SC Point
secure your business

PocketKey+ II

PocketKey 사용 매뉴얼



PocketKey+ II





www.scpoint.co.kr
02-515-5127

목차

01 제품 소개 및 사용 준비 3

02 제품 연결 및 인증 방법 5

03 Windows에서 보안키 설정 6

04 ACS Key Manager 사용 8

05 사이트별 등록 및 로그인 12

06 문제 해결 및 초기화 34

07 자주 묻는 질문 35

08 안전한 사용 및 고객지원 36

01 제품 소개 및 사용 준비

PocketKey+ II 제품 소개

PocketKey+ II는 USB 및 NFC 연결을 지원하는 보안키입니다. USB 연결에서 인증 화면이 제품 확인을 요청하면 제품의 확인 버튼을 누릅니다.

보안키를 사이트 계정에 등록하면 로그인 또는 추가 인증에 사용할 수 있습니다. 지원되는 등록 방식과 인증 요청은 서비스 및 계정 정책에 따라 다릅니다.

제품별 주요 기능

항목	PocketKey+ II	PocketKey+ Bio	NFC Card
연결	USB-C / NFC	USB-C / NFC	NFC
확인 동작	기계식 버튼	지문 센서 (USB)	리더에 카드 제시
패스키 저장 공간	최대 100개	최대 100개	최대 200개
지문 등록	해당 없음	최대 10개	해당 없음
PKI 키 슬롯	최대 150개	-	-
TOTP / HOTP	지원	지원	지원

패스키 저장 공간 용량은 장치에 저장할 수 있는 해당 자격 증명의 수이며, 모든 등록 방식의 계정 수를 의미하지 않습니다. NFC Card의 PC 사용은 ACR1552U 리더기를 기준으로 설명합니다.

준비물 및 사용 환경

Windows PC 및 PocketKey+ II를 준비합니다. 사이트 등록에는 사용할 계정과 브라우저가 필요합니다.

장치 관리에는 ACS FIDO Device Key Manager를 사용합니다. 회사 PC에 프로그램 또는 드라이버 설치 권한이 없는 경우에는 담당자에게 문의합니다.

분실이나 초기화에 대비하여 다른 보안키 또는 계정 복구 수단을 준비하고, 실제로 로그인할 수 있는지 확인합니다.

보안키·패스키·PIN 구분

구분	설명
보안키	로그인할 때 본인 확인에 사용하는 보안 장치입니다.
패스키	사이트에 등록하는 로그인용 자격 증명입니다. 이 매뉴얼은 PocketKey에 저장하는 과정을 설명합니다.
PocketKey PIN	해당 보안키에 설정한 PIN입니다. 장치 관리와 사이트의 보안키 PIN 요청에 사용합니다.
OTP Tool 비밀번호	OTP Tool에 접근할 때 사용합니다. 초기 비밀번호는 00000000이며, 변경한 경우에는 변경된 값을 입력합니다.
Windows Hello PIN	PC 로그인 등에 사용하는 PIN입니다. PocketKey PIN과 별개입니다.

제품의 PIN 설정과 사이트 계정의 보안키 등록은 별개의 과정입니다. PIN 설정 후에는 사용할 사이트에서 보안키를 등록해야 합니다.

02 제품 연결 및 인증 방법

USB 연결

1. PocketKey+ II를 PC의 USB-C 포트에 연결합니다.
2. Windows 설정 또는 ACS Key Manager에서 장치가 인식되는지 확인합니다.
3. 인증 화면의 안내에 따라 PIN을 입력하고 제품의 확인 버튼을 누릅니다.

NFC 연결

NFC를 지원하는 기기 또는 호환 리더기의 인식 영역에 제품을 제시하고 화면 안내에 따라 인증합니다. 연결 가능 여부는 사용하는 기기와 서비스의 지원 조건을 확인합니다.

이 매뉴얼의 Windows 초기 설정과 관리 프로그램 절차는 USB 연결을 기준으로 설명합니다.

03 Windows에서 보안키 설정

다음 절차는 PocketKey의 PIN을 설정하는 과정입니다. Windows 로그인용 PIN(Windows Hello) 설정과 구분하여 진행합니다.

1. 보안키 관리 메뉴 열기

Windows 설정에서 [계정] → [로그인 옵션] → [보안 키] → [관리]를 선택합니다.

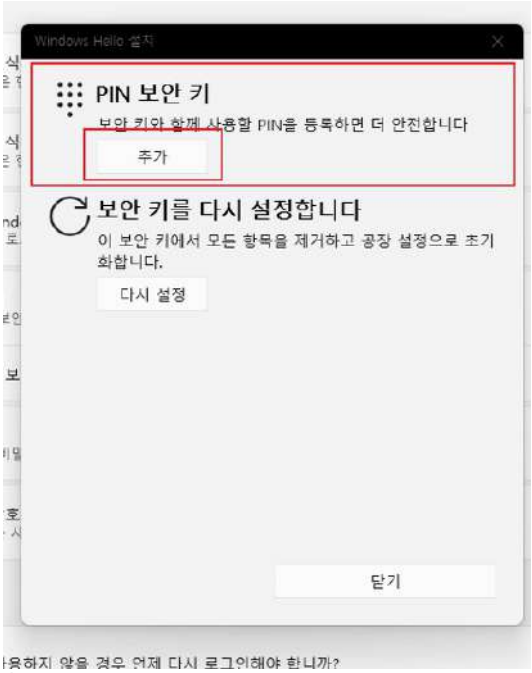
연결 또는 제품 확인 요청이 표시되면 제품별 인증 방법에 따라 진행합니다.



- 윈도우 검색창에 로그인 옵션 검색 후 로그인하는 방법으로 보안 키 선택 후 관리 클릭

2. 보안키 PIN 추가

[PIN 보안 키]에서 [추가]를 선택합니다. 이미 PIN이 설정된 제품은 기존 PIN을 사용합니다.

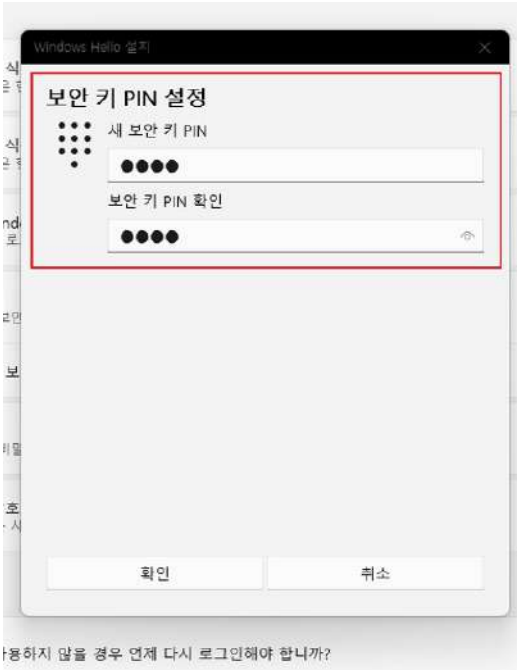


PIN을 설정하기 위해 제품을 먼저 초기화할 필요는 없습니다.

3. PIN 입력 및 설정 완료

[새 보안 키 PIN]과 [보안 키 PIN 확인]에 같은 값을 입력하고 [확인]을 선택합니다.

설정이 완료되면 이후 보안키 PIN 요청에 이 값을 입력합니다.



PIN 길이와 사용 가능한 문자는 화면 안내를 따릅니다. OTP 초기 비밀번호 및 Windows Hello PIN과 혼동하지 않도록 주의합니다.

04 ACS Key Manager 사용

프로그램 실행 및 장치 선택

ACS에서 제공하거나 공급받은 운영체제용 ACS FIDO Device Key Manager를 실행합니다. 제품을 연결한 뒤 Devices에서 사용할 장치를 확인합니다.

OTP Tool 이외의 PIN 인증 메뉴에는 Windows에서 해당 PocketKey에 설정한 PIN을 입력합니다. OTP Tool은 별도의 비밀번호를 사용합니다.

프로그램 캡처는 다른 모델과 버전 2.0.1의 예시입니다. 표시되는 메뉴와 저장 용량은 제품 및 프로그램 버전에 따라 다를 수 있습니다.

장치 정보 확인 (Home)

Home에서 장치 식별 정보, 펌웨어 버전 및 PIN 상태를 확인합니다.



표시 항목	설명
Serial number / AAGUID	장치 일련번호 및 인증 장치 유형의 식별 정보
Firmware version / Version release	펌웨어 버전 및 릴리스 정보
PIN is set / retries left	PIN 설정 여부 및 남은 PIN 입력 시도 횟수

캡처의 남은 시도 횟수는 연결된 장치의 당시 상태입니다. 모든 모델에 동일하게 적용되는 고정값으로 해석하지 않습니다.

Application 메뉴

메뉴	기능
Change PocketKey PIN	보안키 PIN을 변경합니다.
Change OTP PIN	OTP Tool 접근 비밀번호를 변경합니다.
Reset	장치를 초기화합니다. 실행 전 준비 및 절차는 문제 해결 장에서 확인합니다.

PIN 및 OTP 비밀번호 변경

[Change PocketKey PIN]에서 기존 PocketKey PIN으로 인증한 뒤 새 PIN을 설정합니다. 이후 보안키 PIN 요청에는 변경된 값을 입력합니다.

[Change OTP PIN]에서 기존 OTP 비밀번호를 사용하여 새 값을 설정합니다. 최초 비밀번호는 00000000이며, 변경 이력이 있으면 변경된 값을 입력합니다.

변경 완료 안내를 확인한 뒤 해당 메뉴에서 새 값으로 접근되는지 확인합니다. 길이와 사용 가능한 문자는 화면 안내를 따릅니다.

저장된 자격 증명 확인 (Key Slot)

1. [Key Slot]을 선택하고 PocketKey PIN을 입력합니다. [Unlock]이 표시되면 선택하여 잠금을 해제합니다.

2. 목록의 서비스 이름과 사용자 이름을 확인합니다.

3. 현재 사용 수와 전체 용량을 확인합니다. 예시의 2/100은 사용 중인 슬롯 2개와 전체 용량 100개를 나타냅니다. 실제 용량은 모델에 따라 다릅니다.

저장된 자격 증명 삭제

서비스 및 사용자 이름을 확인한 후 삭제할 항목의 체크박스를 선택합니다. [Delete]를 선택하고 확인 안내에 따라 진행합니다.



삭제 전에 대체 인증 수단으로 로그인할 수 있는지 확인합니다. 장치 내부의 자격 증명 삭제와 사이트 계정의 보안키 등록 해제는 별개의 작업입니다.

OTP Tool 접근

[OTP Tool]을 선택하고 OTP 비밀번호를 입력합니다. 초기 비밀번호는 00000000이며, 변경한 경우에는 변경된 값을 입력합니다.



No OTP record는 등록된 OTP 항목이 없다는 뜻입니다. 캡처의 0/20은 해당 화면의 등록 수와 용량을 나타냅니다.

TOTP 및 HOTP

OTP는 일회용 인증 코드입니다. OTP Tool 접근 비밀번호와 사이트에 입력하는 OTP 코드는 서로 다른 값입니다.

TOTP는 시간, HOTP는 카운터를 기준으로 코드를 생성합니다. 사용할 사이트에서 지원하는 방식과 설정에 맞추어 등록합니다.

OTP 등록 및 사용

1. 사이트의 OTP 인증 설정에서 등록 정보 및 복구 수단을 준비합니다.
2. OTP Tool의 [Add]를 선택하고 사이트에서 제공한 정보를 해당 입력란에 입력합니다.
3. 등록 후 목록에 새 항목이 표시되는지 확인하고 화면 안내에 따라 코드를 생성합니다.
4. 사이트의 OTP 확인란에 생성한 코드를 입력하여 등록을 완료합니다.

OTP 설정 비밀키와 QR 코드는 인증 정보입니다. 타인에게 공유하거나 공개하지 않습니다.

OTP 항목 수정 및 삭제

목록에서 대상 항목의 체크박스를 선택하고 [Edit] 또는 [Delete]를 사용합니다. 삭제 전에 사이트의 다른 인증 수단으로 로그인할 수 있는지 확인합니다.

장치의 OTP 항목을 삭제해도 사이트의 OTP 설정이 자동으로 해제되지는 않습니다. OTP Tool 접근 비밀번호는 Application의 [Change OTP PIN]에서 변경합니다.

프로그램 버전 및 도움말 (About)

[About]에서 프로그램 버전을 확인합니다. Document Support의 [User Manual]을 선택하면 공식 도움말을 확인할 수 있습니다.



문의 시 모델명, 프로그램 버전, 사용한 메뉴 및 오류 메시지를 함께 전달합니다.

05 사이트별 등록 및 로그인

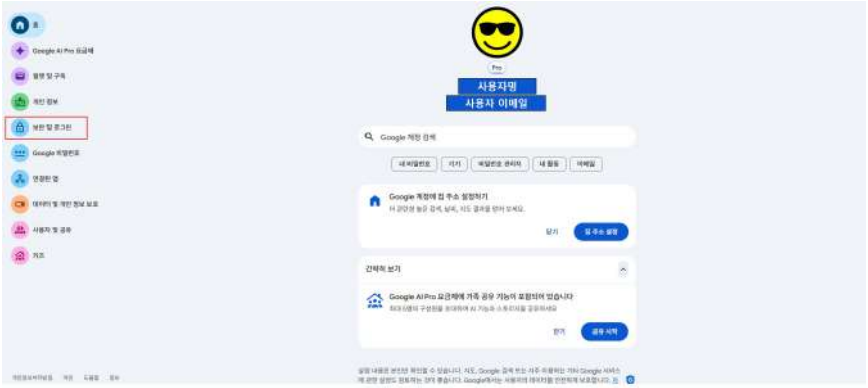
제품의 초기 설정을 마친 뒤 사용할 사이트의 계정 보안 설정에서 보안키를 등록합니다. Google은 등록과 로그인 과정을 설명하는 상세 예시이며, 다른 서비스는 메뉴와 화면 차이를 확인하는 참고 예시입니다.

서비스에 따라 패스키 등록과 2단계 인증용 보안키 등록이 구분됩니다. 실제 계정 화면의 등록 목적과 요청을 확인하고 진행합니다.

Google 등록

1. 계정 보안 메뉴 열기

등록할 Google 계정에 로그인하고 계정 관리 화면에서 [보안 및 로그인]을 선택합니다.



- 사용하는 구글 계정으로 로그인 후 보안 및 로그인 탭으로 이동

2. 2단계 인증 확인

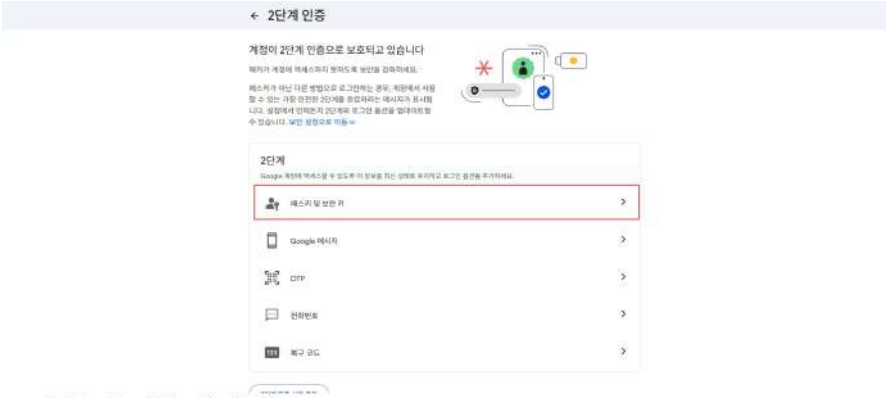
[Google에 로그인하는 방법]에서 [2단계 인증]과 대체 인증 수단을 확인합니다. 필요한 본인 확인은 화면 안내에 따라 진행합니다.



- Google에 로그인하는 방법 카테고리에서 2단계 인증 클릭

3. 패스키 및 보안키 메뉴 열기

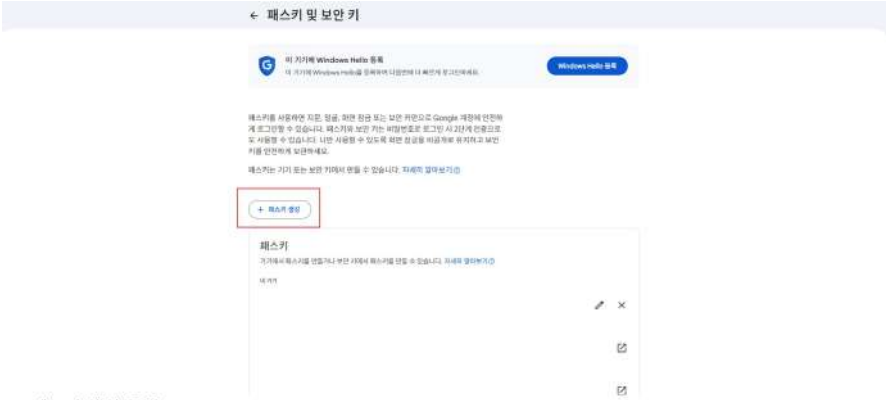
[패스키 및 보안 키]를 선택하고 본인 확인 요청을 진행합니다.



- 2단계 중 패스키 및 보안 키 클릭

4. 패스키 생성

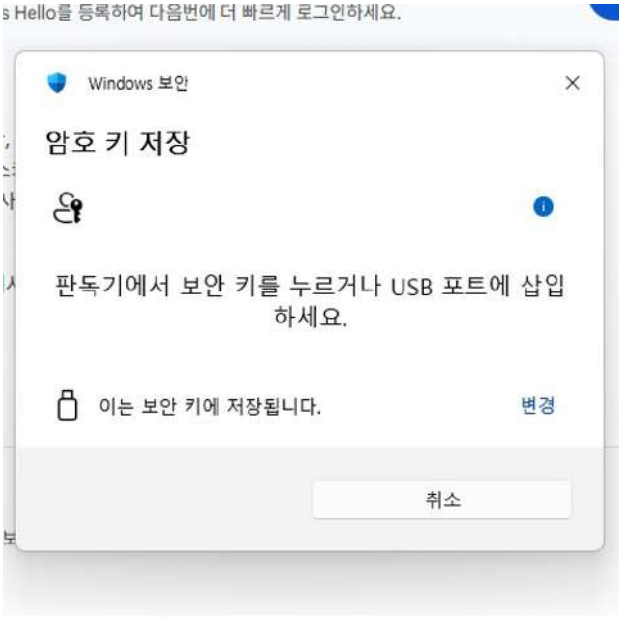
[패스키 생성]을 선택합니다. 저장 위치를 외부 보안키로 선택하여 PocketKey에 저장하는지 확인합니다.



- 패스키 생성 클릭

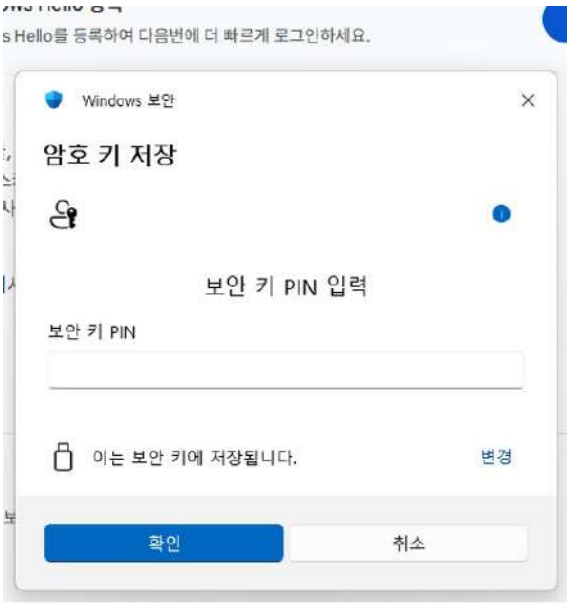
5. 제품 연결

Windows 보안 창의 안내에 따라 PocketKey를 PC에 연결합니다.



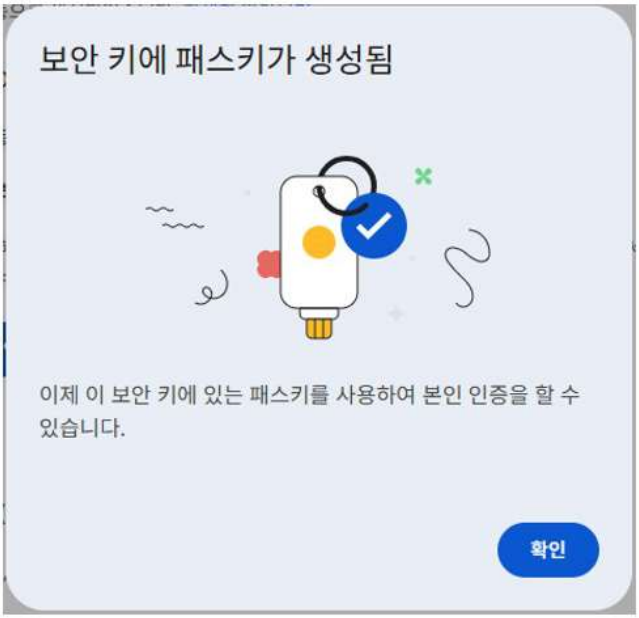
6. 본인 확인

PocketKey PIN을 요청하면 설정한 PIN을 입력합니다. 제품 확인 요청에는 제품의 확인 버튼을 누릅니다.



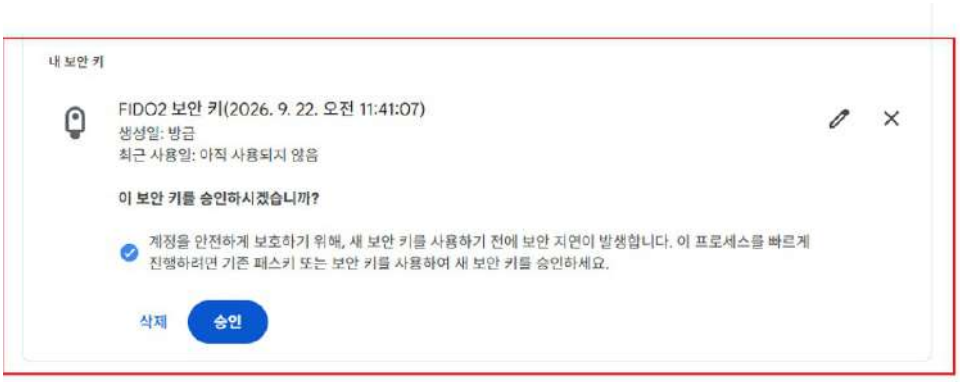
7. 생성 완료 확인

[보안 키에 패스키가 생성됨] 안내를 확인하고 [확인]을 선택합니다.



8. 등록 목록 확인

패스키 관리 화면에서 새 보안키의 이름과 생성일을 확인합니다. 승인 또는 보안 지연 안내가 있으면 계정 화면의 조건에 따릅니다.



Google 로그인 1. 다른 기기의 패스키 선택

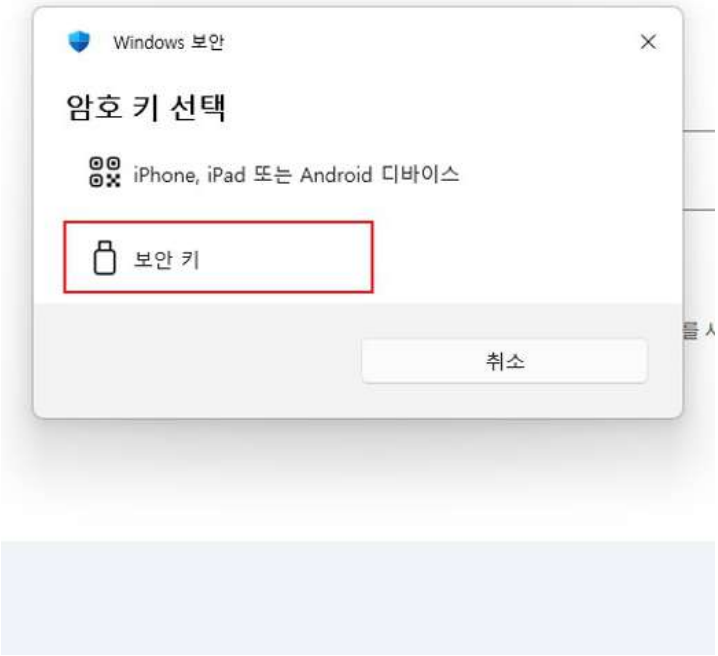
로그아웃 후 로그인 화면에서 [다른 기기의 패스키 사용]을 선택합니다. 표시되지 않는 경우에는 사이트에서 제공하는 다른 로그인 방법을 확인합니다.



- 아이디 창에 마우스를 클릭하면 패스키 사용이 뜨면 클릭

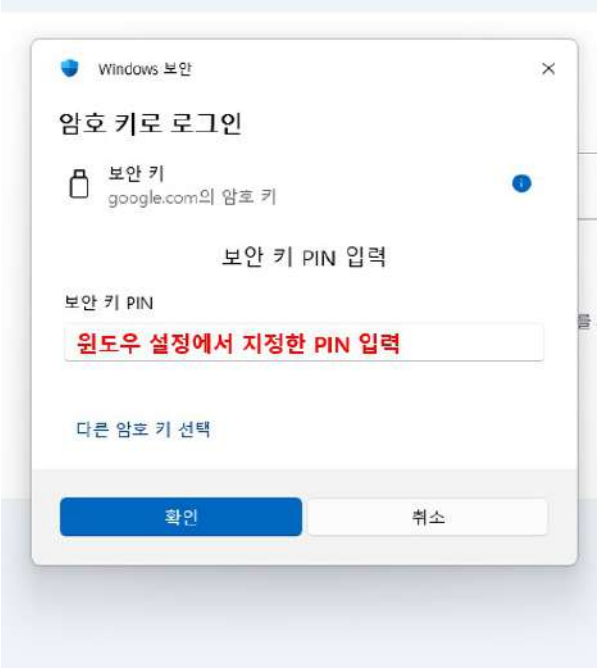
Google 로그인 2. 보안키 선택

Windows의 [암호 키 선택] 창에서 [보안 키]를 선택하고 사용할 제품을 연결합니다.



Google 로그인 3. 인증 및 로그인 완료

PocketKey PIN 및 제품 확인 요청을 진행합니다. 로그인된 계정 화면을 확인하여 등록한 키가 정상적으로 작동하는지 확인합니다.



Google 추가 참고 화면

추가로 제공된 Google 화면입니다. 위의 등록 절차와 함께 계정 화면의 차이를 확인합니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

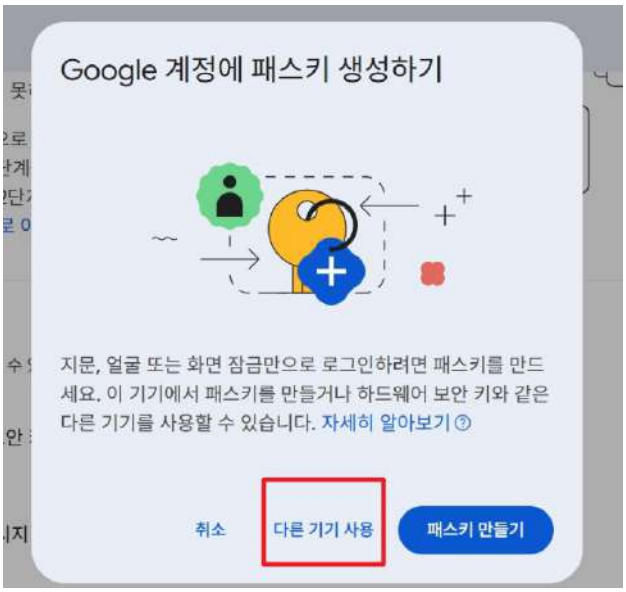
화면 1



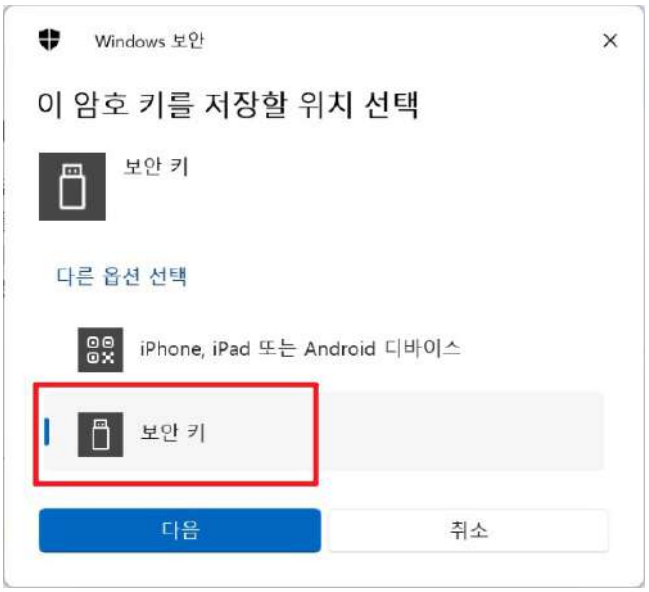
화면 2



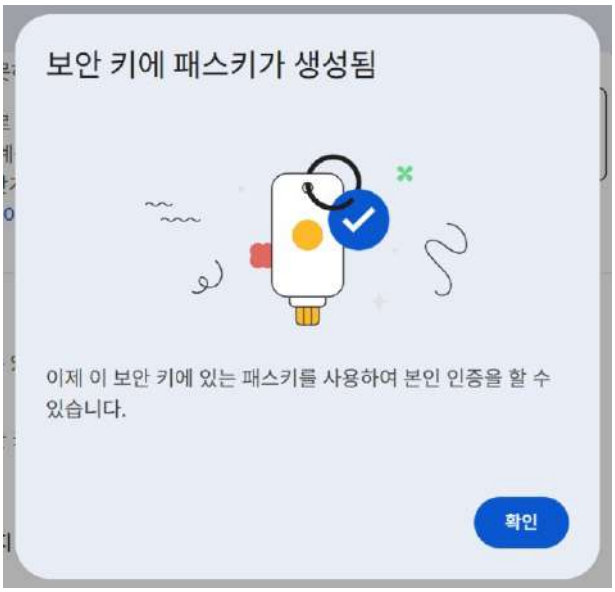
화면 3



화면 4



화면 5



네이버 참고 화면

패스키 메뉴에서 보안키를 선택하고 PIN 및 제품 확인 요청을 진행한 뒤 등록 결과를 확인합니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

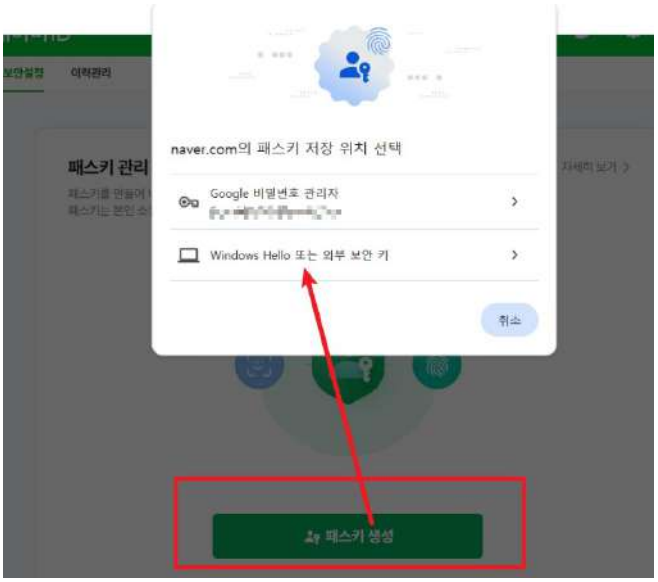
화면 1



화면 2



화면 3



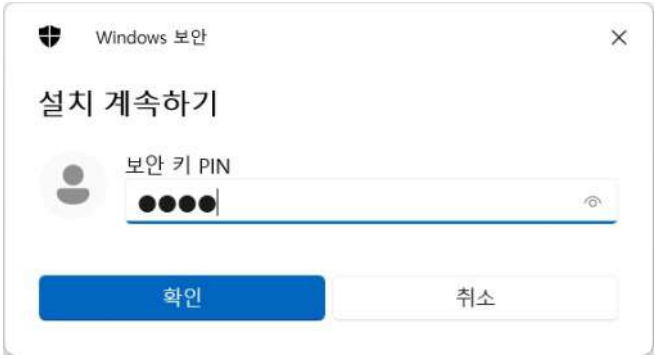
화면 4



화면 5



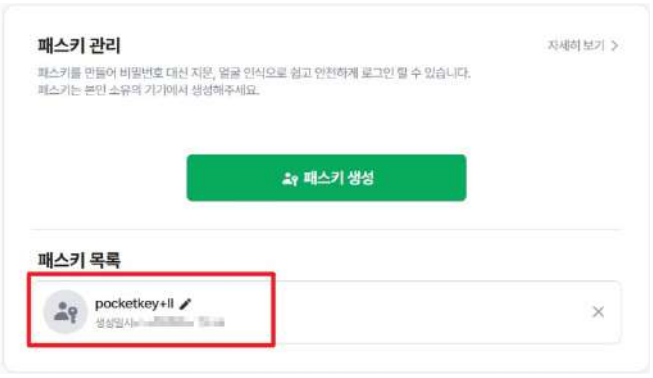
화면 6



화면 7


Windows 보안
설치 계속하기
보안 키를 터치하세요.
취소

화면 8

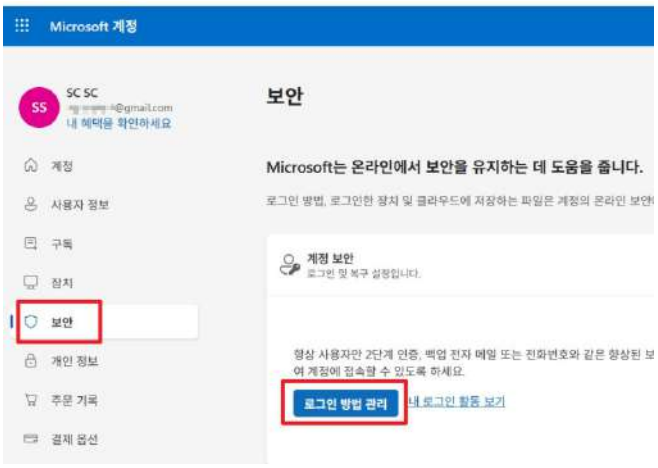

패스키 관리
자세히 보기 >
패스키 생성
패스키 목록
pocketkey+II

Microsoft 참고 화면

계정 보안 설정에서 로그인 방법과 보안키를 선택하는 예시입니다. 조직 계정은 정책에 따라 메뉴가 다를 수 있습니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

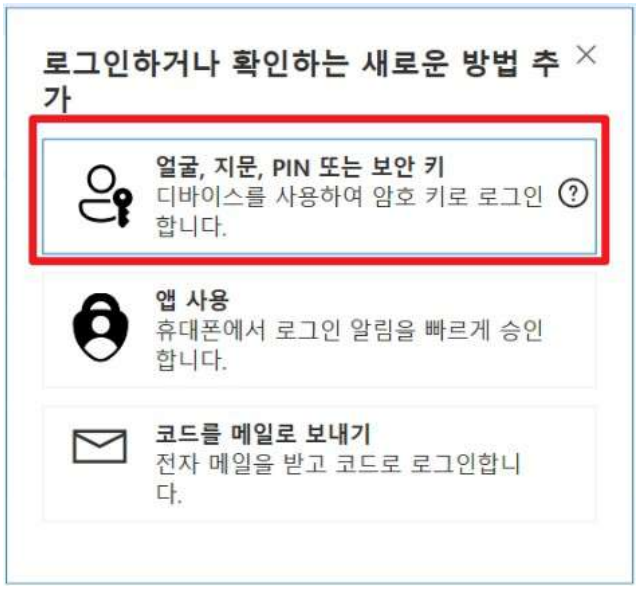
화면 1



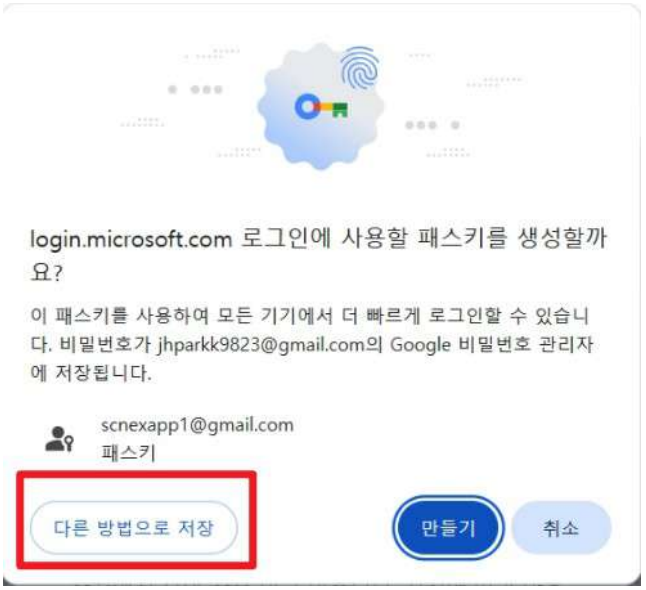
화면 2



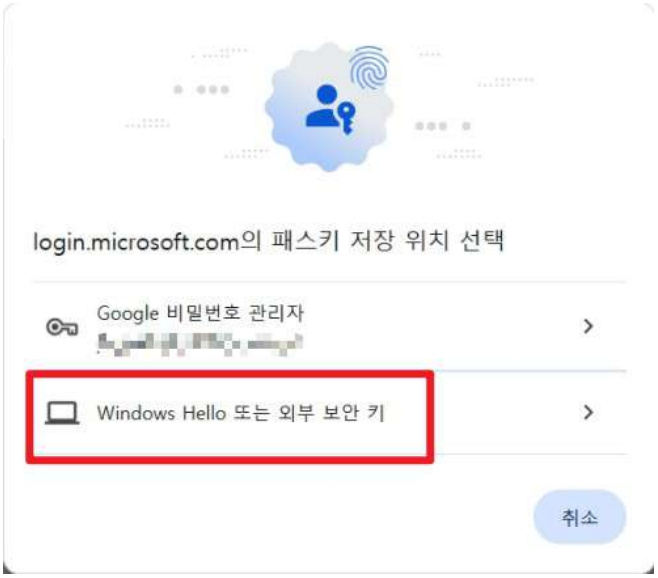
화면 3



화면 4



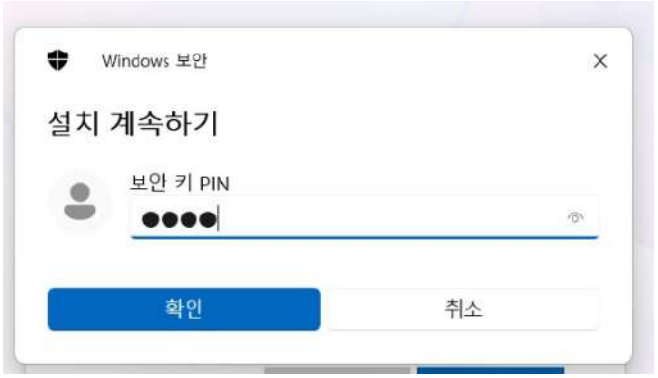
화면 5



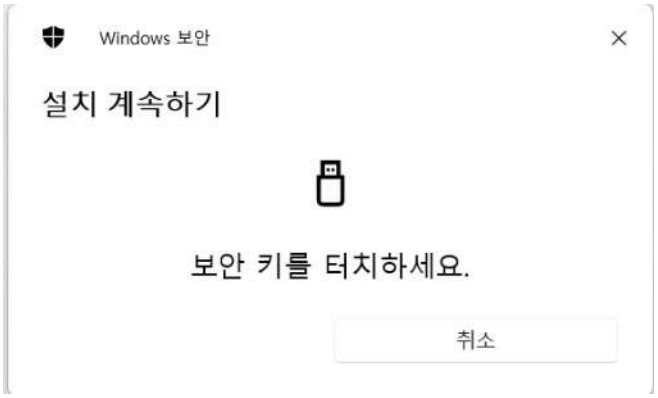
화면 6



화면 7



화면 8



화면 9



Dropbox 참고 화면

계정 보안 설정에서 보안키를 추가하고 등록 목록을 확인하는 예시입니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

화면 1



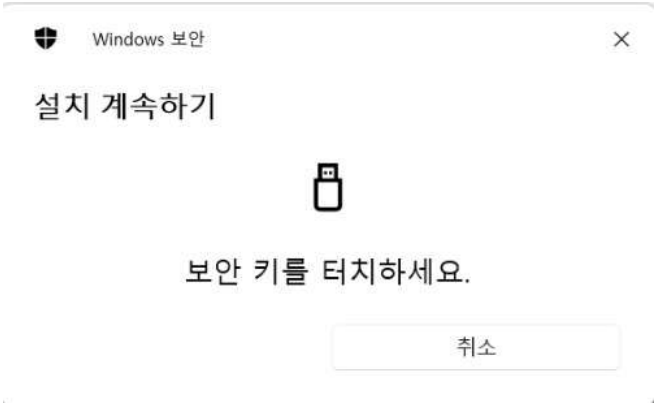
화면 2



화면 3



화면 4



화면 5



OpenAI 참고 화면

계정의 보안 설정에서 패스키 또는 보안키를 선택하는 예시입니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

화면 1



화면 2



화면 3



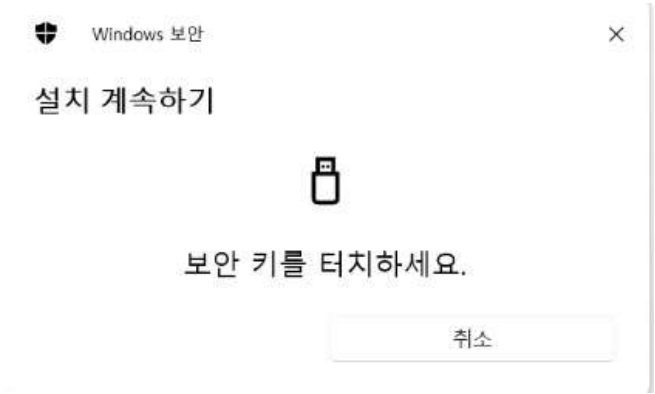
화면 4



화면 5



화면 6



화면 7


Windows 보안
암호가 저장되었습니다.
이제 보안 키를 사용하여 "openai.com"에 로그인할 수 있습니다.
확인

AWS 참고 화면

콘솔에서 MFA 디바이스를 할당하고 패스키 또는 보안키를 선택하는 예시입니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

화면 1



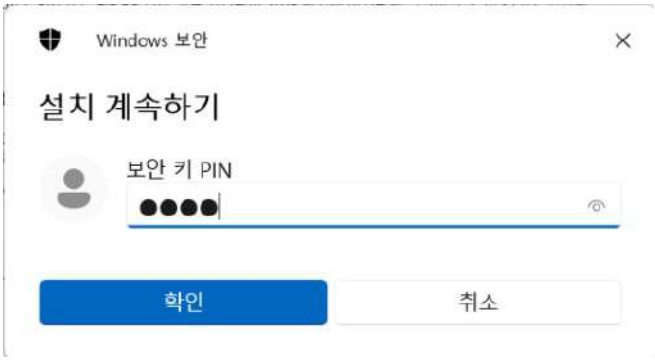
화면 2



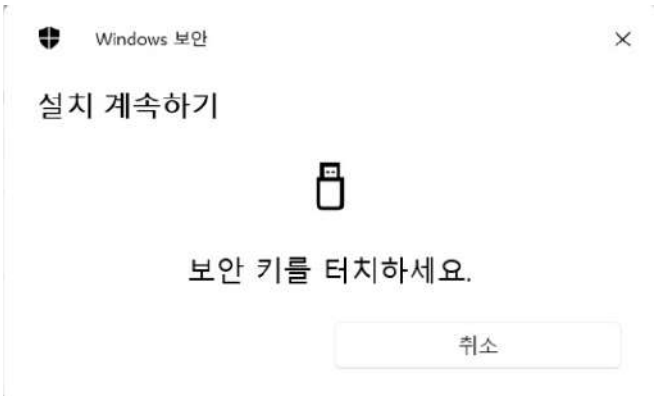
화면 3



화면 4



화면 5



화면 6

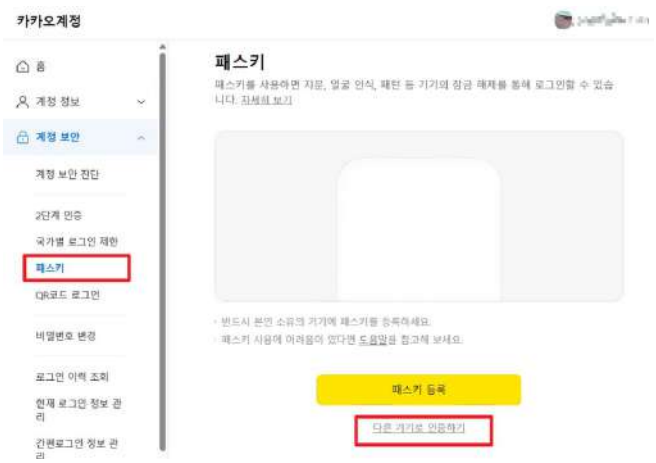


카카오 참고 화면

계정의 패스키 메뉴에서 보안키를 등록하는 예시입니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

화면 1



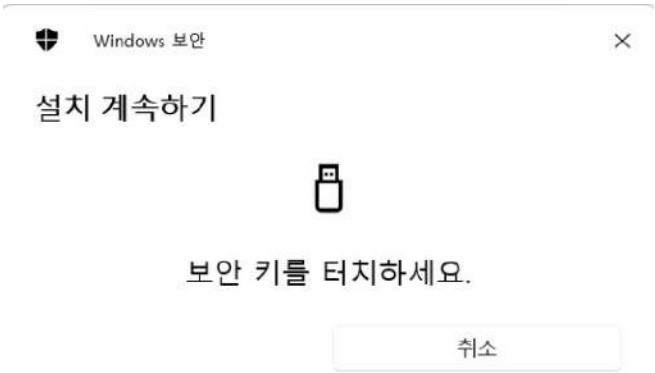
화면 2



화면 3



화면 4



화면 5

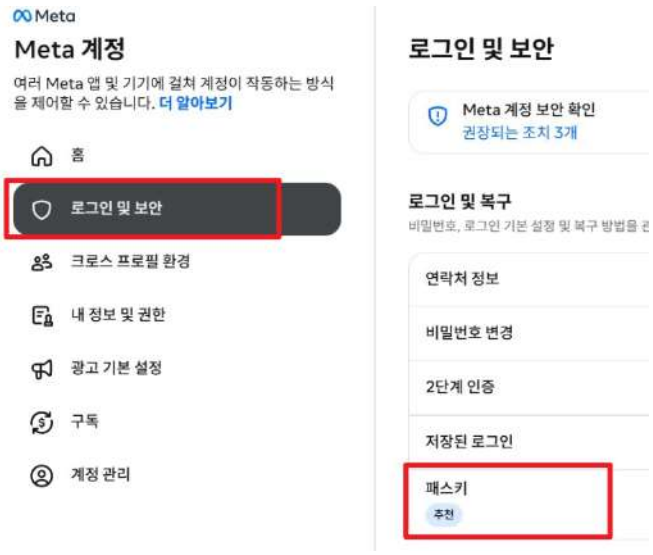


Facebook 참고 화면

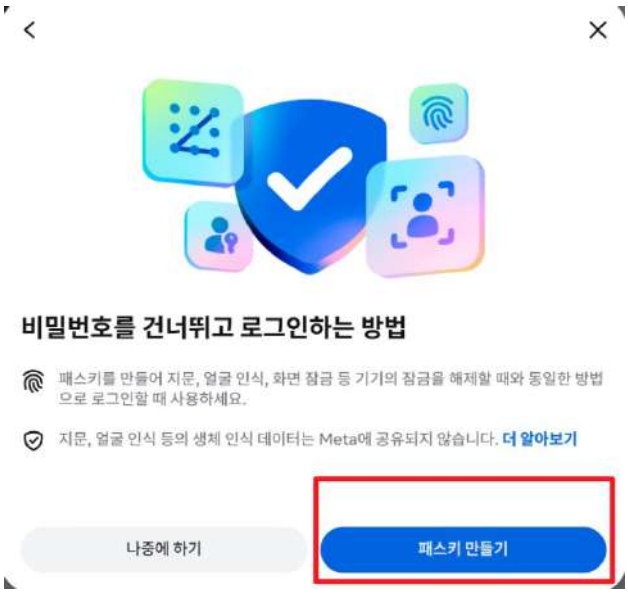
Meta 계정의 로그인 및 보안 메뉴에서 패스키 또는 보안키를 선택하는 예시입니다.

화면에 표시되는 PIN 및 제품 확인 요청에 따라 진행하고, 등록이 끝나면 목록 또는 완료 안내를 확인합니다.

화면 1



화면 2



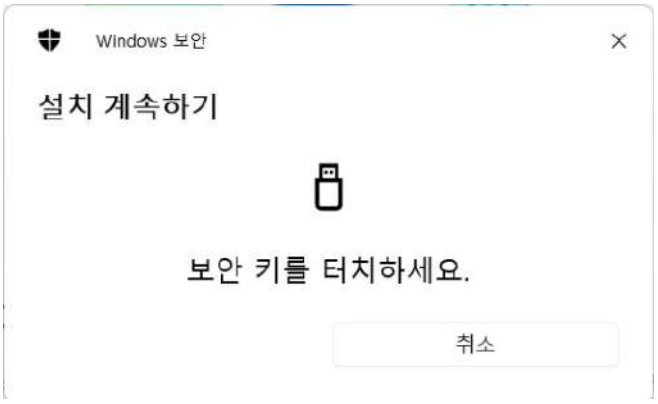
화면 3



화면 4



화면 5


Windows 보안
설치 계속하기
보안 키를 터치하세요.
취소

화면 6


Windows 보안
암호가 저장되었습니다.
이제 보안 키를 사용하여 "facebook.com"에 로그인할 수 있습니다.
확인

Apple 참고 화면

iPhone에서 촬영한 등록 예시입니다.

등록 전 준비 사항

- 사용할 Apple 기기와 호환되는 FIDO 인증 보안키를 2개 이상 준비합니다.
- Apple 계정에 이중 인증을 설정하고, 등록할 기기에 암호를 설정합니다.
- 계정에 로그인된 모든 기기는 iOS 16.3, iPadOS 16.3, macOS 13.2 이상이어야 합니다.
- 웹에서 보안키를 사용할 경우 최신 브라우저를 사용합니다.

공식 안내: support.apple.com/ko-kr/102637

1. 설정 메뉴

[로그인 및 보안] → [이중 인증]으로 이동합니다.





2. 보안키 추가

[보안 키]에서 [보안 키 추가]를 선택합니다.





3. 보안 지연

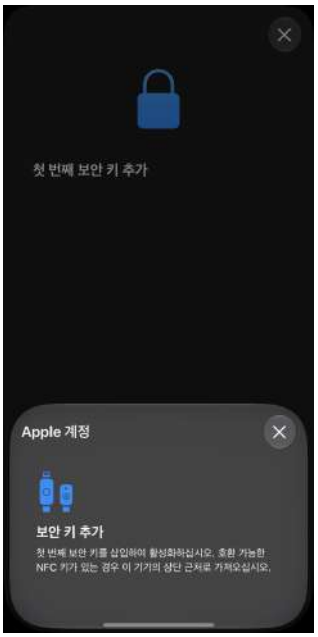
첨부 화면에는 도난당한 기기 보호에 따른 1시간 보안 지연이 표시됩니다. 같은 안내가 나오면 화면의 대기 조건에 따릅니다.

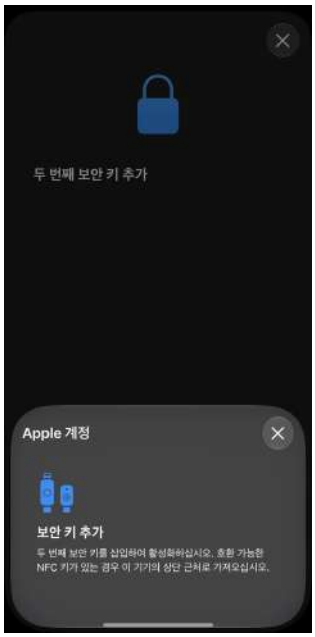




4. 첫 번째 및 두 번째 보안키 등록

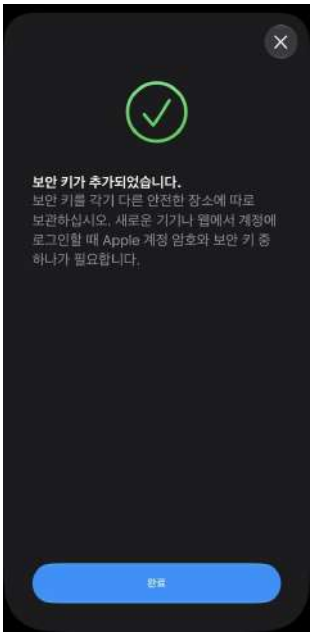
첫 번째 보안키 인증을 완료한 뒤 별도의 두 번째 보안키를 제시합니다. 아래 왼쪽은 첫 번째 키, 오른쪽은 두 번째 키를 추가하는 화면입니다.

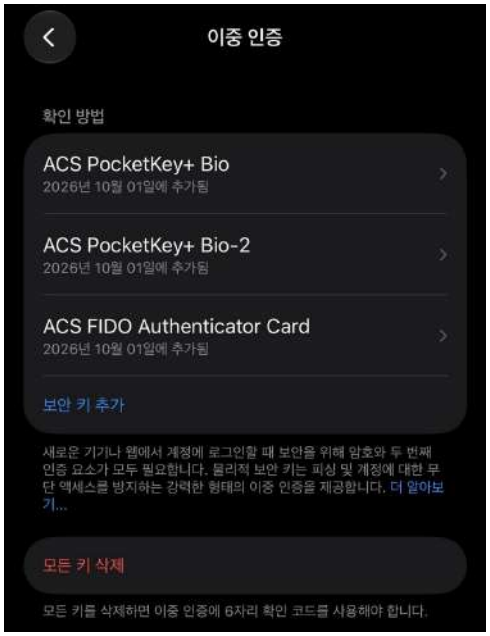




5. 등록 결과

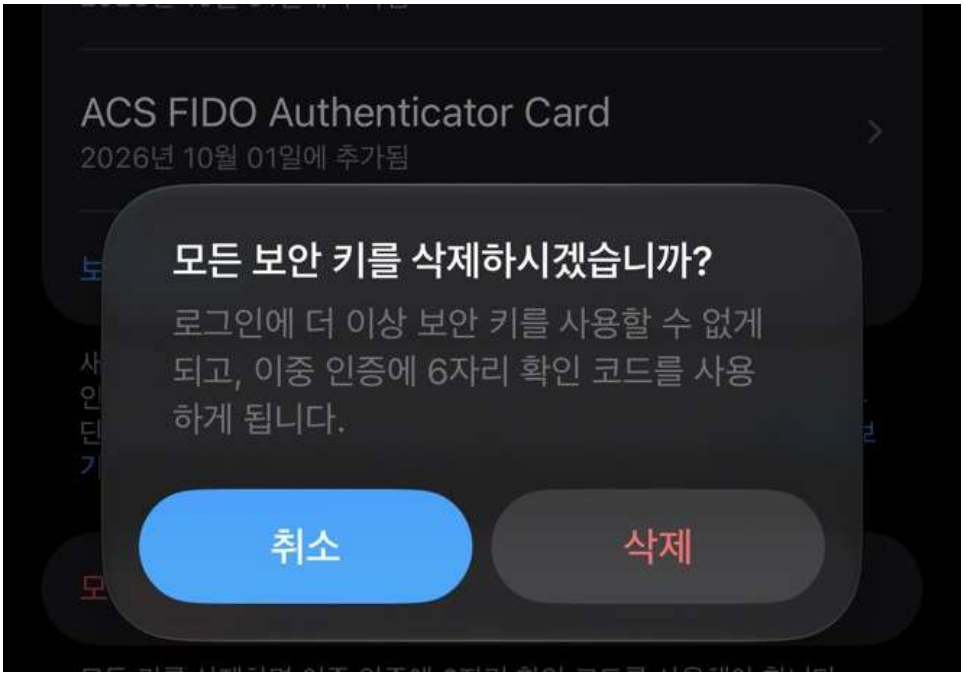
추가 완료 안내와 보안키 목록을 확인합니다. 캡처는 두 개의 보안키를 등록한 예시입니다.





6. 보안키 삭제 확인

[모든 키 삭제]의 확인 화면입니다. 신규 등록 과정에서 실행할 단계가 아닙니다. 필요한 경우에만 확인 창을 읽고 진행합니다.



06 문제 해결 및 초기화

제품이 인식되지 않을 때

USB 연결 상태를 확인하고 제품을 다시 연결합니다. 프로그램 및 브라우저에서 사용할 PocketKey가 선택되어 있는지 확인합니다.

PIN 또는 OTP 비밀번호 오류

현재 창이 요구하는 값이 PocketKey PIN, Windows Hello PIN, 계정 비밀번호 또는 OTP Tool 비밀번호인지 확인합니다. 변경 이력이 있는 경우에는 최신 값을 사용합니다.

정확한 값을 모른 채 입력을 반복하지 않습니다. Home에 남은 시도 횟수가 표시되면 확인하고, 접근이 어려운 경우에는 지원 담당자에게 문의합니다.

초기화 전 준비

다른 보안키 또는 복구 수단으로 관련 계정에 로그인할 수 있는지 먼저 확인합니다. 재등록할 계정 목록을 준비합니다.

초기화는 장치 설정과 저장 정보를 변경할 수 있습니다. 실행 전에 해당 제품의 Reset 확인 창에서 삭제 범위와 경고를 확인합니다.

Key Manager에서 초기화

1. 초기화할 PocketKey를 연결하고 Devices에서 대상 장치를 확인합니다.

2. [Application] → [Reset]을 선택합니다.

3. PIN 등 인증 요청이 표시되면 화면 안내에 따라 진행합니다.

4. 확인 창에서 삭제 범위와 경고를 확인한 후 초기화를 실행합니다.

5. 완료 메시지와 장치 상태를 확인합니다. 필요한 PIN을 설정하고, 삭제된 정보에 따라 사이트 등록을 다시 진행한 뒤 로그인을 확인합니다.

제품을 분실했을 때

대체 인증 수단으로 사이트에 로그인합니다. 계정의 보안 설정에서 분실한 보안키의 등록을 해제하고 새 보안키를 등록합니다.

장치의 자격 증명 삭제와 사이트 계정의 등록 해제는 별개의 작업입니다. 분실한 키는 해당 사이트의 설정에서 처리해야 합니다.

07 자주 묻는 질문

PIN을 입력한 후에도 버튼을 눌러야 하나요?

인증 과정에서 PIN 입력과 제품 확인 요청이 함께 표시될 수 있습니다. 화면에서 제품 확인을 요청하면 확인 버튼을 누릅니다.

제품을 연결하면 바로 로그인할 수 있나요?

사용할 사이트에서 먼저 보안키를 등록해야 합니다. 제품의 PIN 설정과 사이트 등록은 별개의 과정입니다.

보안키 PIN에는 어떤 값을 입력하나요?

Windows의 [보안 키] 관리에서 해당 PocketKey에 설정한 PIN을 입력합니다. PC 로그인용 Windows Hello PIN이나 사이트 계정 비밀번호와 구분합니다.

OTP Tool의 초기 비밀번호는 무엇인가요?

초기 비밀번호는 00000000입니다. 변경한 경우에는 변경된 비밀번호를 사용합니다.

등록했는데 로그인되지 않습니다.

등록한 계정과 사용하는 계정이 같은지, 보안키가 등록 목록에 있는지 확인합니다. 승인 또는 보안 지연 안내가 표시되면 해당 조건을 확인합니다.

08 안전한 사용 및 고객지원

안전한 제품 사용

제품을 임의로 분해하지 않습니다. 연결부가 손상되지 않도록 보관하고 물기와 오염을 피합니다.

PIN, OTP 비밀번호, OTP 설정 비밀키 및 계정 복구 정보는 타인에게 공유하지 않습니다.

제품 분실 또는 초기화에 대비해 대체 인증 수단을 유지합니다.

문의 시 확인할 정보

제품 모델명, Windows 환경, ACS Key Manager 버전, 연결 방식, 오류 메시지 및 오류가 발생한 단계를 확인합니다.

화면을 전달할 때는 PIN, OTP 코드 및 계정의 민감한 정보가 노출되지 않도록 처리합니다.

에스씨포인트 고객지원

홈페이지: www.scpoint.co.kr

전화: 02-515-5127