

# **BaroPAM solution installation summary**

**for multi-layer authentication to strengthen the security of information assets (MAC OS X)**

**May, 2025**



# II . Install BaroPAM Mac OS X

## 1. Pre-requisites

### 1) Check hostname and OS version

```
[root@baropam root]# uname -a
Darwin baropam 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
```

### 2) Check the versions of ssh and openssl to provide ssh and sftp services

```
[root@baropam root]# ssh -V
OpenSSH_9.0p1, LibreSSL 3.3.6
```

```
[root@baropam baropam]# openssl
OpenSSL> version
LibreSSL 3.3.6
OpenSSL> q
```

Remember the following  
Mac OS X information

-Hostname/OS version  
Apple CPU: arm64  
Intel CPU: X86\_64  
-ssh/openssl version

# II. Install BaroPAM Mac OS X

## 2. BaroPAM install

### 1) Create a directory to install the BaroPAM module and set permissions (with the root account)

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

### 2) Authorize the directory to install the BaroPAM module

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

### 3) Download BaroPAM installation module (Check OS version)

<https://mc529.tistory.com/1407>

#### If you know the tar file name to install

```
[root] /usr/local/baropam > wget http://nuriapp.com/download/libpam_baro_auth-osx13.1.1-x64.tar
```

```
[root] /usr/local/baropam > wget http://nuriapp.com/download/libpam_baro_auth-osx13.1.1-arm64.tar
```

### 4) Unpack the BaroPAM installation module (eg for MacOS Ventura 8.x 64bit)

```
[root] /usr/local/baropam > tar -xvf libpam_baro_auth-osx13.1.1-x64.tar → Intel CPU
```

```
[root] /usr/local/baropam > tar -xvf libpam_baro_auth-osx13.1.1-arm64.tar → Apple CPU
```

### 5) Check the BaroPAM module

```
[root] /usr/local/baropam > ls -al
```

Total 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	→ ACL file
-r--r--r--	1	root	root	305	7월 2 14:41	.baro_auth	→ Configuration file for PAM authentication
-r--r--r--	1	root	root	290	6월 30 12:55	.baro_curl	→ Configuration file for cURL authentication
-r--r--r--	1	root	root	287	2월 28 12:19	.baro_sql	→ Connection information linked to MariaDB with PAM authentication
-rwxr-xr-x	1	root	root	69149	4월 6 19:12	baro_auth	→ An executable program that creates environment files for PAM authentication
-rwxr-xr-x	1	root	root	65072	6월 29 16:36	baro_curl	→ An executable program that creates environment files for cURL authentication
-rwxr-xr-x	1	root	root	57074	2월 28 12:18	baro_sql	→ An executable program that generates connection information linked to MariaDB
drwxr-xr-x	2	root	root	4096	7월 20 2021	jilee	→ Directory where PAM authentication security-related files exist
-rwxr-xr-x	1	root	root	152649	6월 9 08:19	pam_baro_auth.so	→ A module that verifies the OTA key of PAM authentication
-rwxr-xr-x	1	root	root	116158	6월 30 12:54	pam_baro_curl.so	→ A module that verifies the OTA key of cURL authentication
-rwxr-xr-x	1	root	root	170863	2월 28 12:18	pam_baro_sql.so	→ A module that verifies the OTA key of PAM authentication(MariaDB)
-rw-r--r--	1	root	root	221	6월 27 15:59	setauth.sh	→ Shell script to create environment file for PAM authentication
-rw-r--r--	1	root	root	150	6월 29 16:29	setcurl.sh	→ Shell script to create environment file for cURL authentication
-rw-r--r--	1	root	root	180	2월 28 12:19	setsql.sh	→ Shell script to create environment file for PAM authentication(MariaDB)

# II . Install BaroPAM Mac OS X

## 3. Create BaroPAM configuration file (PAM authentication: .baro\_auth)

### 1) Shell script to create environment file (setauth.sh)

```
[root] /usr/local/baropam > cat setauth.sh
#!/bin/sh
```

```
export BAROPAM_HOME=/usr/local/baropam;
```

```
$BAROPAM_HOME/baro_auth -r 3 -R 30 -t 30 -k app512 -e no -A deny -a $BAROPAM_HOME/.baro_acl -S j1qlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s $BAROPAM_HOME/.baro_auth
```

### 2) Information on configuration options in the BaroPAM configuration file

Opt no	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	

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**

```
[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
```

### 3) Run the setauth.sh shell script

```
[root] /usr/local/baropam > sh setauth.sh
```

# II . Install BaroPAM Mac OS X

## 3. Create BaroPAM configuration file (PAM authentication: .baro\_sql)

### 1) Shell script to create environment file (setsql.sh)

```
[root] /usr/local/baropam > cat setsql.sh
#!/bin/sh
```

```
export BAROPAM_HOME=/usr/local/baropam;
```

```
$BAROPAM_HOME/baro_sql -H nurit.co.kr -e no -u nurit -p baropams -d baropamdb -P 3306 -s $BAROPAM_HOME/.baro_sql
```

### 2) Information on configuration options in the BaroPAM configuration file

Opt ino	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	3306	
-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	

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

```
[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 j1qlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_TYPE deny
" MIDDLE_TYPE DISALLOW_REUSE
" MIDDLE_TIME 58014762
" ENV_TYPE share
```

### 3) Run the setsql.sh shell script

```
[root] /usr/local/baropam > sh setsql.sh
```

# II . Install BaroPAM Mac OS X

## 3. Create BaroPAM configuration file (cURL authentication: .baro\_curl)

### 1) Create BaroPAM configuration file (cURL authentication)

```
[root] /usr/local/baropam > cat setcurl.sh
```

```
#!/bin/sh
```

```
HOSTNAME=`hostname`
```

```
export BAROPAM_HOME=/usr/local/baropam;
```

```
$BAROPAM_HOME/baro_curl -r 3 -R 30 -t 30 -k app512 -H $HOSTNAME -e no -u http://1.23.456.789/baropam/web/result\_curl.jsp -s
```

```
$BAROPAM_HOME/.baro_curl
```

### 2) Information on configuration options in the BaroPAM configuration file

Option	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 (appl, app256, app384, app512: app, card1, card256, card384, card512: authentication card)	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)	<a href="http://1.23.456.789/baropam/web/result_curl.jsp">http://1.23.456.789/baropam/web/result_curl.jsp</a>	
-s	File name including the directory in which to create the BaroPAM configuration file	/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

```
[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 nurit.co.kr
```

```
" DISALLOW_REUSE
```

### 3) Run the setcurl.sh shell script

```
[root] /usr/local/baropam > sh setcurl.sh
```

# || . Install BaroPAM Mac OS X

## 4. BaroPAM settings (PAM authentication: pam\_baro\_auth.so)

### 1) at the top of the sshd file

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
```

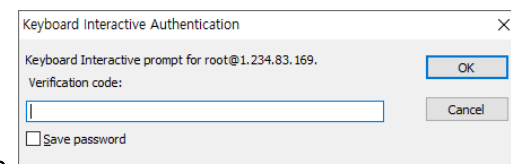
```
auth required /usr/local/baropam/pam_baro_auth.so nullok secret=/usr/local/baropam/.baro_auth encrypt=no
```

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

```
auth required /usr/local/baropam/pam_baro_auth.so forward_pass secret=/usr/local/baropam/.baro_auth encrypt=no
```

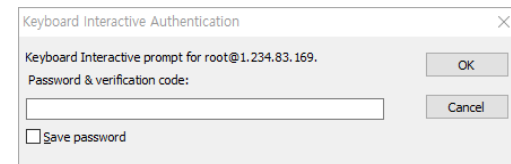
→ When entering a **OTA key** like a password in the password input window (Password & verification code:) using **forward\_pass**, enter the password first and then enter the **OTA key** without a space. For example, if the password is "baropam" and the **OTA key** is "123456", enter "baropam123456"

Note) xrdp supports only the "forward\_pass" option in /etc/pam.d/xrdp-sesman configuration.



### 2) 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↵	no↵	yes↵	↵
KbdInteractiveAuthentication↵			
UsePAM↵	no↵	yes↵	↵



### 3) When using the BaroPAM module, the ACL for the account to be excluded from 2nd authentication needs to be excluded

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

```
barokey
```

```
baropam
```

### 4) Set at the top of screensaver, authentication file, etc

```
[root] /usr/local/baropam > vi /etc/pam.d/screensaver, authentication
```

```
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 "123456", enter "baropam123456".



# II. Install BaroPAM Mac OS X

## 4. BaroPAM settings (PAM authentication: pam\_baro\_sql.so)

### 1) at the top of the sshd file

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
```

```
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

→ The auth parameter sets sshd, su, sudo, screensaver, xrdp-sesman, etc., which are places that authenticate using BaroPAM.

```
auth required /usr/local/baropam/pam_baro_sql.so forward_pass secret=/usr/local/baropam/.baro_sql encrypt=no auth=sshd
```

→ When entering a OTA key like a password in the password input window (Password & verification code:) using forward\_pass, enter the password first and then enter the OTA key without a space. For example, if the password is "baropam" and the OTA key is "123456", enter "baropam123456"

Note) xrdp supports only the "forward\_pass" option in /etc/pam.d/xrdp-sesman configuration.

### 2) 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	

### 3) When using the BaroPAM module, if you need to exclude an account from 2nd authentication in the ACL, you must use Mariadb's ACL setting table

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

```
barokey
```

```
baropam
```

### 4) Set at the top of screensaver, authentication file, etc

```
[root] /usr/local/baropam > vi /etc/pam.d/screensaver, authentication
```

```
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 "123456", enter "baropam123456".



# II. Install BaroPAM Mac OS X

## 4. BaroPAM settings (cURL authentication: pam\_baro\_curl.so)

### 1) at the top of the sshd file

```
[root] /usr/local/baropam > vi /etc/pam.d/sshd
```

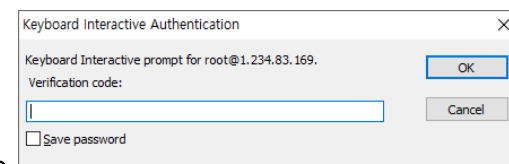
```
auth required /usr/local/baropam/pam_baro_curl.so nullok secret=/usr/local/baropam/.baro_curl encrypt=no
```

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

```
auth required /usr/local/baropam/pam_baro_curl.so forward_pass secret=/usr/local/baropam/.baro_curl encrypt=no
```

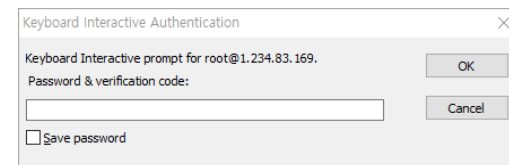
→ When entering a **OTA key** like a password in the password input window (Password & verification code:) using **forward\_pass**, enter the password first and then enter the **OTA key** without a space. For example, if the password is "baropam" and the **OTA key** is "123456", enter "baropam123456"

Note) xrdp supports only the "forward\_pass" option in /etc/pam.d/xrdp-sesman configuration.



### 2) 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	no	yes	
KbdInteractiveAuthentication			
UsePAM	no	yes	



### 3) When using the BaroPAM module, the ACL for the account to be excluded from 2nd authentication needs to be excluded

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

```
barokey
```

```
baropam
```

### 4) Set at the top of screensaver, authentication file, etc

```
[root] /usr/local/baropam > vi /etc/pam.d/screensaver, authentication
```

```
auth required /usr/local/baropam/pam_baro_curl.so use_first_pass forward_pass nullok secret=/usr/local/baropam/.baro_curl 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 "123456", enter "baropam123456".

# II . Install BaroPAM Mac OS X

## 5. How to apply BaroPAM

**Password alone is never safe when logging in to all information assets, and new application methods (additional authentication, password replacement, new password) that can replace or additionally authenticate the password (2nd authentication) are required each time it is used**

### 1) additional authentication

**Apply one-time authentication key as additional authentication (2nd authentication) other than account (login-ID) and password(ID/PW/OTA)**

```
auth required /usr/local/baropam/pam_baro_auth.so nullok secret=/usr/local/baropam/.baro_auth encrypt=no
auth required /usr/local/baropam/pam_baro_sql.so nullok secret=/usr/local/baropam/.baro_sql encrypt=no auth=sshd
auth required /usr/local/baropam/pam_baro_curl.so nullok secret=/usr/local/baropam/.baro_curl encrypt=no
```

### 2) password replacement

**Remove password and replace with OTA key (ID/OTA) – OTA key**

```
auth required /usr/local/baropam/pam_baro_auth.so forward_pass secret=/usr/local/baropam/.baro_auth encrypt=no
auth required /usr/local/baropam/pam_baro_sql.so forward_pass secret=/usr/local/baropam/.baro_sql encrypt=no auth=sshd
auth required /usr/local/baropam/pam_baro_curl.so forward_pass secret=/usr/local/baropam/.baro_curl encrypt=no
```

**Note) When replacing the password with a OTA key, the password of the account (login-ID) must be set the same as the account.**

### 3) new password

**By combining the password and the OTA key, a new OTP is generated and applied for each OTA key generation cycle(ID/PW+OTA)**

```
auth required /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no
auth required /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql encrypt=no auth=sshd
auth required /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no
```

**Note) Mac OS X does not support the autologin function, so a password must exist.**



### Added) How to apply .baro\_auth



auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no	→ Default setting
auth required /usr/baropam/pam_baro_auth.so nullok secret={HOME}/.baro_auth encrypt=no	→ Set in the home directory per account
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/auth/.{USER}_auth encrypt=no	→ Configuration file settings per account

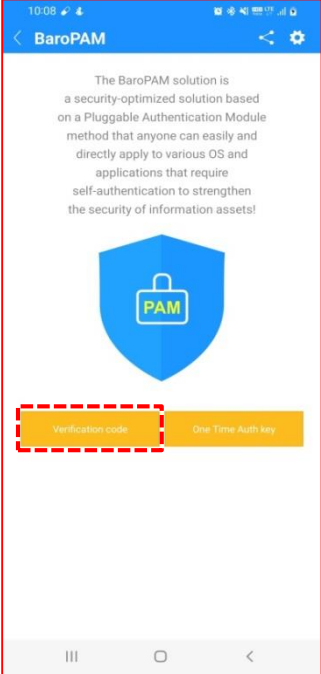
# || . Install BaroPAM Mac OS X

## 6. Install the BaroPAM app and set up information

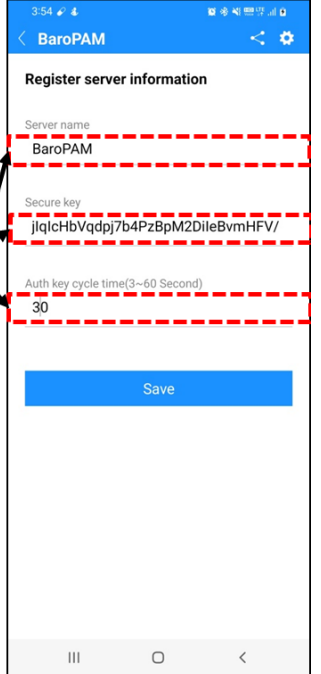
### BaroPAM App Download







```
$ cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME BaroPAM
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```



**BaroPAM** app can be used on Android 6.0 (Marshmalliw) API 23, iOS 13.0 or higher, and does not support landscape mode. After installing the BaroPAM app, launch the BaroPAM app and click the "Verification Code" button on the menu selection screen to enter the BaroPAM configuration file ".baro\_auth". You must enter the same "cycle time, secure key, server name" set in the "Register server information" screen of the BaroPAM app. If you set the app code (kr: Korean, en: English, jp: Japanese, cn: Chinese) on the **BaroPAM** app settings -> change screen settings screen, the **BaroPAM** app changes accordingly.

**Message:** The "OTA key" is incorrect because the date and time of the Android phone or iPhone are different from the current time.

**Cause:** This is caused by not using the time provided by the network for the Android or iPhone's date and time.

**Action:** For Android phones, go to "Settings" -> "General management" -> "Date and time" -> "Automatic date and time" and "Automatic time zone" -> "Allow" For iPhone, go to "Settings" -> "Date & Time" -> "Set Automatically" -> "Allow"

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

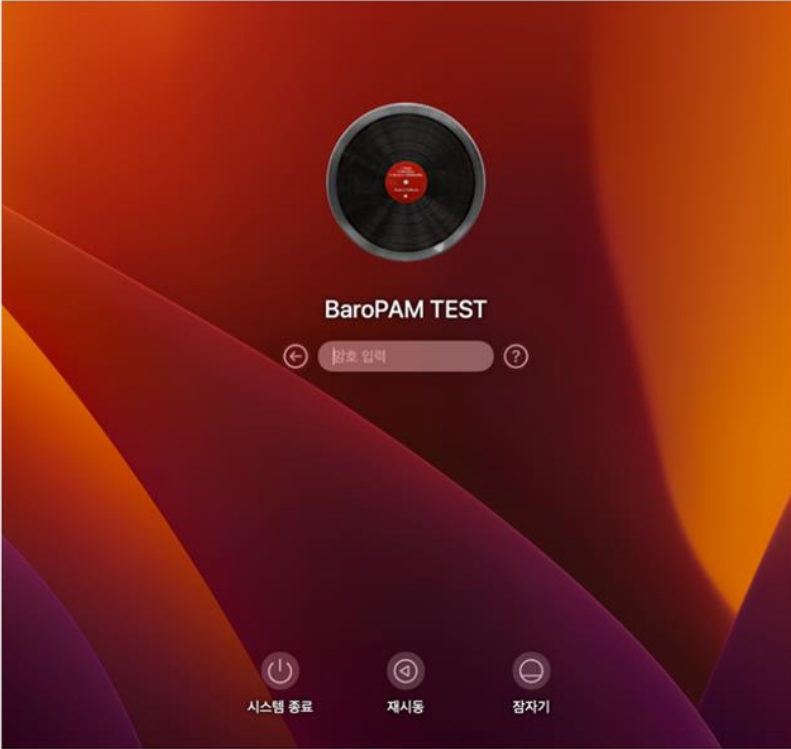
**Cause:** BaroPAM is a time synchronization method, so the time of the phone and Server must be the same.

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

## II. Install BaroPAM Mac OS X

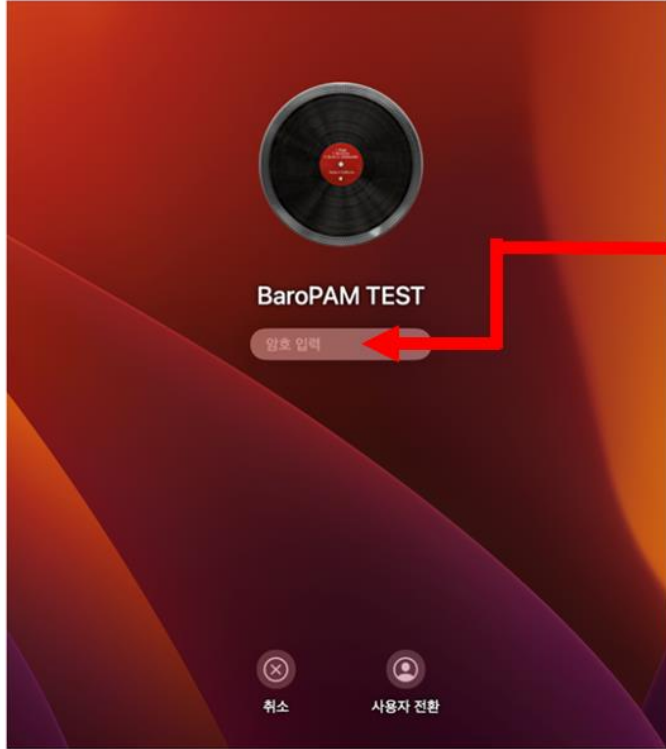
### 7. Mac OS X login (Login or Screen Saver screen)

#### Login Screen

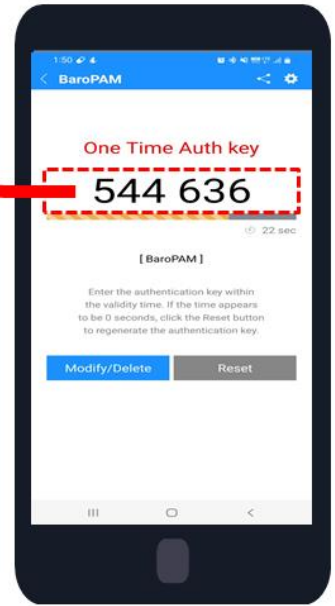


The Login Screen features a vinyl record icon at the top. Below it, the text "BaroPAM TEST" is displayed. A password input field with the placeholder "암호 입력" (Password Input) is shown, flanked by back and forward arrows. At the bottom, there are three icons: a power button labeled "시스템 종료" (System Shutdown), a power button labeled "재시동" (Restart), and a power button labeled "잠자기" (Sleep).

#### Screen Saver



The Screen Saver also features a vinyl record icon at the top. Below it, the text "BaroPAM TEST" is displayed. A password input field with the placeholder "암호 입력" (Password Input) is shown, flanked by back and forward arrows. At the bottom, there are two icons: a power button labeled "취소" (Cancel) and a power button labeled "사용자 전환" (Switch User).

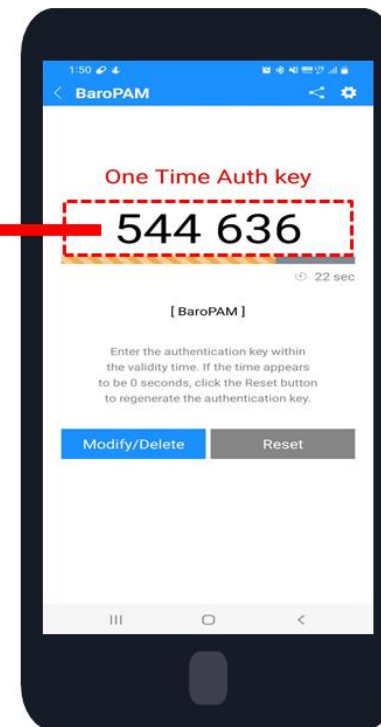
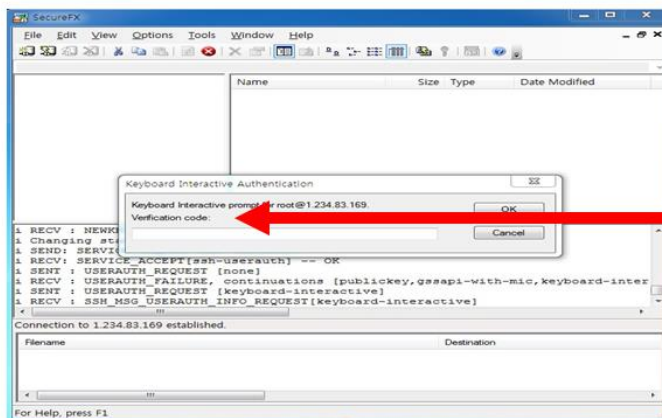
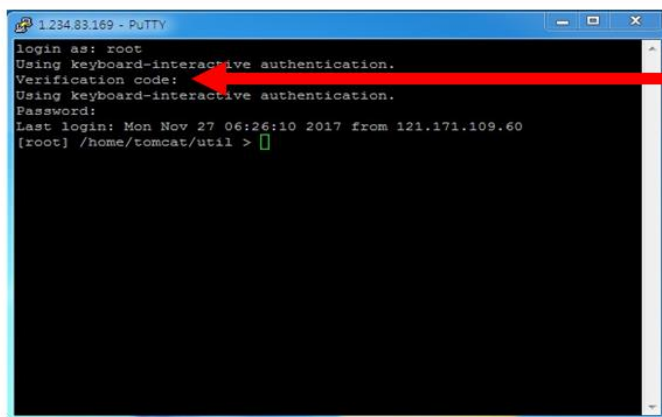


The BaroPAM app on a smartphone displays a "One Time Auth key" of "544 636" within a red dashed box. A red arrow points from this key to the password input field on the Screen Saver. Below the key, it says "[ BaroPAM ]" and "Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key." There are two buttons at the bottom: "Modify/Delete" and "Reset".

Enter your Linux user account (Username), generate a **OTA key** in the **BaroPAM** app on your smartphone, and create a **OTA key** in "Verification code" and Linux "Password", click "Enter" or "OK" button to request authentication to the **BaroPAM** module, and if verification is successful, Linux is logged in.

# || . Install BaroPAM Mac OS X

## 7. Mac OS X login (ssh/sftp access tool)



Enter the user account (Username) of Mac OS X, generate a **OTA key** in the **BaroPAM** app on the smartphone, and then enter the **OTA key** generated in "Verification code" and "Password" of Mac OS X, and enter "Enter If you click the " or "OK" button, authentication is requested to the **BaroPAM** module, and if verification is successful, you are logged in to Mac OS X

# || . Install BaroPAM Mac OS X

## 8. What to check when a problem occurs

### 1) Check system login Syslog

Check the message that "pam\_baro\_auth" exists in the /var/log/system.log file

### 2) Check Mac OS X system information

\$ uname -a

### 3) Check Openssl information

\$ openssl version

### 4) Check the BaroPAM installation directory and file permissions

\$ ls -al /usr/local/baropam

### 5) Check the BaroPAM installed module

\$ file pam\_baro\_auth.so

\$ otool -L pam\_baro\_auth.so

### 6) Check BaroPAM configuration information

\$ cat /usr/local/baropam/.baro\_auth

### 7) Check your PAM settings

\$cat /etc/pam.d/sshd or su or sudo or screensaver or authotization etc

### 8) Check sshd\_config settings

\$ cat /etc/ssh/sshd\_config

### 9) Check NTP settings and status

\$ cat /etc/ntp.conf

\$ ntpq -p



**Password** you don't need to remember!  
**BaroPAM** will be with you.

**Thank You!**

[www.nurit.co.kr](http://www.nurit.co.kr)  
**mc529@nurit.co.kr**