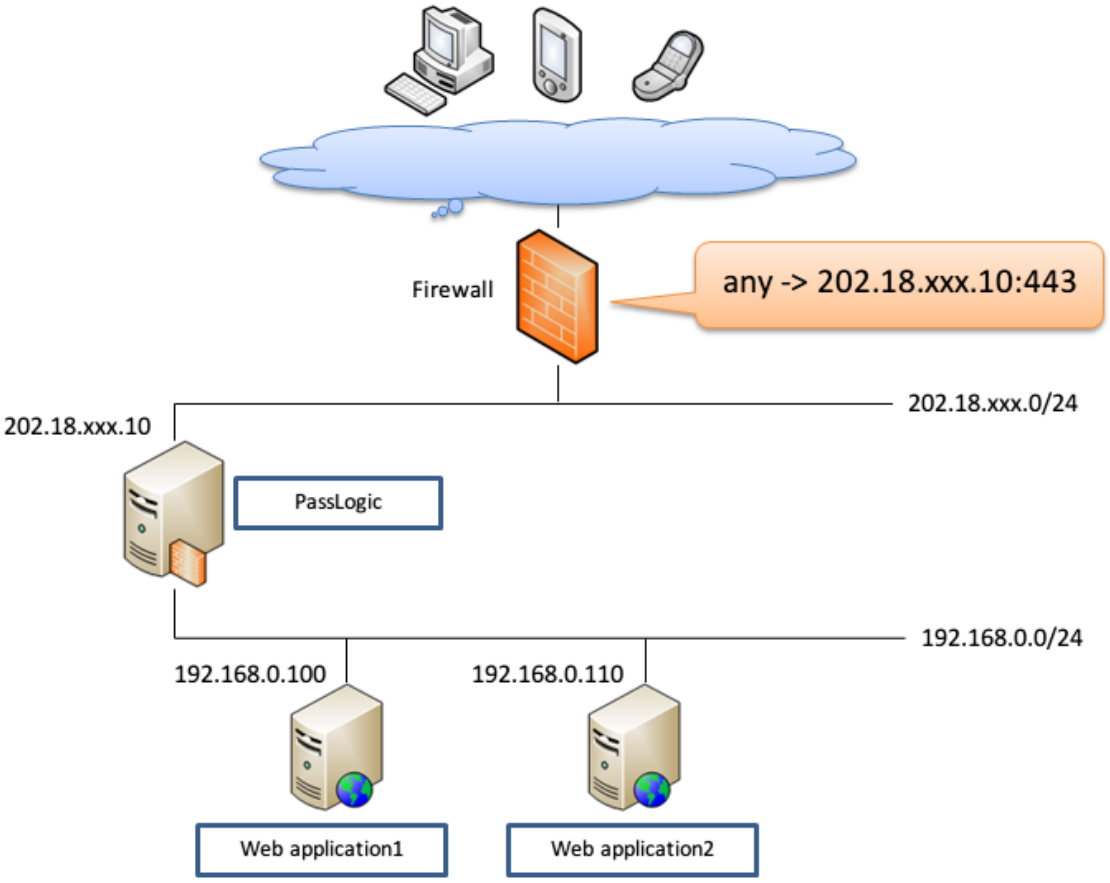
・CHAP

```
# echo "User-Name=test, CHAP-Password=0772" |
radclient -x 192.168.0.203 auth secret
Sending Access-Request of id 42 to 192.168.0.203 port 1812
        User-Name = "test"
        CHAP-Password = 0x2a49ec0d72c3bbc6dbe850ef2edda47f32
rad_recv: Access-Accept packet from host 192.168.0.203:1812, id=42,
length=20
```

2.10 WebAPP

This function enables users to access internal web applications remotely through PassLogic because PassLogic is running as a reverse proxy.

Example of remote access network



Because a user ID after authentication is contained in the http header and sent to internal application, it can be used for web application implementation.

http header example (User ID: testuser)

```
Accept: */*
Accept-Language: ja
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
Host: www.example.com
PL-Uid: testuser
PL-Authid: testuser@local
Connection: Keep-Alive
```

Implementation example when an authenticated user ID is acquired with an application

```
<?php
$uid = $_SERVER['HTTP_PL_UID'];
$authid = $_SERVER['HTTP_PL_AUTHID'];
?>
```

WebAPP

Map a local application URL and a virtual path, and perform reverse proxy settings.

<<Setting steps>>

(i) Click Management tool left menu [WebAPP] > [WebAPP] > [Add].

(ii) Edit the WebAPP Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[No.]	Enter the sort number (ascending) of the user's menu after log in to PassLogic. Set 0, not to display on the menu (skip the menu screen is possible).
[Application Name]	Specified name is displayed on the menu page after login to PassLogic. Enter a name. * &(ampersand), #(number sign), and +(plus sign) cannot be used.
[Local virtual path]	Enter a path when access an application. *The following path cannot be used. "/" "/passlogic-admin/" "/passlogic/" "/ui/"
[URL for the remote server]	Specify the URL of a local application. If the application server is an IIS server, put a checkmark in the checkbox.
[Access Group]	Select groups that can have access. *If not specified, all users are available.
[URL Mapping Rules] *1	Map a URL for local application image, JavaScript, CSS, etc. to a directory, so that it can be referred. [Virtual path]: Allocated path [Partial URL]: Local URL applied to a virtual path *Virtual path that overlap in the system cannot be specified.

[Rewrite HTML response body] *2*3*4	Convert local application contents. Enter characters to search and replace in contents. [String to search]: Characters to be replaced [String to replace]: Characters after replacing. They are case sensitive. Regular expression is not supported.

*1:Perform URL mapping setting by referring to the httpd error log. (Set that no errors are output on all pages in a Web application.)

Command example

```
tail -f /var/log/httpd/access_log | grep 404
tail -f /var/log/httpd/ssl_access_log | grep 404
```

*2:Symbol "|" (pipe) and spaces (single byte space) cannot be used for characters to both search and replace.

*3:Applications that send compressed contents (gzip compressed contents, etc.) are not compatible.

*4:Characters used for searching and replacing are UTF-8. In applications that Japanese character code is not UTF-8, Japanese characters cannot be converted.

WebSSO

WebSSO enables automatic form authentication for web applications. The integration of web applications with PassLogic can skip logging into each web application.

A form authentication is a method that users are authenticated by sending user specified necessary information instead of using the standard authentication function of web servers and web browsers, "Basic authentication". For example, users are authenticated by entering either their e-mail address and password or User ID and password.

Following methods are compatible with WebSSO (automatic form authentication) of PassLogic.

Data sending method	POST data
	Query String (GET data)
Session managing method after authentication	Notification to browsers by cookie headers
Operation after authentication	Without redirecting
	Redirect with location headers (to other URL)
	Redirect with location headers (to same URL)

<<Setting steps>>

(i) Register a definition of WebAPP for WebSSO.

(ii) Click Management tool left menu [WebAPP] > [WebSSO] > [Add].

(iii) Edit the WebSSO Settings as necessary, and click [Next].

(iv) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[Application Name]	Select applications registered with WebAPP. Specify applications to make compliant with WebSSO.
[Name of LoginID] *1	Enter a name of the name attribute of the login ID (User ID) used for application login. (Example: UserID) *The corresponding value is a uid of PasssLogic.
[Value of LoginID]	Select a form of the login ID (User ID) from [Uid Only], [PassLogic Domain (uid@PassLogic Domain)], [ActiveDirectory Domain (uid@AD Domain)] or [NT Domain (NT Domain¥uid)]. *PassLogic Domain refers to "Domain Name" of the Domains list screen. *Active Directory Domain and NT Domain refer to "Active Directory Domain Name or NT Domain Name" of LDAP Settings of Domains. *When the "local" domain user tries SSO, always the form of login ID is treated as [Uid Only]. *When the user without [Active Directory Domain name or NT Domain name] tries SSO, the form of login ID is treated as [Uid Only].
[AD password]	When you send the login parameters to the application, and then send the AD password. Specify the name attribute of AD password at [Name of AD password].
[HTTP Method]	Select GET or POST.
[Way of posting a password] *1	Select an “Automatic auth. for server side”, “Automatic auth. for client Javascript” or “SSO program of specific application”.

[Web application login page URL.] *2	Set the URL of a login page, only when it is necessary to acquire specific information (entity) contained in the login page. *Enter a URL that can be accessed from PassLogic authentication server. *The acquired entity is sent along with the login information to the destination URL. [Retrieval data name from login page] Enter the name of an entity, when there is an entity to acquire from the login page.
[Destination URL where SSO information should be posted]	Enter a URL for login in addition to the URL defined in WebAPP. If not specified, logging into the URL of a local application is tried. *If Way of posting a password is “Automatic auth. for server side”, Enter a URL that can be accessed from PassLogic authentication server. * If Way of posting a password is “Automatic auth. for client Javascript”, Enter a URL that can be accessed from Client via PassLogic proxy server.
[Additional parameters]	Set parameters other than a login ID and a password necessary for application login. It is different per application.
[Parameters of each user]	Specify the name attribute of a parameter to POST per user. WebSSO param1 to 10 during user registration (user information CSV batch loading item websso param1 to 10) are compatible as value attributes. will be the price the user after login established from password1 to 5.

*1:Because name attributes on login ID and password are different in each application, check the HTML source in each application's login page.

```
Sample of HTML source of application's login page.
<form method="post" name="LoginForm" action="login.cgi">
Login ID: <input type="text" name="user_id"><br />
Password: <input type="password" name="password"><br />
<br />
<input type="submit" name="submit" value="login">
<input type="hidden" name="mode" value="login">
</form>
```

In the example above, Register the following settings.

[Name of LoginID] : user_id

[Parameters of each user] param1: password

Application password is set into websso param1 of each user.

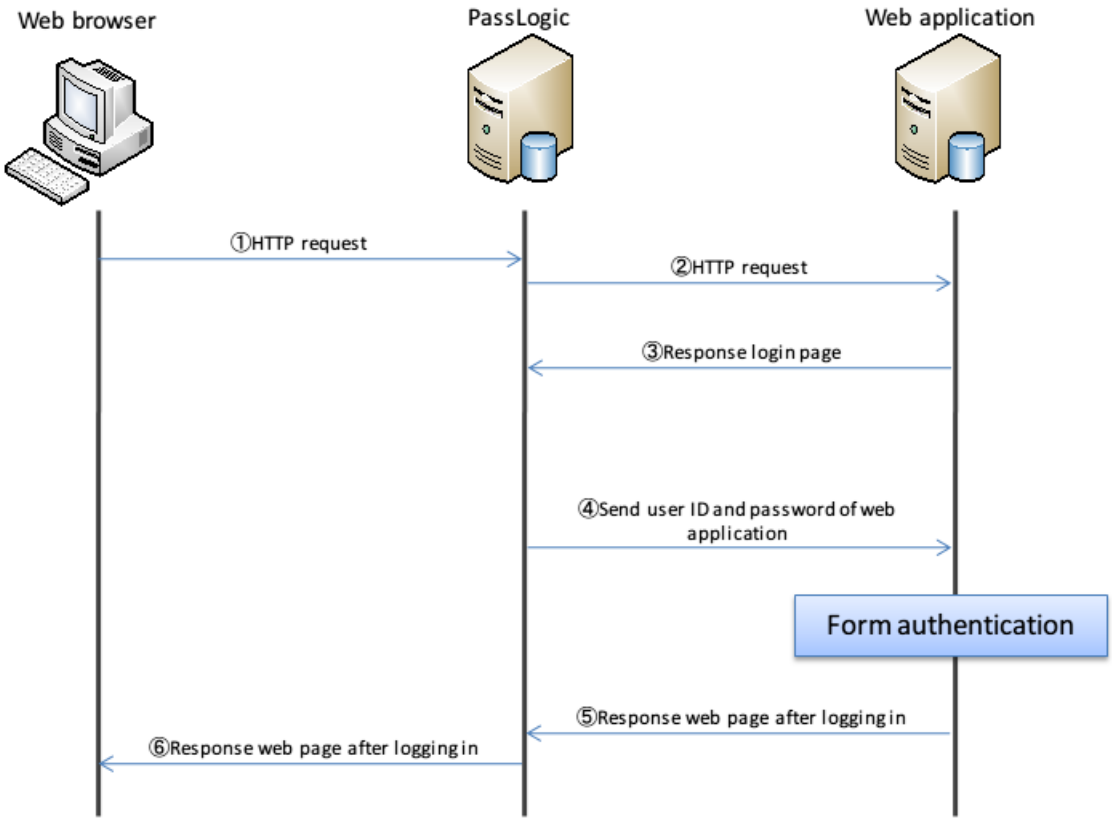
[Additional parameters]

[Name of a paramater] : mode

[Value of a parameter] : login

*2:The difference between " Automatic auth. for server side" and " Automatic auth. for client Javascript" is shown below. Typically, select " Automatic auth. for server side". When WebSSO does not function with " Automatic auth. for server side", " Automatic auth. for client Javascript" is used.

Sequence figure of Automatic auth. for serverside

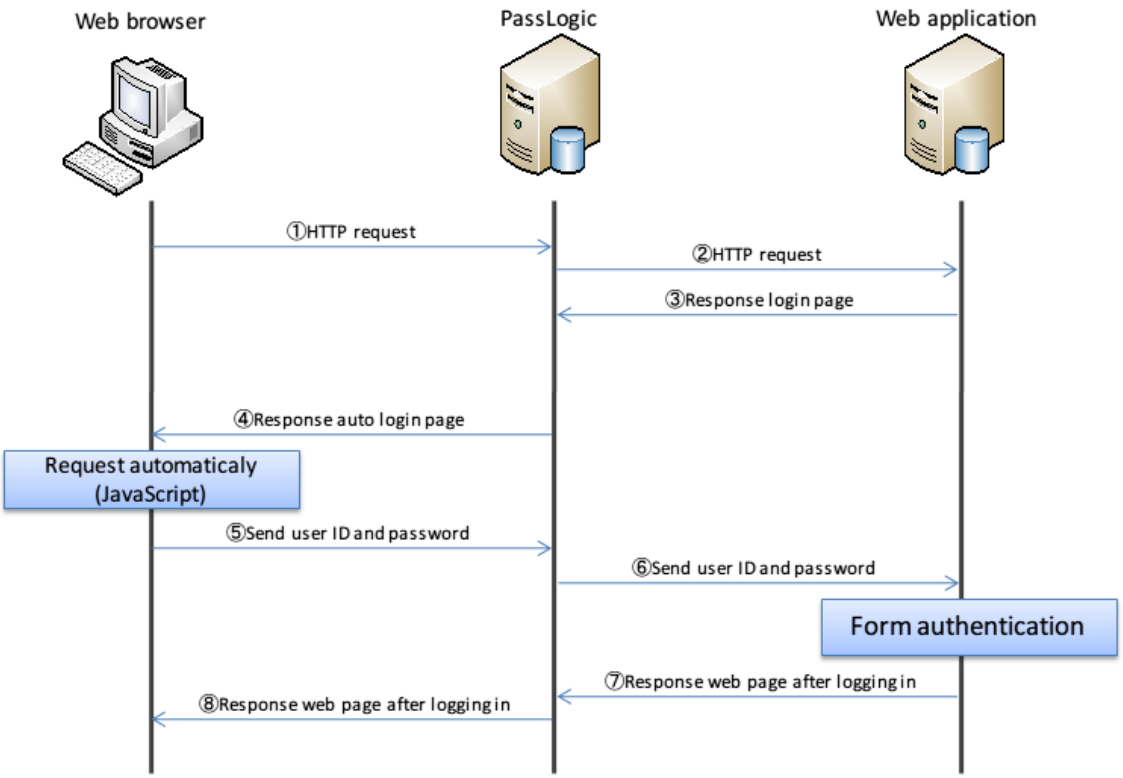


The PassLogic authentication server sends a user ID and a password to an application as a proxy. Depending on applications, logins may not succeed, but it is a secure method, since user IDs and passwords of an application are not exposed to external network.

*Because it does not support applications that conduct automatic redirection after login, use a client authentication (JavaScript) instead.

*It is not compatible with applications that send encrypted passwords with JavaScript on login.

Sequence figure of Automatic auth. for client Javascript



An applicable range becomes wide, because it goes through a client (web browser) once; however, user IDs and passwords of an application are exposed to external network, so that avoid security risks by connecting with SSL.

Example of HTML sending to a client (Sent after automatically generated with a PassLogic authentication server and automatically processed with JavaScript)

```
<html>
<head>
<title>PassLogic Auto Login Agent</title>
<script language="javascript" type="text/javascript">
<!--
window.onload = function login() {
        document.form1.submit();
}
-->
</script>
<body>
<form name="form1" method="POST" action="/login.cgi">
<input type="hidden" id="user_id" name="user_id" value="USER" />
<input type="hidden" id="password" name="password" value="PASSWORD" />
<input type="submit" name="login" value="login">
</form>
<div align="center">PassLogic Auto Login Process</div>
</body>
</html>
```

2.11 Cloud

Authentication linking with SAML (Security Assertion Markup Language) 2.0 is available.

Registering SP

Register a SP (Service Provider) to PassLogic management tool.

<<Setting steps>>

(i) Click Management tool left menu [Cloud] > [SP Settings] > [Add].

(ii) Edit the SP Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

<<Item explanation>>

[No.]	Enter the sort number (ascending) of the user's menu after log in to PassLogic. Set 0, not to display on the menu (skip the menu screen is possible).
[Provider Name]	Enter name which is displayed on the menu page after login to PassLogic.
[SAML Type]	Select either [SP initiated SSO] or [Idp initiated SSO]. It depends on specifications of a service provider.
[UID Type]	Select whether to contain or not contain a domain name in the user name sent to a service provider.
[Domain]	Enter a domain name.
[RelayStateURL]	Destination URL after the SAML authentication. Enter according specifications of a SP.
[Recipient]	SP ACS URL, Destination of SAML response. Enter according specifications of a SP.
[Destination]	SP ACS URL, Destination attribute's value in SAML response. Enter according specifications of a SP.
[Issuer]	IdP EntityID・Issuer attribute's value in SAML response. Enter according specifications of a SP.
[Audience]	Audience attribute's value in SAML response. Enter according specifications of a SP.
[PassLogic FQDN]	Enter a part of the URL for PassLogic users. "http(s)://<PassLogicFQDN>" *Required for Idp metadata download.
[Attribute mapping] 1-5	Enter sets of key and value as SAML Response attributes, according specifications of a SP.
[Access Group]	Select groups that can access. *If not specified, all users are available.

*In case of SP initiated SSO, SAML Request reciever is the following URL.
http(s)://[PassLogic FQDN]/ui/idp.php?target=[Provider Name]

Certificate

Upload a set of certificate and private key for SAML to PassLogic management tool.
*Please prepare the set of certificate and private key by yourself.

<<Certificate uploading steps>>
(i) Click Management tool left menu [Cloud] > [Certificate].
(ii) Click [Select] on the right of “Certificate” > “Upload”, and select a certificate file.
(iii) Click [Save] at the right of [Select].
*When you upload the certificate file with the correct format, the issuer information and the expiration date will be displayed.
*If you click “Download”, then you can download certificate file that has been uploaded.

<<Private key uploading steps>>
(i) Click Management tool left menu [Cloud] > [Certificate].
(ii) Click [Select] on the right of “Private Key” > “Upload”, and select a private key file.
(iii) Click [Save] at the right of [Select].

2.12 Backup/restore

Backup / restore user information and setting information of the PassLogic authentication server. It is recommended to conduct a backup periodically.

Backup

Enter a password (required when restoring and specify with alphanumeric characters only), and click the [Send] button. The backup file starts downloading.

A backup file can be also created with a command line.

```
# sh /opt/passlogic/apps/tools/backup.sh  [password of backup file]
```

*A backup file is output to /opt/passlogic/tmp/passlogicbackup.zip.

Restore

Select a backup file, enter a password set when the backup file is created, and click the [Send] button. The backup file starts uploading.

2.13 Acquiring technical support file

Our support staff may ask you to acquire a support file for technical support. Enter your password, and click the [Send] button to start downloading a file.

*In the support file, settings and logs are included. Personal information such as user name, etc. is not included.

*To acquire a file, 2 GB or more free space is necessary in the server.

Files acquired for technical support

OS type (version, etc.)
Server setting files (/etc/httpd/conf, /etc/httpd/conf.d, /etc/php.ini)
PassLogic setting file (/opt/passlogic/data)
Log files (/var/log/httpd, /var/log/radiusd, /var/log/passlogic , /var/log/passlogic-pgpool, /opt/passlogic/pgsql/data/serverlog)

*Also, inform the password set during downloading to the support staff.

2.14 Recreating administrator (admin) password

Perform the steps in "Accessing the management tool" to recreate a password for admin.

2.15 Monitoring processes

Perform the following process monitoring in the PassLogic authentication server.

(RHEL6/CentOS6)

/usr/sbin/httpd
/usr/sbin/radiusd
/opt/passlogic/pgpool/bin/pgpool
/opt/passlogic/pgsql/bin/postmaster

(RHEL7/CentOS7)

/usr/sbin/httpd	UNIT NAME:httpd.service
/usr/sbin/radiusd	UNIT NAME:radiusd.service
/opt/passlogic/pgpool/bin/pgpool	UNIT NAME:passlogic-pgpool.service
/opt/passlogic/pgsql/bin/postgres	UNIT NAME:passlogic-pgsql.service
*Command "# systemctl status UNIT_NAME" can monitor the status and process list.	

2.16 Including target value to URL in user interface

By sending a query string when a user login, the user can automatically login to SSL-VPN, web applications, and cloud services after logging in to PassLogic. Users who have to change their password can login automatically after changing their password.

SSL-VPN:

https://[PassLogic server hostname]/ui/?sso-vpn=[Appliction name]

WebAPP:

https://[PassLogic server hostname]/ui/?sso-webapp=[Application name]

Cloud:

https://[PassLogic server hostname]/ui/?sso-saml=[Provider name]

2.17 Password reminder

This function allows users who forget their login password to recreate a password by themselves.
*Users who have policy that permits to access password reminder can use this function.

<<Steps to follow>>
(i) Access https://[PassLogic server hostname]/ui/reminder.php.
(ii) Enter user name and e-mail address registered on user account, then click [Next].
(iii) When the combination of the entered user name and e-mail address matches, the notification e-mail containing a URL for password reissuing is sent to the registered e-mail address.
(iv) When the user accesses to the URL specified in the e-mail, a new password is reissued, and the notification e-mail containing a new password is sent to the registered address.
*The URL for password reissuing is valid for only one transaction. In addition, the URL is valid for 24 hours after it is created. If 24 hours passed, perform the steps from (i) again.
*Use the latest URL for password reissuing.
*The reissued password is the random secret pattern with the length set in [Config] > [Policy settings] > [Length of an Auto Generated Pattern (secret pattern)].

3 User administrator guide

3.1 Creating new user

This is the procedure to manually register a new user account on the management tool.

*In case of a LDAP linking, it is not necessary to create users manually. Information linked from an AD is e-mail addresses only (mail attribute values on the AD).

<<Registration steps>>

(i) Click [Users] > [Create New User] from the left menu on the management tool.

(ii) Edit as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Save].

<<Item explanation>>

[uid] (required)	Enter a user ID. Alphanumeric (case-sensitive) characters and the following three symbols can be used (1 to 30 characters). . (period) - (hyphen) and _ (underscore)
[Domain]	Choose a domain name that belongs in the PassLogic.
[E-mail address]	It is required within 255 characters at maximum when notifying user creation results.
[Name]	255 characters maximum
[Employee number]	255 characters maximum
[Section]	255 characters maximum
[Phone]	255 characters maximum
[Policy]	Select a policy. *If not specified, Default Policy is applied.
[Group]	Select a group.
[Secret pattern (One-Time Password)]	Specify an initial value of a secret pattern. A notification example is shown below. 1234 5678 9ABC DE** **** **** **** **** **** **** **** **** *Use alphabets [A-Z,a-z] for 10 digits or more. *Random generation is enabled by checking the [Set secret pattern randomly] checkbox. It will follow in section 2.2 of the setting when you want to generate.

[Static Password]	Specify a static password initial value appended after a one-time password. Alphanumeric (case-sensitive) characters and the following symbols can be used. _ . ( ) { } [ ] ~ - / ' ! # $ ^ ? @ % + ¥ ` & * = | ; " < > (Unable to use a comma and a colon) When you input "random" it will be randomly generated. It will follow in section 2.2 of the setting when you want to generate.
[Active/Inactive]	Select to enable or disable a user account.
[Expiration date]	Set an effective period of an account.
[Notes]	255 characters maximum
Client Settings	When linking SSL-VPN, if different attributes need to be sent for each user from PassLogic to a RADIUS client, the entered value can be used.
SSO	When linking SSL-VPN, if different parameters need to be sent for each user to perform SSO from PassLogic to a target device, the entered value can be used.
WebSSO	When linking WebSSO, if different parameters need to be sent for each user from PassLogic to a target application, the entered value can be used.

3.2 Device restriction

Device restriction is checked in Config > PassLogic Setting can restrict devices (browsers) that user can access (five devices maximum). When a user logged in to PassLogic menu page for the first time, the devices (browser) used at that time can be activated automatically. When the user needs to activate other devices, please look at the following instruction.

<<Steps to registration>>

(i) Click the applicable uid in User List.

(ii) Click "Issue" link in No. 1 to No. 5.

(iii) Enter E-mail address and Notes, and click Next.

(iv) Click [Issue].

(v) Click [Send the notification by e-mail] to send the activation e-mail to the e-mail address entered in (iii), or click [Print the notification] to display the notification contents.

*If there is not user's e-mail address, [Send the notification by e-mail] is not displayed.

(vi) Activation is completed after the user clicks the link in the e-mail and login into PassLogic.

3.3 Performing user batch registration and downloading CSV

Create users from a csv file or output user information to a csv file.

<<Registration steps>>

(i) Click [Users] > [Import] from the left menu on the management tool.

(ii) Select an import file, and click [Next].

File format	CSV (comma-separated text file)
Character code	ShiftJIS
[CSV format]	[delflag],[uid],[domain],[uemail],[uname],[employee_number],[section],[phone],[policy],[group1],[group2],[group3],[group4],[group5],[udisabled],[uexpiry],[ucomment],[attribute1],[attribute2],[attribute3],[attribute4],[attribute5],[attribute6],[attribute7],[attribute8],[attribute9],[attribute10],[sslvpn param1],[sslvpn param2],[sslvpn param3],[sslvpn param4],[sslvpn param5],[sslvpn param6],[sslvpn param7],[sslvpn param8],[sslvpn param9],[sslvpn param10],[websso param1],[websso param2],[websso param3],[websso param4],[websso param5],[websso param6],[websso param7],[websso param8],[websso param9],[websso param10],[locked],[secret_pattern],[static_pattern]

(iii) Check the following settings, confirm the contents of CSV, and click [Save].

[The first row is skipped as field names]	Place a checkmark when skipping the first row as the item name.
[Send the notification by e-mail]	Place a checkmark to send e-mail notifications, when users are created. The e-mail address item is required. * E-mail is sent to new user only. (not sent to updated or deleted user)

*Importing cannot be executed multiply.

*If “LDAP ID Sync” is executed, then you cannot execute importing. If you have set “LDAP ID Sync” to run automatically, then please you take care not to run multiple.

*If updating lock status to locked, the user’s locked time is set the csv upload time.

<<Downloading steps>>

(i) Click [Users] > [Import] from the left menu on the management tool.

(ii) Click [Download a CSV file.].

<<CSV file format>>

Item name		Settable value	Remarks
delflag	[Delete Flag]	d	Set d on users to delete.
uid	[uid] (required)	Alphanumeric characters and symbols (- _ .)	1 to 30 characters
domain	[Domain] (required)	Alphanumeric characters and symbols (- .)	Specify a domain on the AD server registered with the PassLogic management tool. If non AD user, specifies the fixed value "local".
uemail	[E-mail address]	E-mail address format	
uname	[Name]	No restriction *1	
employee_number	[Employee number]		
section	[Section]		
phone	[Phone number]		
policy	[Policy]	Alphanumeric characters and symbols (- _)	A policy name registered with the PassLogic management tool can be specified.
group1	[Group1]	Alphanumeric characters and symbols (- _)	A group name registered with the PassLogic management tool can be specified.
group2	[Group2]		
group3	[Group3]		
group4	[Group4]		
group5	[Group5]		
udisabled	[Active / Inactive]	0/1	Enable/Disable
uexpiry	[Expiration date]	yyyyMMdd yyyy/MM/dd yyyy-MM-dd	User's effective period. When that is left blank, there is no expiration limit.
ucomment	Notes	No restriction *1	Remarks on user
attribute1-10	[Radius attribute1-10]	No restriction *1	A value used when linking to other system.
sslvpn param1-10	[SSL-VPN SSO1-10]	No restriction *1	A value used when linking to other system.

websso param1-10	[WebSSO parameter1-10]	No restriction *1	A value used when linking to other system.
locked	[lock out]	0 / 1	0: unlocked 1: locked
secret_pattern	[secret pattern]	Numbers of 1-48(separated by comma), “random” *2	Use only when a new user registration. Not downloadable.
static_password	[static password]	Numbers, lower case and upper case, “random” *3	Use only when a new user registration. Not downloadable.
lastauthdate	[Last authentication time]	yyyy/mm/dd hh:mm:ss	Download only. It is not possible to import.
passsetdate	[Password change time]	yyyy/mm/dd hh:mm:ss	Download only. It is not possible to import.

*1：When entering one double quote, enter two double quotes that will be regarded as one double quote. (Example: "Test"01"User" -> "Test""01""User")

*2: If you write “random” it will be randomly generated by the length of “ [Length of an Auto Generated Pattern (secret pattern)]” of policy.

*3: If you write “random” it will be randomly generated by the length of “ [Length of an Auto Generated Pattern (static password)]” of policy.

*Up to 255 characters can be registered for the items which number of characters is not specified.

* If the download CSV file is edited with Microsoft Office Excel, data may be corrupted. When editing the file, it is recommended to use a text editor and an editor for CSV file.

When loading a CSV file periodically with cron, create a setup file, and execute the following command.

Config file name：

/opt/passlogic/tmp/userimport_configfile

Setting item：

Number of rows	Set value
1	[The first row is skipped as field names] [1]: Skip / [0]: Do not skip
2	[Send the notification by e-mail] [1]: Send e-mail / [0]: Do not send e-mail
3	[CSV column definitions] See the sample shown below.

Config file sample:

```
1
1
delflag,uid,domain,uemail,uname,employee_number,section,phone,policy,group1,group2,group3,group4,group5,udisabled,uexpiry,ucomment,attribute1,attribute2,attribute3,attribute4,attribute5,attribute6,attribute7,attribute8,attribute9,attribute10,sslvpnsso1,sslvpnsso2,sslvpnsso3,sslvpnsso4,sslvpnsso5,sslvpnsso6,sslvpnsso7,sslvpnsso8,sslvpnsso9,sslvpnsso10,param1,param2,param3,param4,param5,param6,param7,param8,param9,param10,locked,secret_pattern,static_password
```

Command example:

```
# /usr/bin/php /opt/passlogic/apps/admin/cgi/userimport.php {CSV file path} {Config file path}
```

*After executing the command, the config file and the CSV file are automatically deleted.

3.4 Domain

It will manage the domain to apply to users in the PassLogic. Import users from LDAP server.

PassLogic Domain

<<Domain name additional steps>>

(i) Click [Domains] and click [Add]

(ii) Enter new domain name and click [Next]

(iii) Check the input content and click the [Save]

* The domain name alphanumeric characters, periods, hyphens only can be used, it is up to a maximum of 20 characters.

* You cannot overlap with the domain name that is already registered.

LDAP Settings

<<Setting steps of "LDAP Settings">>

(i) Click Management tool left menu [Domains] and click [Edit] of column of "LDAP Settings".

(ii) Edit the AD Settings as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Submit].

*On confirm screen, the upper limit number of displayed user is "MaxPageSize" of ActiveDirectory.

<<Item explanation>>

LDAP Server Connection Settings	
[LDAP Type]	Select ActiveDirectory or OpenLDAP according to your LDAP server.
[Server Name]	Enter a hostname or IP address of an Active Directory server.
[Port Number]	Enter a port number of an AD server. It is typically 389.
[Bind DN]	Enter a binding DN. Example: cn=administrator,cn=Users,dc=win2008,dc=passlogy,dc=com
[Bind password]	Enter a password for binding.
[TOP tree DN]	Enter DN of a target object. *Users that belong under the DN can use PassLogic. Example: cn=Users,dc=win2008,dc=passlogy,dc=com
[Search filter]	Enter filter criteria of a target object. Example: (memberOf=CN=passlogic, CN=Users, dc=win2008,dc=passlogy,dc=com) *User that matches the search filter is available to PassLogic. *Search filter strings to except for AD invalid users. (!(userAccountControl:1.2.840.113556.1.4.803:=2))
[Active Directory Domain name or NT Domain name]	Enter an Active Directory domain name or an NT domain name. Example of Active Directory domain name : win2008.passlogy.com Example of NT domain name : WIN2008 *When LDAP Type is "ActiveDirectory", This setting value is used to "uid@<this value>" as the RDN. *When LDAP Type is "OpenLDAP", Please enter an arbitrary text.
[Default Policy]	Select a LDAP linked user's initial policy. *When first login (AD authentication succeess), the default policy is applying to the user. Subsequently, the user's policy will not be updated automatically.
LDAP Attribute Mapping	
[User ID](required)	Enter an LDAP attribute corresponding to user ID.
[E-mail Address] (required)	Enter an LDAP attribute corresponding to e-mail address.
[Name]	Enter an LDAP attribute corresponding to name.
[Employee Number]	Enter an LDAP attribute corresponding to employee number.
[Section]	Enter an LDAP attribute corresponding to section.
[Phone]	Enter an LDAP attribute corresponding to phone.
[Group1-5]	Enter LDAP attributes corresponding to "Group1–5" of user

	information.
[Expiration Date]	Enter an LDAP attribute corresponding to expiration date. *ActiveDirectory attribute “accountExpires” cannot be specified because the format is different.
[Notes]	Enter an LDAP attribute corresponding to notes.
[attribute1-10]	Enter LDAP attributes corresponding to attribute1–10 of user information “Client Settings”.
[sslvpn param1-10]	Enter LDAP attributes corresponding to param1–10 of user information “SSO”.
[websso param1-10]	Enter LDAP attributes corresponding to param1–10 of user information “WebSSO”.

*Refer 3.3 <<CSV file format>> regarding data format of attribute values.
*Newline characters cannot be used in LDAP attributes of values.
*Every login to PassLogic (AD authentication success), update the user’s value according to mapping definitions.
*If attribute values on LDAP server are empty, empty information is overwritten.

Script of deleting LDAP linked user

The following command is for deleting users on PassLogic that ware deleted on Active Directory.
Command:

```
# /usr/bin/php /opt/passlogic/apps/tools/passlogic_adsync.php
```

Log file:
/var/log/passlogic/passlogic_adsync.log

Sample log:

```
Log of 2 users Deletion:
2014/12/16 15:24:23 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:24:23 user deleted., arumo0@passlogy.com, Delete user.(30003)
2014/12/16 15:24:23 user deleted., arumo1@passlogy.com, Delete user.(30003)
2014/12/16 15:24:23 Finish synchronizing users from Active Directory.(31102)

Log of 0 user Deletion:
2014/12/16 15:29:56 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:29:56 Finish synchronizing users from Active Directory.(31102)

Log of AD Bind Error:
2014/12/16 15:29:23 Start synchronizing users from Active Directory.(31101)
2014/12/16 15:29:23 ldap bind error. domain=passlogy.com
2014/12/16 15:29:23 Finish synchronizing users from Active Directory.(31102)
```

Group mapping

Using this function, value linking to a security group of the Active Directory as RADIUS attribute can be sent to SSL-VPN. This function is for Active Directory only.

<<Setting steps>>

(i) Click Management tool left menu [AD Settings] > [AD Server Settings] > “group mapping” link.

(ii) Click [group mapping].

(iii) Check AD Security Groups, select an attribute, edit the attribute value and click [Next].

(iv) Confirm the contents you have entered, and click [Save].

(v) Edit the mapping priority, and click [Next].

(vi) Confirm the contents you have entered, and click [Save].

<<Item explanation>>

Attribute value screen

[AD Security Group]	Select Active Directory Security groups that are condition to allocate a value. *When multiple groups are selected, users should belong to selected all groups.
[PassLogic Attribute Value]	Select a position to allocate a value from attribute 1 to 10, and enter a setting value to allocate.

Mapping list screen

[mapping priority]	Enter a number of mapping priority. *Mapping to user in ascending order.

*If an attribute value to allocate a user is already set, it is overwritten.

*A primary group set as an AD user is not regarded as a belonging AD group.

LDAP ID Sync

<<LDAP ID Sync registration step>>

(i) Click [Users] > [LDAP Sync] > [Add] from the left menu on the management tool.

(ii) Edit as necessary, and click [Next].

(iii) Confirm the contents you have entered, and click [Save].

* Only one setting can be set up.

<<Item explanation>>

LDAP Server Connection Settings	
[LDAP Type]	Select ActiveDirectory or OpenLDAP according to your LDAP server.
[Server1] (required)	Enter a host name or IP address of LDAP server.
[Server2]	In case that Server1 has replication server, Enter the host name or IP address of replication server. *When Server1 cannot be connected, PassLogic tries connecting to Server2.
[Port Number]	Enter a port number of the LDAP server. If empty, it sets default value 389.
[Bind DN] (required)	Enter a binding DN to execute an LDAP Search.
[Bind Password] (required)	Enter a password for binding.

[Top DN of Target Tree] (required)	Enter a DN of the target object. *Only users that belong under the DN are a synchronization target.
[Search Filter] (required)	Enter filter criteria of the target object. *Only users corresponding to the search filter are synchronized. *If you want to exclude disabled users on ActiveDirectory, Add following strings as filter. (!(userAccountControl:1.2.840.113556.1.4.803:=2))
LDAP Server Synchronize Settings	
[Synchronization Mode]	Select to “Add / Update” or “Add / Update / Inactive”. [Add / Update] Addition of unregistered users and updating attributes of registered users. [Add / Update / Delete] Besides “Add / Update”, deleting users that are not existing on LDAP search results.
[Sending E-mail]	If checked, sending mail that defined in Policy Settings for added users. *If the attribute value mapping of email address is not specified and if user email address is not set, mail cannot be sent.
[Synchronization Interval]	Select one of the followings. [Once a day at the specified time] Run a synchronization process at the specified time every day. [Time intervals] Every 10 minutes : Every hour 00, 10, 20, 30, 40 and 50 minutes. Every 20 minutes : Every hour 00, 20 and 40 minutes. Every 30 minutes : Every hour 00 and 30 minutes. Every 60 minutes : Every hour 00 minutes. *Set a time interval not to start the next process during previous synchronization. [Not automatic] Automatic execution is not performed. *To execute manual synchronization, Click [Execute synchronize now]. *You can not run synchronization processing in parallel for the same domain. While synchronization process is running, the lock file is created for each domain below /opt/passlogic/tmp/. If you remove the lock file or it has passed more than 5 minutes from being created,

	then you can run the synchronization process.
LDAP Attribute Mapping	
[User ID](required)	Enter an LDAP attribute corresponding to user ID.
[E-mail Address]	Enter an LDAP attribute corresponding to e-mail address.
[Name]	Enter an LDAP attribute corresponding to name.
[Employee Number]	Enter an LDAP attribute corresponding to employee number.
[Section]	Enter an LDAP attribute corresponding to section.
[Phone]	Enter an LDAP attribute corresponding to phone.
[Policy]	Enter an LDAP attribute corresponding to policy. *If not set, the policy that you selected to [Default Value] is applied. *Default value "--" means " Default Policy" of policy definition.
[Group1-5]	Enter LDAP attributes corresponding to "Group1–5" of user information.
[Expiration Date]	Enter an LDAP attribute corresponding to expiration date. *ActiveDirectory attribute "accountExpires" cannot be specified because the format is different.
[Notes]	Enter an LDAP attribute corresponding to notes.
[attribute1-10]	Enter LDAP attributes corresponding to attribute1–10 of user information "Client Settings".
[sslvpn param1-10]	Enter LDAP attributes corresponding to param1–10 of user information "SSO".
[websso param1-10]	Enter LDAP attributes corresponding to param1–10 of user information "WebSSO".

*Refer 3.3<<CSV file format>> regarding data format of attribute values.
*Newline characters cannot be used in LDAP attributes of values.
*Blank items are not synchronized and not overwritten in synchronization process.
*If attribute values on LDAP server are empty, empty information is overwritten.
*The default maxPageSize limit in ActiveDirectory is 1000. When synchronizing over 1000 objects (users), please modify maxPageSize in ActiveDirectory.
*Up to 20,000 users synchronization has been verified with both Active Directory and OpenLDAP.
*In the case of PassLogic server replication configuration, register LDAP ID Sync setting with either authentication server.

3.5 Releasing method of lock

Background of locked items becomes red, and the string turns to [Unlock] for users who are locked. Click the [Unlock] characters to release the lock. This operation can be executed in [User List], [Locked User List], and [User Search].

3.6 Reissuing method of password

When a user forgets his/her password, administrator can reissue new password.

<<Steps to reissue>>

(i) Click [Users] > [User List] from the left menu on the management tool.

(ii) Click [Recreate password] on the user.

(iii) Edit as necessary, and click [Next].

(iv) Confirm the contents you have entered, and click [Save].

(v) Click [Send the notification by e-mail] to send the notification to the e-mail address entered in (iii), or click [Print the notification] to display the notification contents.

*If there is not user's e-mail address, [Send the notification by e-mail] is not displayed.

(vi) The user can login into PassLogic by new password.

*If the user's policy setting "Require to change the initial pattern" is "Yes", after first login by new password, the user is require changing password.

<<Item explanation>>

[E-mail address]	The reissued secret pattern is sent to the e-mail address entered here. * Entered e-mail address is reflected on user information.
[Secret pattern (One-Time Password)]	Set a new secret pattern. Place a checkmark to issue the random one automatically.
[Static Password]	Enter a static password to append after the one-time password. It is not a required item.

3.7 Resetting PassClip

When users who have policy of PassClip need to reactivate PassClip application on another mobile phone, administrator can send E-mail to activate PassClip.

<<Steps to reset>>

(i) Click [Users] > [User List] from the left menu on the management tool.

(ii) Click [Reset PassClip] on the user.

(iii) Edit as necessary, and click [Next].

*E-mail address registered in the user information is initially displayed.

*If changing the e-mail address, e-mail address of the user information will be updated.

(iv) Confirm the contents you have entered, and click [Save].

(v) Click [Send the notification by e-mail] to send the notification to the e-mail address entered in (iii), or click [Print the notification] to display the notification contents.

*If there is not user's e-mail address, [Send the notification by e-mail] is not displayed.

(vi) After the user access to the activation URL by the PassClip device, a new PassLogic slot is added to the PassClip.

3.8 Changing administrator password

Click [Change password] on the left menu to change the password of an administrator account by the administrator himself who is currently logged in.

*Set an administrator password according to "Default Policy".

4 User guide

4.1 User’s parameter setting

When permitting use of the parameter setting function, the price of the permitted parameter can be changed in "Config" after login (in case of default).

<<Item explanation>>

Item name		Settable value	Remarks
Users Edit > Client Settings	attribute1-10	255 characters maximum	[Users] > [User List] There are data and string of the target user.
Users Edit > SSO	param1-10	255 characters maximum	[Users] > [User List] There are data and string of the target user.
Users Edit > WebSSO	param1-10	255 characters maximum	[Users] > [User List] There are data and string of the target user.
Only himself can edit	password1-5	159 byte maximum	It’s impossible to change admin. Only the person himself is the change possible value.

*name of the indicated item name will be the established name in policy setting.

5 Log reference

5.1 Log reference

code	level	message
10099	warning	Invalid mode.
30001	notice	Create user.
30002	notice	Edit user.
30003	notice	Delete user.
30004	notice	User locked out.
30005	notice	User unlocked.
30006	notice	User activated.
30007	notice	User inactivated.
30008	notice	Recreated user password.
30009	notice	Reset PassClip secret.
30011	info	The user already exists.
30012	notice	The user does not exist.
30101	notice	Password reminder e-mail has been sent.
30102	notice	User reset password.
30103	notice	Password reset e-mail has been sent.
30111	err	User does not exist.
30112	err	E-mail address is incorrect.
30113	err	Failed to send password reminder e-mail.
30114	err	Password reminder use is not allowed.
30119	err	Database Transaction Error.
30121	err	URL key is not valid.
30122	err	URL key is expired.
30123	err	User has no e-mail address.
30124	err	Failed to recreate a new secret pattern.
30125	err	Failed to send a new secret pattern e-mail.
30126	err	Password reminder use is not allowed.
30129	err	Database Transaction Error.
31012	notice	Invalid input data.
31014	err	Failed to send e-mail.
31015	err	E-mail address is not set.

31094	emerg	Over maximum number of users.
31097	emerg	The license is expired.
31101	notice	Start synchronizing users from Active Directory.
31102	notice	Finish synchronizing users from Active Directory.
31201	notice	Start exporting user data to PassLogic from LDAP.
31202	notice	Finish exporting user data to PassLogic from LDAP.
31211	err	LDAP Definition has not been specified.
31212	err	The LDAP Definition does not exist.
31213	err	LDAP connection error occurred.
31214	err	The LDAP does not support the protocol version 3.
31215	err	The LDAP connection cannot set off to the referral options.
31216	err	LDAP bind error occurred.
31217	err	LDAP search error occurred.
31218	err	LDAP get entries error occurred.
31301	notice	Start importing user data to PassLogic from CSV.
31302	notice	Finish importing user data to PassLogic from CSV.
31303	warning	User import process is running.
31999	err	Database Transaction Error.
32001	notice	Retrieve backup file.
32002	notice	Restore system from backup file.
32010	notice	Retrieve technical support file.
33001	notice	Standard data fetch start.
33002	notice	Standard data fetch end.
33010	notice	Exists user.
33011	notice	Update error user.
33012	notice	Failed to open passlogicdata.
34001	notice	Start send email to password expiring user.
34002	notice	Finish send email to password expiring user.
34003	err	Password expiration date is unlimited.
34004	err	Invalid email notification settings.
34005	err	Incorrect email notification settings.
34006	err	Days must be a lower number than the validity period.
34007	notice	Successed to send e-mail.
34008	err	Email address is not registered.
40001	notice	Done trim(param1).
40002	notice	Done trim(param2).
40003	notice	Done trim(param3).

40004	notice	Done trim(param4).
40005	notice	Done trim(param5).
40006	notice	Done trim(param6).
40007	notice	Done trim(param7).
40008	notice	Done trim(param8).
40009	notice	Done trim(param9).
40010	notice	Done trim(param10).
40011	notice	Done trim(group1).
40016	notice	Done trim(name).
40017	notice	Done trim(email).
40018	notice	Done trim(comment).
40019	notice	Done trim(apppass).
40100	notice	Invalid input data(uid).
40101	notice	Invalid input data(group1).
40102	notice	Invalid input data(email).
40103	notice	Invalid input data(uexpiry).
40104	notice	Invalid input data(group).
50100	err	Invalid input data.
50101	err	The user does not exist.
50200	info	User information is retrieved successfully.
50300	err	Invalid input data.
50301	err	The user does not exist.
50302	err	Update parameter is required.
50400	notice	User information has updated successfully.
50499	crit	System error occurred.
51100	err	Invalid input data.
51200	notice	Create ticket.
51299	crit	System error occurred.
52100	err	Invalid input data.
52101	err	AD authentication is rejected.
52102	notice	AD authentication is accepted.
52109	crit	AD connection is failed.
52199	crit	System error occurred.
52200	notice	Create random number.
52201	notice	Create dummy random number.
54100	err	Invalid input data.
54101	warning	Random number is expired. Please retry.

54102	warning	User has been expired. Please contact your administrator.
54103	warning	User is not permitted. Please contact your administrator.
54104	warning	Access is not allowed.
54105	warning	User is locked. Please contact your administrator.
54106	warning	The uid or password you entered is incorrect.
54108	warning	Invalid browser.
54109	warning	Failed to find the authentication box.
54199	crit	System error occurred.
54200	notice	User is required to change current password.
54201	notice	Authentication success.
55100	warning	Invalid input data.
55101	warning	RADIUS Authentication is rejected.
55102	warning	Random number is expired. Please retry.
55103	warning	User is locked.
55104	warning	User is not permitted.
55105	warning	There is no Random Number.
56100	warning	Invalid input data.
56101	warning	RADIUS Authentication is rejected.
56200	notice	RADIUS Authentication is accepted.
57100	warning	Invalid input data.
57101	warning	Session ID is invalid. Please start again from the beginning.
57102	warning	The secret pattern is not identified.
57103	warning	The password length is not allowed.
57104	warning	The pattern is not allowed. Please setup a different pattern.
57105	warning	It is not allowed to set the same password in the past.
57106	warning	The password is invalid.
57199	err	Database Transaction Error.
57200	notice	Changing password process.
57201	notice	Changing password is cancelled.
57202	notice	Password has been changed.
59999	err	Database Transaction Error.
70100	err	Invalid input data.
70102	warning	User has been expired. Please contact your administrator.
70103	warning	User is not permitted. Please contact your administrator.
70104	warning	Access is not allowed.
70105	warning	User is locked. Please contact your administrator.
70106	warning	The uid or password you entered is incorrect.

70107	warning	Failed to find the secret code.
70108	warning	Invalid browser.
70199	crit	System error occurred.
70201	notice	Authentication success.
80401	notice	SAML Certificate File uploaded.
80402	notice	SAML Private Key File uploaded.
80409	warning	Failed to File upload.
80411	notice	PKCS12 File uploaded.
80419	warning	Failed to create a PKCS12 File.
91101	notice	Start importing user data to PassLogic from CSV.
91102	notice	Finish importing user data to PassLogic from CSV.
91199	err	Database Transaction Error.

5.2 Log files

PassLogic application log

The same contents with the log displayed in [Displaying Logs] in the management tool are output.

File path	/var/log/passlogic/passlogic.log
Log rotation	/usr/sbin/logrotate
Rotation definition	/etc/logrotate.d/passlogic (Definition contents can be changed, and deleted when uninstalled)

pgpool log

Starting and stopping log on the pgpool process, and the database fault log are output.

File path	/var/log/passlogic-pgpool/pgpool.log
Log rotation	/usr/sbin/logrotate
Rotation definition	/etc/logrotate.d/passlogic-pgpool (Definition contents can be changed, and deleted when uninstalled)

PostgreSQL archive clear log

A log of the process for deleting unnecessary files from the PostgreSQL archive log files is output.

File path	/var/log/passlogic/passlogic_archivecleanup.log
Log rotation	/usr/sbin/logrotate
Rotation definition	/etc/logrotate.d/passlogic (Definition contents can be changed, and deleted when uninstalled)

Deletion procedures of archive log files are registered in /etc/cron.daily/passlogic-archivecleanup.cron.

Deletion Script log for LDAP linked users

In case of the LDAP linking, a log of the process for deleting the users, who were erased from the AD, from the PassLogic database is output.

File path	/var/log/passlogic/passlogic_adsync.log
Log rotation	/usr/sbin/logrotate
Rotation definition	/etc/logrotate.d/passlogic (Definition contents can be changed, and deleted when uninstalled)

Please perform user deletion script with manual execution or periodical execution using cron.