

BaroPAM Guide (Mac OS X)

Index

Index	0
1. Install BaroPAM.....	1
1.1 Preparation before installing BaroPAM.....	1
1.2 Download BaroPAM installation module.....	1
1.3 Create BaroPAM configuration file.....	3
1.4 BaroPAM environment settings.....	7
2. BaroPAM application.....	16
2.1 BaroPAM application process.....	16
2.2 BaroPAM application screen.....	16
2.3 Mac OS X login method.....	17
2.4 ssh/sftp connection tool.....	19
3. Remove BaroPAM.....	24
3.1 Remove the BaroPAM environment.....	24
4. BaroPAM FAQ.....	25
5. About BaroPAM.....	29

1. Install BaroPAM

1.1 Preparation before installing BaroPAM

Mac OS X is divided into a mobile CPU architecture (arm64) made by Apple and X86, a CPU architecture made by Intel. Execute the following command to check.

Note) In the case of arm64, a mobile CPU architecture made by Apple

```
[root] /root > uname -a
Darwin igoun-ui-MacBookAir.local 22.3.0 Darwin Kernel Version 22.3.0: Mon Jan 30 20:39:35 PST 2023; root:xnu-8792.81.3~2/RELEASE_ARM64_T8103 arm64
```

Note) In case of X86 CPU architecture made by Intel

```
[root] /root > uname -a
Darwin lamp_macos1 22.3.0 Darwin Kernel Version 22.3.0: Mon Jan 30 20:42:11 PST 2023; root:xnu-8792.81.3~2/RELEASE_X86_64 x86_64
```

In order to access information assets and use PAM module, OpenSSH (Open Secure Shell) package must be installed to provide reliable and safe ssh/sftp service. To check the installation, run the following command. If not installed, install "brew install openssh" and "brew install openssl".

```
[root] /root > ssh -V
OpenSSH_9.0p1, LibreSSL 3.3.6
```

When setting environment setting information to MariaDB during PAM authentication, MariaDB Client must be installed.

```
[dhs] /Users/dhs > brew install mariadb
```

In order to download and install the BaroPAM authentication module, connect with the root account (log in with a general account. Log in with the "sudo -i" command). Create a directory (/usr/local/baropam) to download and install the BaroPAM authentication module as follows.

```
[root]# mkdir /usr/local/baropam
```

Grant permissions (read, write, execute) of the directory to download and install the BaroPAM module as follows.

```
[root]# chmod -R 777 /usr/local/baropam
```

1.2 Download BaroPAM installation module

After accessing the BaroPAM authentication module with the root account, move to the directory (/usr/local/baropam) to download and install the module, and download the module as follows.

```
[root] /usr/local/baropam > wget http://nuriapp.com/download/libpam_baro_auth-x.x.tar
```

When the download of the BaroPAM authentication module is complete, the tar file is decompressed as follows.

```
[root] /usr/local/baropam > tar -xvf libpam_baro_auth-x.x.tar
```

When the BaroPAM authentication module is unzipped, the following BaroPAM related modules are created in the baropam directory.

```
[root] /usr/local/baropam > ls -al
합계 180
drwxrwxrwx  7 root  root  4096  8월 23 09:59 .
drwxr-xr-x 17 root  root  4096  2월 10 2017 ..
-r--r--r--  1 root  root    8  3월 24 2021 .baro_acl
-r--r--r--  1 root  root  305  7월  2 14:41 .baro_auth
-r--r--r--  1 root  root  290  6월 30 12:55 .baro_curl
-r--r--r--  1 root  root  287  2월 28 12:19 .baro_sql
-rwxr-xr-x  1 root  root 69149  4월  6 19:12 baro_auth
-rwxr-xr-x  1 root  root 65072  6월 29 16:36 baro_curl
-rwxr-xr-x  1 root  root 57074  2월 28 12:18 baro_sql
drwxr-xr-x  2 root  root  4096  7월 20 2021 jilee
-rwxr-xr-x  1 root  root 152649  6월  9 08:19 pam_baro_auth.so
-rwxr-xr-x  1 root  root 116158  6월 30 12:54 pam_baro_curl.so
-rwxr-xr-x  1 root  root 170863  2월 28 12:18 pam_baro_sql.so
-rw-r--r--  1 root  root   221  6월 27 15:59 setauth.sh
-rw-r--r--  1 root  root   150  6월 29 16:29 setcurl.sh
-rw-r--r--  1 root  root   180  2월 28 12:19 setsql.sh
```

Note) In the case of arm64, a mobile CPU architecture made by Apple

```
[root] /usr/local/baropam > file pam_baro_auth.so
pam_baro_auth.so: Mach-O 64-bit dynamically linked shared library arm64

[root] /usr/local/baropam > otool -L pam_baro_auth.so
pam_baro_auth.so:
    pam_baro_auth.so (compatibility version 0.0.0, current version 0.0.0)
    /usr/lib/libpam.2.dylib (compatibility version 3.0.0, current version 3.0.0)
    /opt/homebrew/opt/openssl@1.1/lib/libssl.1.1.dylib (compatibility version 1.1.0, current
version 1.1.0)
    /opt/homebrew/opt/openssl@1.1/lib/libcrypto.1.1.dylib (compatibility version 1.1.0,
current version 1.1.0)
    /usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1319.0.0)
    /usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.11)
```

Note) In case of X86 CPU architecture made by Intel

```
[root] /usr/local/baropam > file pam_baro_auth.so
pam_baro_auth.so.0: Mach-O 64-bit dynamically linked shared library x86_64

[root] /usr/local/baropam > otool -L pam_baro_auth.so
pam_baro_auth.so.0:
    pam_baro_auth.so (compatibility version 0.0.0, current version 0.0.0)
```

```

/usr/lib/libpam.2.dylib (compatibility version 3.0.0, current version 3.0.0)
/usr/local/opt/openssl@1.1/lib/libssl.1.1.dylib (compatibility version 1.1.0, current
version 1.1.0)
/usr/local/opt/openssl@1.1/lib/libcrypto.1.1.dylib (compatibility version 1.1.0, current
version 1.1.0)
/usr/lib/libSystem.B.dylib (compatibility version 1.0.0, current version 1319.0.0)
/usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.11)

```

1.3 Create BaroPAM configuration file

1) PAM authentication(.baro_auth): Set environment setting information in File

The BaroPAM environment setting file must be created by executing the **baro_auth** program, and it must be located under **/usr/local/baropam**, the directory of the BaroPAM authentication module.

Format)

```
baro_auth -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -A acl_type -a
acl_filename -S secure_key -s filename
```

The configuration options of the BaroPAM configuration file are as follows.

Optino	Documentation	Set value	Etc
-r	OTA key limited number of times (1~10)	3	
-R	OTA key time limit (15~600 sec)	30	
-t	OTA key authentication cycle (3~60 sec)	30	
-k	OTA key authentication method (app1, app256, app384, app512)	app512	
-e	Encryption of configuration files (yes or no)	no	
-A	Choose whether to allow or deny 2nd authentication	deny	
-a	ACL file name for the account to allow or deny from 2nd authentication (file access permission is 444)	/usr/local/baropam/.baro_acl	
-S	Secure key (license key) provided by the vendor	j1qlcHbVqdpj7b4PzBpM2DileBvmHFV/	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/local/baropam/.baro_auth	

Note) The filename of the -s option is the name of the file including the directory where the BaroPAM configuration file will be created (file access permission is 444).

Ex of use)

```
[root] /usr/local/baropam > ./baro_auth -r 3 -R 30 -t 30 -l 0 -k app512 -e no -A deny -a
/usr/local/baropam/.baro_acl -S j1qlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s /usr/local/baropam/.baro_auth
```

If the BaroPAM environment setting file is set for each account, connect to the account and proceed with the work. (Not root)

```
[root] /usr/local/baropam > ./baro_auth -r 3 -R 30 -t 30 -l 0 -k app512 -e no -A deny -a
~/baro_acl -S j1qlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s ~/.baro_auth
```

1) Your emergency one-time authentication keys are:

The emergency **OTA key** is a super authentication key that can be used to access the SSH server again in case you lose it when the **OTA key** generator, the **BaroPAM** app, is unavailable, so it is good to write it down somewhere.

2) Enter "y" for all the questions that follow.

Do you want me to update your "/usr/local/baropam/.baro_auth" file (y/n) **y**

Preventing man-in-the-middle attacks (y/n) **y**

The contents set in **.baro_auth**, the **BaroPAM** environment setting file, are as follows.

```
[root] /usr/local/baropam > cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY j1qlchbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/local/baropam/.baro_acl
" ACL_TYPE deny
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

The setting items of **.baro_auth**, a **BaroPAM** configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
RATE_LIMIT	OTA key limit count (1~10), time limit (15~600 sec)	3 30	
KEY_METHOD	OTA key authentication method (app1, app256, app384, app512)	app512	
CYCLE_TIME	OTA key authentication cycle (3~60 sec)	30	
SECURE_KEY	Secure key (license key) provided by the vendor	j1qlchbVqdpj7b4PzBpM2DileBvmHFV/	
ACL_TYPE	Differentiate between allow and deny in 2nd authentication	deny	
ACL_NAME	ACL Filename for the account to be allowed or excluded from 2nd authentication (file access permission is 444)	/usr/local/baropam/.baro_acl	
DISALLOW_REUSE or ALLOW_REUSE	To prevent a man-in-the-middle attack, if "DISALLOW_REUSE" is set, other users cannot log in during the authentication cycle of the OTA key . If allowed, set "ALLOW_REUSE".	DISALLOW_REUSE	

2) PAM authentication (.baro_sql): Set environment configuration information in MariaDB

Connection information for linking with Mariadb, where **BaroPAM** configuration information exists,

must be created by running the **baro_sql** program, and must be located under **/usr/local/baropam**, the directory of the BaroPAM authentication module.

Format)

```
baro_sql -H hostname -u username -p password -d dbname -P portno -e encrypt_flag -s filename
```

The configuration options of the **BaroPAM** configuration file are as follows.

Optino	Documentation	Set value	Etc
-H	Hostname or IP address of the MariaDB server	nurit.co.kr	
-u	MariaDB username	nurit	
-p	Password for the MariaDB user	baropam	
-d	MariaDB name to connect to	baropamdb	
-P	Port number of the MariaDB server	3308	
-e	Encryption of configuration files (yes or no)	no	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/local/baropam/.baro_sql	

Note) The filename of the **-s** option is the file name containing the directory where the **BaroPAM** configuration file will be created (file access permission is 444).

Ex of use)

```
[root] /usr/local/baropam > ./baro_sql -H nurit.co.kr -e no -u nurit -p baropams -d baropamdb -P 3306 -s /usr/local/baropam/.baro_sql
```

1) Enter "y" for all the questions that follow.

Do you want me to update your "/usr/local/baropam/.baro_sql" file (y/n) y

The contents set in **.baro_sql**, the **BaroPAM** environment setting file, are as follows.

```
[root] /usr/local/baropam > cat .baro_sql
" AUTH_KEY
" HOSTNAME nurit.co.kr
" USERNAME nurit
" PASSWORD baropams
" DBNAME baropamdb
" PORTNO 3306
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY j1qlchbVqdpj7b4PzBpM2Di1eBvmHFV/
" ACL_TYPE deny
" MIDDLE_TYPE DISALLOW_REUSE
" MIDDLE_TIME 58014762
" ENV_TYPE share
```

The setting items of **.baro_sql**, a **BaroPAM** configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
HOSTNAME	Hostname or IP address of the MariaDB server	nurit.co.kr	
USERNAME	MariaDB username	nurit	

PASSWORD	Password for the MariaDB user	baropam	
DBNAME	MariaDB name to connect to	baropamdb	
PORTNO	Port number of the MariaDB server	3308	
Other than that	The rest is used for internal use.		

3) curl authentication(.baro_curl)

The name curl stands for "client URL" and was first released in 1997. That is, the client requests data from the server as a script. BaroPAM requests authentication by calling the http/https authentication site with curl.

The BaroPAM environment setting file must be created by executing the baro_curl program, and it must be located under /usr/local/baropam, the directory of the BaroPAM authentication module.

Format)

```
baro_curl -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -H hostname -u auth_url -s filename
```

The contents of the setting options of the BaroPAM configuration file are as follows.

Optino	Documentation	Set value	Etc
-r	OTA key limited number of times (1~10)	3	
-R	OTA key time limit (15~600 sec)	30	
-t	OTA key authentication cycle (3~60 sec)	30	
-k	OTA key authentication method (app1, app256, app384, app512)	app512	
-e	Encryption of configuration files (yes or no)	no	
-H	Server's hostname (uname -n)	nurit.co.kr	
-u	The URL to be called includes parameters such as host name (hostname), user account (username), authentication cycle (cycle_time), and OTA key (auth_key).	http://1.23.456.789/baropam/web/result_curl.jsp	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/local/baropam/.baro_curl	

Note) The filename of the -s option is the name of the file including the directory where the BaroPAM configuration file will be created (file access permission is 444). If the hostname of the set server does not match, BaroPAM may not operate normally. If the hostname is changed, it must be reflected in the relevant item of the environment setting.

Ex of use)

```
[root] /usr/local/baropam > ./baro_curl -r 3 -R 30 -t 30 -k app512 -e no -H nurit.co.kr -u http://1.23.456.789/baropam/web/result_curl.jsp -s /usr/local/baropam/.baro_curl
```

1) Enter "y" for all the questions that follow.

Do you want me to update your "/usr/local/baropam/.baro_auth" file (y/n) y

Preventing man-in-the-middle attacks (y/n) y

The contents set in .baro_curl, the BaroPAM environment setting file, are as follows.

```
[root] /usr/local/baropam > cat .baro_curl
```

```
" AUTH_KEY
" RATE_LIMIT 3 30
" AUTH_URL http://1.23.456.789/baropam/web/result_curl.jsp
" KEY_METHOD app512
" CYCLE_TIME 30
" HOSTNAME baropam
" DISALLOW_REUSE
```

The setting items of `.baro_curl`, a BaroPAM configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
RATE_LIMIT	OTA key limit count (1~10), time limit (15~600 sec)	3 30	
AUTH_URL	The URL to be called includes parameters such as host name (hostname), user account (username), authentication cycle (cycle_time), and OTA key (auth_key).	http://1.23.456.789/baropam/web/result_curl.jsp	
KEY_METHOD	OTA key authentication method (app1, app256, app384, app512)	app512	
CYCLE_TIME	OTA key authentication cycle (3~60 sec)	30	
HOSTNAME	Secure key (license key) provided by the vendor	nurit.co.kr	
DISALLOW_REUSE or ALLOW_REUSE	To prevent a man-in-the-middle attack, if "DISALLOW_REUSE" is set, other users cannot log in during the authentication cycle of the OTA key. If allowed, set "ALLOW_REUSE".	DISALLOW_REUSE	

1.4 BaroPAM environment settings

1) PAM authentication: Set environment setting information in File

To configure the BaroPAM module, enter it at the top as follows to configure sshd, su, and sudo files.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_auth.so nullok secret=/usr/local/baropam/.baro_auth
encrypt=no
```

* "nullok" means that the called PAM module allows entering a password with a null value.

For reference, the **secret** parameter sets the BaroPAM configuration file name, and the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the BaroPAM configuration file.

If the BaroPAM environment setting file is set for each account, the way to set the sshd file to set the BaroPAM module is entered at the top as follows.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_auth.so nullok secret=${HOME}/.baro_auth encrypt=no
```

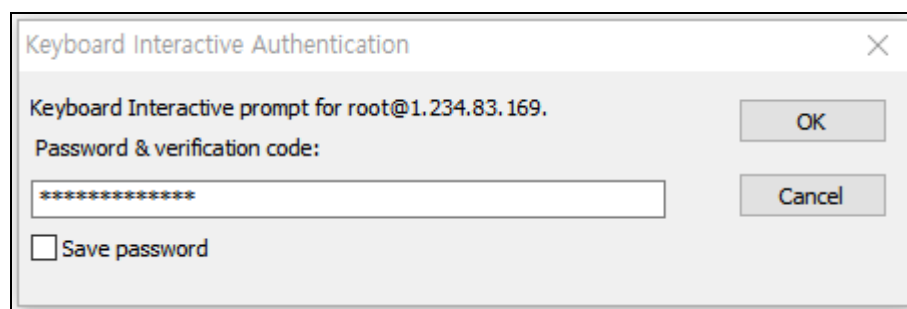

If you want to set different BaroPAM environment configuration files for each account in a specific directory instead of setting BaroPAM environment configuration files for each account, enter the following at the top to configure the BaroPAM module in the sshd file.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
##PAM-1.0
auth            required                               /usr/local/baropam/pam_baro_auth.so          nullok
secret=/usr/local/baropam/auth/.$${USER}_auth encrypt=no
```

For programs like filezilla that cannot perform "Interactive process", the only way is to use the **forward_pass** option in PAM to enter the **OTA key** when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
##PAM-1.0
auth required /usr/local/baropam/pam_baro_auth.so forward_pass
secret=/usr/local/baropam/.baro_auth encrypt=no
```

Enter the **OTA key** in the password input window (Password & verification code:) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".



Using **forward_pass**, you can enable **2nd authentication** for most services that require authentication.

```
[root] /usr/local/baropam > vi /etc/pam.d/su
##PAM-1.0
auth required /usr/local/baropam/pam_baro_auth.so nullok secret=/usr/local/baropam/.baro_auth
encrypt=no
```

If you add the BaroPAM module to the top of the /etc/pam.d/su file, you can apply the **2nd authentication (additional authentication)** input even when a general account tries to ascend to "root" with the "su" command for security. this is further improved.

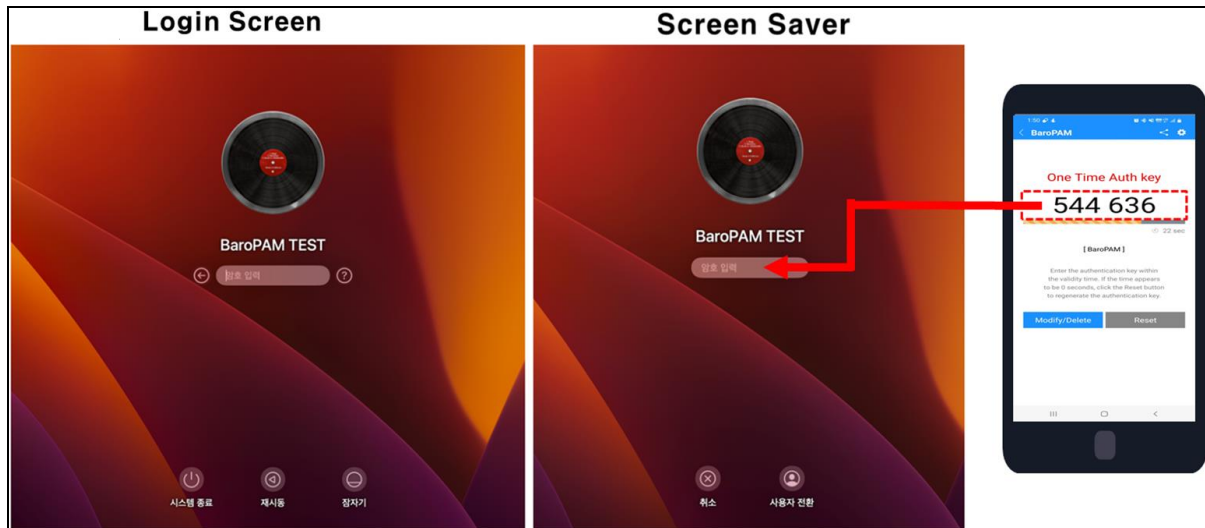
```
$ su - root
Verification code:
```

If you want to use BaroPAM on the GUI login screen of Mac OS X, the setting method is as follows.

```
[root] /usr/local/baropam > vi /etc/pam.d/screensaver, authotization
##PAM-1.0
auth            required                               /usr/local/baropam/pam_baro_auth.so          use_first_pass forward_pass nullok
```

```
secret=/usr/local/baropam/.baro_auth encrypt=no
```

On the GUI login screen of Mac OS X, enter the password first, followed by the **OTA key** without spaces. For example, if the password is "baropam" and the **OTA key** is "544636", enter "baropam544636".



Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/local/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_auth.so forward_pass
secret=/usr/local/baropam/.baro_auth encrypt=no
```

Enter the **OTA key** in the password input window (Password) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".

2) PAM authentication: Set environment setting information in MariaDB

To configure the **BaroPAM** module, enter it at the top as follows to configure sshd, su, and sudo files.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_sql.so nullok secret=/usr/local/baropam/.baro_sql
encrypt=no auth=sshd
```

* "nullok" means that the called PAM module allows entering a password with a null value.

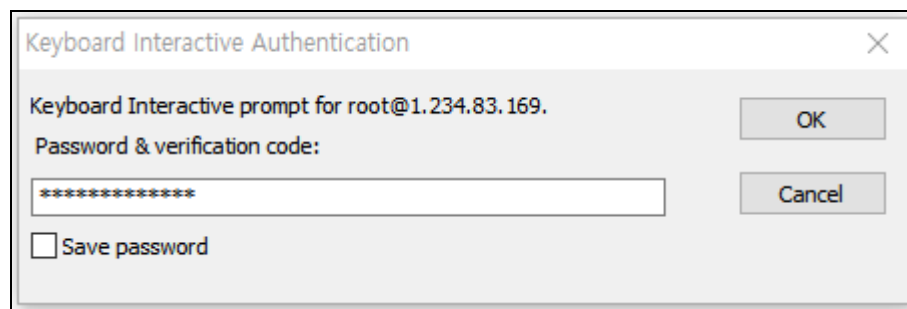
For reference, the **secret** parameter sets the BaroPAM configuration file name, the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the **BaroPAM** configuration file, and the **auth** parameter sets **sshd**, **su**, **sudo**, **screensaver**, **xrdp-sesman**, etc., which are places that use **BaroPAM** for authentication.

For programs like filezilla that cannot perform "Interactive process", the only way is to use the **forward_pass** option in PAM to enter the **OTA key** when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no

choice but to input like this.

```
[root] /usr/local/baropam > vi /etc/pam.d/ssh
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_sql.so forward_pass
secret=/usr/local/baropam/.baro_sql encrypt=no auth=ssh
```

Enter the **OTA key** in the password input window (Password & verification code:) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".



Using **forward_pass**, you can enable **2nd authentication** for most services that require authentication.

```
[root] /usr/local/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_sql.so nullok secret=/usr/local/baropam/.baro_sql
encrypt=no auth=su
```

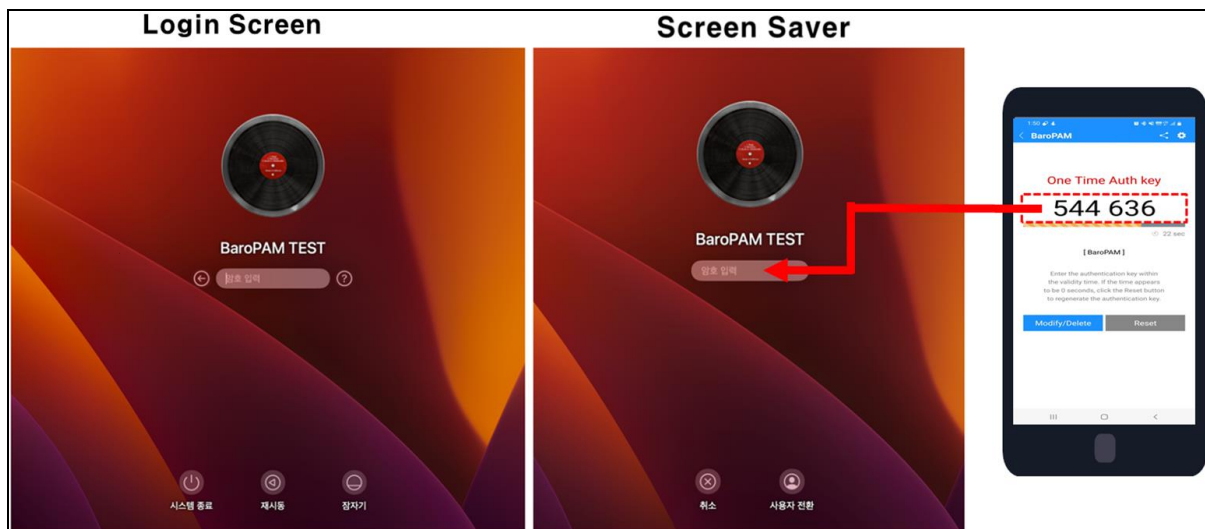
If you add the **BaroPAM** module to the top of the **/etc/pam.d/su** file, you can apply the **2nd authentication (additional authentication)** input even when a general account tries to ascend to "root" with the "su" command for security. this is further improved.

```
$ su - root
Verification code:
```

If you want to use **BaroPAM** on the GUI login screen of Mac OS X, the setting method is as follows.

```
[root] /usr/local/baropam > vi /etc/pam.d/ screensaver, authotization
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_sql.so use_first_pass forward_pass nullok
secret=/usr/local/baropam/.baro_sql encrypt=no auth=screensaver
```

On the GUI login screen of Mac OS X, enter the password first, followed by the **OTA key** without spaces. For example, if the password is "baropam" and the **OTA key** is "544636", enter "baropam544636".



Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/local/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_sql.so forward_pass
secret=/usr/local/baropam/.baro_sql encrypt=no auth=xrdp-sesman
```

Enter the **OTA key** in the password input window (Password) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".

3) curl authentication

To configure the **BaroPAM** module, enter it at the top as follows to configure sshd, su, and sudo files.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_curl.so nullok secret=/usr/local/baropam/.baro_curl
encrypt=no
```

* "nullok" means that the called PAM module allows entering a password with a null value.

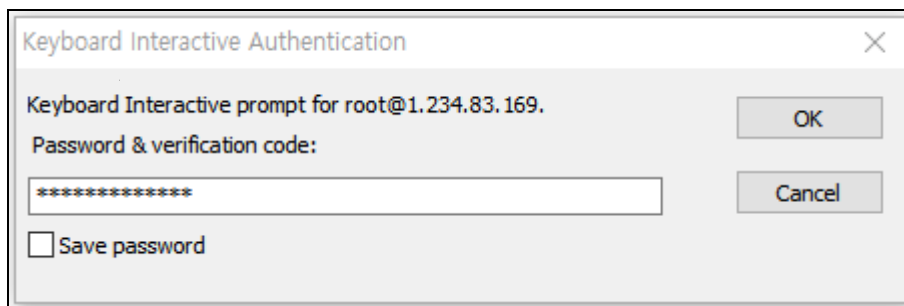
For reference, the **secret** parameter sets the **BaroPAM** configuration file name, and the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the **BaroPAM** configuration file.

For programs like filezilla that cannot perform "Interactive process", the only way is to use the **forward_pass** option in PAM to enter the **OTA key** when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_curl.so forward_pass
secret=/usr/local/baropam/.baro_curl encrypt=no
```

forward_pass option in PAM to enter the **OTA key** when entering the password. In this case, the

openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this. Enter the **OTA key** in the password input window (Password & verification code:) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".



Using **forward_pass**, you can enable **2nd authentication** for most services that require authentication.

```
[root] /usr/local/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth            required            /usr/local/baropam/pam_baro_curl.so      forward_pass
secret=/usr/local/baropam/.baro_curl encrypt=no
```

If you add the **BaroPAM** module to the top of the **/etc/pam.d/su** file, you can apply the **2nd authentication (additional authentication)** input even when a general account tries to ascend to "root" with the "su" command for security. this is further improved.

```
$ su - root
Password & verification code:
```

If you want to use **BaroPAM** on the GUI login screen of Mac OS X, the setting method is as follows.

```
[root] /usr/local/baropam > vi /etc/pam.d/screensaver, authotization
#%PAM-1.0
auth    required    /usr/local/baropam/pam_baro_curl.so  use_first_pass  forward_pass  nullok
secret=/usr/local/baropam/.baro_curl encrypt=no
```

Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/local/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth required /usr/local/baropam/pam_baro_curl.so forward_pass
secret=/usr/local/baropam/.baro_curl encrypt=no
```

Enter the **OTA key** in the password input window (Password) using **forward_pass**. For example, if the **OTA key** is "123456", just enter "123456".

3) Configuration of the sshd daemon

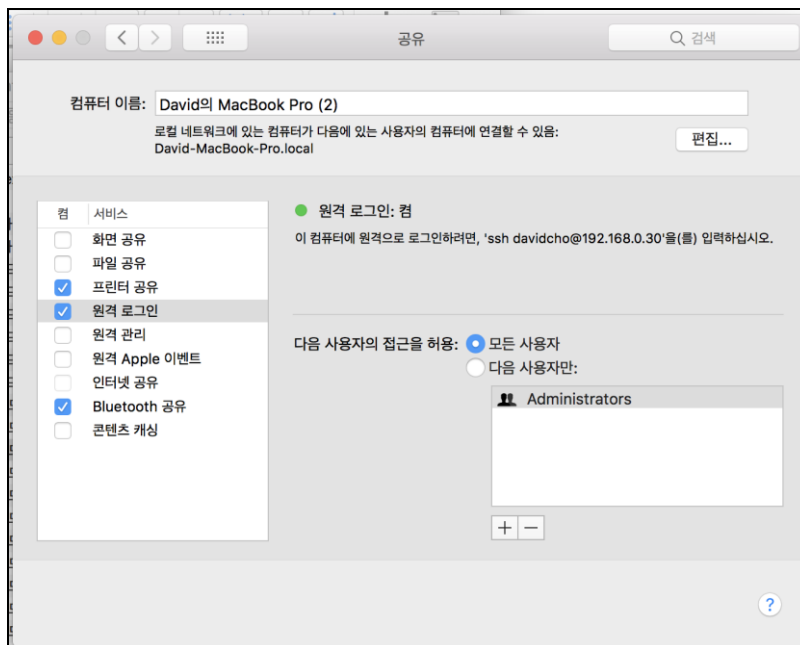
Among the contents of the **"/etc/ssh/sshd_config"** file, which is a configuration file for setting the sshd daemon, the following parameters need to be changed.

Factor	Before	After	Etc
PasswordAuthentication	yes	no	
ChallengeResponseAuthentication or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

After completing the sshd configuration, make sure that the PAM module is properly added, and then restart the SSH Server.

```
[root] /usr/local/baropam > launchctl stop com.openssh.sshd
[root] /usr/local/baropam > launchctl start com.openssh.sshd
```

After configuring sshd, be sure to reboot the ssh daemon after confirming that the PAM module is properly added. (System Settings → General → Sharing → Remote Login → Remote Login: on, you must set to allow access for the next user.)



4) ACL(Access Control list) settings

1) In the case of PAM authentication (Set environment setting information in File) When using the BaroPAM module, if it is necessary to exclude from the ACL for the account to be excluded from the 2nd authentication, create an ACL file in the directory set when setting the BaroPAM environment, and enter the account to be excluded as follows. (The file access permission for .baro_acl must be set to 444.)

```
[root] /usr/local/baropam > vi .baro_acl
barokey
baropam
```

2) In case of PAM authentication (Set environment configuration information in MariaDB), Mariadb's ACL setting table must be used.

5) NTP(Network Time Protocol) settings

Since BaroPAM is a time synchronization method, if the server's time is different from the current time, login to the server may not be possible because the OTA keys do not match.

Recently, as a method of time synchronization (time server time synchronization) for information assets, the system time can be set to the current time in the root account using NTP (Network Time Protocol).

To use NTP, the NTP package must be installed by default. To check the installation, run the following command. If it is not installed, install it with the "**brew install ntp**" command.

```
[root]# brew install ntp
```

NTP servers operating in Korea are as follows.

```
server kr.pool.ntp.org
server time.bora.net
server time.kornet.net
```

Set the NTP server operating in Korea in `"/etc/ntp.conf"`, the configuration file for the ntpd daemon configuration, as follows.

```
[root]# vi /etc/ntp.conf
#
# NTP
#
server kr.pool.ntp.org iburst
server time.bora.net iburst
server time.kornet.net iburst
```

The **iburst** option is a kind of option setting that shortens the time required for synchronization.

After the setup for the ntpd daemon setup is complete, it is absolutely necessary to restart the NTP daemon after confirming that the NTP setup has been properly added.

```
[root]# sudo launchctl stop ntpd
[root]# sudo launchctl start ntpd
```

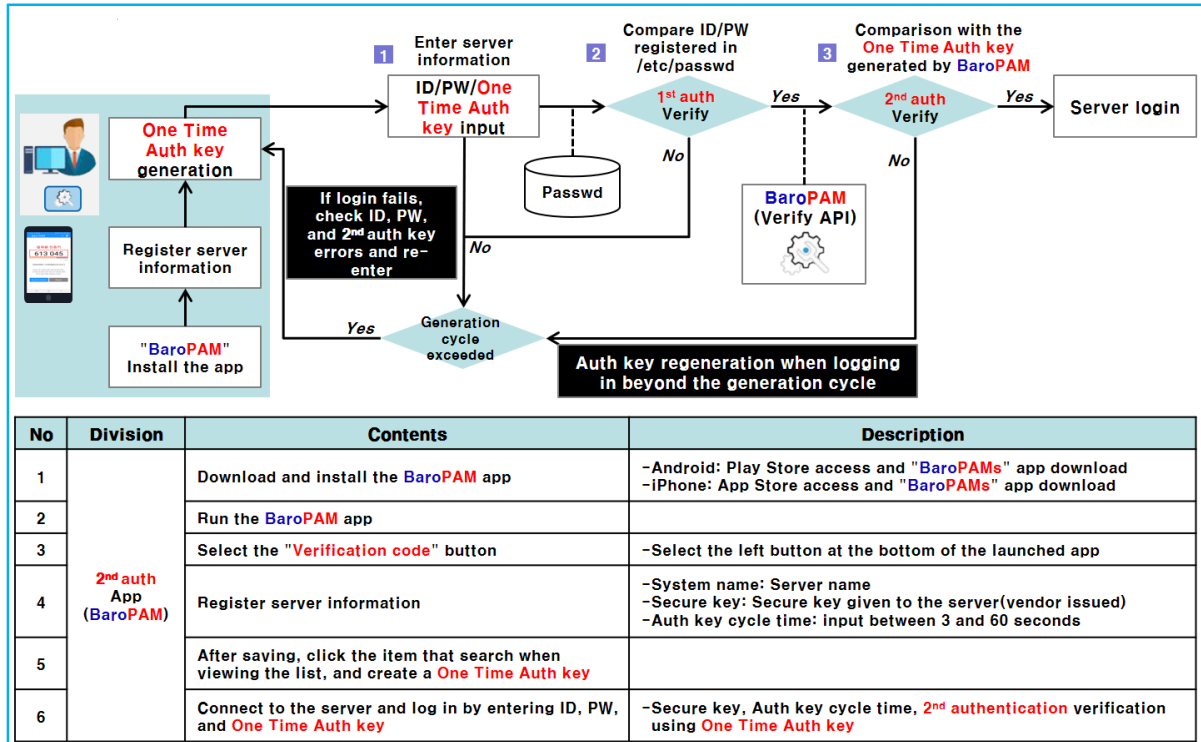
You can check the ntpd time with the following command.

```
[root]# ntpq -p
remote          refid      st t when poll reach  delay  offset  jitter
=====
0.freebsd.pool. .POOL.      16 p   - 64    0   0.000  0.000  0.000
106.247.248.106 141.223.182.106 2 u   7 64    1   4.412  0.544  0.000
time.bora.net    204.123.2.5   2 u   7 64    1   5.206  7.741  0.000
*send.mx.cdnetwo 204.123.2.5   2 u   1 64    1   3.968  3.807  0.446
211.52.209.148  216.239.35.12 2 u   1 64    1  11.862  2.838  0.259
dadns.cdnetwork 204.123.2.5   2 u   2 64    1   4.833  0.005  0.408
92.223.73.5 (st 106.247.248.106 3 u   - 64    1   5.015  1.397  0.482
```

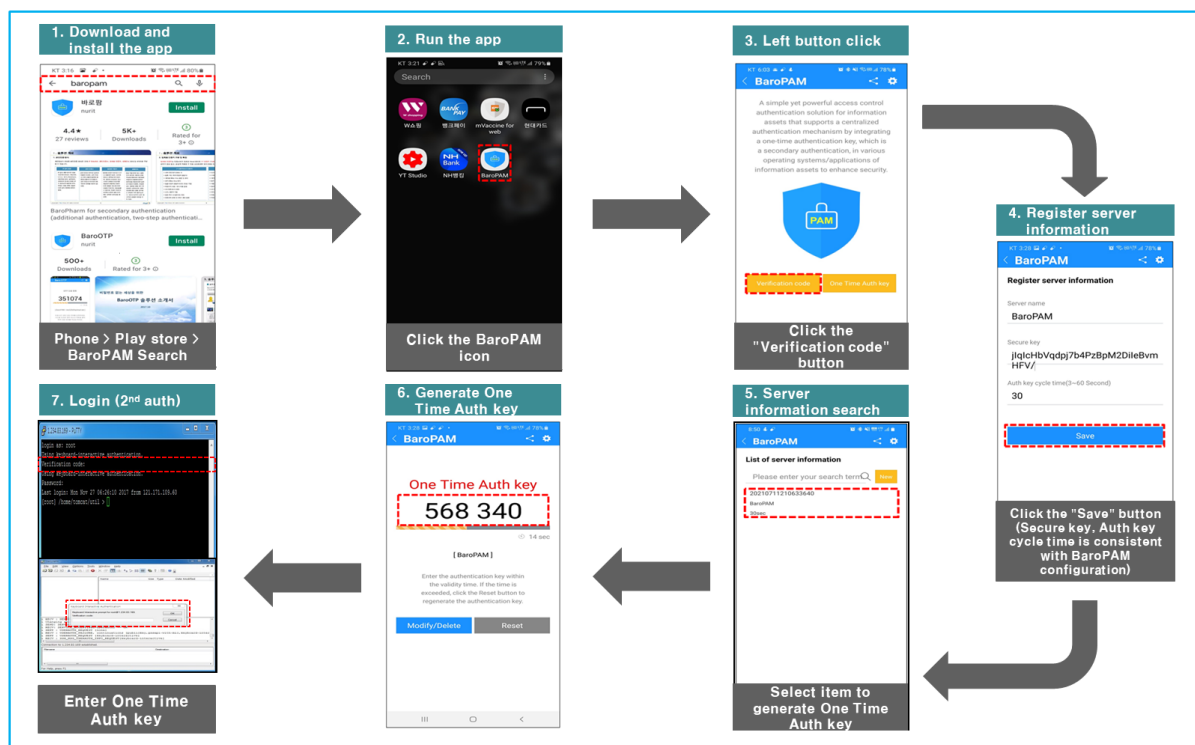
- * The displayed ip is the ntp server getting the current time

2. BaroPAM application

2.1 BaroPAM application process

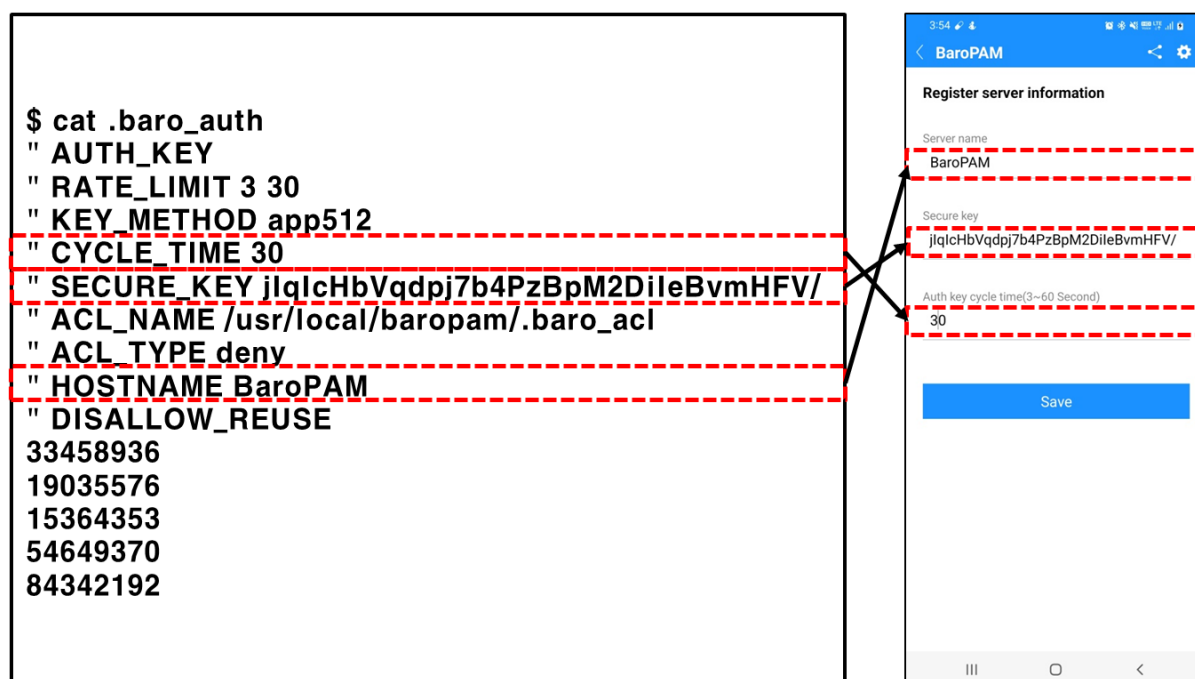


2.2 BaroPAM application screen



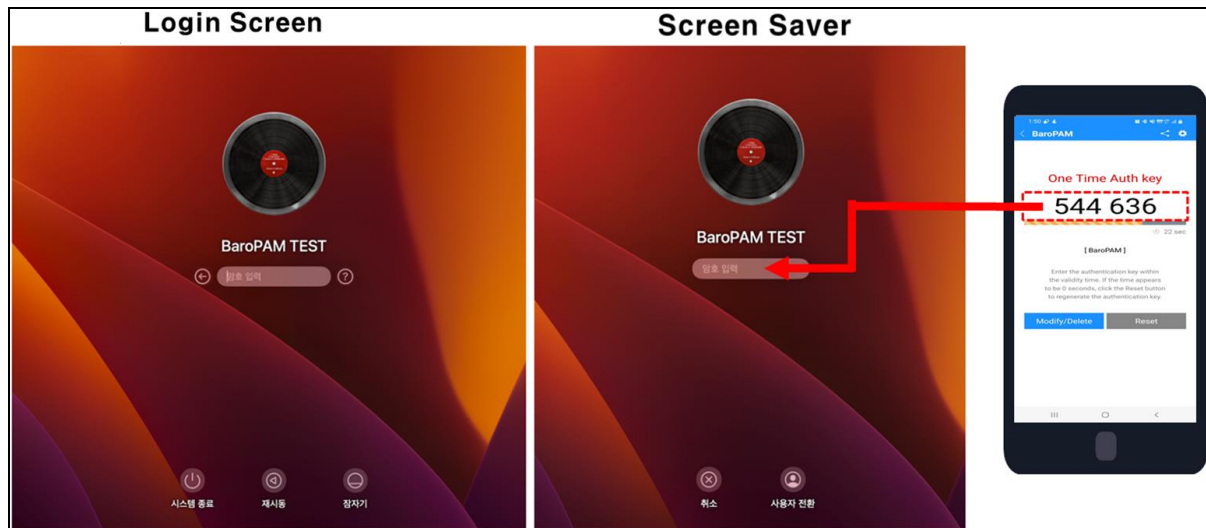
2.3 Mac OS X login method

First, you must enter the same "cycle time, secure key, server name" entered on the "BaroPAM Setup" screen on the "Server Information Registration" screen of the "BaroPAM" app.



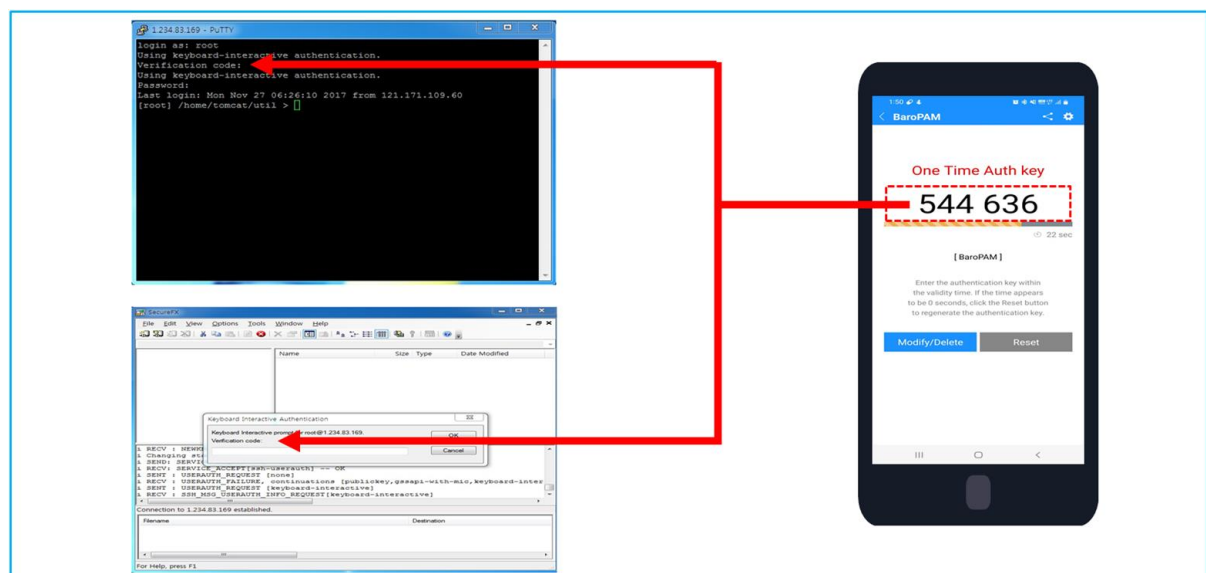
1) GUI login and screen saver screen

Just enter the password first on the GUI login screen or Screen Saver screen of Mac OS X, create a **OTA key** in the **BaroPAM** app on your smartphone, and then enter the **OTA key**. For example, if the password is "baropam" and the **OTA key** is "544636", enter "baropam544636".



2) ssh/sftp connect tool

When logging in to the Mac OS X environment, enter your user account (Username), generate a **OTA key** in the "BaroPAM" app on your smartphone, and enter the **OTA key** and "Password" you created in "Verification code:". Clicking the "Enter" button requests authentication from the **BaroPAM** module, and if verification succeeds, the login authentication policy of Mac OS X is activated.



If the **BaroPAM** verification module fails to authenticate the **OTA key** entered on the Mac OS X login screen, an "Access denied." message appears on the login screen. Various messages related to **BaroPAM** authentication are left in syslog.

```
Mar 25 11:10:42 qsh-0415 sshd[27482]: pam_unix(sshd:session): session closed for user root
```

```

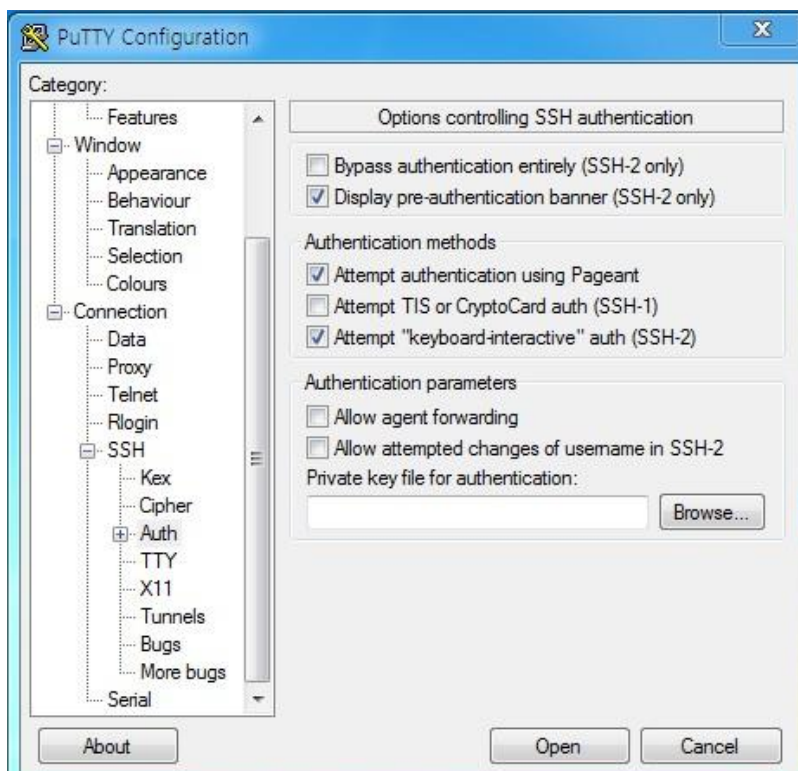
Mar 25 13:52:25 qsh-0415 sshd(pam_baro_auth)[2052]: Try to update RATE_LIMIT line.[3 30
1648183945]
Mar 25 13:52:45 qsh-0415 sshd[2050]: Accepted keyboard-interactive/pam for root from
222.108.117.41 port 49835 ssh2
Mar 25 13:52:45 qsh-0415 sshd[2050]: pam_unix(sshd:session): session opened for user root by
(uid=0)
Mar 25 15:25:47 qsh-0415 sshd(pam_baro_auth)[14119]: Try to update RATE_LIMIT line.[3 30
1648189547]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Verification code generation
failed.[Success]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Invalid verification code
Mar 25 15:25:51 qsh-0415 sshd[14118]: Received disconnect from 222.108.117.41: 13: The user
canceled au

```

2.4 ssh/sftp connection tool

For putty)

When connecting with Putty, you can do the same as the normal connection process, but there is one thing you need to set. After selecting **attempt "Keyboard-Interactive" auth (SSH-2)** in "**connection - > SSH -> auth**" in the environment setting, connect to SSH.

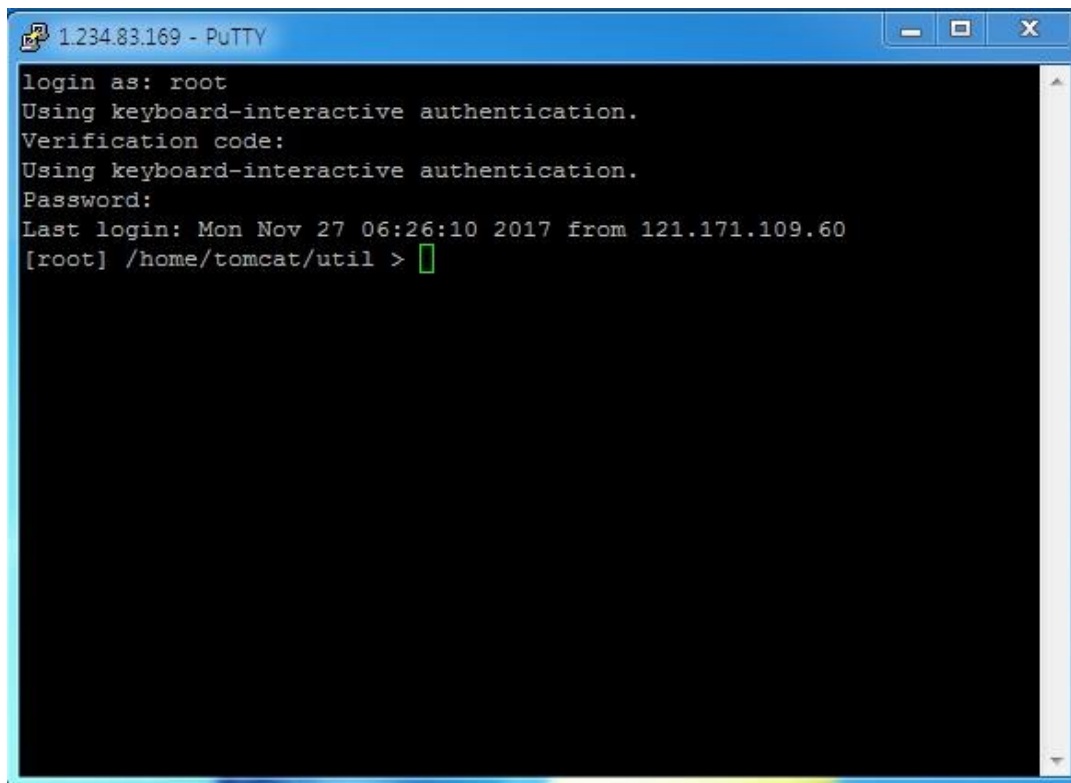


Putty Download and Documentation can be found at the following URL.

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

When prompted to enter "**Verification code:**", enter the **OTA key** generated by the **BaroPAM** app.

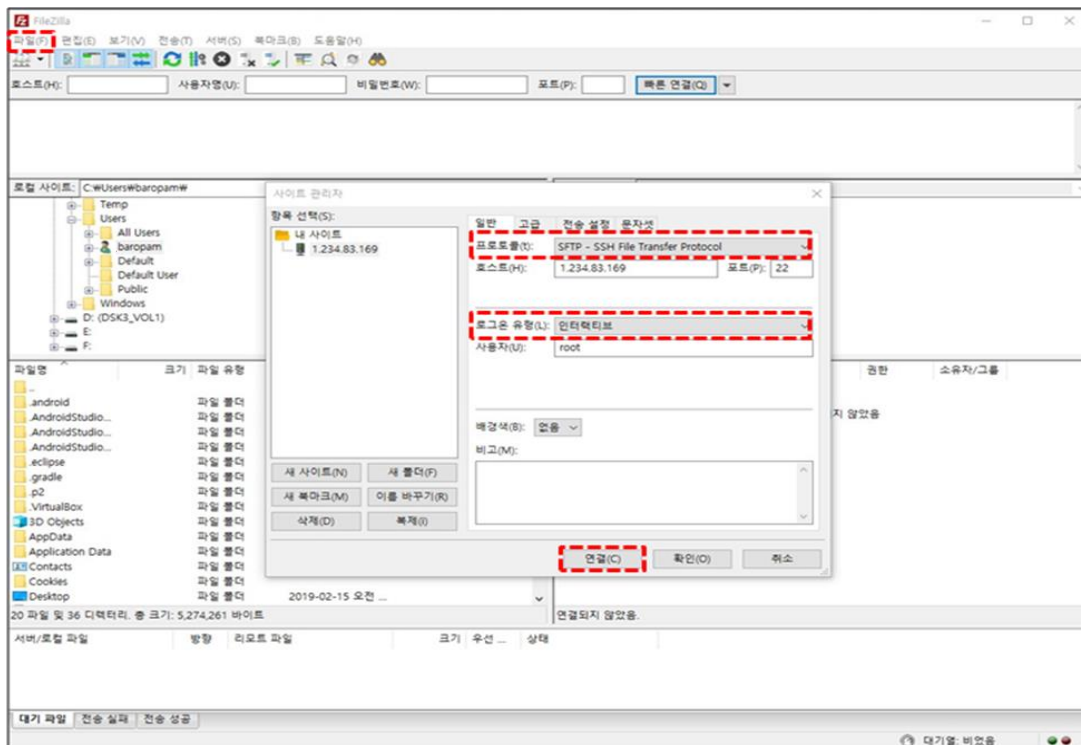
If authentication is successful, you can enter your SSH login password as follows.

A screenshot of a PuTTY terminal window titled "1.234.83.169 - PuTTY". The terminal displays the following text: "login as: root", "Using keyboard-interactive authentication.", "Verification code:", "Using keyboard-interactive authentication.", "Password:", "Last login: Mon Nov 27 06:26:10 2017 from 121.171.109.60", and "[root] /home/tomcat/util >". A green cursor is visible at the end of the command line.

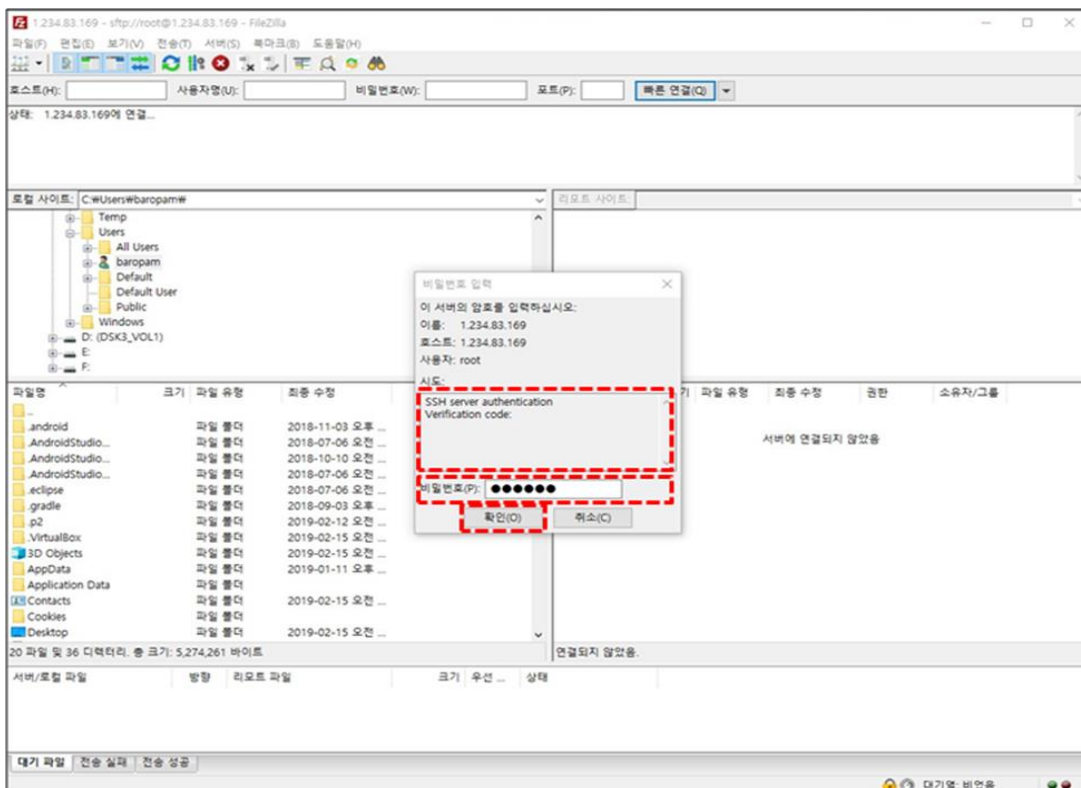
```
login as: root
Using keyboard-interactive authentication.
Verification code:
Using keyboard-interactive authentication.
Password:
Last login: Mon Nov 27 06:26:10 2017 from 121.171.109.60
[root] /home/tomcat/util >
```

For FileZilla)

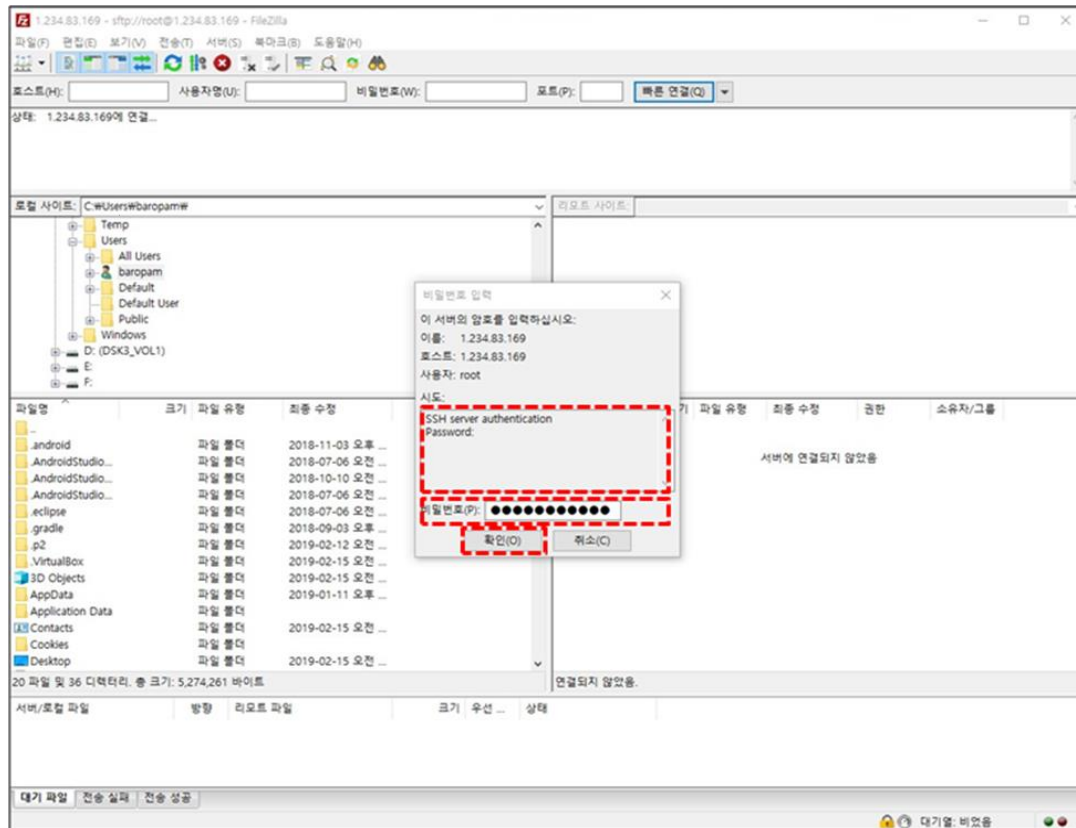
When connecting with FileZilla, it is different from the normal connection process. Select "File(F) → Site Manager(S)" from the top left menu and select "SFTP – SSH File Transfer Protocol" from the "Protocol(t):" item on the general tab screen. and "Logon type(L):" items, select "Interactive" and click the "Connect(C)" button as follows.



Then, the password input screen appears as follows. Check the contents of "Attempt:" on the password input screen, enter the **OTA key** generated on the smartphone into the "Password(P):" input field, and click the "OK(O)" button.



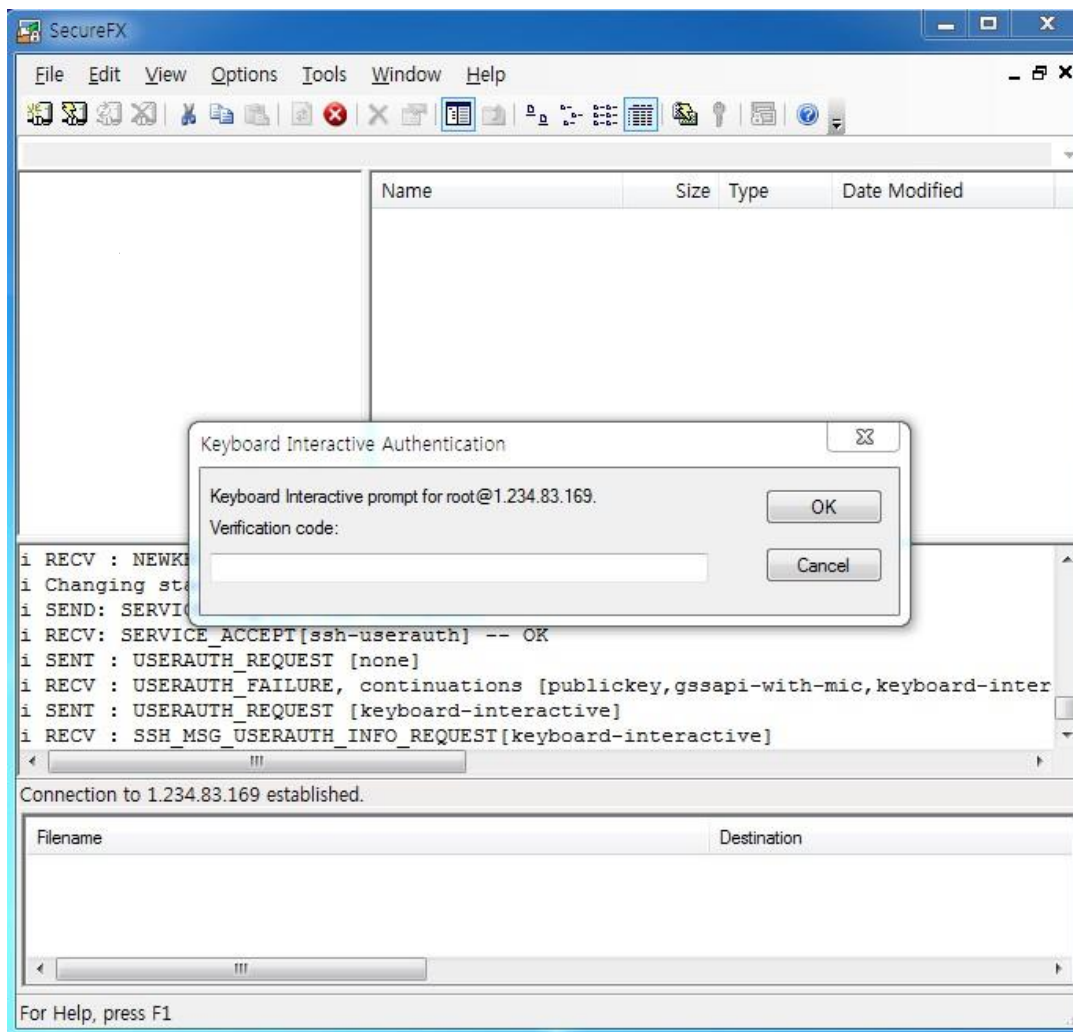
Then, the password input screen appears as follows. Check the "Attempt:" content on the password input screen, enter the password for the login account in the "Password(P):" input field, and click the "OK(O)" button to connect to the server.



For SFTP)

When prompted to enter "Verification code:", enter the **OTA key** generated by the **BaroPAM** app.

If authentication is successful, you can enter your SFTP login password as follows.



SecureFX Download and Documentation related materials can be found at the following URL.

<https://www.vandyke.com/>

In conclusion, **2nd authentication** can be an effective means of protecting password authentication by adding an extra layer of protection. Whether or not to use it depends on the user's choice, but the adoption of **2nd authentication** is an industry trend.

3. Remove BaroPAM

3.1 Remove the BaroPAM environment

If you do not use the BaroPAM module while BaroPAM is installed, comment (#) or delete the settings in the sshd, su, and sudo files as follows.

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
#auth required /usr/local/baropam/pam_baro_auth.so nullok secret=/usr/local/baropam/.baro_auth
```

Among the contents of the "/etc/ssh/sshd_config" file configured for the sshd daemon, the following parameters must be changed.

Factor	Before	After	Etc
PasswordAuthentication	no	yes	
ChallengeResponseAuthentication	yes	no	
UsePAM	yes	no	

After completing the sshd configuration, make sure that the PAM module is properly removed and restart the SSH Server.

```
[root] /usr/local/baropam > launchctl stop com.openssh.sshd
[root] /usr/local/baropam > launchctl start com.openssh.sshd
```

4. BaroPAM FAQ

Message: If you cannot log in because the OTA key does not match

Cause: BaroPAM is a time synchronization method, so the time of the phone and Windows or Server must be the same.

Action: Check if the phone and Windows or Server time are correct.

Message: Feb 7 07:59:09 eactive sshd(pam_baro_auth)[29657]: ACL file ".baro_acl" must only be accessible by user id root

Cause: Permission of .baro_acl file is different.

Action: Set Permission of .baro_acl file to 444.

Message: Feb 7 08:02:15 eactive sshd(pam_baro_auth)[29739]: Failed to acl file read ".baro_acl"

Cause: Occurs when the .baro_acl file does not exist.

Action: Create a .baro_acl file in the baropam home directory. (Set Permission to 444)

Message: Cannot look up user id xxxxx

Cause: Occurs when user ID xxxxx cannot be retrieved.

Action: Register user id xxxxx in /etc/passwd file.

Message: Failed to secret file read .baro_auth

Cause: Occurs when the secret file does not exist.

Action: Check the existence of the secret file.

Message: Secret file .baro_auth must only be accessible by root

Cause: Occurs when the permission of the .baro_auth file is different.

Action: Set Permission of .baro_auth file to 444.

Message: Invalid file size for .baro_auth

Cause: Occurs when the size of the .baro_auth file is not $1 < \text{size} < 64K$.

Action: Check the size of the .baro_auth file.

Message: Could not read .baro_auth

Cause: Occurs when the .baro_auth file does not exist or the permission of the file is not 444.

Action: Check the existence of the .baro_auth file and the permission of the file.

Message: Invalid file contents in .baro_auth

Cause: Occurs when the content (rule) of the .baro_auth file is incorrect.

Action: Check the contents of the .baro_auth file.

Message: Failed to create tmp secret file[*error message*]

Cause: Occurs when a temporary secret file cannot be created.

Action: Check the error message for the reason why the temporary secret file could not be created.

Message: Failed to open tmp secret file .baro_auth~[*error message*]

Cause: Occurs when the temporary secret file .baro_auth~ could not be opened.

Action: Check the error message for the reason why the temporary secret file .baro_auth~ could not be opened.

Message: Secret file .baro_auth changed while trying to use one-time authentication key

Cause: Occurs when secret file .baro_auth is changed while using OTA key.

Action: Try logging in again.

Message: Failed to update secret file .baro_auth[error message]

Cause: Occurs when the secret file cannot be changed.

Action: Check the error message for why the secret file could not be changed.

Message: Invalid RATE_LIMIT option. Check .baro_auth

Cause: Occurs when the RATE_LIMIT setting value of the secret file .baro_auth file is set incorrectly.

Action: Check the setting values of the limit count ($1 < \text{RATE_LIMIT} < 100$) and the limit time ($1 < \text{interval} < 3600$).

Message: Invalid list of timestamps in RATE_LIMIT. Check .baro_auth

Cause: Occurs when updated timestamps in the RATE_LIMIT option among the contents of the .baro_auth file, which is a secret file, are incorrect.

Action: Check the updated timestamps in the RATE_LIMIT option of the .baro_auth file, which is the secret file.

Message: Try to update RATE_LIMIT line.

Cause: The message displayed when you log in normally.

Action: No action

Message: Too many concurrent login attempts. Please try again.

Cause: When the DISALLOW_REUSE option of the .baro_auth file, which is the secret file, (In the OTA key generation cycle, one login only) is set.

Occurs when login is retried within the OTA key creation cycle after successful login.

Action: Login retry after OTA key generation cycle.

Message: Trying to reuse a previously used time-based code.

Retry again in 30 seconds.

Warning! This might mean, you are currently subject to a man-in-the-middle attack.

Cause: The DISALLOW_REUSE option of the .baro_auth file, which is the secret file, is an option in preparation for man-in-the-middle attacks.

A man-in-the-middle attack occurs when an unauthorized entity places itself between two communication systems and intercepts the passing of information that is currently in progress.

In a nutshell, what could be called a modern wiretapping system.

Action: No action

Message: Failed to allocate memory when updating .baro_auth

Cause: Occurs when memory allocation fails when updating the secret file, .baro_auth.

Action: Technical support

Message: Can't find SECURE_KEY[error message]

Cause: Occurs when there is no SECURE_KEY option or set value in the .baro_auth file, which is the secret file.

Action: Check the SECURE_KEY option or setting value of the .baro_auth file, which is the secret file.

Message: Verification code generation failed.[error message]

Cause: Occurs when OTA key verification fails.

Action: Login retry.

Message: Invalid verification code

Cause: Occurs when OTA key verification fails.

Action: Login retry.

Message: Invalid verification code

Can not make/remove entry for session.

Cause: The server's system time is not correct.

Action: Check if the system time of the server is correct with the date command, and if it is incorrect, adjust the time.

1. date Command Change the server's system time (temporary solution)
2. Check whether ntp is set, and if it is set, reduce the cycle for setting the ntp time.
If not set, ntp must be set.

Message: Mar 12 15:37:01 baropam gdm(pam_baro_auth)[1215]: [ID 128276 auth.error] No user name available when checking verification code

Cause: If you are not a usable user when verifying the authorization code (occurs when you are not a registered user).

Action: Check with your system administrator to see if your Login-ID is registered.

Message: Apr 3 13:06:13 kdn sshd[3577]: PAM unable to dlopen(/usr/local/baropam/pam_baro_auth.so): /usr/local/baropam/pam_baro_auth.so: cannot open shared object file: No such file or directory

Apr 3 13:06:13 kdn sshd[3577]: PAM adding faulty module: /usr/local/baropam/pam_baro_auth.so

Cause: It occurs because the /usr/local/baropam/pam_baro_auth.so file does not exist.

Action: Check if the BaroPAM module file (pam_baro_auth.so) exists. If not, copy it from the BaroPAM installation file.

Message: mm_log_handler: write: Broken pipe

mm_request_send: write: Broken pipe

Cause: This is how often keepalive messages should be sent to the server within seconds.

The server may close connections that have been idle for too long. client (ServerAliveInterval) or You can update the server (ClientAliveInterval).

Action: You can set ServerAliveInterval in /etc/ssh/ssh_config on the client machine or ClientAliveInterval in /etc/ssh/sshd_config on the server machine. If the error persists, the interval should be reduced.

ServerAliveInterval ==> If no data is received from the server, ssh sets the timeout interval in seconds to request a response from the server by sending a message over an encrypted channel. Defaults to 0, indicating that this message is not sent to the server. This option only applies to protocol version 2.

ClientAliveInterval ==> If no data is received from the client, sshd sends a message over an encrypted channel to request a response from the client. Default is 0. Indicates that this message is not sent to the client. This option only applies to protocol version 2.

To update your server(and restart your sshd) ==> Update the server (to restart sshd) and echo "ClientAliveInterval 60" | sudo tee -a /etc/ssh/sshd_config

Or client-side: ==> Or client-side:

echo "ServerAliveInterval 60" >> ~/.ssh/config

ClientAliveInterval: Interval to check if client is alive

ClientAliveCountMax: The number of times the connection is maintained even if there is no response from the client

For example, if ClientAliveInterval=15, ClientAliveCountMax=3, disconnect after 45 seconds

Message: May 19 12:37:37 baropam sshd(pam_baro_auth)[1416]: Failed to acl file read "(null)"

Cause: Occurs due to acl file existence and file permission issues.

Action: Create empty acl file .baro_acl file with 444 permissions.

Message: Failed to compute location of secret file

Cause: Occurs when the secret file set in pam does not exist in the directory.

Action: If the secret file set in pam does not exist in the directory, the secret file must be created in the directory.

ex) auth required /usr/local/baropam/pam_baro_auth.so nullok
secret=/usr/local/baropam/.baro_auth
encrypt=no

Message: Failed to compute location of encrypt flag

Cause: Occurs when the encryption flag does not exist in pam.

Action: Encryption flags (yes, no) must be set in pam.

ex) auth required /usr/local/baropam/pam_baro_auth.so nullok
secret=/usr/local/baropam/.baro_auth
encrypt=no

Message: If ssh connection is not available after installing HamoniKR OS

Cause: It occurs because the firewall of HamoniKR OS is set.

Action: After disabling the firewall of HamoniKR OS, restart ufw.

> sudo ufw disable
> sudo service ufw restart

Message: BaroPAM applied to Screen saver is released after rebooting Grooroom OS

Cause: When Grooroom OS is rebooted, lightdm, a setting file related to Screen saver, is initialized.

Action: Just set BaroPAM in the restore file "/usr/share/debian-system-adjustments/pam.d/lightdm".

Message: Oct 14 10:09:43 baropam sshd[18075]: PAM unable to dlopen(/usr/local/baropam/pam_baro_auth.so):

/usr/local/baropam/pam_baro_auth.so: undefined symbol: curl_easy_setopt

Cause: It occurs because the library related to the web development tool cURL (Client for URLs) does not exist.

Action: For Redhat series, use "yum install curl" and others with "sudo apt-get install curl" command.

Message: Did not receive verification code from user

error: ssh_msg_send: write: Broken pipe

Cause: Occurs when the secure key is set incorrectly.

Action: Check the set Secure key.

Check if the secure key is provided by the vendor.

Message: PAM: authentication thread exited unexpectedly.

*** glibc detected *** su: free(): invalid pointer: 0x00002aede020c9e2 ***

Cause: Occurs when the BaroPAM environment setting file (.baro_nurit) does not exist.

Action: Check if the BaroPAM environment setting file (.baro_nurit) exists. If not, copy it from the BaroPAM installation file.

5. About BaroPAM



Version 1.0 – Official Release – 2016.12.1
Copyright © Nurit corp. All rights reserved.
<http://www.nurit.co.kr>

Company: Nurit Co., Ltd.
Registration Number: 258-87-00901
CEO: Jongil Lee
Tel: +8210-2771-4076(Technical support, sales inquiry)
email: mc529@nurit.co.kr
Address: #913, 15, Magokjungang 2-ro, Gangseo-gu, Seoul (Magok-dong, Magok Techno Tower 2)