nurit

Application of BaroPAM solution

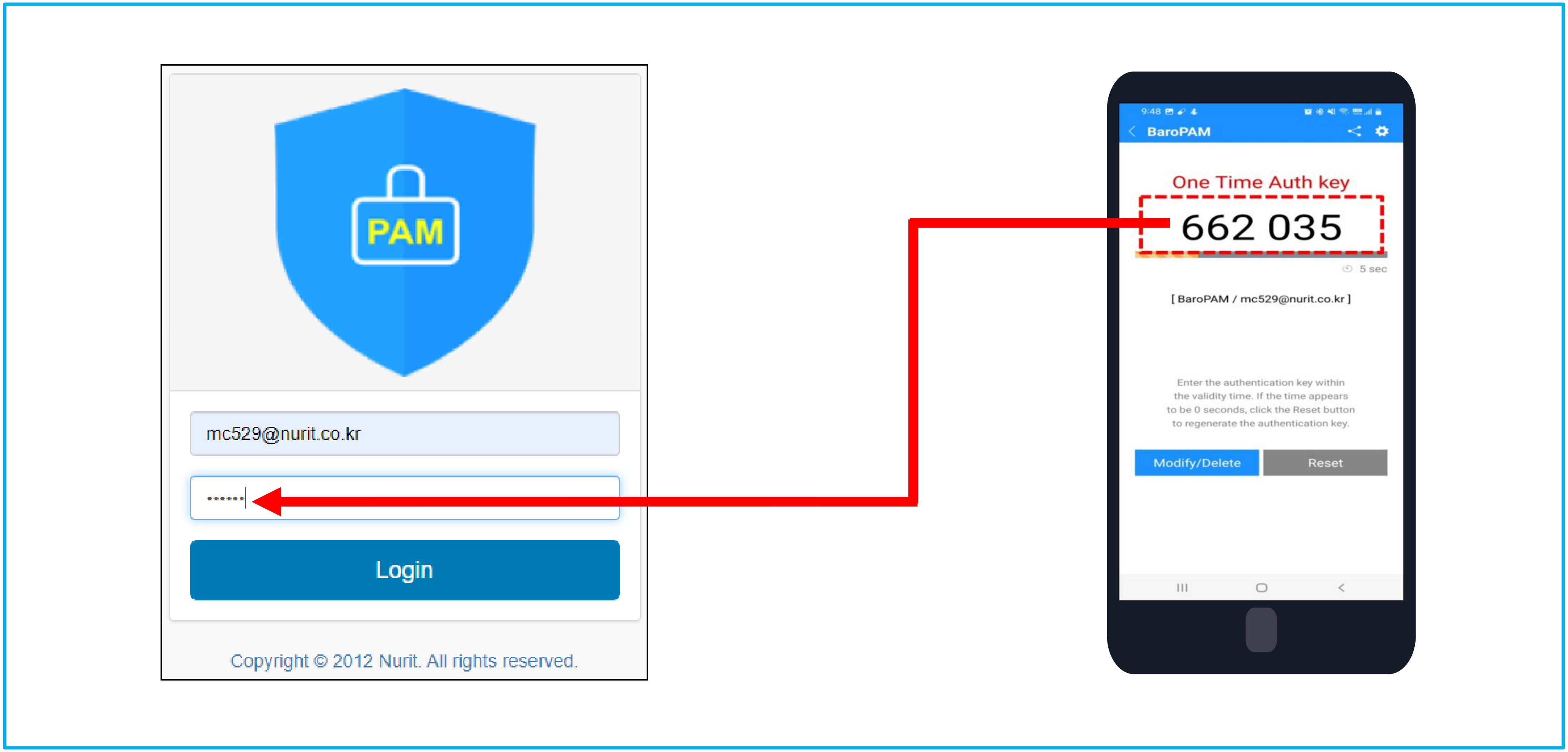
for multi-layer authentication that strengthens the security of information assets

Nov, 2024

Appendix. Application appearance

1. Application login

When logging in to applications such as ERP/groupware/electronic payment/portal, enter the login-ID for user identification and authentication to enhance security and generate a OTA key in the BaroPAM app. Enter the OTA key you created and click the login button to log in to the application.



mc529@nurit.co.kr

••••••

Copyright © 2012 Nurit. All rights reserved.

9:48

One Time Auth key

662 035

5 sec

[BaroPAM / mc529@nurit.co.kr]

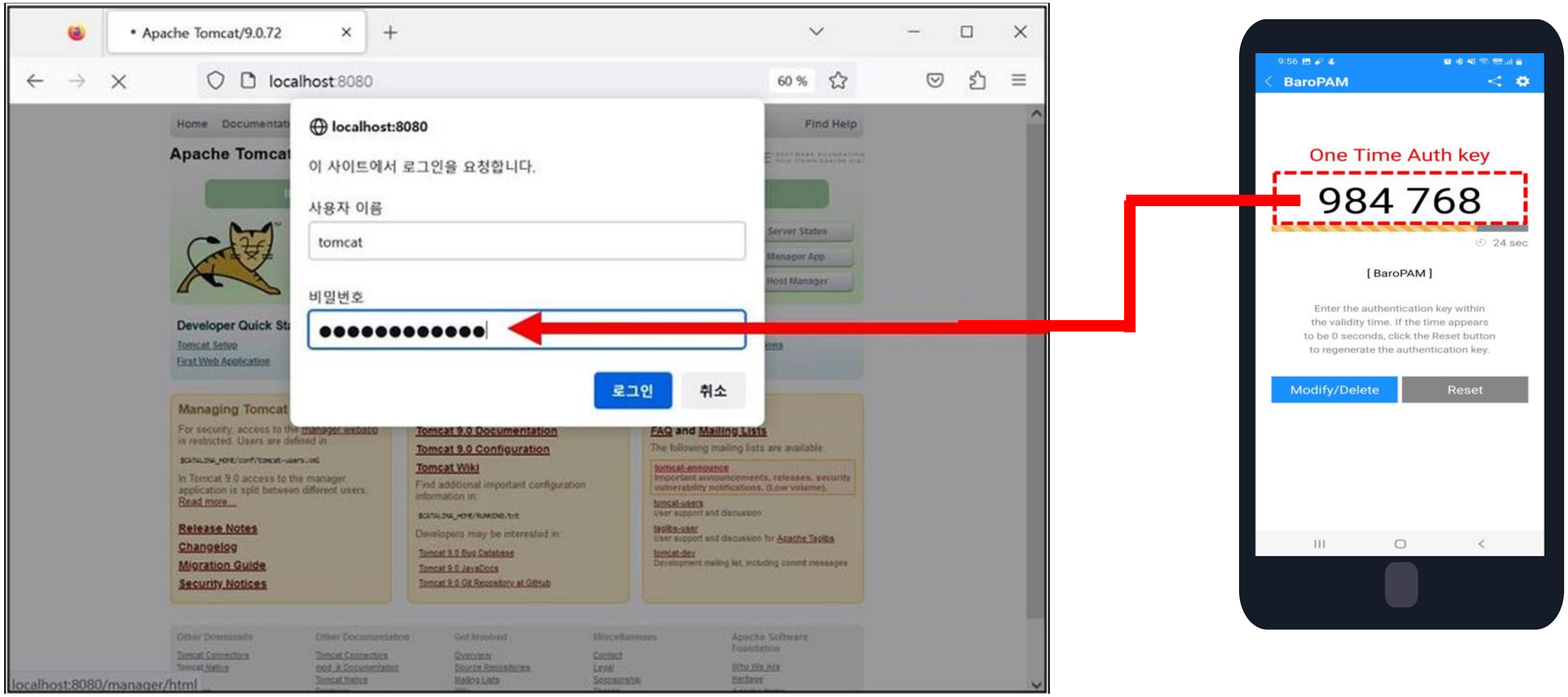
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

2. WAS console login

Security is strengthened by applying BaroPAM for user identification and authentication to improve security vulnerabilities when logging in to WAS (Web Application Server) consoles such as Weblogic, JEUS, Tomcat, etc.



localhost:8080

이 사이트에서 로그인을 요청합니다.

사용자 이름: tomcat

비밀번호: ●●●●●●●●●●●●●

로그인 취소

One Time Auth key

984 768

24 sec

[BaroPAM]

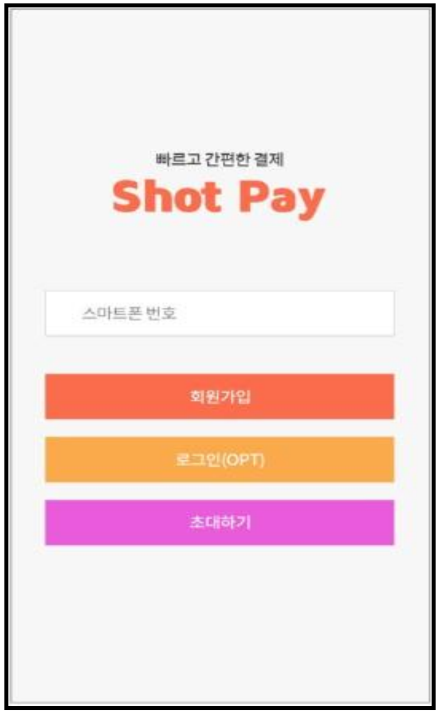
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

On the WAS console login screen, enter your password first and then enter the OTA key without a space. for example, If the password is "tomcat" and the OTA key is "984 768", enter "tomcat984768".

Appendix. Application appearance

3. Simple payment/account transfer authentication (Fintech)

When making simple payments or bank transfers, click the OTP number generation button in the app. The generated OTP number is displayed in the app, and security is strengthened by clicking the payment button to pay.


빠르고 간편한 결제

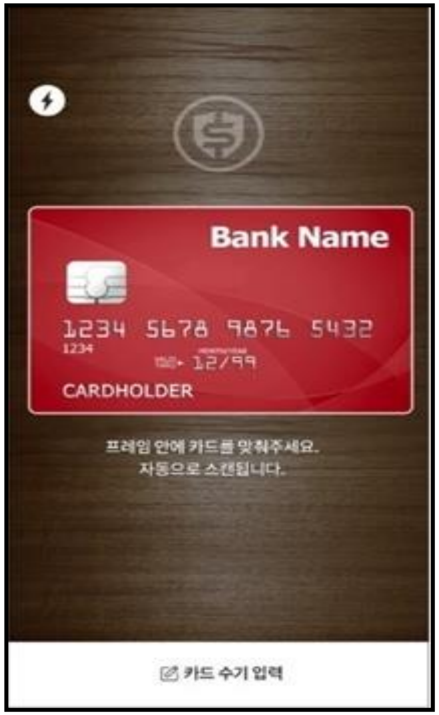
Shot Pay

스마트폰 번호

회원가입

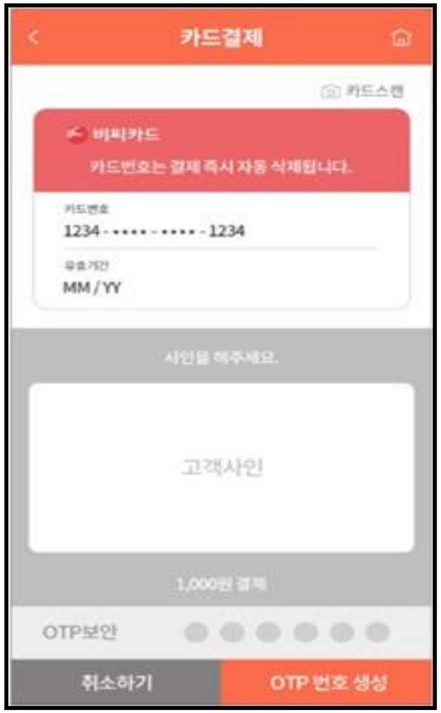
로그인(OPT)

초대하기



프레임 안에 카드를 맞춰주세요.
자동으로 스캔됩니다.

카드 수기 입력


카드결제

카드스캔

비씨카드

카드번호는 결제 즉시 자동 삭제됩니다.

카드번호

1234 - •••• - •••• - 1234

유효기간

MM / YY

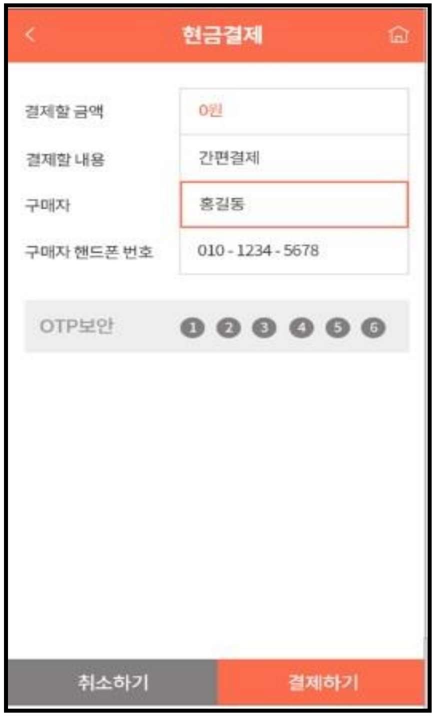
사인을 해주세요.

고객사인

1,000원 결제

OTP보안 ● ● ● ● ● ●

취소하기 | OTP 번호 생성


현금결제

결제할 금액	0원
결제할 내용	간편결제
구매자	홍길동
구매자 핸드폰 번호	010 - 1234 - 5678

OTP보안 ❶ ❷ ❸ ❹ ❺ ❻

취소하기 | 결제하기

OTP generation rule when paying by card = card number
+ payment amount + unique number
OTP generation rules for account transfer = account number
+ transfer amount + unique number

→

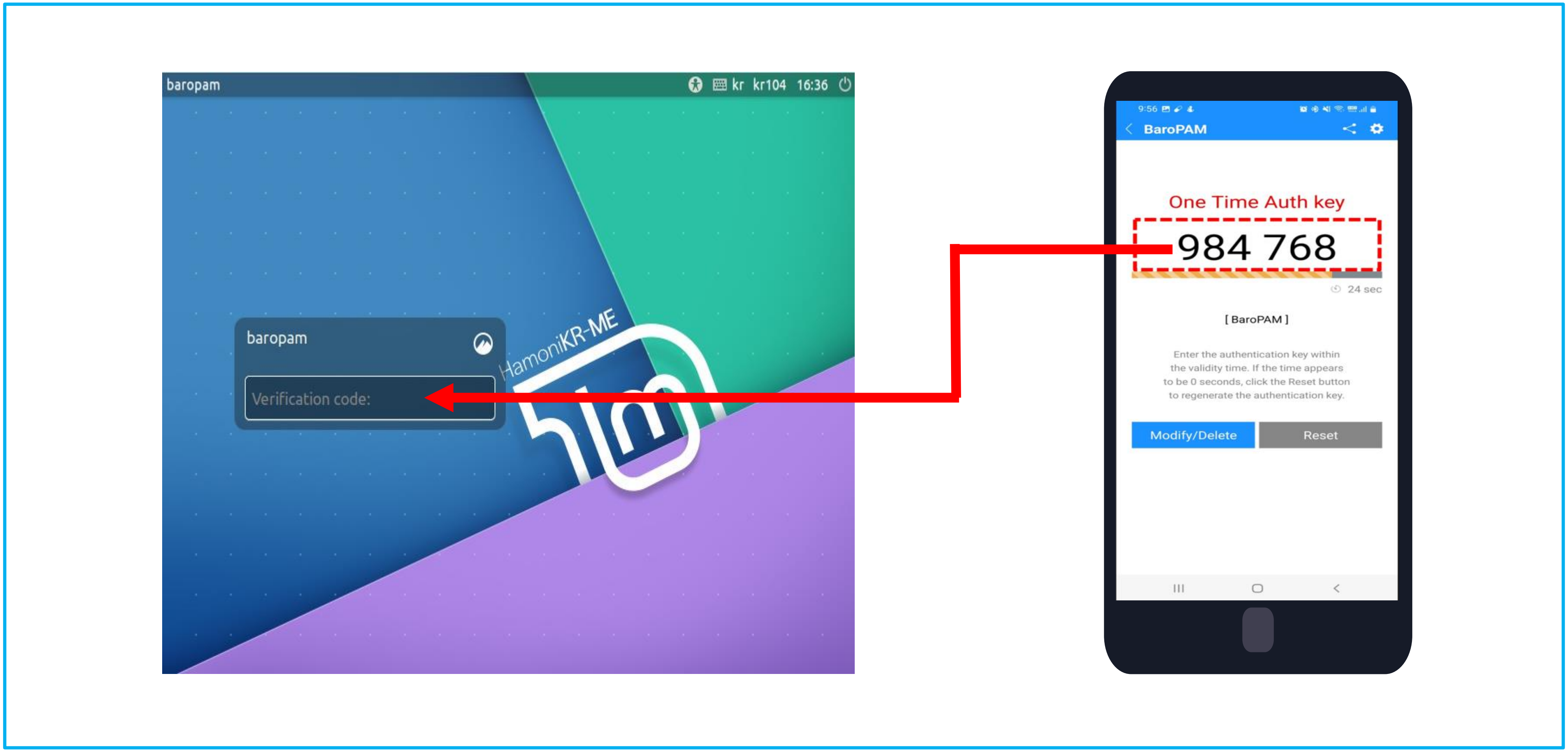
Check whether payment/transfer information has been forged or altered through OTP verification on the server.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

4. Open OS login (Hamonika OS / Gooroom OS / TmaxOS)

When logging into Open OS, a domestic OS that replaces the Windows environment and is strong in security, enter the login-ID for user identification and authentication for enhanced security and generate a OTA key in the BaroPAM app. Enter the OTA key you created and click the login button to log in.



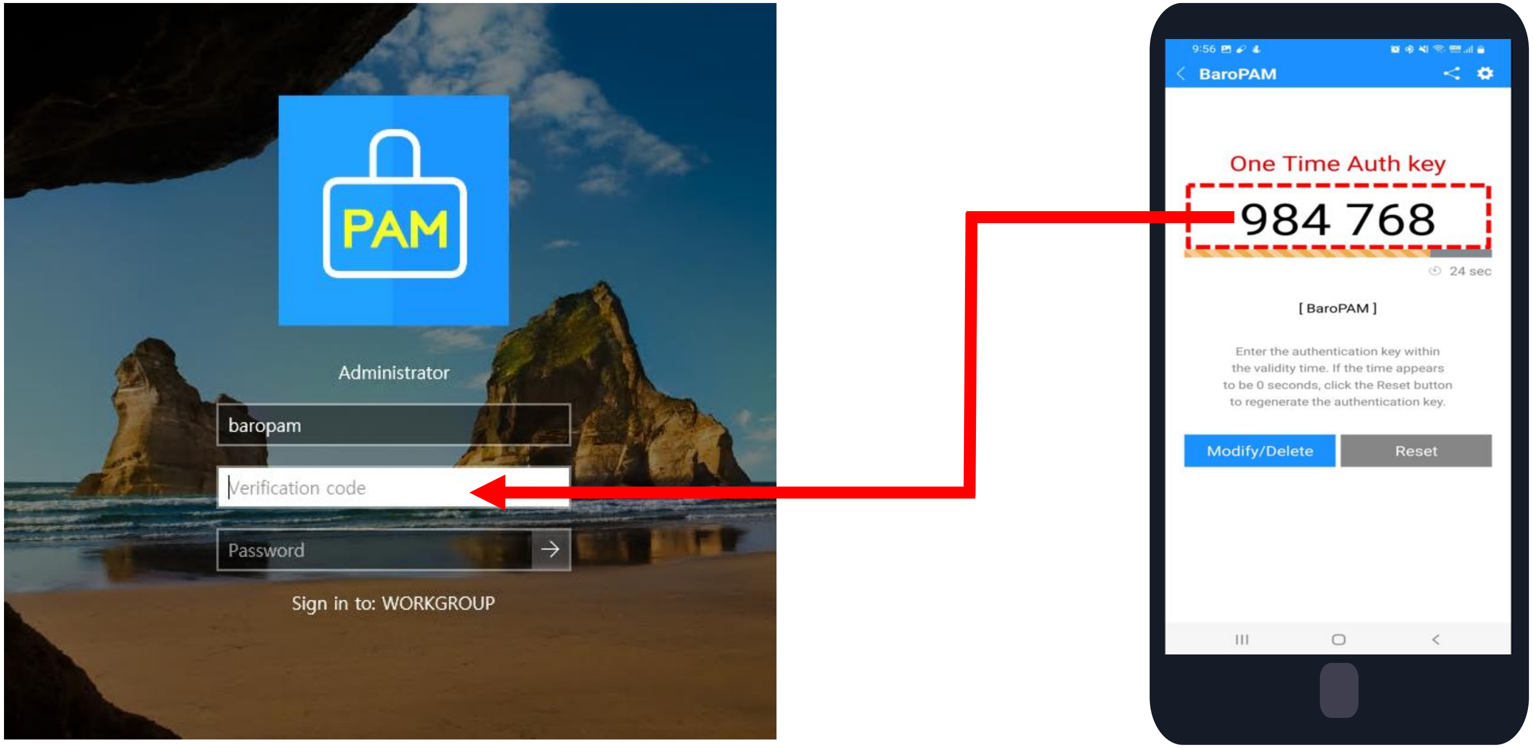
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

5. Windows logon

For user identification and authentication to enhance security when logging on to Windows, the BaroPAM app generates a OTA key. After entering the OTA key and password you created, click the Log On button to log on to Windows to strengthen security.



baropam

Verification code

Password

Sign in to: WORKGROUP

One Time Auth key

984 768

24 sec

[BaroPAM]

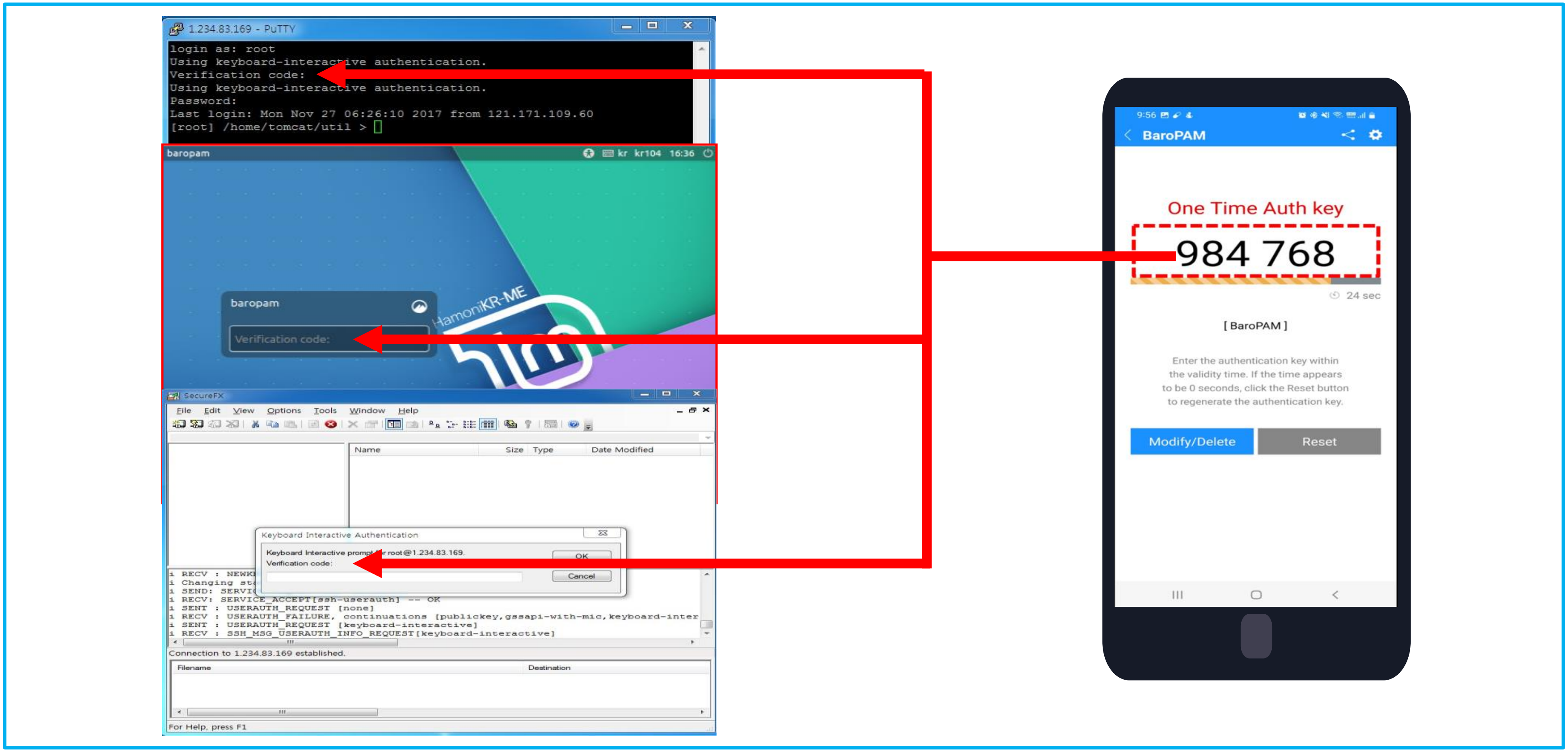
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

6. Linux / Unix login

When logging in to a Linux/Unix environment, enter your login-ID for user identification and authentication to enhance security and generate a OTA key in the BaroPAM app. Strengthen security by entering the OTA key you created and then clicking the login button to log in.



```
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 >
```

Keyboard Interactive prompt for root@1.234.83.169.
Verification code:

```
i RECV : NEWKE
i Changing st
i SEND: SERVI
i RECV: SERVICE_ACCEPT[ssh-userauth] -- OK
i SENT : USERAUTH_REQUEST [none]
i RECV : USERAUTH_FAILURE, continuations [publickey,gssapi-with-mic,keyboard-inter
i SENT : USERAUTH_REQUEST [keyboard-interactive]
i RECV : SSH_MSG_USERAUTH_INFO_REQUEST[keyboard-interactive]
```

Connection to 1.234.83.169 established.

One Time Auth key

984 768

24 sec

[BaroPAM]

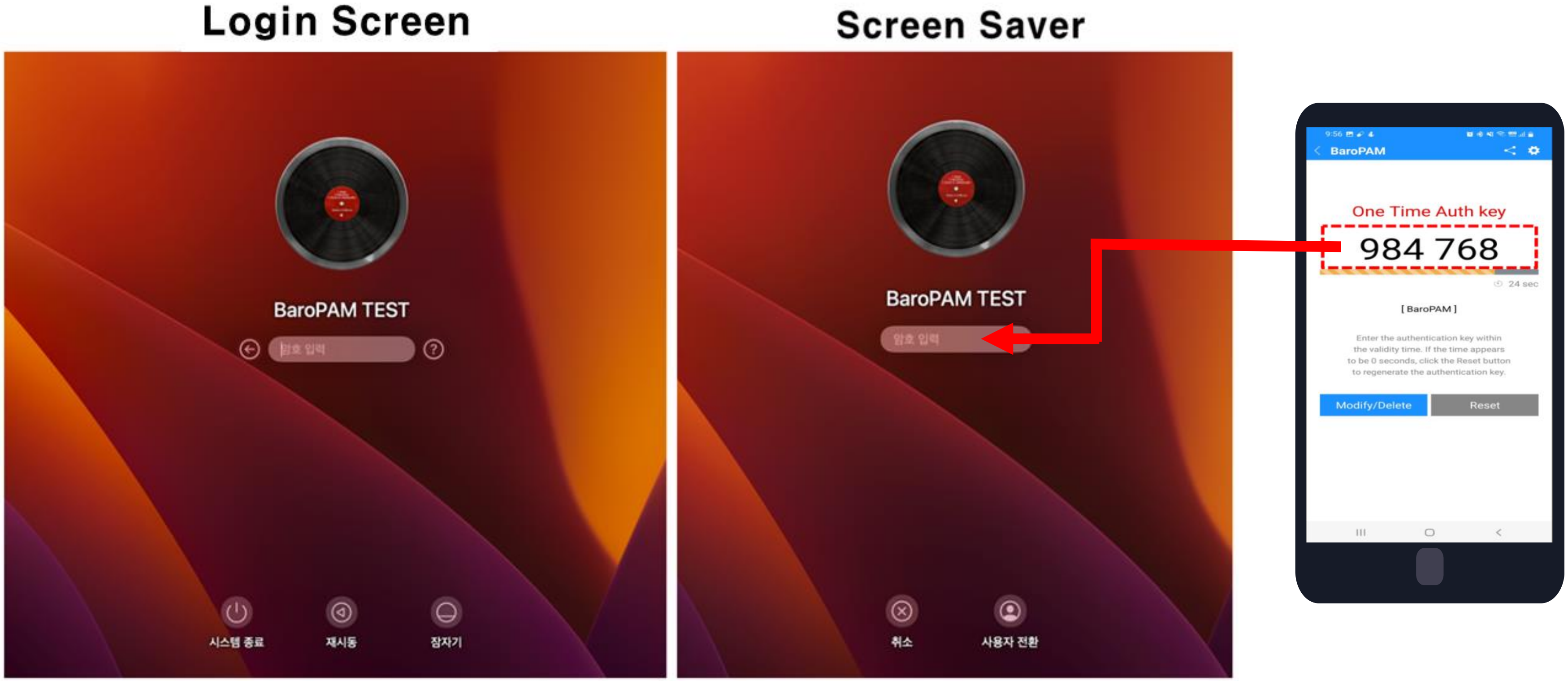
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

7. MacOS login

When logging in to the MacOS environment, enter the login-ID for user identification and authentication for enhanced security and generate a OTA key in the BaroPAM app. Strengthen security by entering the OTA key you created and then clicking the login button to log in.



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.

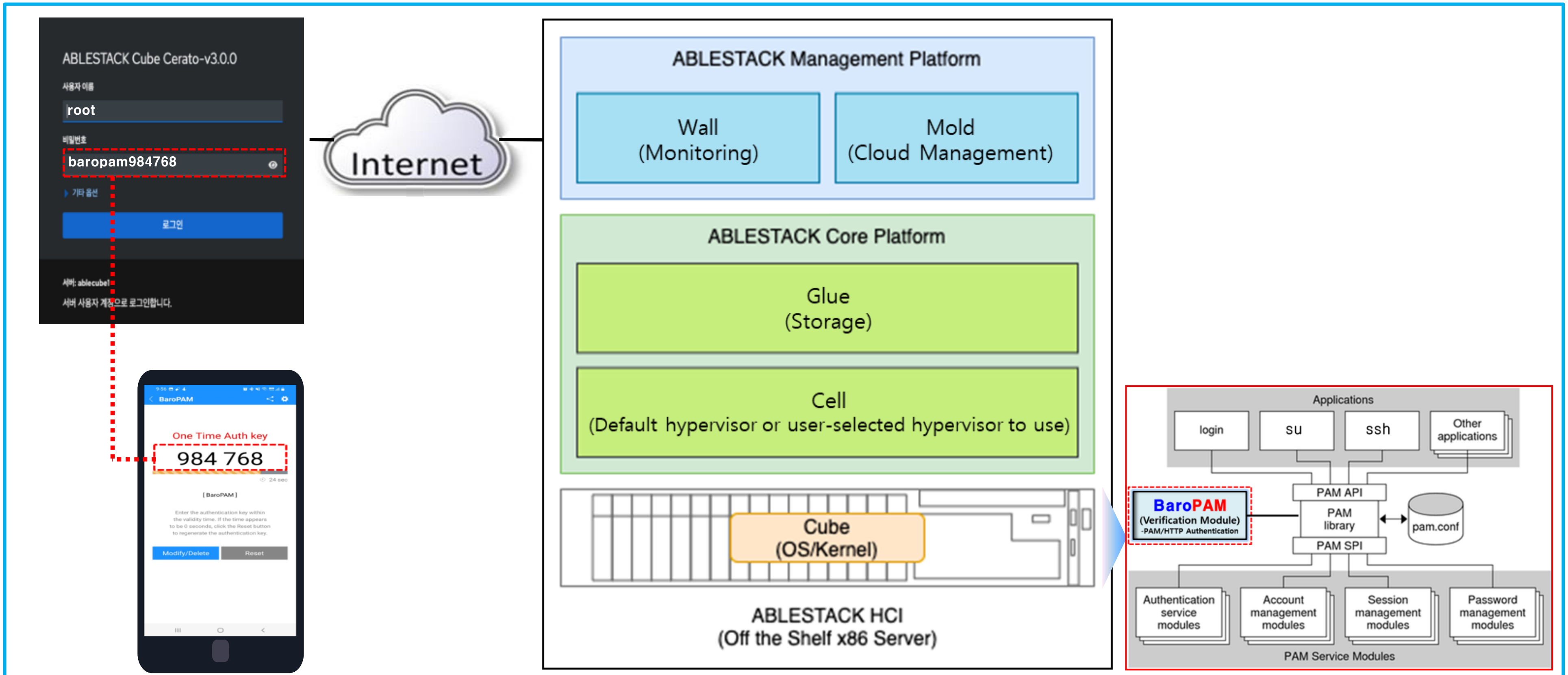
Enter your password first on the GUI login screen or Screen Saver screen of Mac OS X. Just create a OTA key in the BaroPAM app on your smartphone and enter the OTA key without a space after the password. For example, if the password is "baropam" and the OTA key is "984 768", enter "baropam984768".

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

8. ABLESTACK Cube Management Console Login

Security is strengthened by applying BaroPAM for user identification and authentication to improve security vulnerabilities when logging into the ABLESTACK Cube management console. (Cube can easily apply BaroPAM based on CentOS, the downstream of Enterprise Linux OS, to provide a stable operating environment in an enterprise environment)



ABLESTACK Cube Cerato-v3.0.0

사용자 이름: root

비밀번호: baropam984768

기타 옵션

로그인

서버: ablecube1

서버 사용자 계정으로 로그인합니다.

9:56

BaroPAM

One Time Auth key

984 768

24 sec

[BaroPAM]

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.

Modify/Delete | Reset

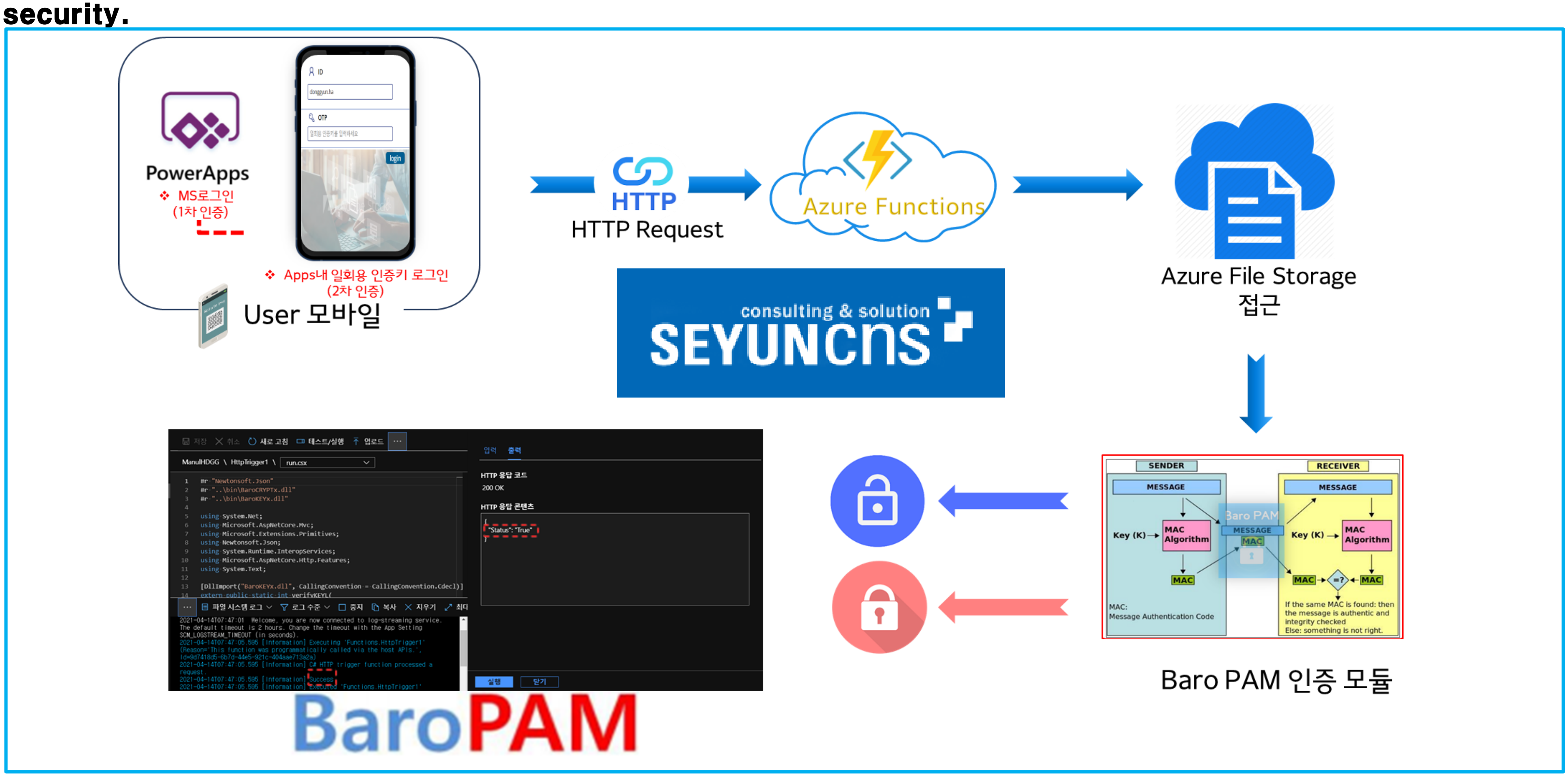
On the management console login screen, enter your password first and then enter the OTA key without a space. for example, If the password is "baropam" and the OTA key is "984 768", enter "baropam195921".

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

9. Integration with MS Azure environment

Using the MS Azure (Function, File Storage) environment, use Power Apps in the user mobile environment to perform 2nd authentication for user identification and authentication to strengthen security. BaroPAM authentication by accessing the Azure environment through HTTP Request. Proceed with strengthening security.



```
#r "Newtonsoft.Json"
#r "..\bin\BaroCRYPTx.dll"
#r "..\bin\BaroKEYx.dll"

using System.Net;
using Microsoft.AspNetCore.Mvc;
using Microsoft.Extensions.Primitives;
using Newtonsoft.Json;
using System.Runtime.InteropServices;
using Microsoft.AspNetCore.Http.Features;
using System.Text;

[DllImport("BaroKEYx.dll", CallingConvention = CallingConvention.Cdecl)]
extern public static int verifyKEYL(
```

```
2021-04-14T07:47:01  Welcome, you are now connected to log-streaming service.
The default timeout is 2 hours. Change the timeout with the App Setting
SCM_LOGSTREAM_TIMEOUT (in seconds).
2021-04-14T07:47:05.595 [Information] Executing 'Functions.HttpTrigger1'
(Reason='This function was programmatically called via the host APIs.',
Id=9d7418d5-6b7d-44e5-921c-404aae713a2a)
2021-04-14T07:47:05.595 [Information] C# HTTP trigger function processed a
request.
2021-04-14T07:47:05.595 [Information] Success
2021-04-14T07:47:05.595 [Information] Executed 'Functions.HttpTrigger1'
```

HTTP 응답 코드

200 OK

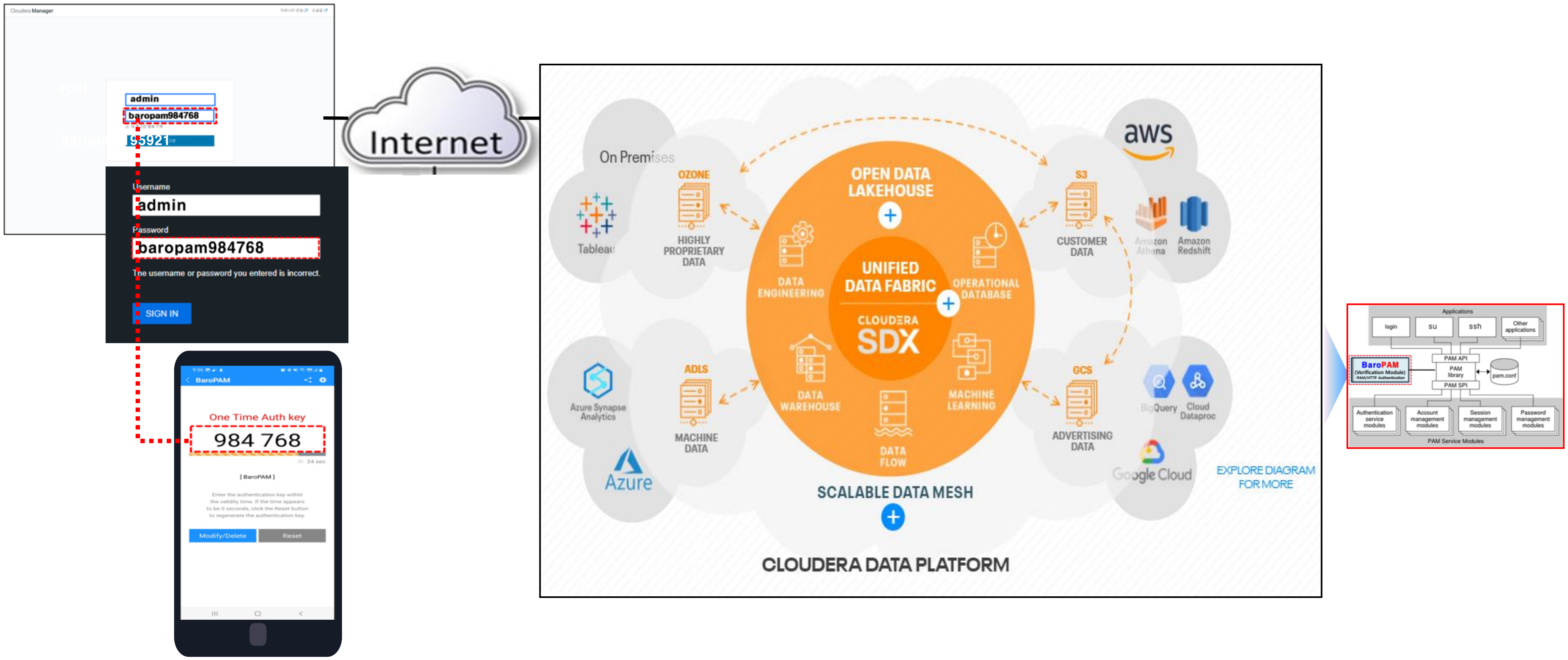
HTTP 응답 콘텐츠

```
{
 "Status": "True"
}
```

Appendix. Application appearance

10. Log in to Cloudera Manager in Cloudera Data Platform

CDP (Cloudera Data Platform) is a solution that provides the freedom to safely move data, applications, and users in both directions between data centers and multiple data clouds regardless of the data's location. It is designed to improve security vulnerabilities when logging into Cloudera Manager. Security is strengthened by applying BaroPAM for user identification and authentication.



Username

admin

Password

baropam984768

The username or password you entered is incorrect.

SIGN IN

BaroPAM

One Time Auth key

984 768

24 sec

[BaroPAM]

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.

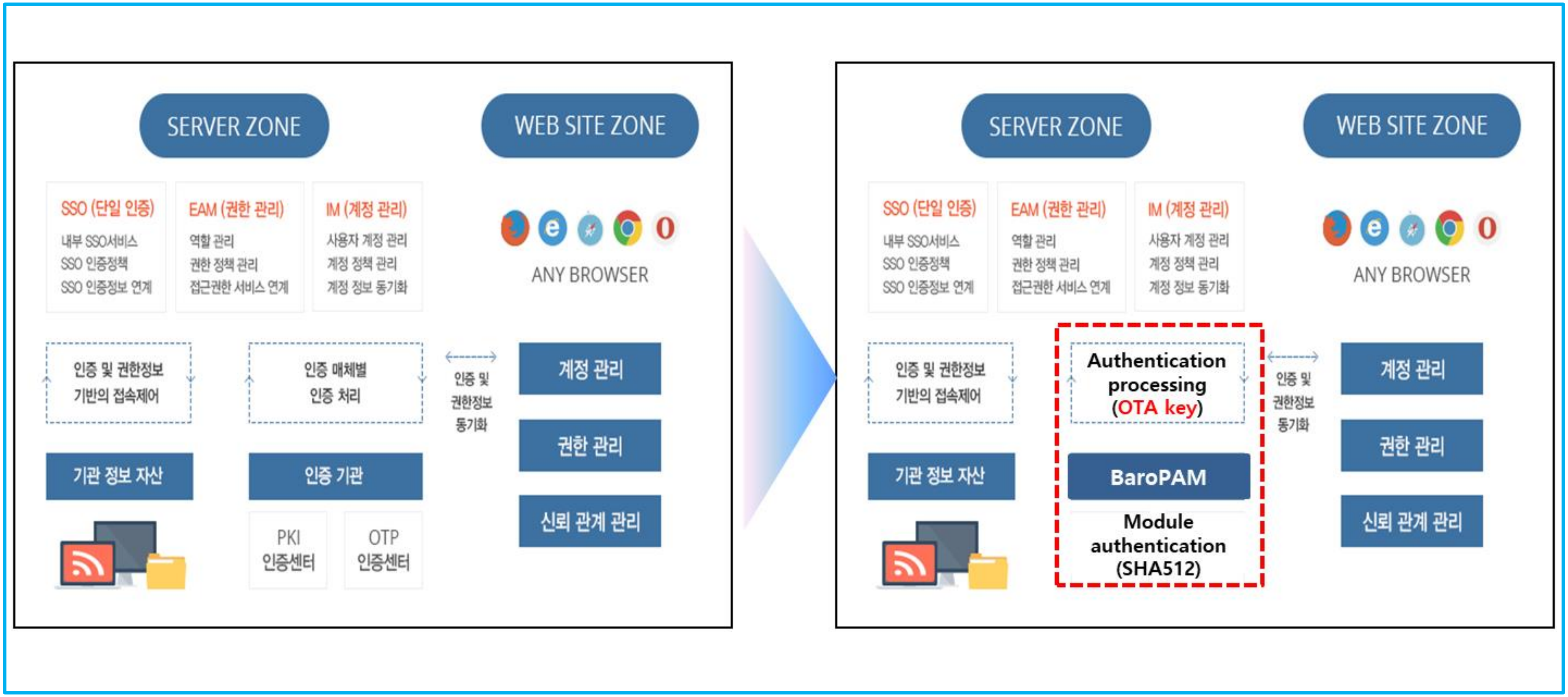
On the Cloudera Manager login screen, enter your password first and then enter the OTA key without a space. For example, if the password is "baropam" and the OTA key is "984 768", enter "baropam984768".

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

11. Convergence with SSO (Single Sign On) solution

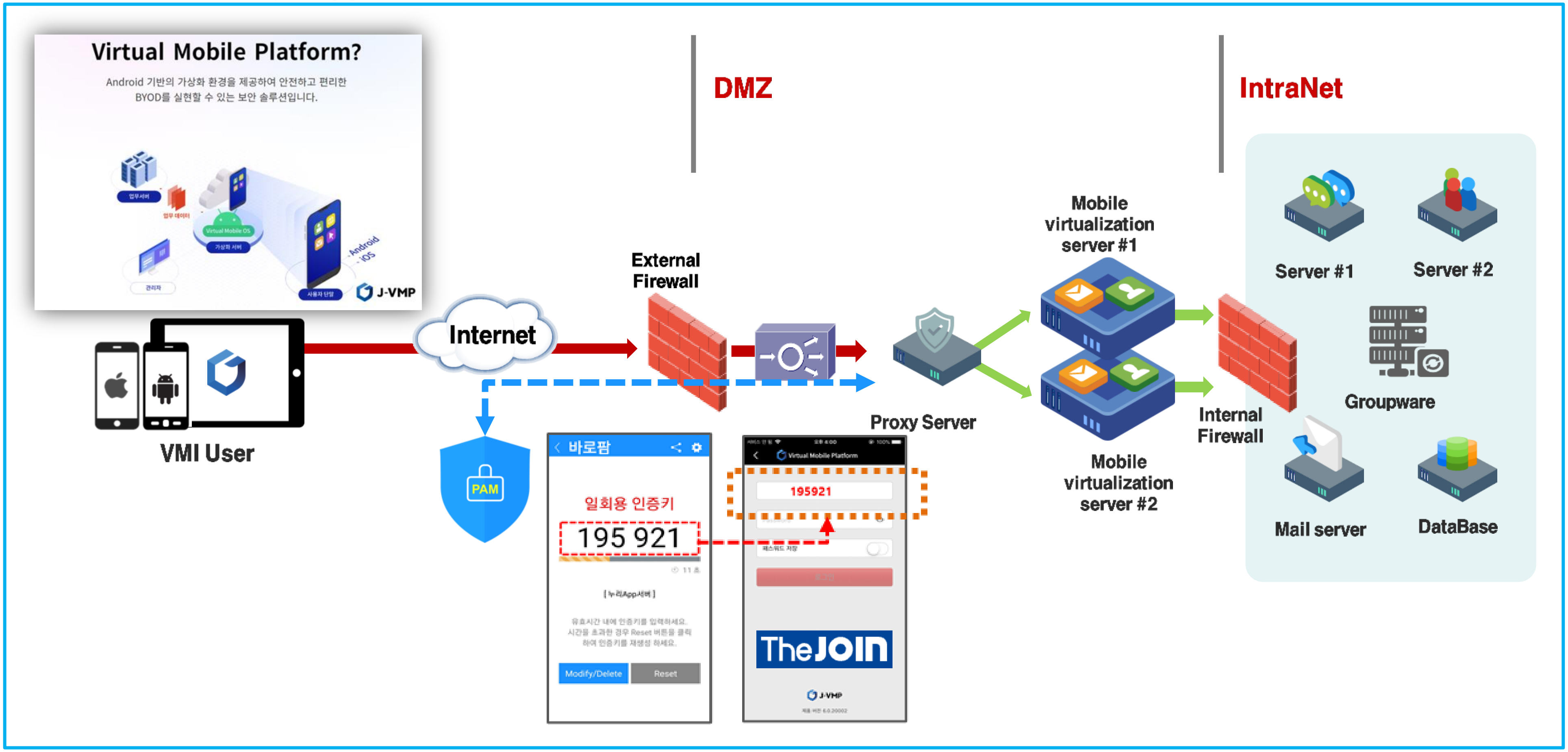
SSO (Single Sign On) is an integrated authentication function that allows you to use multiple systems with OTA. When logging in with a unified ID, each work system is accessed differentially and selectively according to authority without a separate authentication process. Security is strengthened by applying BaroPAM for user identification and authentication to solutions that provide an enabling environment.



Copyright © Nurit Corp. All rights reserved.

12. Application of VMI (Virtual Mobile Infrastructure) solution

Mobile Virtualization Platform (VMI) is a platform that provides a mobile work environment that is completely physically separated from the personal mobile area by accessing the mobile virtual (individual user) area on the server. BaroPAM is used for user identification and authentication to strengthen security. Apply to strengthen security.



Virtual Mobile Platform?

Android 기반의 가상화 환경을 제공하여 안전하고 편리한 BYOD를 실현할 수 있는 보안 솔루션입니다.

일회용 인증키

195 921

11 초

[누리App서버]

유효시간 내에 인증키를 입력하세요. 시간을 초과한 경우 Reset 버튼을 클릭하여 인증키를 재생성 하세요.

Modify/Delete | Reset

Virtual Mobile Platform

195921

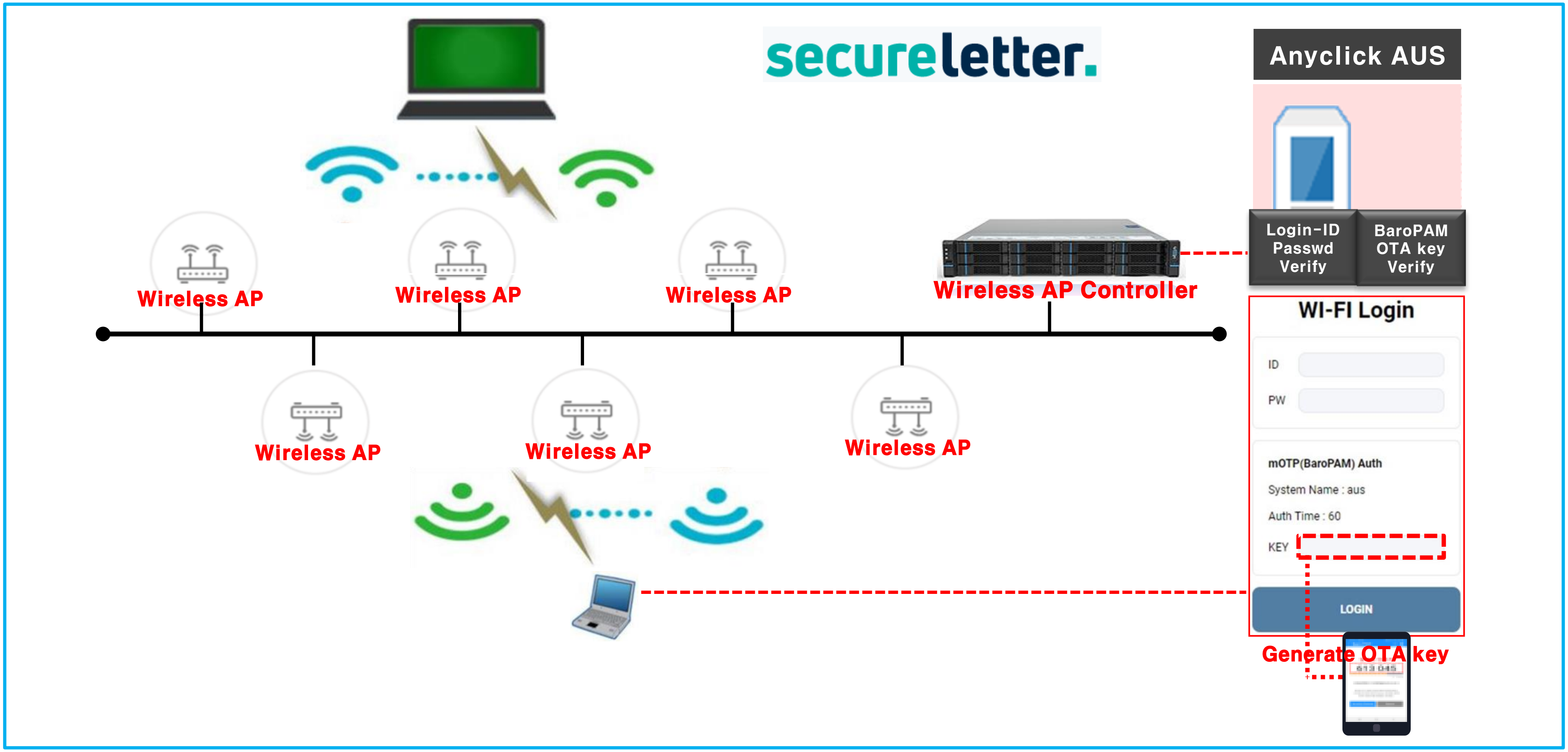
패스워드 저장

로그인

Appendix. Application appearance

13. Convergence with wireless AP solution

A wireless access point (WAP), also called a wireless AP, is a device that allows wireless devices to connect to wired devices using related standards using Wi-Fi in a computer network, transforming a wired LAN-based work environment into a 5G-based mobile environment. To enhance security, security is strengthened by applying BaroPAM for wireless user identification and authentication.



WI-FI Login

ID

PW

mOTP(BaroPAM) Auth

System Name : aus

Auth Time : 60

KEY

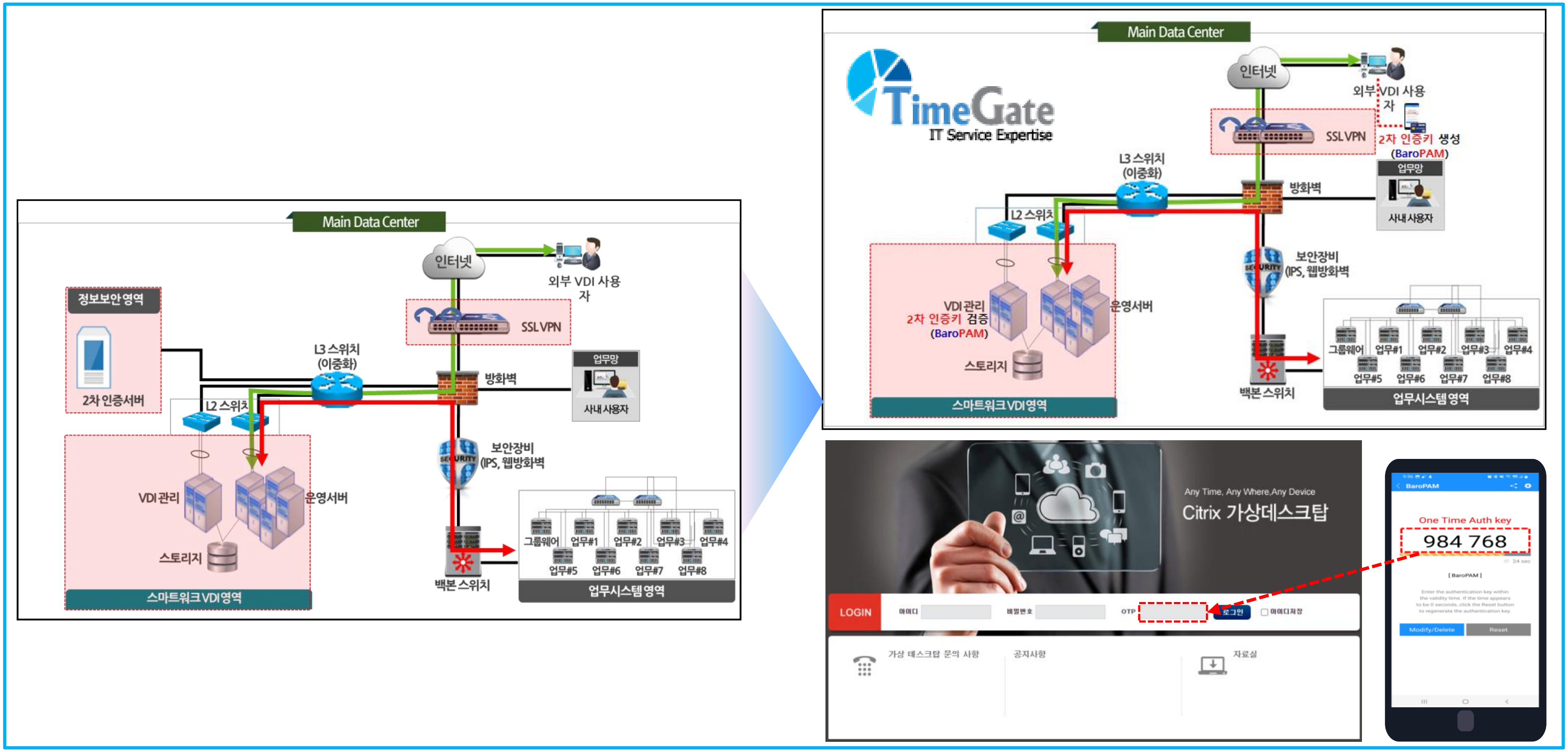
LOGIN

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

14. Convergence with VDI (Virtual Desktop Infrastructure) solution

VDI (Virtual Desktop Infrastructure) enhances security by applying BaroPAM for user identification and authentication to enhance security in a solution that virtualizes desktops using software and provides them to the user environment from a central location.



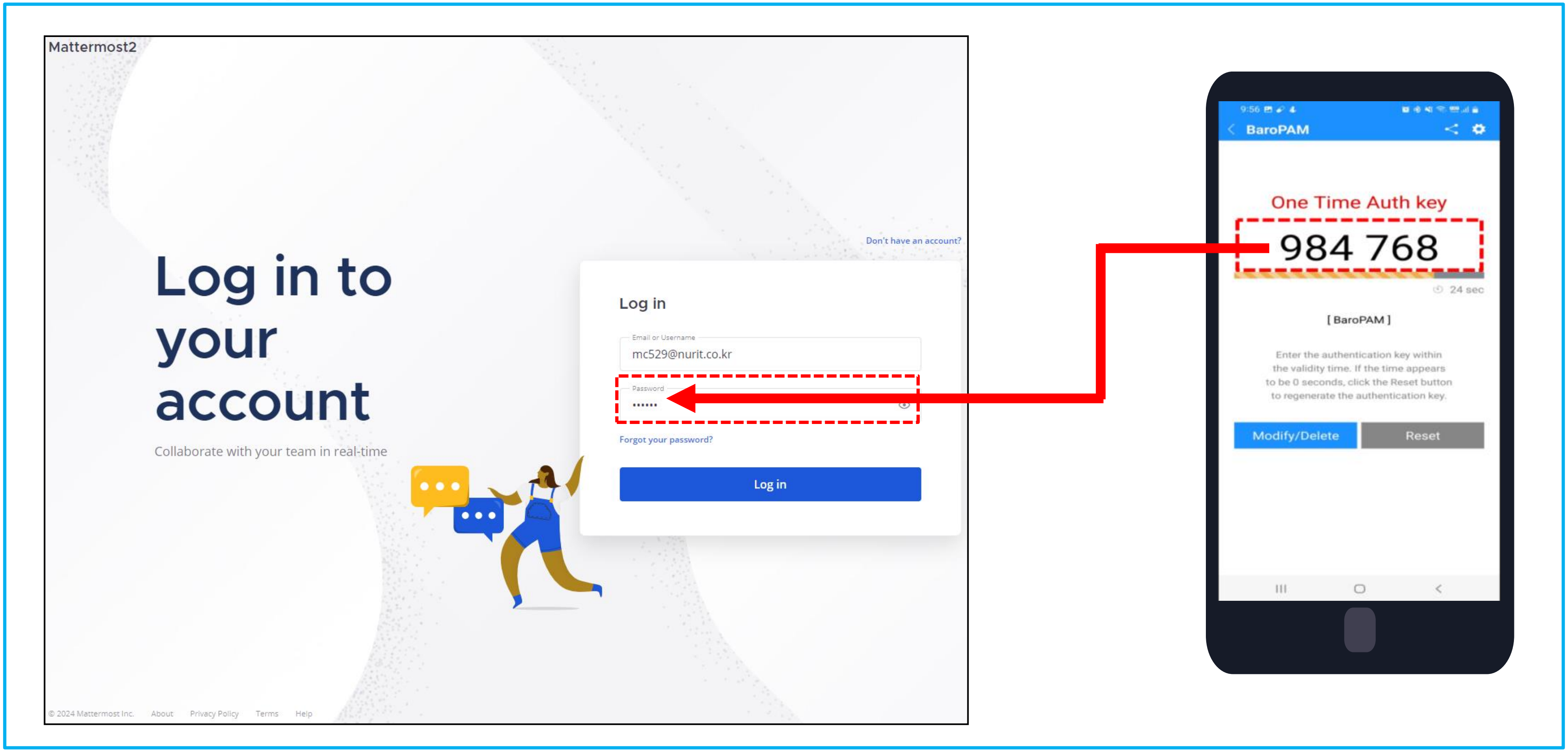
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

15. Integration with Mattermost solutions

Mattermost is an open source, self-hosted online chat service that provides file sharing, search, and integration capabilities. It is designed as an internal chat for organizations and businesses, and largely describes itself as a secure, open source alternative to Slack and Microsoft Teams. Security is strengthened by applying BaroPAM for user identification and authentication.



Mattermost2

Log in to your account

Collaborate with your team in real-time

Don't have an account?

Log in

Email or Username: mc529@nurit.co.kr

Password: ••••••

Forgot your password?

Log in

© 2024 Mattermost Inc. About Privacy Policy Terms Help

BaroPAM

One Time Auth key

984 768

24 sec

[BaroPAM]

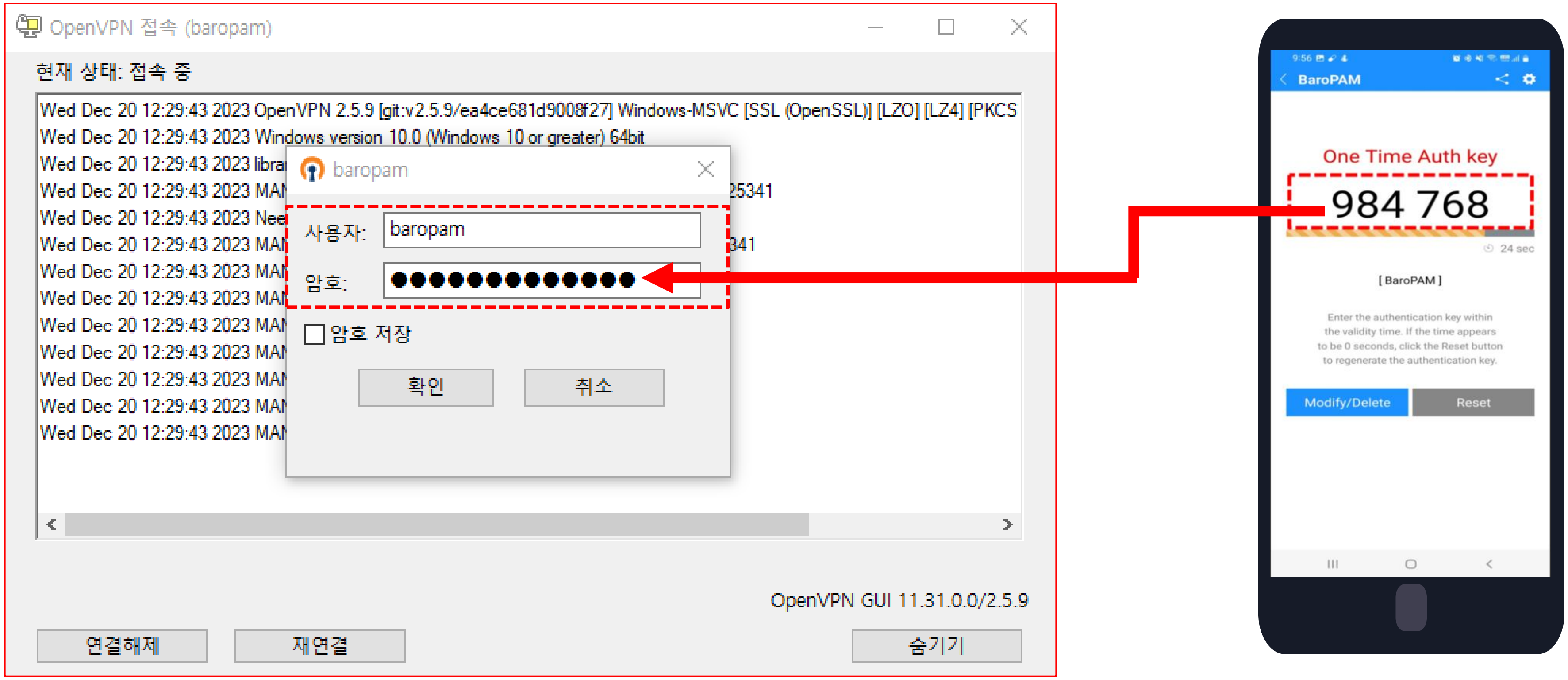
Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Modify/Delete Reset

Copyright © Nurit Corp. All rights reserved.

16. Convergence with OpenVPN solution

A virtual private network (VPN) is a network that allows you to build a wide area network (WAN) at low cost by connecting points between points using a tunneling protocol (communication protocol) based on encryption technology without a separate private network. As a solution, security is strengthened by applying BaroPAM for user identification and authentication to enhance security.



OpenVPN 접속 (baropam)

현재 상태: 접속 중

```
Wed Dec 20 12:29:43 2023 OpenVPN 2.5.9 [git:v2.5.9/ea4ce681d9008f27] Windows-MSVC [SSL (OpenSSL)] [LZO] [LZ4] [PKCS
Wed Dec 20 12:29:43 2023 Windows version 10.0 (Windows 10 or greater) 64bit
Wed Dec 20 12:29:43 2023 libra
Wed Dec 20 12:29:43 2023 MAN                                                        25341
Wed Dec 20 12:29:43 2023 Nee
Wed Dec 20 12:29:43 2023 MAN                                                        341
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
Wed Dec 20 12:29:43 2023 MAN
```

baropam

사용자: baropam

암호: ●●●●●●●●●●●●●●

□ 암호 저장

984 768

24 sec

[BaroPAM]

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.

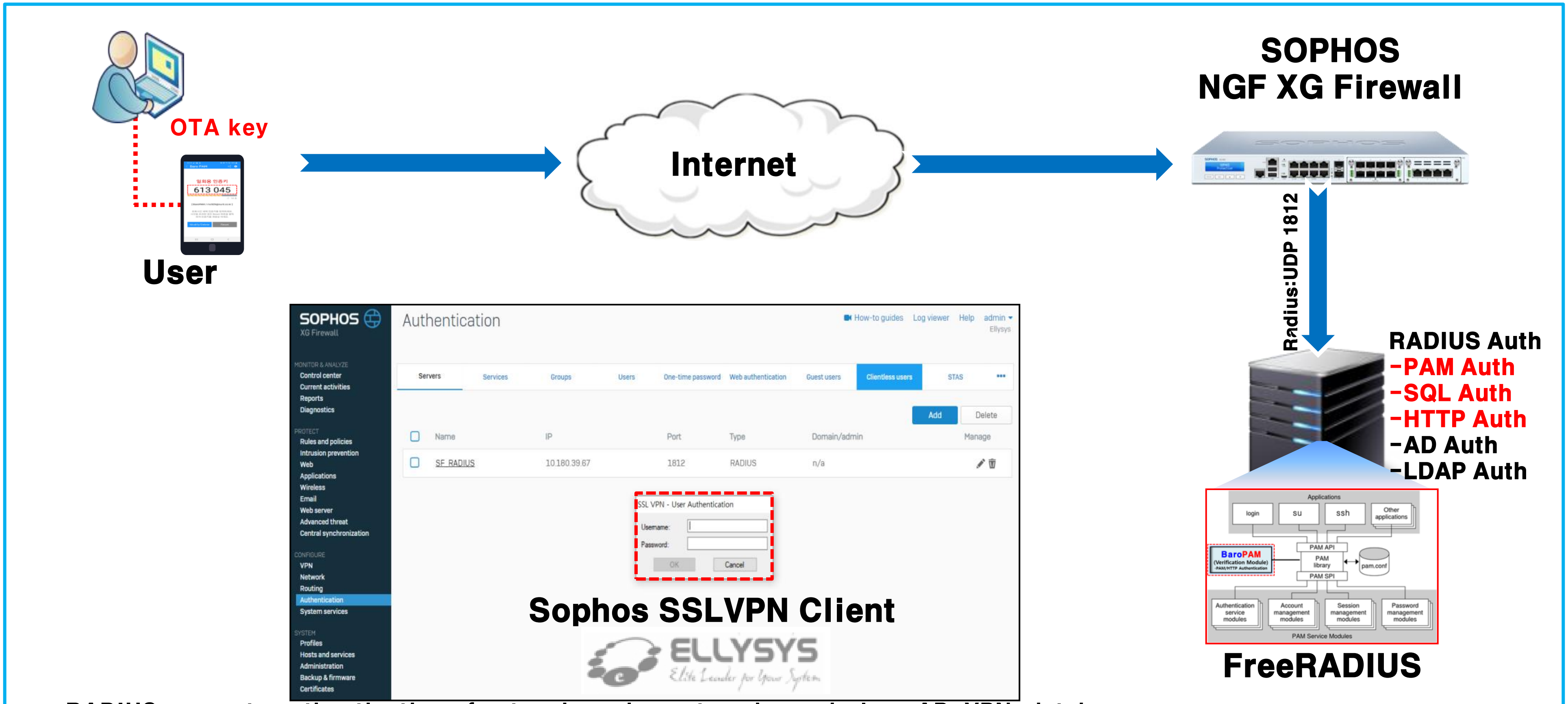
On the VPN login screen, enter your password first, then enter the OTA key without a space. for example, If the password is "nurit" and the OTA key is "984 768", enter "nurit984768".

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

17. Integration with RADIUS solution

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized authentication for users to connect to the network and receive network services. It enhances security by applying BaroPAM for user identification and authentication to enhance security.



Authentication

□	Name	IP	Port	Type	Domain/admin	Manage
□	SF_RADIUS	10.180.39.67	1812	RADIUS	n/a	

SSL VPN - User Authentication

Username:

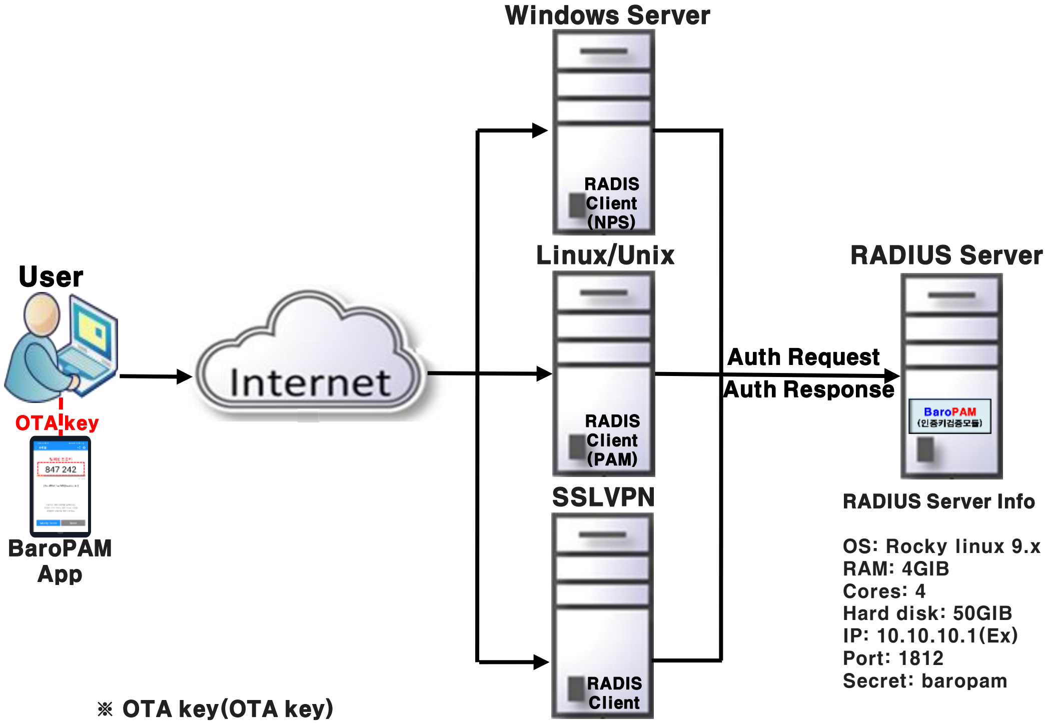
Password:

※ RADIUS supports authentication of network equipment such as wireless AP, VPN, database, VMWare, etc.

Copyright © Nurit Corp. All rights reserved.

18. Integrated account/authentication management linked to RADIUS

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that strengthens security by applying BaroPAM for integrated account management and integrated authentication to enhance security through centralized authentication for users to connect to the network and receive network services.



RADIUS Server Info

OS: Rocky linux 9.x
RAM: 4GIB
Cores: 4
Hard disk: 50GIB
IP: 10.10.10.1(Ex)
Port: 1812
Secret: baropam

※ OTA key(OTA key)

RADIUS Server Info
IP: 10.10.10.1(Ex)
Port: 1812
Secret: baropam

RADIUS Client module installation and env settings
Windows server sets up RADIUS in NPS

Features

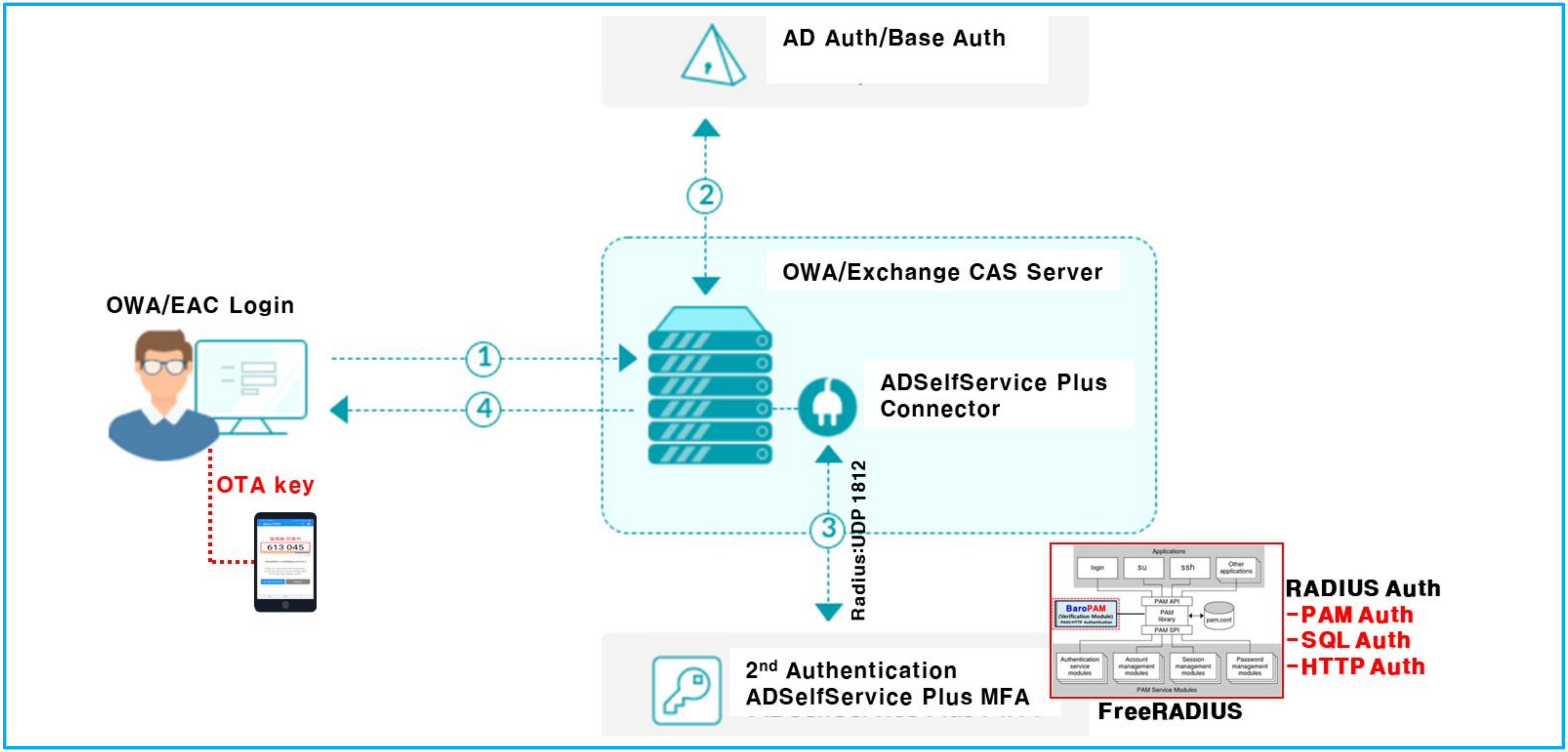
- ▶Integrated management and integrated authentication of information asset accounts (ID/password)
- ▶Use OS account for information asset account (ID/password)
- ▶Use of the globally recognized 512Bit standard Hash function (HMac-SHA512 / Internet security standard IETF RFC 6238)
- ▶Time-Sync, dynamic HMac Key method recommended by the Financial Supervisory Service
- ▶Dynamic security such as one-time/volatile that changes every time or is used once and then discarded
- ▶Guaranteed service with fast authentication speed (average authentication time within 0.01 seconds)
- ▶Even if the authentication information is forged or altered during the authentication process, bypass authentication is not possible.
- ▶Individual grant of one-time authentication key and generation cycle for each information asset/account
- ▶Authentication bypass (bypass techniques, fatigue attacks, etc.) and MFA fatigue attacks are impossible.
- ▶Login is not possible even if account information is stolen by abusing the automatic login function.
- ▶Provides the ability to set the authentication limit number and time limit (e.g. 3 times in 30 seconds)
- ▶Provides a function to prevent man-in-the-middle attacks
- ▶Provides ACL function for accounts that can be allowed/excluded from secondary authentication

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

19. Integration with OWA (Outlook Web Access) solution

Outlook on the web, or Outlook Web Access (OWA), is a browser-based counterpart to Microsoft Outlook, an on-premises email and task management application that provides user identification and authentication to enhance security against the risk of exposing sensitive business information and confidential email correspondence between users. Security is strengthened by applying BaroPAM for authentication.

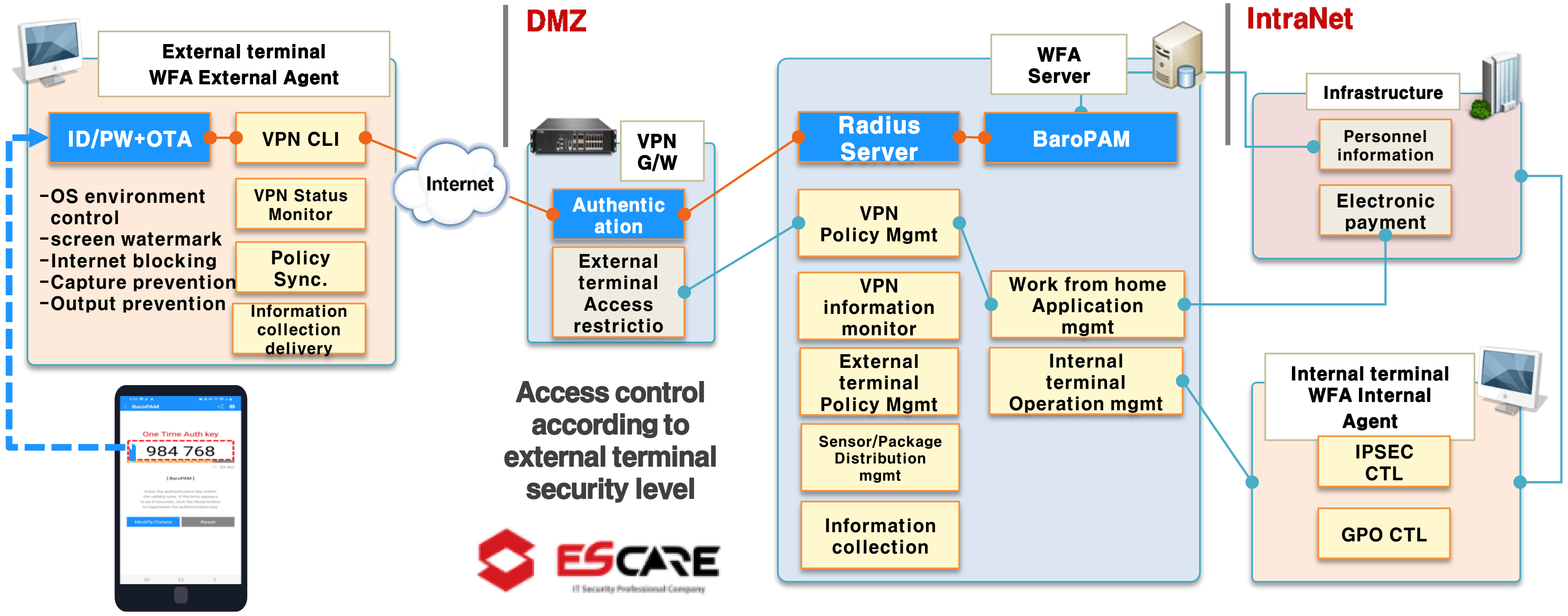


Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

20. Convergence with WFA (Work From Anywhere) solution

WFA verifies the integrity of the terminal in an environment where external user terminals must access and work internally and applies a security system for internal access rights according to the terminal status to eliminate security risks of internal access and provide a differentiated network access control environment according to the terminal status. It is a solution that provides security by applying BaroPAM to identify and authenticate internal accessors to strengthen security.



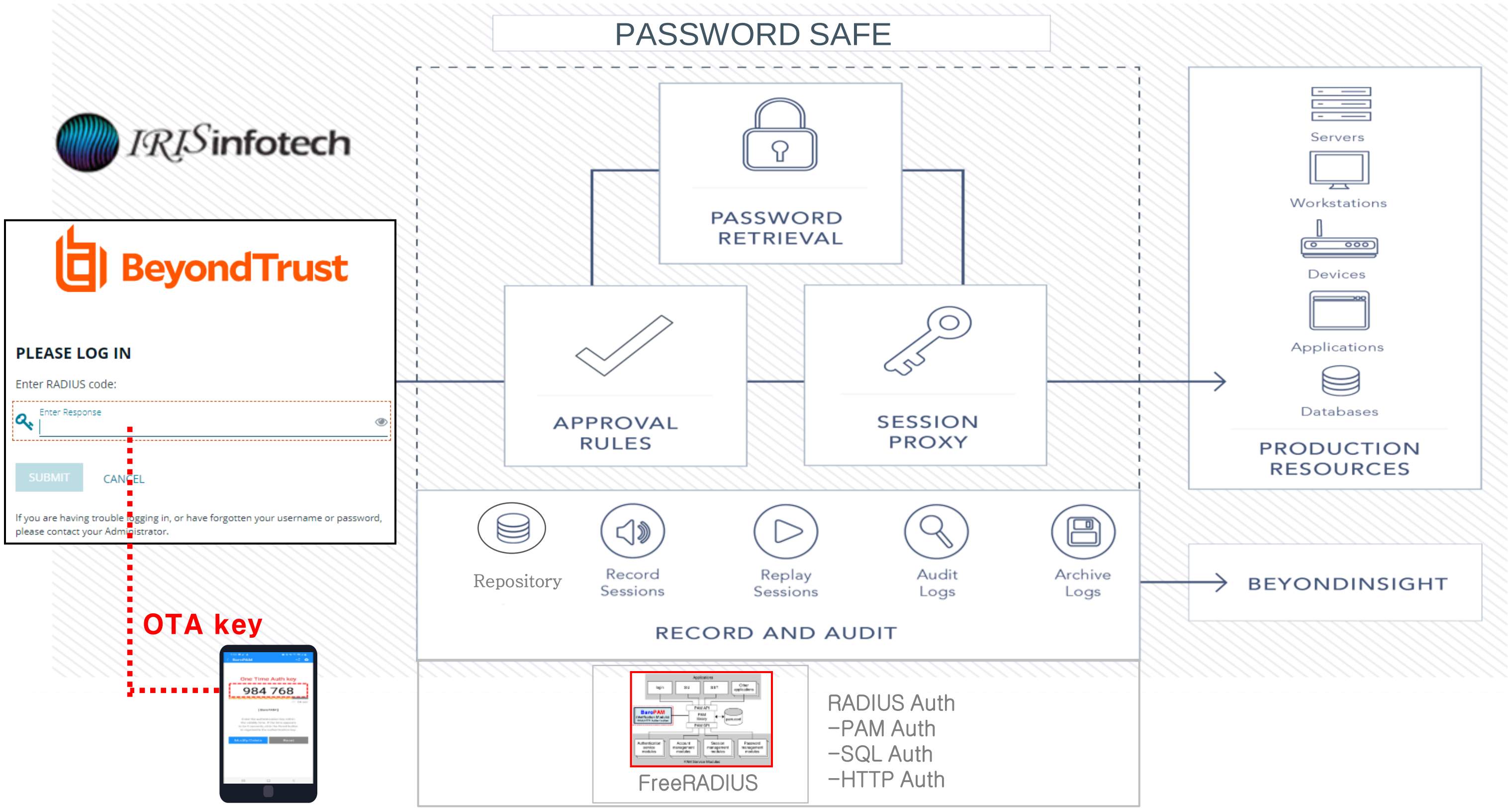
※ Microsoft's AD (Active Directory) authentication is replaced with PAM authentication using BaroPAM.

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

21. Convergence with access control/password management solutions

To strengthen security, it is a comprehensive access control solution that restricts unauthorized access by granting only "minimum privileges" to applications, users, and information assets, and monitors and analyzes access attempts to audit the form and type of security breach. Security is strengthened by applying BaroPAM for user identification and authentication.



PLEASE LOG IN

Enter RADIUS code:

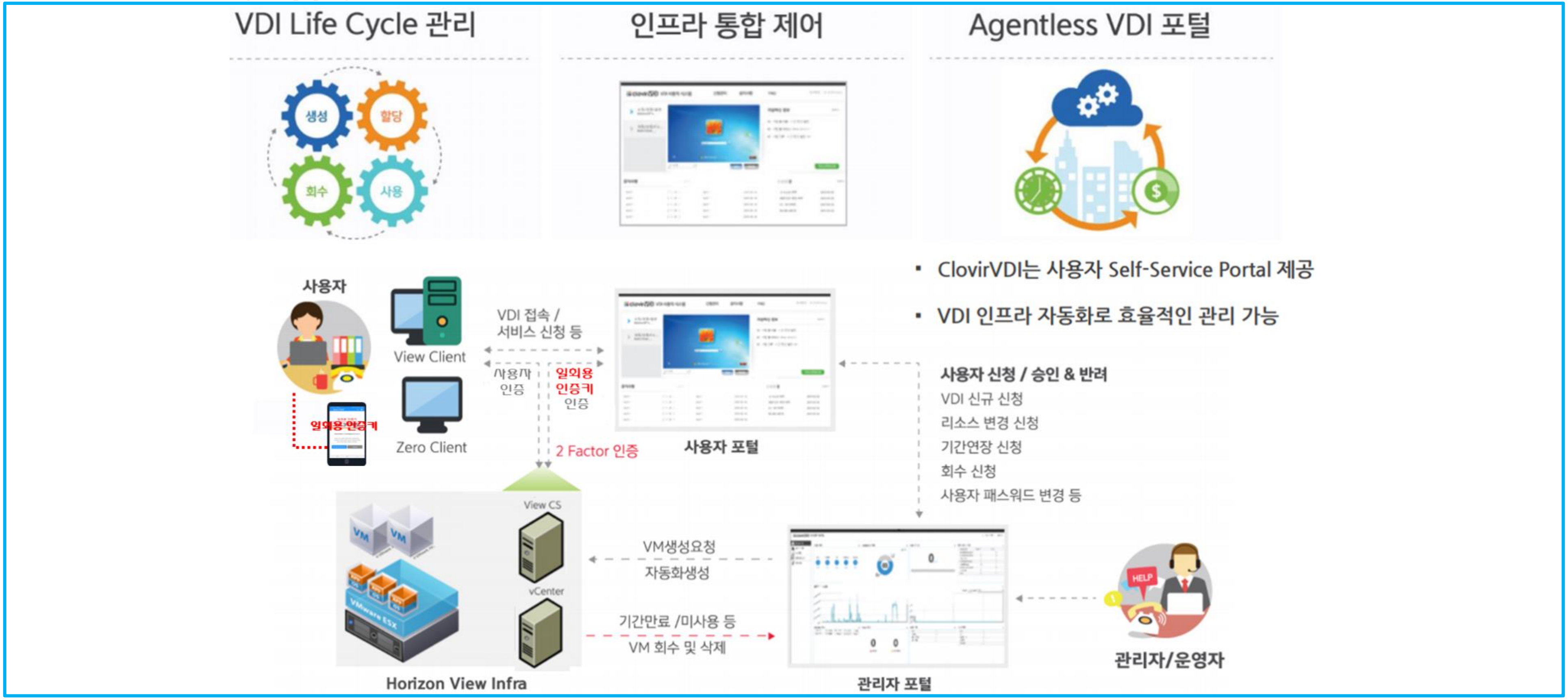
If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

RADIUS Auth
–PAM Auth
–SQL Auth
–HTTP Auth

Appendix. Application appearance

22. Convergence with smart work solutions

Smart work is a flexible work environment that uses IT to work without restrictions on time and place. For information security, terminal security and power saving functions are set, such as screen blocking for 5 minutes, screen saver for 10 minutes, and forced shutdown for 4 hours. However, information security is strengthened, user inconvenience is minimized, and security is strengthened by applying BaroPAM for user identification and authentication.



- ClovirVDI는 사용자 Self-Service Portal 제공
- VDI 인프라 자동화로 효율적인 관리 가능

사용자 신청 / 승인 & 반려

VDI 신규 신청
리소스 변경 신청
기간연장 신청
회수 신청
사용자 패스워드 변경 등

Appendix. Application appearance

23. Convergence with SAC (Server Access Control) solution

A server access control solution that controls and manages all access and tasks to the network and server IT infrastructure operating system, and thoroughly controls and supervises users through real-time monitoring of work details and storage of log records, as well as multi-layer authentication of information assets. The BaroPAM solution, which blocks account theft, privilege escalation, illegal bypass/remote access, and man-in-the-middle attacks, can be combined to create a synergy effect that strengthens the security of information assets.

IT asset security = Server access control solution + Muti-layer auth solution (BaroPAM)

Windows NT Server

Mac OS

Linux / Unix Server

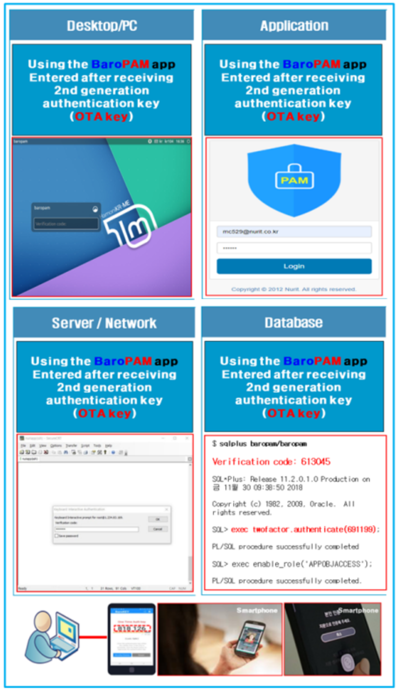
Application

Database

Network, IoT Device

Storage

- ▶Access authority control
- ▶System command control
- ▶Real-time session control
- ▶Work log recording/audit



Desktop/PC: Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)

Application: Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)

mc529@nurit.co.kr

Copyright © 2012 Nurit. All rights reserved.

Server / Network: Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)

Database: Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)

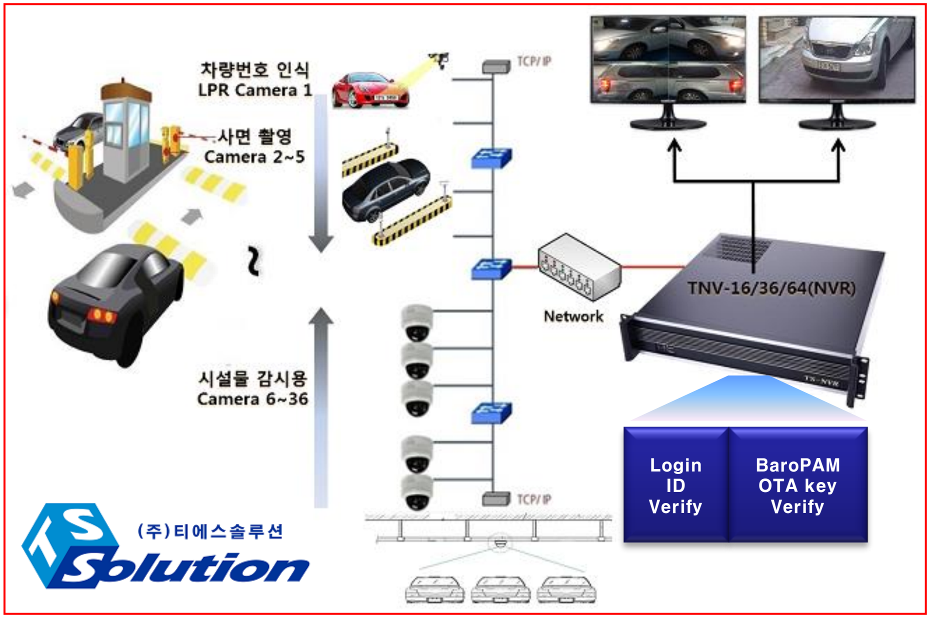
```
$ sqlplus baropam/baropam
Verification code: 613045
SQL*Plus: Release 11.2.0.1.0 Production on
금 11월 30 09:38:50 2018
Copyright (c) 1982, 2009, Oracle.  All
rights reserved.
SQL> exec twofactor.authenticate(691199);
PL/SQL procedure successfully completed
SQL> exec enable_role('APPOBJACCESS');
PL/SQL procedure successfully completed.
```

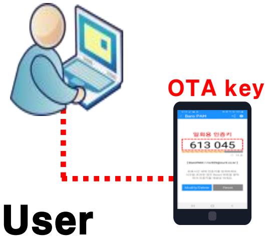
Copyright © Nurit Corp. All rights reserved.

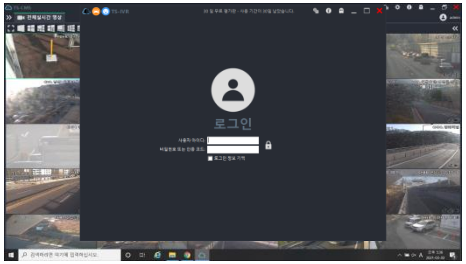
Appendix. Application appearance

24. Convergence with CCTV solutions

Intelligent CCTV strengthens security by applying BaroPAM for user identification and authentication to a CCTV solution equipped with various functions that analyze the video while recording the scene, unlike general CCTV that simply records and displays the scene.







Problems / Improvements

- Password change instructions to public institutions and CCTV management agencies
  - -For CCTV products, use the default password as is
  - -Easy access to CCTV via the Internet to access the internal network
- CCTV control centers have hundreds or thousands of CCTVs
  - -Consignment of stored CCTV footage to a private company
  - - Impossible to manually manage numerous CCTVs (one-time authentication)
- Necessity of compliance with the Personal Video Information Protection Act and response to audits

- Protect CCTV information assets with 2nd authentication (additional authentication)
- Prevent illegal use by replacing passwords with OTA keys
- Establish and operate video information protection measures
- Encryption and decryption applied when backing up video information
- Enhance security by applying 2nd authentication (additional authentication) to IP cameras

Copyright © Nurit Corp. All rights reserved.

Appendix. Application appearance

24. Authentication of VDI/SSO/VMI/wireless AP/VPN/SAC/CCTV, etc.

When logging in to VDI/SSO/VMI/wireless AP/VPN/SAC/CCTV, etc., enter the login-ID and generate a OTA key in the BaroPAM app. Security is strengthened by applying BaroPAM for user identification and authentication by entering the generated OTA key.

Before applying the OTA key

❖ Use fixed password for each information asset/account

❖ Apply password creation rules

❖ Store password information in DB

❖ Requires security measures (one-way encryption) using encryption technology, etc.

❖ Risk of leakage and damage

❖ Mandatory password change cycle applied

❖ Password syndrome/password reset syndrome complaints

After applying the OTA key

❖ Use of OTA key for each information asset / account

❖ Apply value generated from hash algorithm (SHA512)

❖ Create directly from the BaroPAM app when needed

❖ No need for security measures using encryption technology, etc.

❖ No risk of leakage or damage

❖ Apply individual authentication key generation cycle (3~60 sec)

❖ Password syndrome/password reset syndrome does not occur

Copyright © Nurit Corp. All rights reserved.

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

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr