통합키 관리 솔루션

NeoKeyManager 4.0

관리 웹 운용 매뉴얼

MDS 인텔리전스

목차

I. NeoKeyManager 개요

1. 개요

- ✓ 대규모 개인정보 유출 사고가 지속적으로 발생됨에 따라 암호화는 선택이 아닌 필수
- ✓ 주요 정보 암호화에 사용되는 '암호키' 관리의 필요성이 높아짐
- ✓ 암호키의 외부 노출을 방지하고 효율적인 키 관리를 위해 HSM 기반의 국제 키 관리 상호 운용 표준(KMIP : Key Management Interoperability Protocol)을 준수하는 통합 키 관리 서버 'NeoKeyManager(NKM) '를 개발
- ✓ NKM은 Appliance 장비로써 안전한 키 관리를 위해 HSM에 연동하여 키를 보관하고 키의 라이프사이클 관리 및 그룹 관리를 통해 키 접근 제어 등의 기능을 제공

2. 구성

1) 전체 구성도

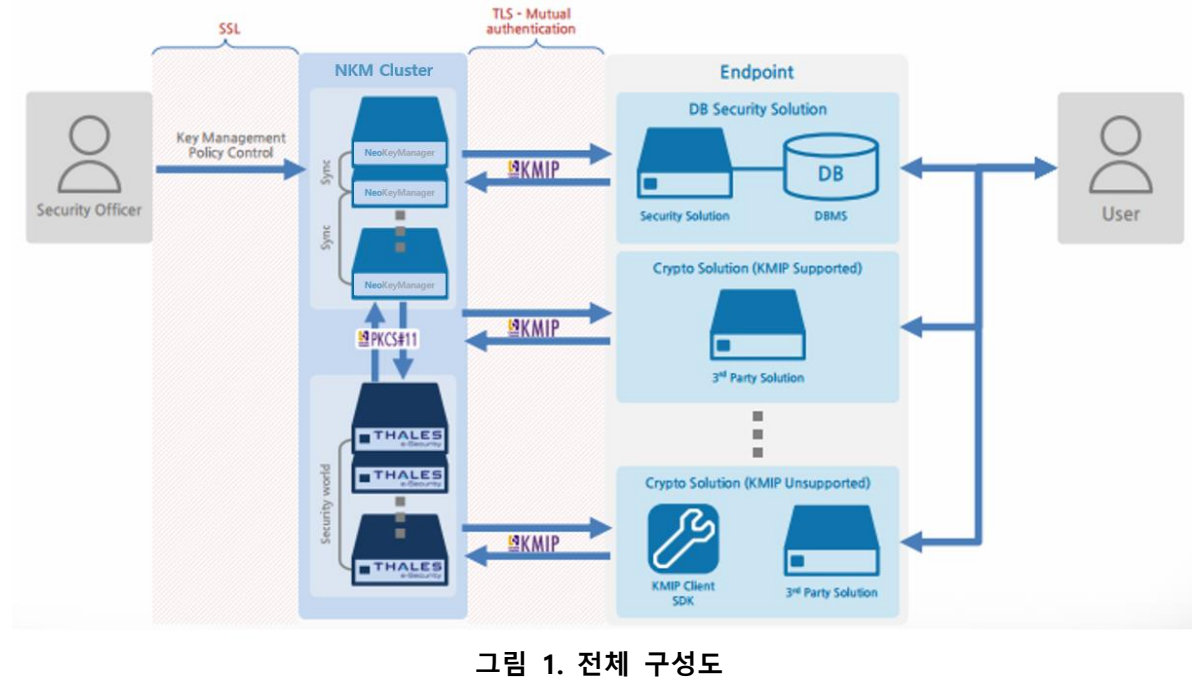
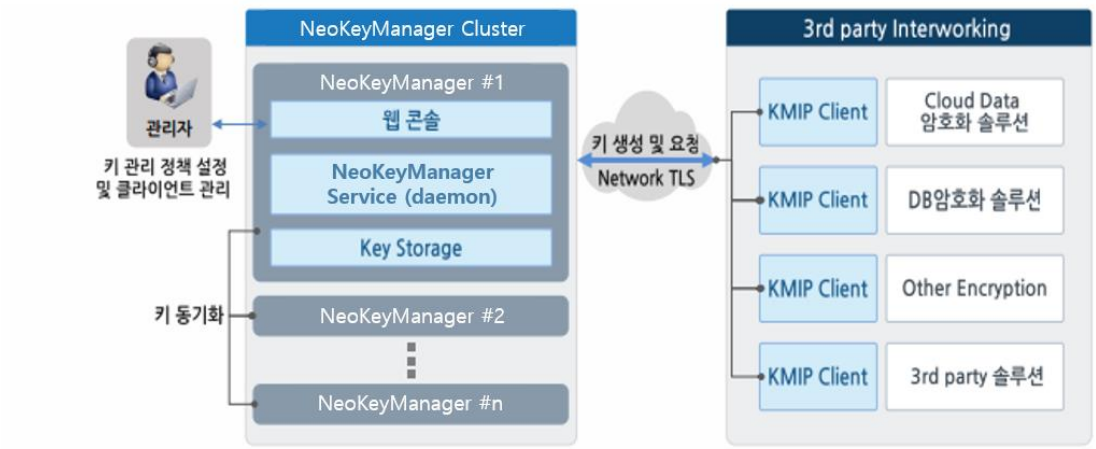


그림 1. 전체 구성도

2) 시스템 구조



구성요소	기능
웹 콘솔	• NeoKeyManager 환경설정, 키 관리 정책 설정 및 관리, 접속 허용 클라이언트 목록 관리, 클라이언트 그룹 관리, HA 기능 관리, 키 목록 조회, 키 백업 및 복구, 연산 및 키 별 통계, 감사
NeoKeyManager Service (daemon)	• KMIP 연산 대응, 등록된 클라이언트와 TLS 통신 채널 구축, TTLV(Tag Type Length Value)를 이용한 키 관리 메시지 송수신
Key Storage	• HSM을 이용하여 암호화 된 키의 저장

그림 2. 시스템 구조

3) 운용 시나리오

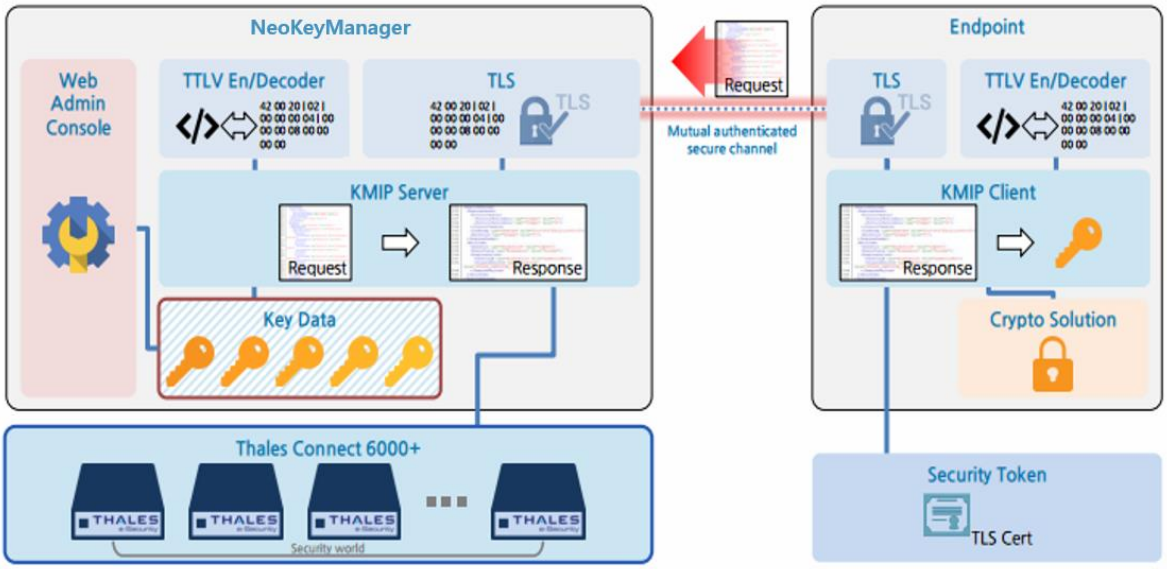


그림 3. 운용 시나리오

- ✓ NKM과 엔드포인트 간 TLS 통신 채널 구축
- ✓ TTLV를 이용한 KMIP 연산 대응 및 키 관리 메시지 송·수신

3. 암호키 라이프사이클 관리

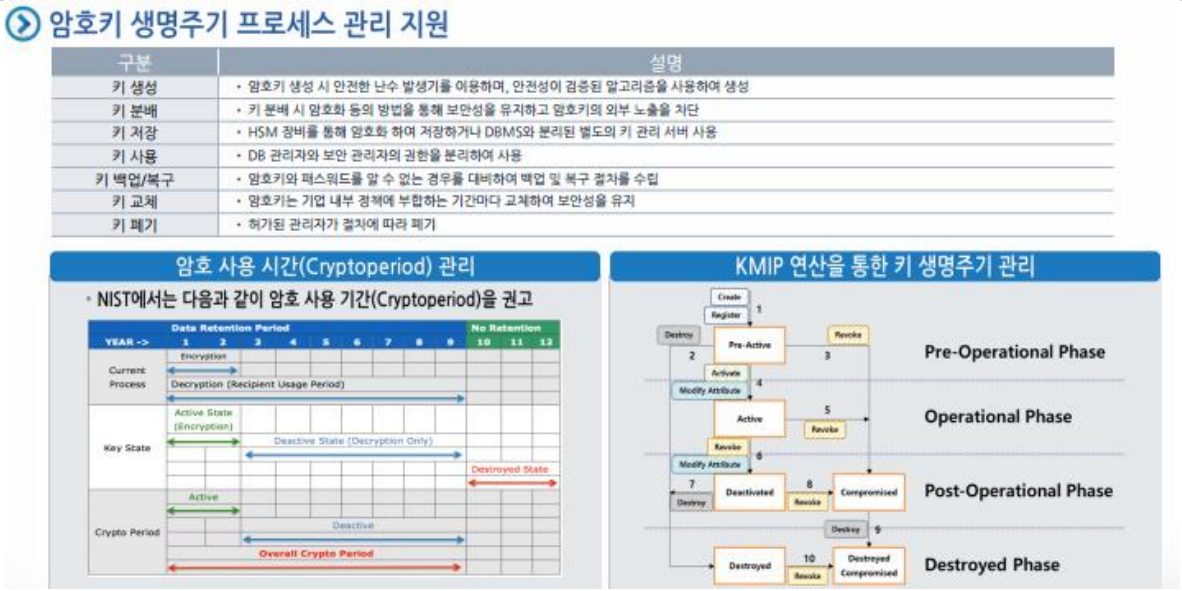


그림 4. 암호키 라이프사이클 관리

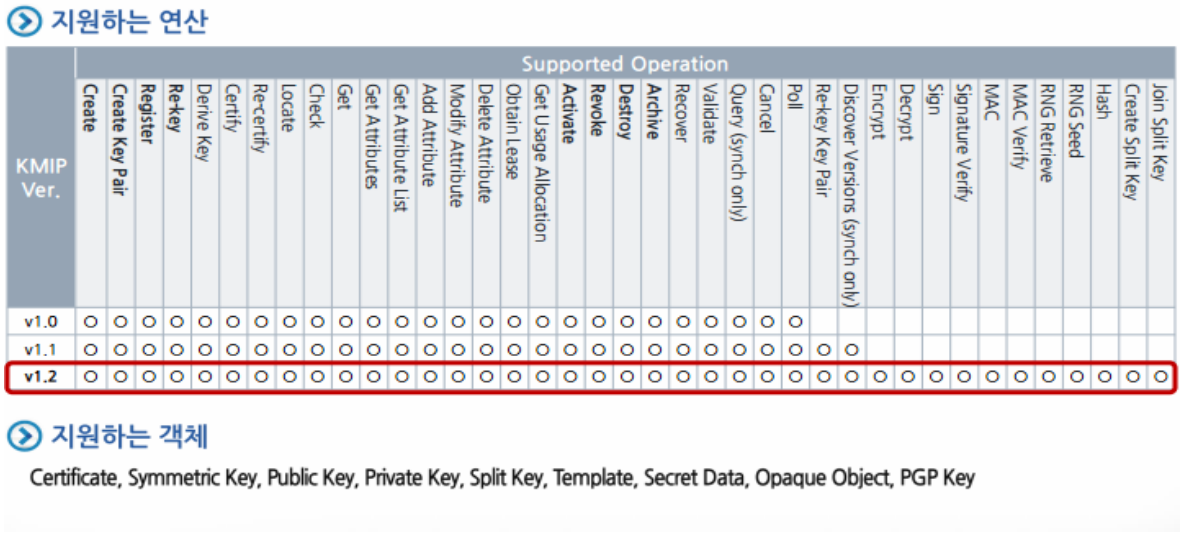
✓ **NKM은 국제 표준 KMIP를 준수함으로써 복잡한 암호키의 생명 주기를 자동화 관리**

✓ **암호키 상태(State) 관련 정의**

- NKM에서 사용하는 오브젝트의 상태를 표시하는 속성값
- 오브젝트 상태는 Modify Attribute 연산에 의해 수정될 수 없으며 특정 연산(Destroy, Revoke 등)에 의해서만 변경됨

✓ **암호키 주요 상태 관련 정의**

1) Pre-Active : 최초 암호키(오브젝트)를 생성한 후 갖게 되는 상태 값
   - 암호화 목적으로 사용될 수 없음
2) Active : 암호화 목적으로 사용 가능한 상태
   - Cryptographic usage mask 속성에 의해 허용된 용도로만 사용 가능
   - Process Start Date 속성이 설정된 경우, 프로세스 시작 날짜 이전에 암호화 목적으로 사용 될 수 없음
   - Protect Stop Date 속성이 설정된 경우 프로세스 중지 날짜 이후에 암호화 목적으로 사용 될 수 없음
3) Deactivated : 암호화 목적으로 사용될 수 없음(SHALL NOT)
   - Cryptographic Usage Mask 속성에 의해 허용된 암호화 목적으로만 사용될 수 있음
   - 해당키로 암호화된 데이터를 복호화하는 목적으로 사용 가능
4) Compromised : 암호화 목적으로 사용될 수 없음
   - Cryptographic Usage Mask 속성에 의해 허용된 암호화 목적으로만 사용될 수 있음
   - 해당키로 암호화된 데이터를 복호화하는 목적으로 사용 가능
5) Destroyed : 암호화 목적으로 사용될 수 없음
   - Destroyed Compromised : 어떤 암호화 목적으로도 사용될 수 없음



지원하는 연산

KMIP Ver.	Supported Operation																																		
	Create	**Create Key Pair**	**Register**	**Re-key**	Derive Key	Certify	Re-certify	Locate	Check	Get	Get Attributes	Get Attribute List	Add Attribute	Modify Attribute	Delete Attribute	Obtain Lease	Get Usage Allocation	**Activate**	**Revoke**	**Destroy**	**Archive**	Recover	Validate	Query (synch only)	Cancel	Poll	Re-key Key Pair	Discover Versions (synch only)	Encrypt	Decrypt	Sign	Signature Verify	MAC	MAC Verify	RNG Retrieve	RNG Seed	Hash	Create Split Key	Join Split Key
v1.0	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O												
v1.1	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O										
v1.2	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O

지원하는 객체

Certificate, Symmetric Key, Public Key, Private Key, Split Key, Template, Secret Data, Opaque Object, PGP Key

그림 5. KMIP 연산 객체

✓ NKM은 다양한 암호키 관리 Operation에 대한 연산을 지원

4. NKM 특징 및 장점

그림 6. NKM 외관

▼ NeoKeyManager의 특징 및 장점

제품 상세 내용

구분	규격
Concurrent client	100
Max Keys	1,000,000
FIPS 140-2 Support	Level 2
HSM Integration	Yes
KCMVP Crypto Module	Yes
HDD	8 x 3.5" Hot-swap drive support SATA Disk
LAN	2 Integrated 10Gb ports (Intel® Ethernet Controller X540)
Dimensions	16.93" x 27.95" x 3.44"
Chassis	Intel 2U Rack Mount Chassis
Power supply	2 x 1100W Platinum efficiency common redundant power supplies
FAN	Six managed 40mm dual rotor system fan

특징 및 장점

- ✓ 신뢰성
  - KMIP 표준을 준용한 키 Lifecycle 관리
  - 상호인증 TLS(Transport Layer Security)를 통한 안전한 키 전송
  - FIPS 140-2 Level 3인증 받은 HSM을 사용한 안전한 키 저장
- ✓ 호환성
  - KMIP Client SDK 및 기술 지원
  - KMIP 프로토콜을 지원하는 모든 클라이언트 지원
  - KMIP 지원 암호 솔루션: HP, Oracle, IBM, Dell, Quantum 등
- ✓ 편리성
  - GUI를 통한 관리자 도구 지원
  - 편리한 감사 및 추적 기능 제공
- ✓ 가용성
  - 서버 다중화 지원
  - 서버 장애 복구 지원
- ✓ 비용 절감
  - 구축 비용 절감
  - 시스템 도입으로 다양한 암호 솔루션 지원 가능
- ✓ 운용 비용 절감
  - 중앙화된 서버를 통한 운영자 업무 감소 및 운용 비용 절감

그림 7. NKM 특징 및 장점

II. NKM 관리 웹 운용

1. NKM 관리 웹 접속

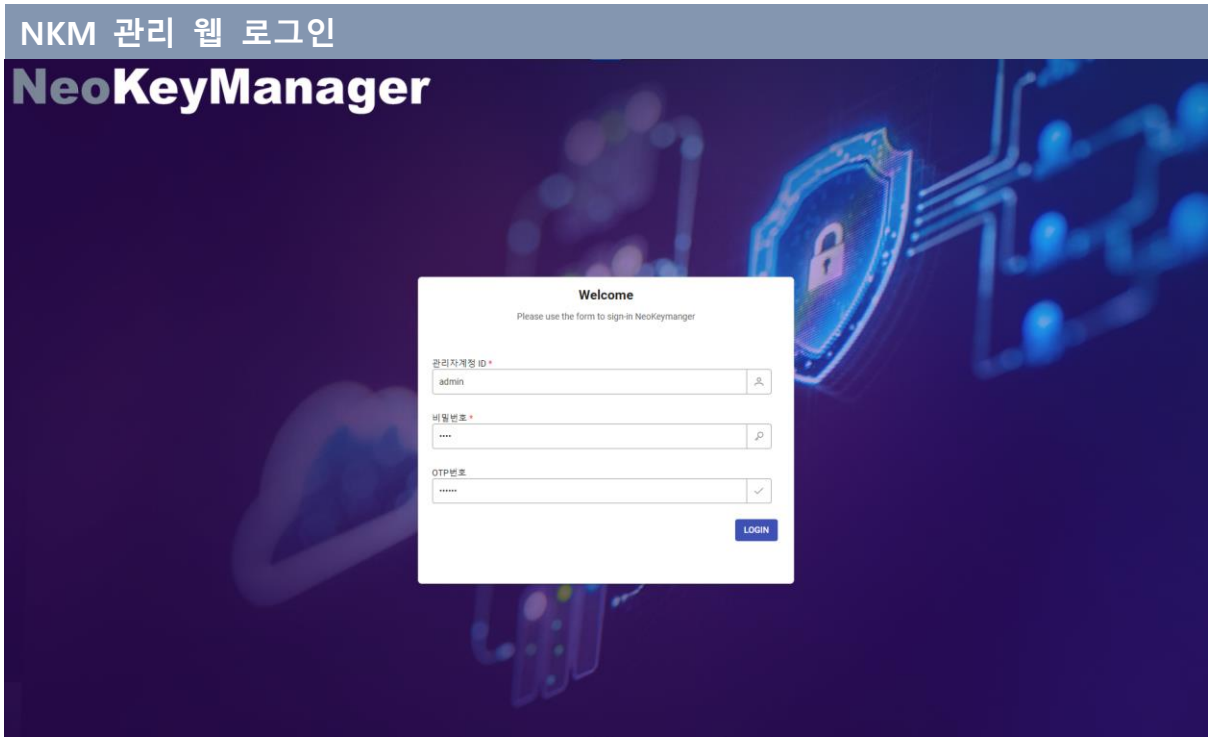


그림 8. NKM 관리 웹 로그인

- ✓ NKM은 관리자 편의를 위한 관리 웹을 제공
- ✓ Chrome 또는 Internet Explorer를 실행 후 아래의 예시 URL을 참고하여 주소 창에 입력(NKM 관리 웹은 Chrome에 최적화되어 있으므로 Chrome 사용을 권장)
  예시) https://192.168.70.201
  192.168.70.201 : NKM 서버 IP
- ✓ NKM 관리 웹 초기 화면에서 관리자 계정(ID, PW)으로 로그인
- ✓ NKM은 서비스 방식에 따라 OTP를 이용한 Two-factor 인증 기능을 제공

2. 메뉴

표 1. NKM 관리 웹 기본 메뉴 세부 구성

대메뉴	중메뉴	소메뉴	설명
RESOURCE	관리자 계정	-	- 새로운 계정 생성 및 삭제 기능 - 해당 역할 관리자 계정을 ID, 이름, 그룹 ID, 역할 별로 조회 가능
	그룹 관리	-	- 그룹 생성 및 삭제 기능 - 그룹 ID, 그룹 명 조회 가능
	엔드포인트 관리	-	- 엔드포인트 ID, 이름, 그룹 ID 조회 기능 제공 - 엔드포인트 생성 및 삭제 기능 제공
	승인 관리	-	- 하위 관리자(GSO,GA)에서 신청한 관리자계정, 엔드포인트, 그룹 생성 승인 관리 기능 제공
KEY	키 관리	전체키 관리	- 전체 모든 키에 대한 조회 기능 제공 - 키 UUID, 키 이름, 키 대체이름, 그룹 ID 등의 정보로 조회 가능 - 키 생성, 갱신, 인증, 재인증, 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		대칭키 관리	- 대칭키 알고리즘에 대한 조회 가능 - 키 생성, 갱신, 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		공개키 관리	- 공개키에 대한 조회 가능 - 키 생성, 인증, 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		개인키 관리	- 개인키에 대한 조회 가능 - 키 생성, 갱신, 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		인증서 관리	- 인증서 파일에 대한 조회 가능 - 재인증, 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		분할키 관리	- 분할키에 대한 조회 가능 - 분할키에 대한 취소, 파기, 삭제 기능
		비밀 데이터 관리	- 비밀 데이터에 대한 조회 가능 - 키 반출, 키 반입, 취소, 파기, 삭제, 키 유효기한 수정 기능
		불투명 객체 관리	- 불투명 객체에 대한 조회 가능 - 불투명 객체에 대한 취소, 파기, 삭제 기능
	키 보관소	-	- 키 유출과 같은 위급 상황이나 필요 시 키 관리의 특정 키를 선택하여 KMS와 분리 보관할 수 있는 별도의 보관소를 제공 - 키 유출이 아닌 것으로 확인 시 KMS로 복구 가능함.
	키 휴지통	-	- Deactivated 상태인 키들 중 미사용 키들을 키 휴지통으로 보낼 수 있음. - 키 휴지통으로 이동 시 파기(Destroyed) 상태로 변경됨.

KM서버 연계승인 관리	승인서버 운영하기	-	- 승인 목록 관리 ㄴ Tier KMS 요청 처리 (승인완료 또는 승인거절) - 승인서버 환경설정 ㄴ OEM 승인서버의 환경 설정
	승인요청 관리	-	- 승인요청 목록 관리 ㄴ Tier KMS에서 승인요청에 대한 목록 제공 - 승인서버 등록관리
HISTORY	KMIP관리 로그	KMIP연산 로그	- 키 연산 상태 및 결과 메시지 등에 대한 로그 확인 가능 - 로그 내역에 대한 엑셀 파일로 내려받기 기능 제공
	관리 로그	메뉴 접속 로그	- 사용자의 각 메뉴 접속에 대한 로그 확인 가능 - 로그 내역에 대한 엑셀 파일로 내려받기 기능 제공
		감사 로그	- 사용자의 이벤트 타입 별(로그인, 로그아웃 등) 로그 확인 가능 - 로그 내역에 대한 엑셀 파일로 내려받기 기능 제공
CONFIGURATION	환경 설정	일반정책	- 접근 보안 정책 ㄴ 관리 웹 계정의 패스워드 정책 설정 - SMTP 설정 ㄴ 이메일 알림을 위한 SMTP 환경 설정
		알림정책	- 알림정책 등록관리 ㄴ 키 상태 알림, 키 만료 알림 등 알림 정책과 수신 Client 설정 - 알림 수신 클라이언트 등록관리 ㄴ 알림을 수신할 URL 또는 이메일 설정

3. RESOURCE

1) 관리자 계정 관리

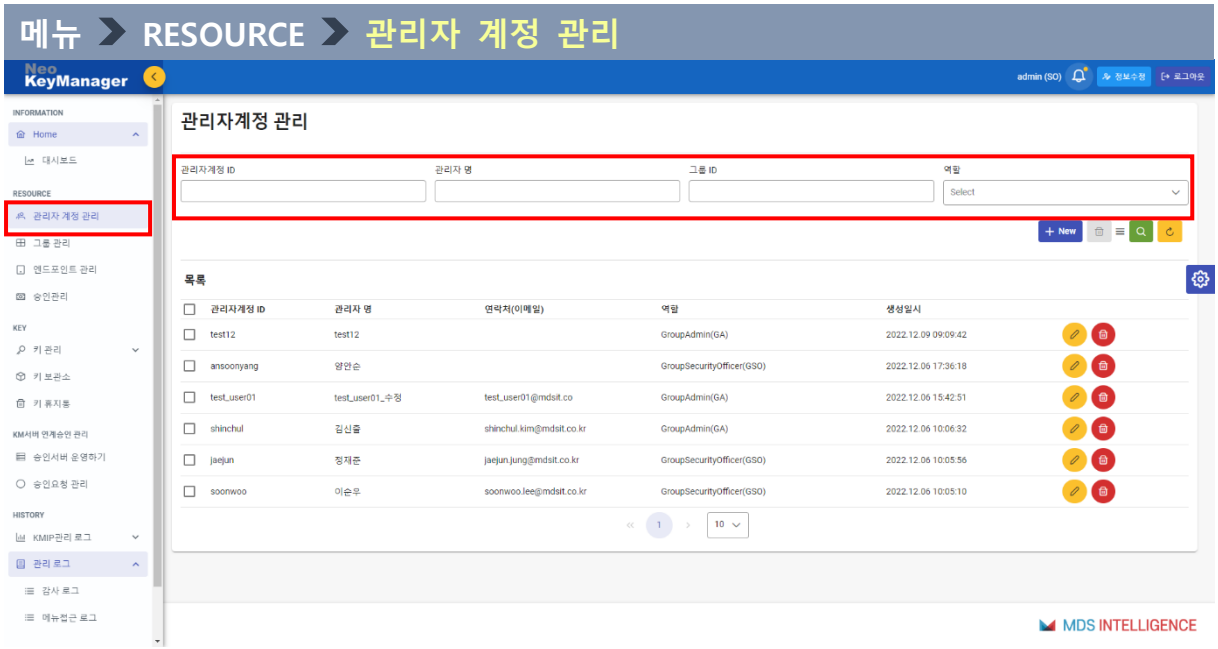


그림 9. 관리자 계정 요약정보

✓ 관리자 계정 ID, 관리자 명, 그룹 ID, 역할 선택 조회 가능 ✓ 관리자 계정 생성 및 삭제 가능	
관리자 계정 ID	- 조회하고자 하는 관리자 계정 ID 입력
관리자 명	- 조회하고자 관리자 명 입력
그룹 ID	- 조회하고자 그룹 ID 입력
역할	- 조회하고자 하는 역할 선택

(1) 관리자 계정 생성

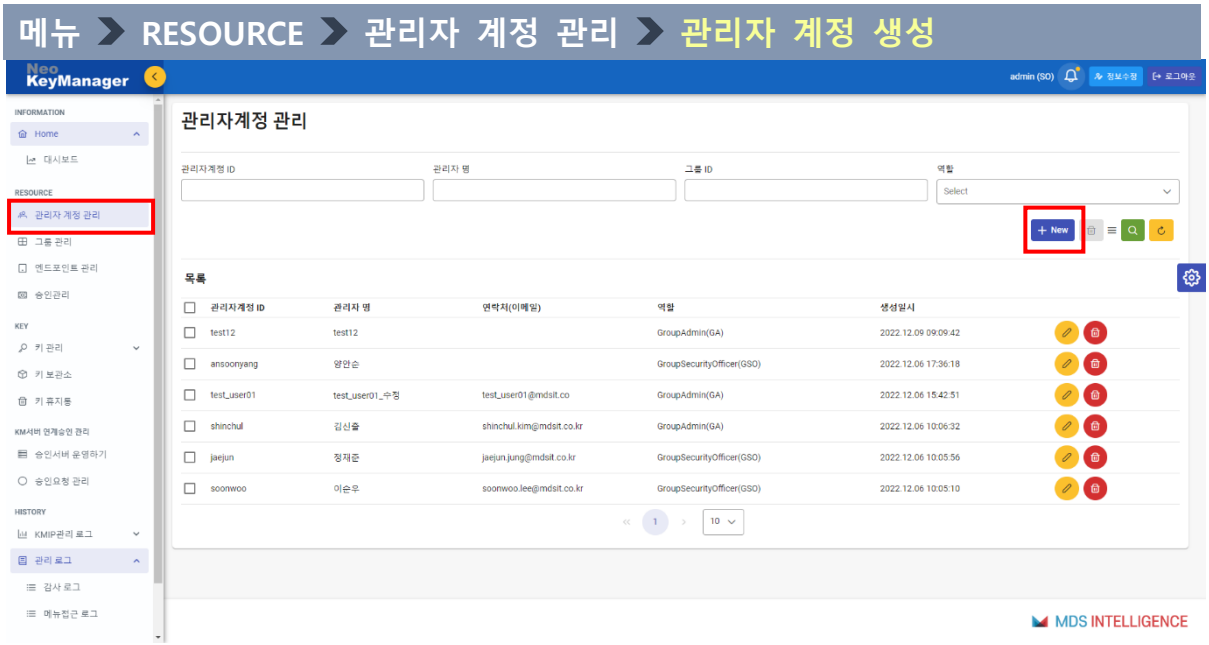


그림 10. 관리자 계정 생성

- ✓ 그룹 별 관리자에 대한 관리 기능 제공
- ✓ GSO, GA, AU 생성 및 허용 IP 설정 가능
- ✓ OTP 기능 제공

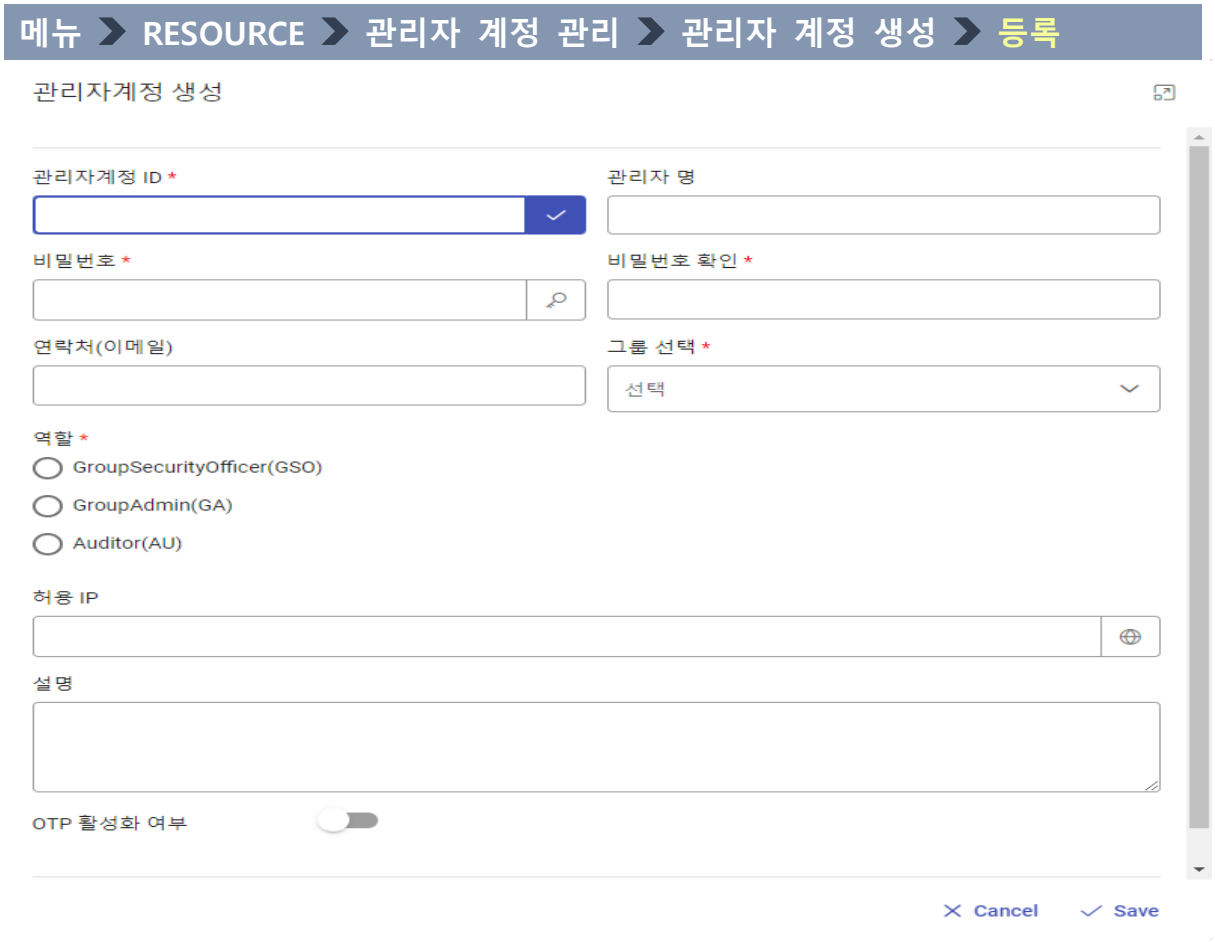


그림 11. 관리자 계정 생성 및 권한 부여

✓ 각 항목 별 입력 후 저장 (* : 필수 입력 항목)
✓ OPT 활성화 여부 가능 (GSO 관리자는 OTP가 자동으로 활성화됨.)

관리자 계정 ID	- 관리자 계정 ID 입력 및 중복 확인 기능
관리자명	- 관리자 이름 입력
비밀번호	- 로그인 시 사용할 비밀번호 입력
비밀번호 확인	- 입력한 비밀번호 재입력
연락처(이메일)	- 연락처(이메일) 입력
그룹 선택	- 그룹 검색 및 선택
역할	- GSO, GA, AU 중 역할 선택
허용 IP	- 해당 계정의 접속 허용 IP 제한 시 사용 (허용 IP 입력)
설명	- 해당 계정에 대한 부가 설명 입력
OTP 활성화 여부	- OTP 활성화를 통해 Two Factor 인증 지원

(2) 관리자 계정 수정/삭제

그림 12. 관리자 계정 수정 및 삭제

✓ 관리자 계정 수정 및 삭제 기능

① 관리자 계정 수정

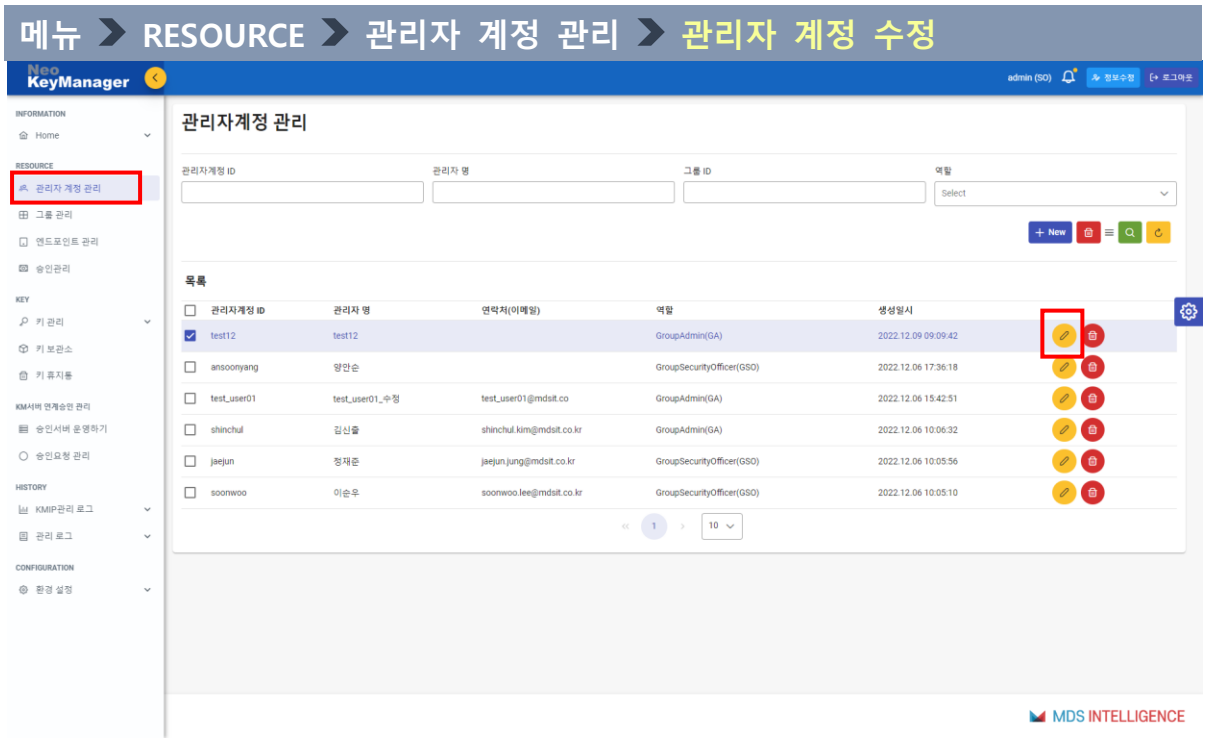


그림 13. 관리자 계정 수정 클릭 화면

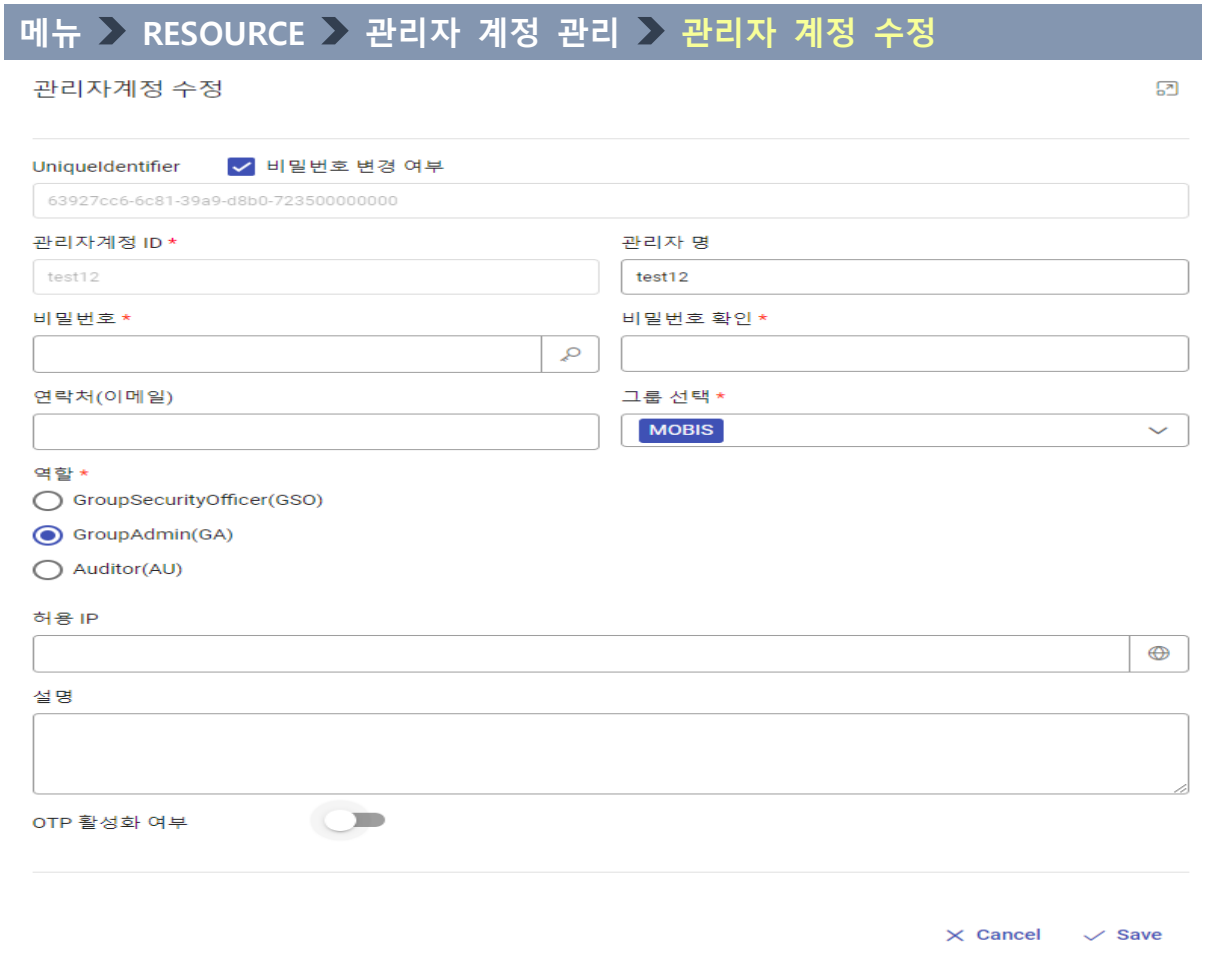


그림 14. 관리자 계정 수정 화면

✓ 관리자 계정 수정, 관리자계정 ID, 관리자 명, 비밀번호, 역할 등 수정 정보 입력	
관리자명	- 관리자 이름 수정
비밀번호	- 비밀번호 변경 여부 체크 시 변경할 비밀번호 입력
비밀번호 확인	- 입력한 비밀번호 재입력
연락처(이메일)	- 연락처(이메일) 입력 수정
그룹 선택	- 그룹 변경 시 변경하고자 하는 그룹 선택
역할	- 그룹관리와 로그관리 담당 권한 역할 선택 기능
허용 IP	- 허용 가능한 IP 추가 또는 변경
설명	- 해당 계정에 대한 부가 설명 추가 또는 변경
OTP 활성화 여부	- OTP 활성화 여부 기능 변경

② 관리자 계정 삭제

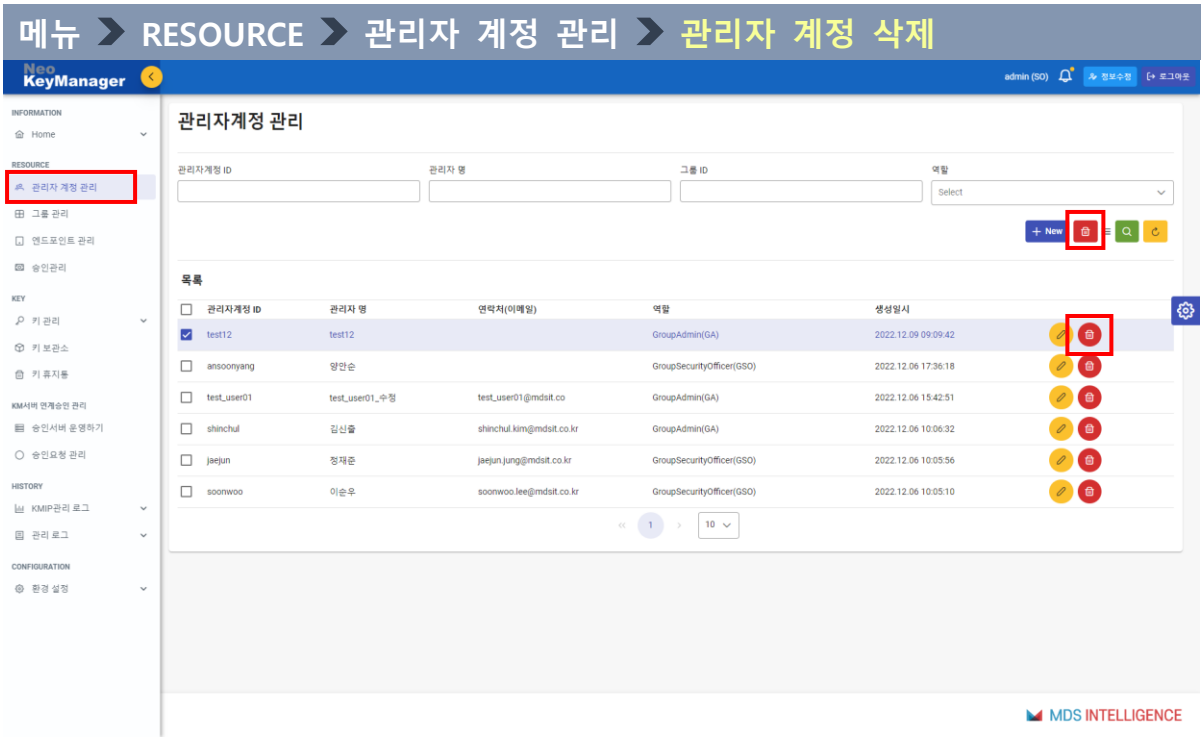


그림 15. 관리자 계정 삭제 화면

✓ 관리자 계정 선택 후 삭제

2) 그룹 관리

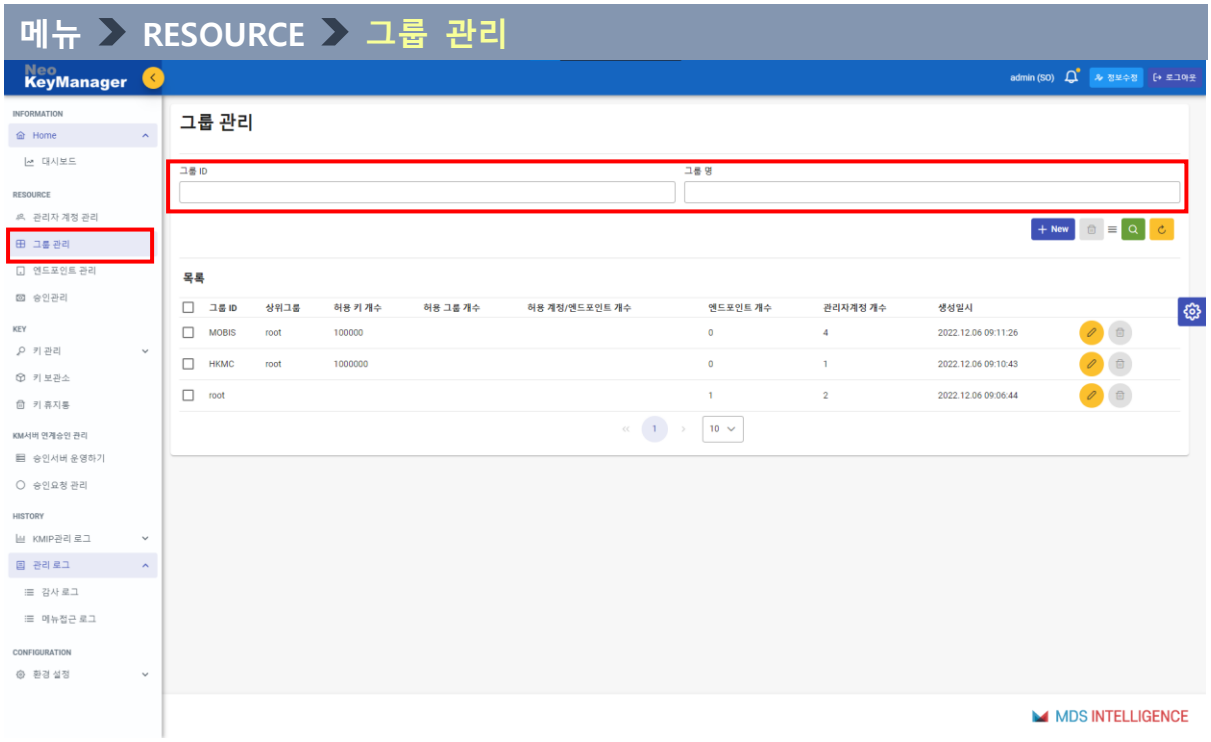


그림 16. 그룹 관리 정보 목록

✓ 같은 암호키를 공유 및 사용하는 엔드포인트(NKM과 연동되는 보안 솔루션)의 그룹 ✓ 그룹 ID 조회 및 이름 검색 ✓ 그룹 생성 및 삭제 가능	
그룹 ID	- 조회하고자 하는 그룹 ID 입력
그룹 명	- 조회하고자 그룹 명 입력

(1) 그룹 생성

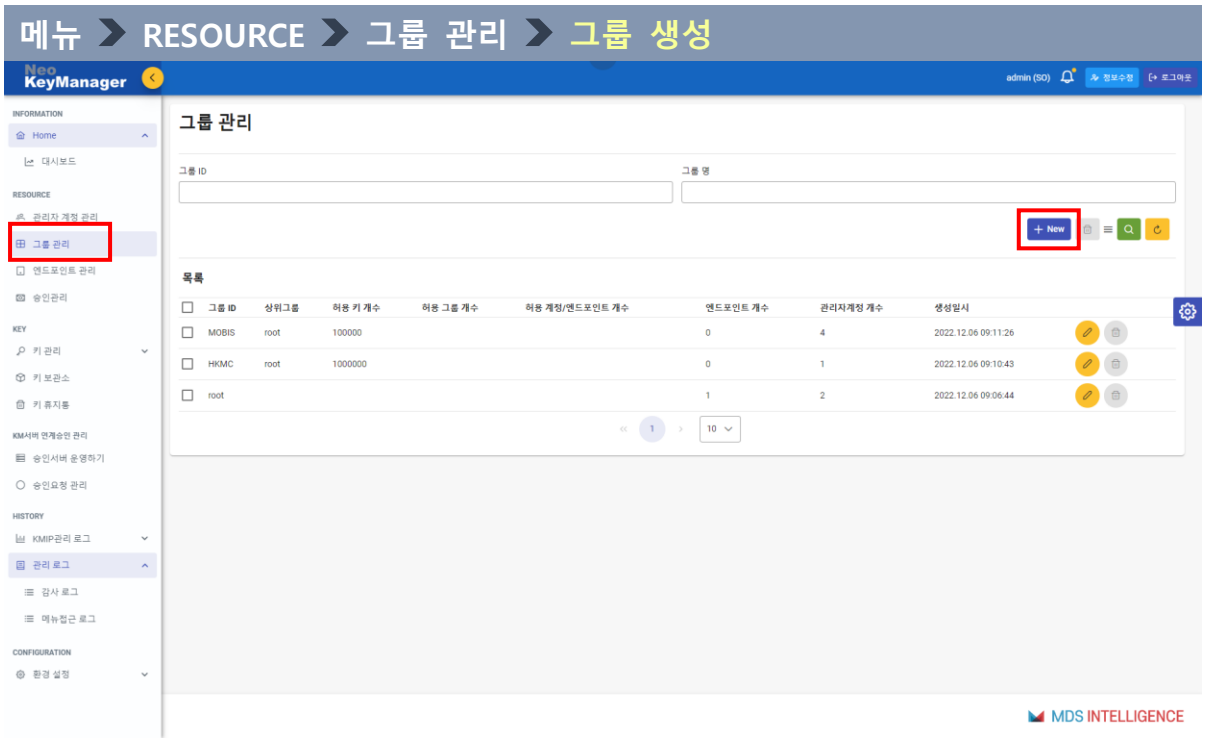


그림 17. 그룹 생성

✓ 위 그림과 같이 [+New] 버튼 클릭 시 그룹 생성 화면으로 이동

그림 18. 그룹 생성 화면

✓ 그룹 생성, ID, 이름, 허용 키 개수, 상위 그룹 등 생성 정보 입력	
그룹 ID	- 그룹 ID 입력 및 중복 확인
그룹 명	- 그룹 명 입력
허용 키 개수	- 그룹 당 허용 키 개수 입력
허용 계정/ 엔드포인트 개수	- 허용 계정 및 엔드포인트 개수 입력
허용 그룹 개수	- 허용 그룹 개수 입력
상위 그룹	- 상위 그룹 선택
설명	- 해당 그룹에 대한 부가 설명 입력

(2) 그룹 수정

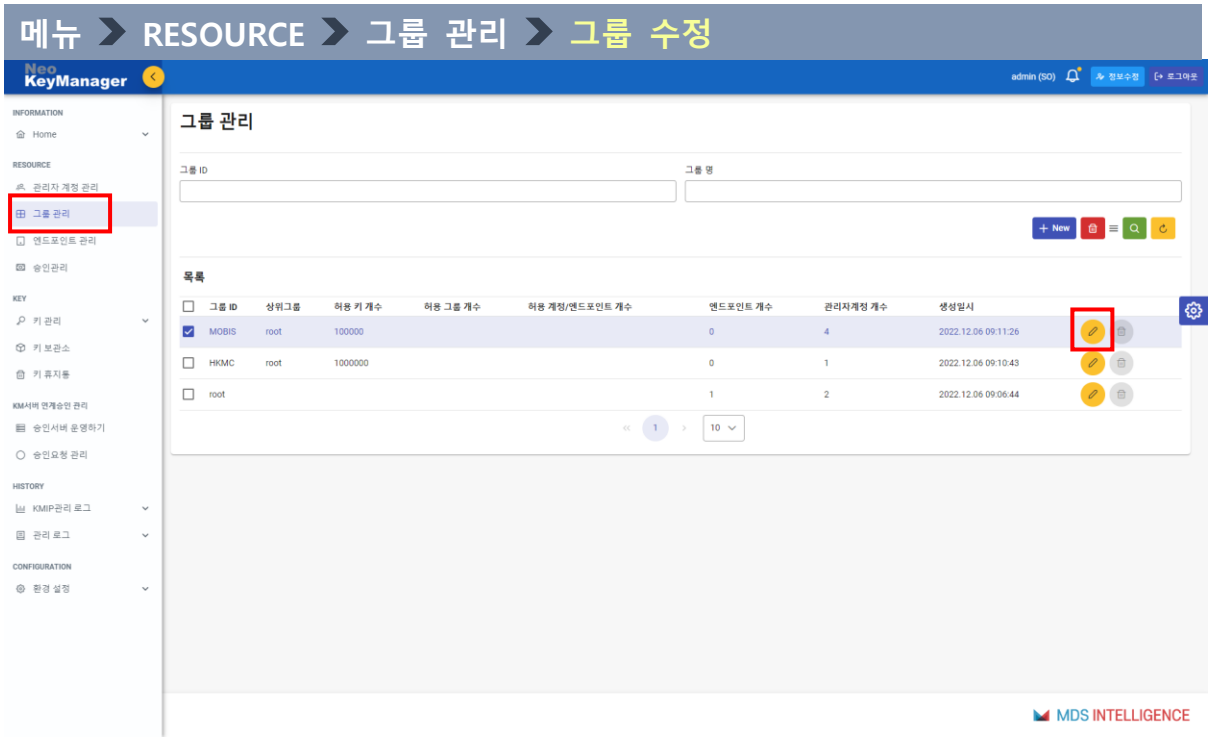


그림 19. 그룹 수정

✓ 위 그림과 같이 수정 버튼 클릭 시 그룹 수정 화면으로 이동

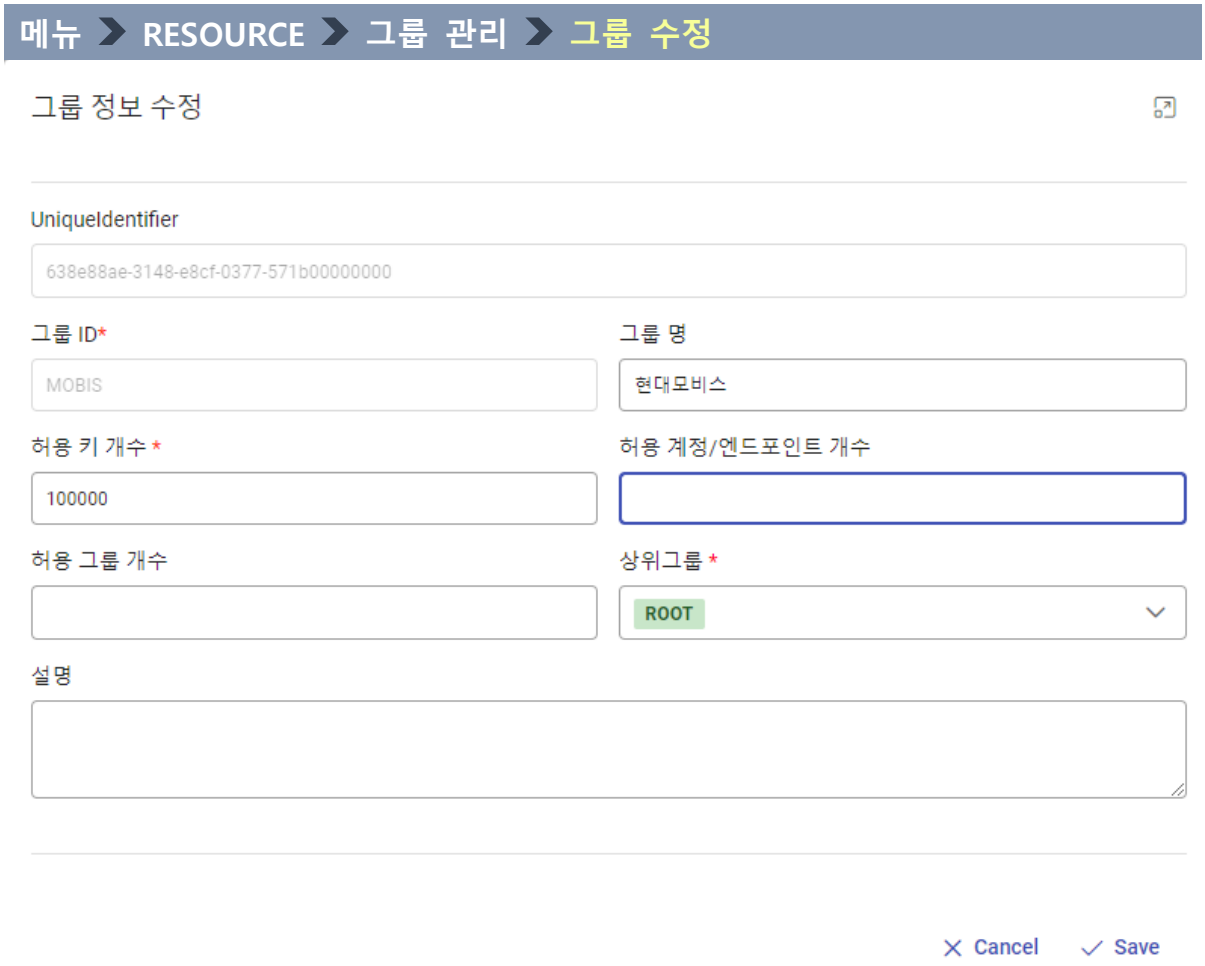


그림 20. 그룹 수정 화면

✓ 그룹 수정, 그룹 명, 허용 키 개수, 상위 그룹 등 수정 정보 입력	
그룹 명	- 그룹 이름 수정
허용 키 개수	- 허용 키 개수 수정
허용 계정/ 엔드포인트 개수	- 허용 계정 및 엔드포인트 개수 수정
허용 그룹 개수	- 허용 그룹 개수 수정
상위그룹	- 변경하고자 하는 상위그룹 선택
설명	- 해당 그룹에 대한 부가 설명 추가 또는 변경

(3) 그룹 삭제

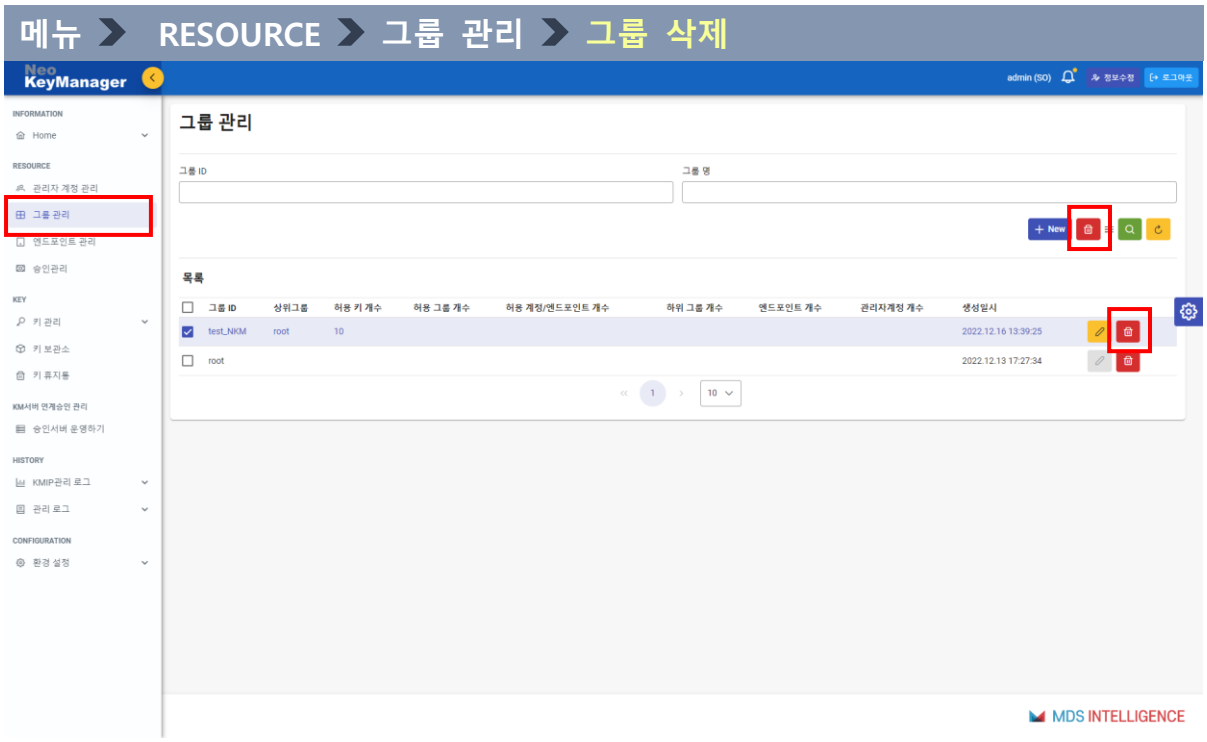


그림 21. 그룹 삭제 화면

- ✓ 위 그림과 같이 삭제 버튼 클릭 시 삭제
- ✓ 그룹에 할당된 사용자 또는 엔드포인트가 존재할 경우 삭제 불가

3) 엔드포인트 관리

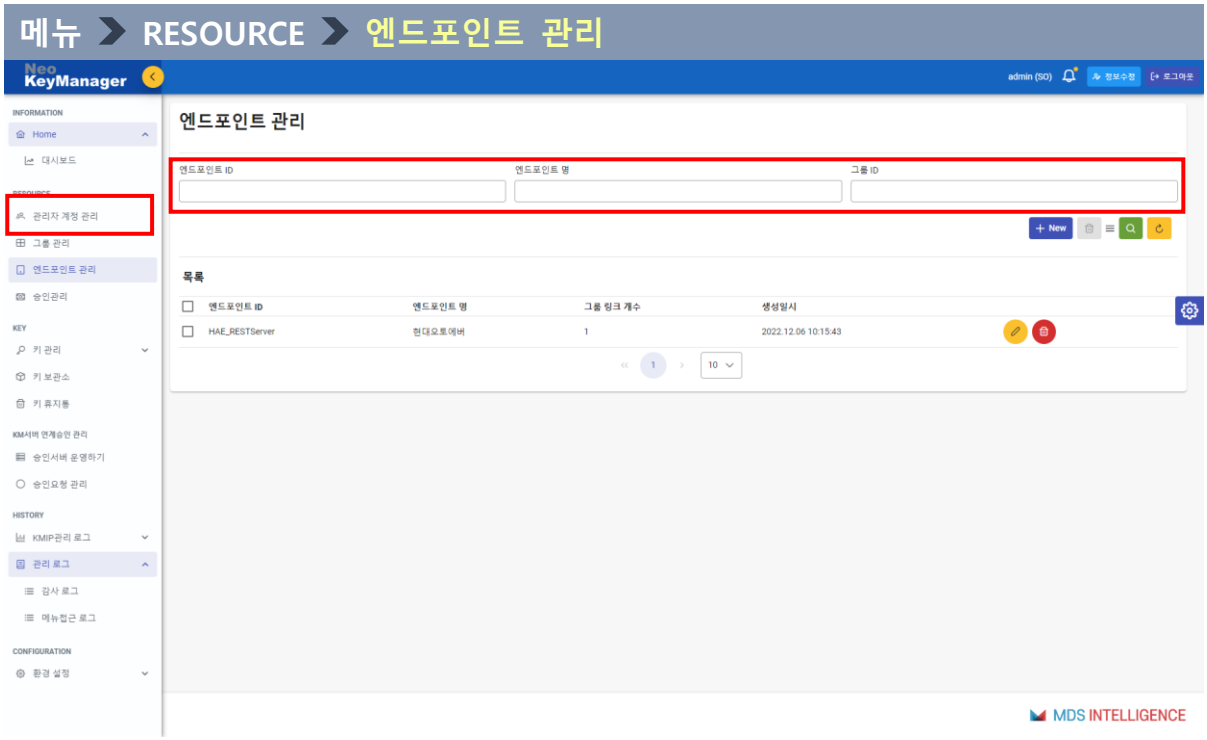


그림 22. 엔드포인트 관리 화면

✓ [엔드포인트] 탭에서는 NKM과 연동되는 업무 시스템(엔드포인트)의 관리 기능 제공 ✓ 시스템에 등록되어 있는 엔드포인트 목록을 나타내며 해당 정보를 조회하고 신규 엔드포인트를 등록할 수 있음	
엔드포인트 ID	- 조회하고자 하는 엔드포인트 ID 입력
엔드포인트 명	- 조회하고자 하는 엔드포인트 명 입력
그룹 ID	- 조회하고자 하는 그룹 ID 입력 기능

(1) 엔드포인트 생성

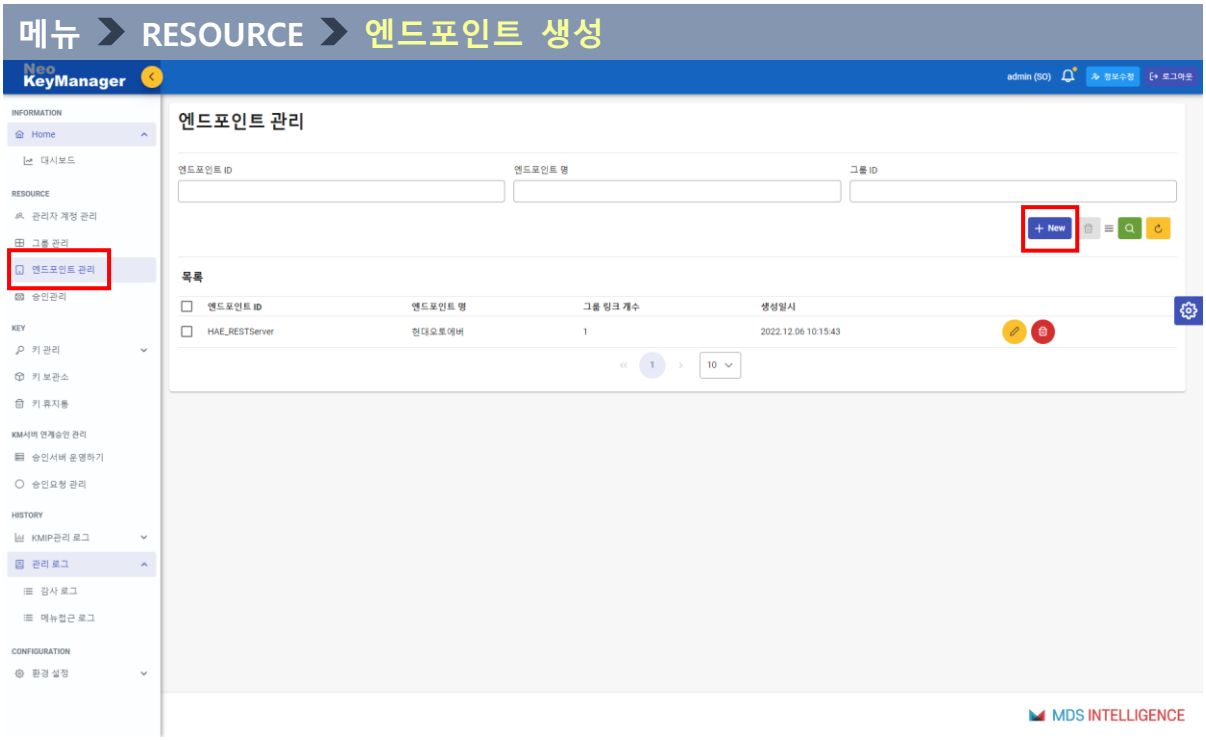


그림 23. 엔드포인트 생성 화면

✓ 위 그림과 같이 [+ New] 버튼 클릭 시 엔드포인트 생성 화면으로 이동

그림 24. 엔드포인트 생성 화면

✓ 엔드포인트 ID, 엔드포인트 명, 그룹 선택, 허용 IP, Credential 설정 등 정보 입력	
엔드포인트 ID	- 엔드포인트 ID 입력
엔드포인트 명	- 엔드포인트 명 입력
그룹 선택	- 해당 엔드포인트가 속할 그룹 선택
허용 IP	- 해당 엔드포인트의 접속 허용 IP 제한 시 사용 (허용 IP 입력)
Credential 설정	- Credential 유형 선택 (Password와 Certificate 중 선택) - Certificate를 선택한 경우, 인증서 파일 업로드 - Credential 세부 유형 설정 (OTP와 Device 중 선택)
설명	- 해당 엔드포인트에 대한 부가 설명 입력

(2) 엔드포인트 수정

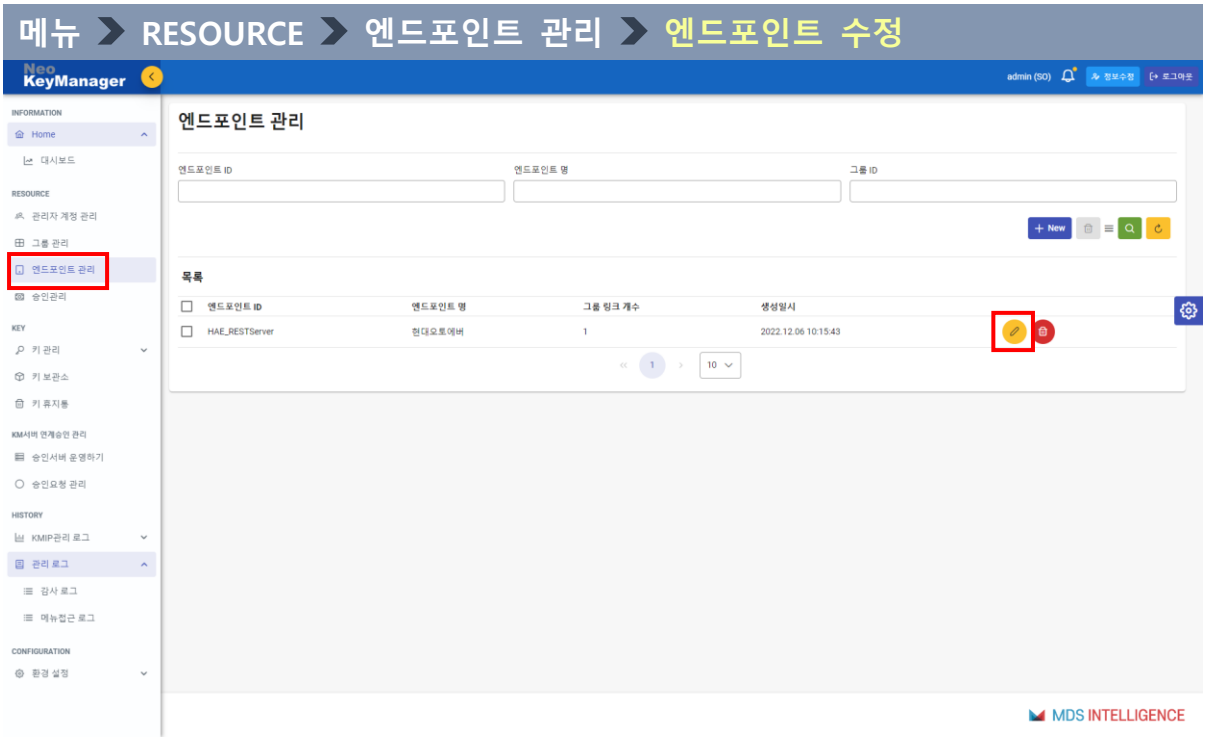


그림 25. 엔드포인트 수정 화면

✓ 위 그림과 같이 수정 버튼 클릭 시 수정 화면으로 이동

그림 26. 엔드포인트 수정 화면

✓ 엔드포인트 명, 그룹 선택, 허용 IP, Credential 설정 등 수정할 정보 입력	
엔드포인트 명	- 엔드포인트 명 수정
그룹 선택	- 변경하고자 하는 그룹 선택
허용 IP	- 허용 IP 추가 및 변경
Credential변경 여부	- Credential변경 여부 체크 시 credential 유형 변경 가능
설명	- 부가 설명 추가 및 변경

(3) 엔드포인트 삭제

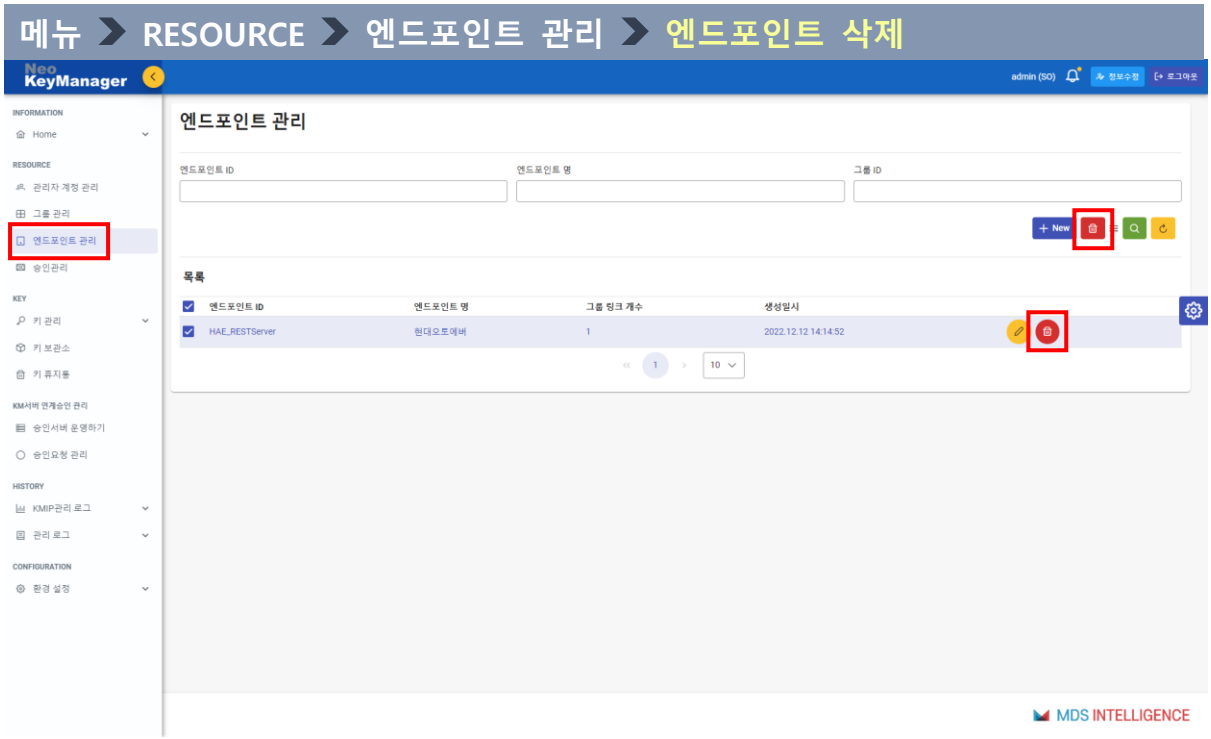


그림 27. 엔드포인트 삭제 화면

✓ 위 그림과 같이 삭제 버튼 클릭 시 엔드포인트 삭제

4) 승인 관리

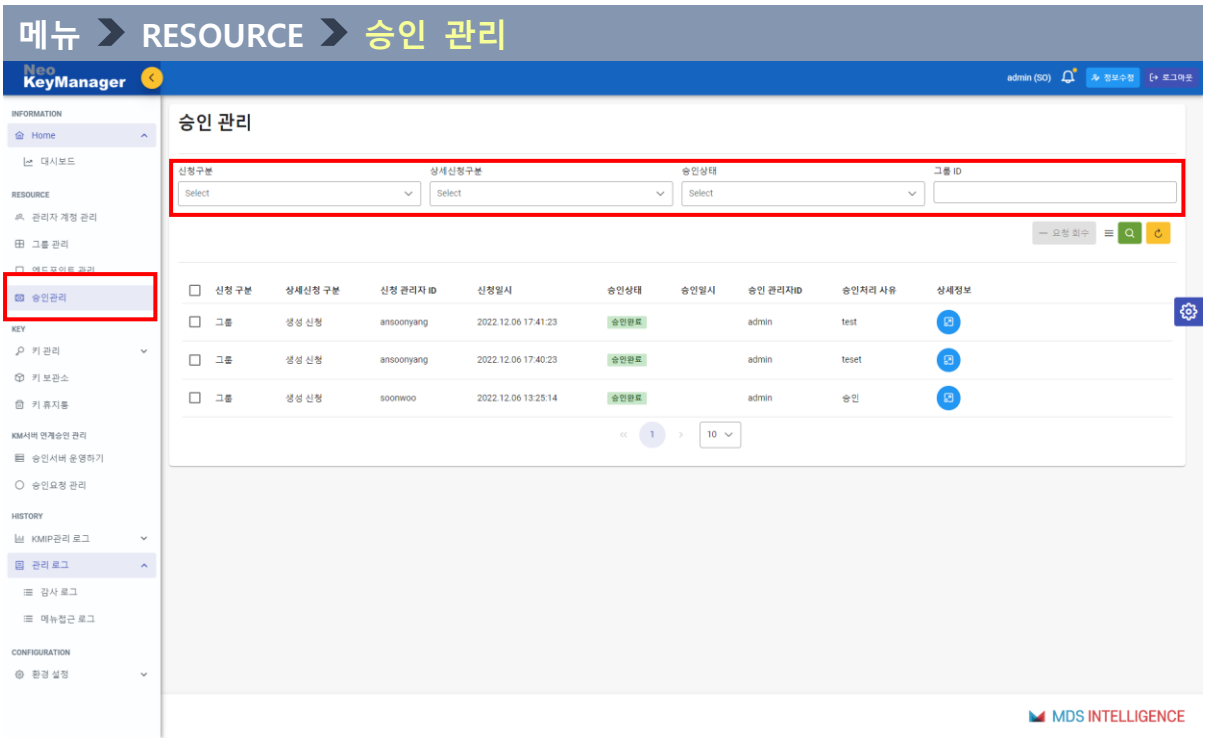


그림 28. 승인 관리 화면

✓ OEM KMS를 통한 내부 승인 처리 시 사용	
신청구분	- 조회하고자 하는 신청구분 선택 - 엔드 포인트, 그룹, 관리자 계정 중 선택
상세신청구분	- 조회하고자 하는 승인신청구분 선택 - 생성, 수정, 삭제 중 선택
승인상태	- 조회하고자 하는 승인상태 선택 - 승인 요청중(미승인), 승인완료, 승인 거절, 요청 회수 중 선택
그룹 ID	- 조회하고자 하는 그룹 ID 입력

(1) 상세정보

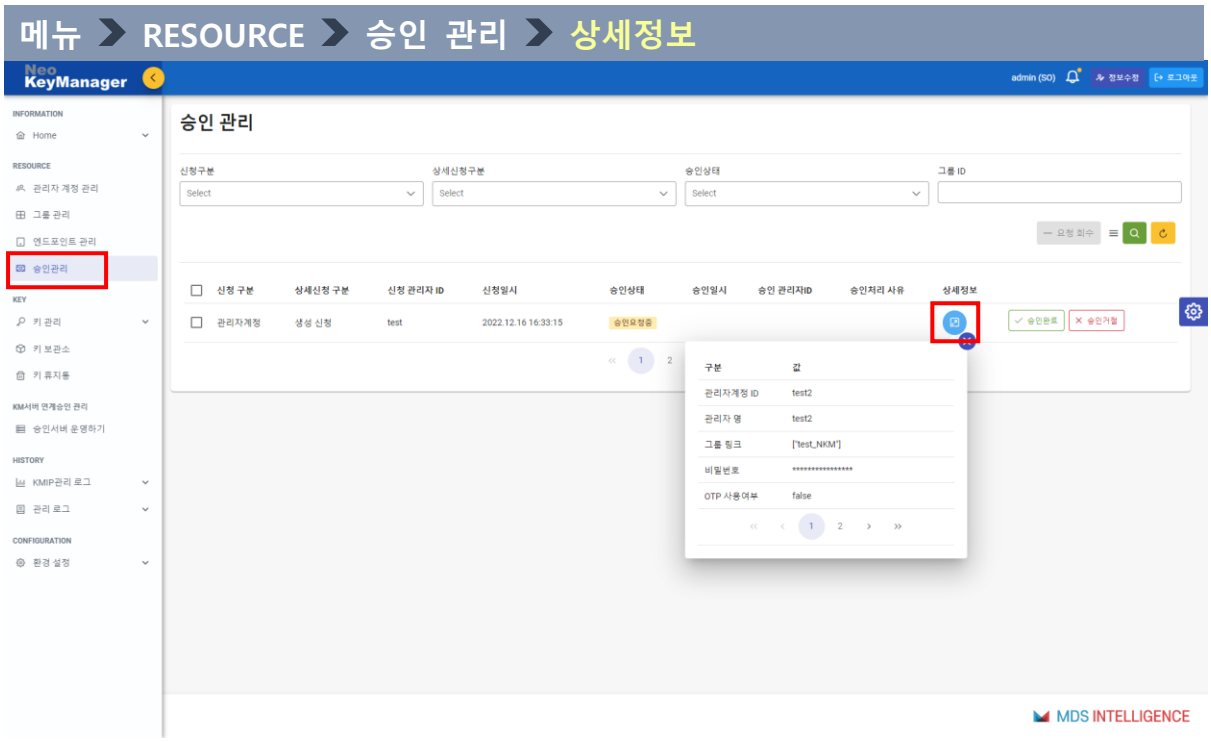


그림 29. 승인 관리 상세정보 화면

- ✓ 위 그림과 같이 [상세정보] 버튼 클릭
- ✓ 관리자계정 ID, 관리자 명, 그룹 링크 등 신청자 정보 확인

(2) 승인 완료/거절

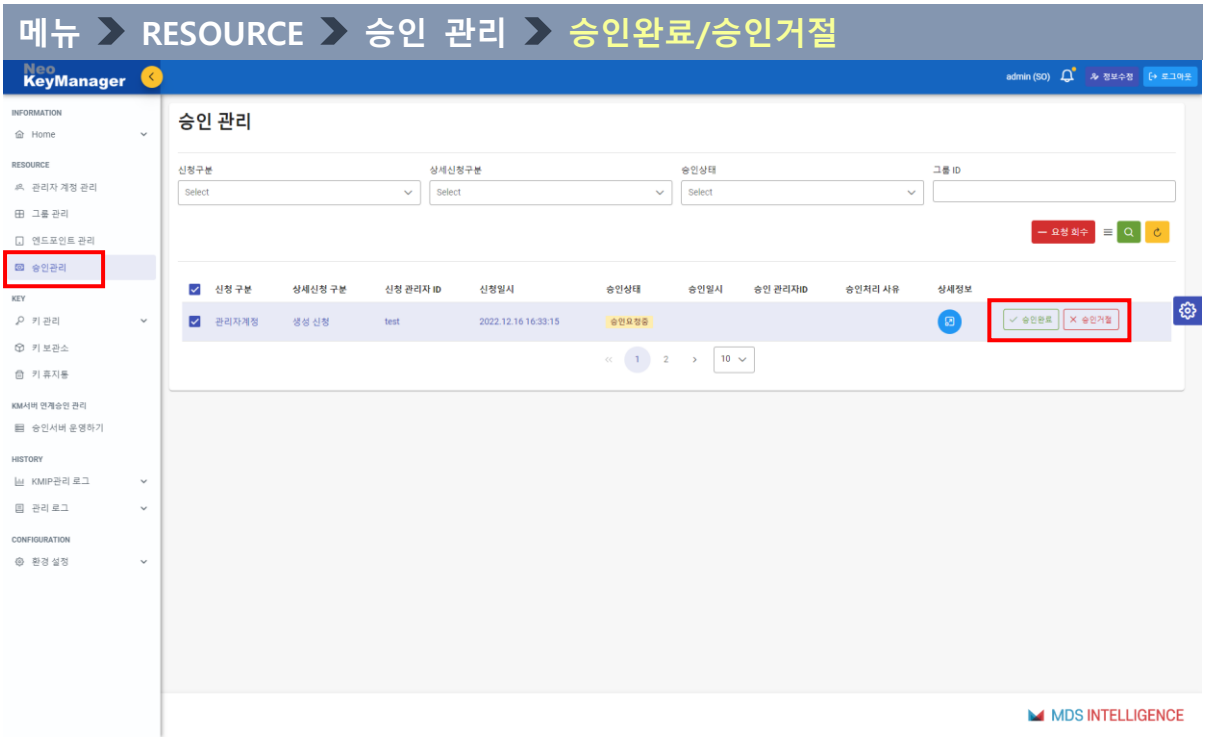


그림 30. 승인완료/승인거절 화면

- ✓ 위 그림과 같이 [승인완료] 또는 [승인거절] 버튼 클릭
- ✓ OEM KMS 내부 승인 요청 건에 대한 승인 완료 또는 승인 거절

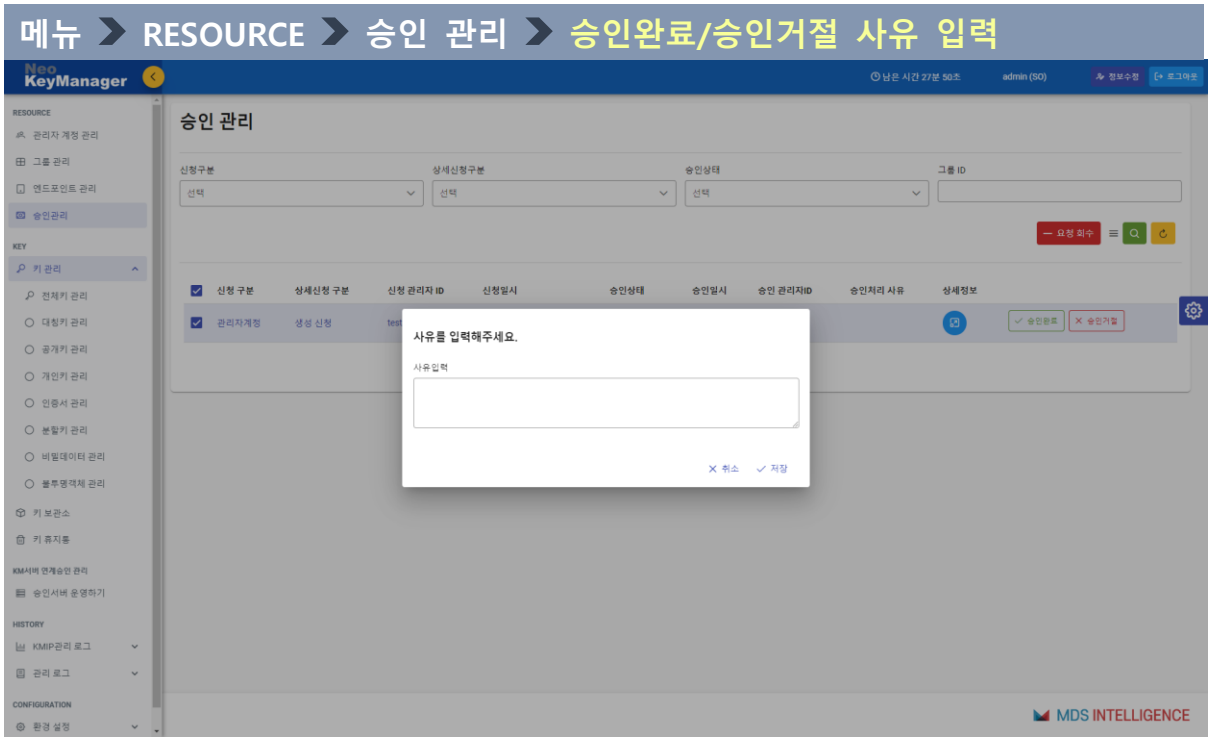


그림 31. 승인완료/승인거절 사유 입력 화면

✓ 승인완료 또는 승인거절 사유를 입력 후 저장

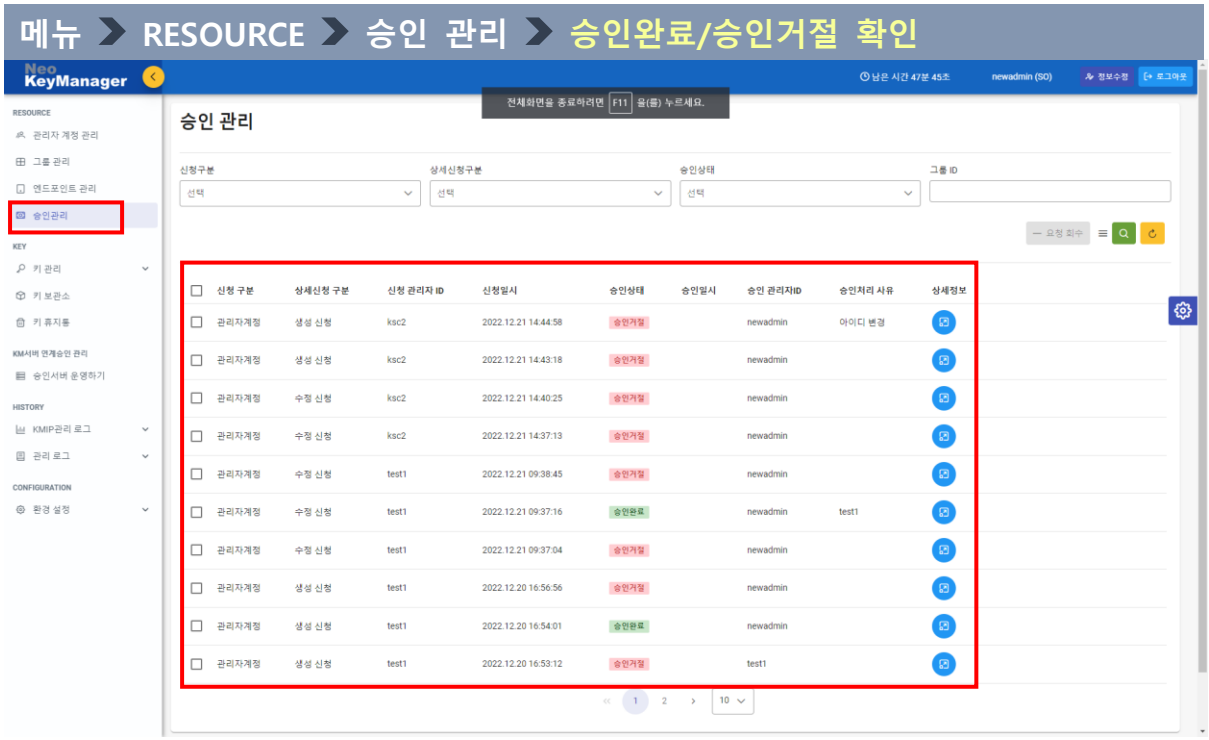


그림 32. 승인 관리 화면에서 승인완료/승인거절 내역 확인

✓ 승인완료 또는 승인거절 후 승인 관리 화면에서 승인 여부 확인 가능

4. KEY

1) 전체키 관리

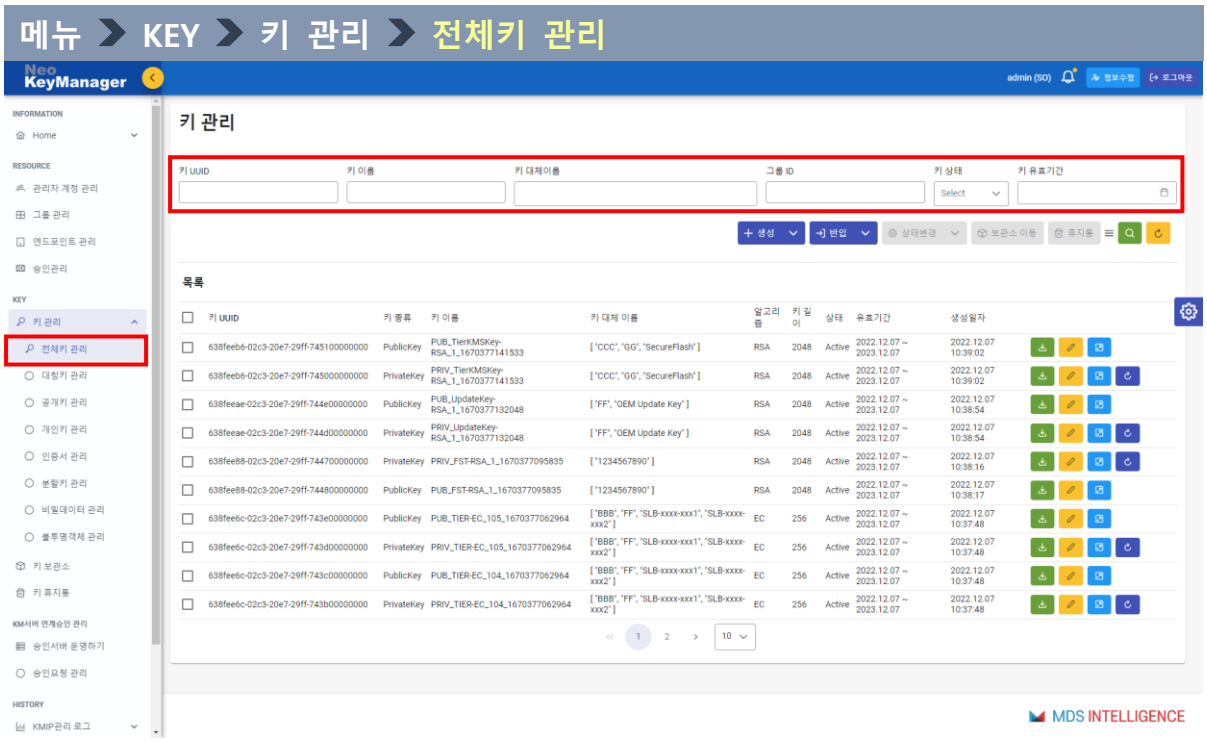


그림 33. 키 관리 목록

✓ [전체키 관리] 탭에서 키 UUID, 키 이름, 키 대체이름, 그룹 ID, 키 상태 등으로 키 조회	
키 UUID	- 조회하고자 하는 키 UUID 입력
키 이름	- 조회하고자 하는 키 이름 입력
키 대체 이름	- 조회하고자 하는 키 대체 이름 입력
그룹 ID	- 조회하고자 하는 그룹 ID 입력
키 상태	- 조회하고자 하는 키 상태 선택 - PreActive, Active, Deactivated 중 선택
키 유효기간	- 조회하고자 하는 키 유효기간 설정

(1) 키 생성

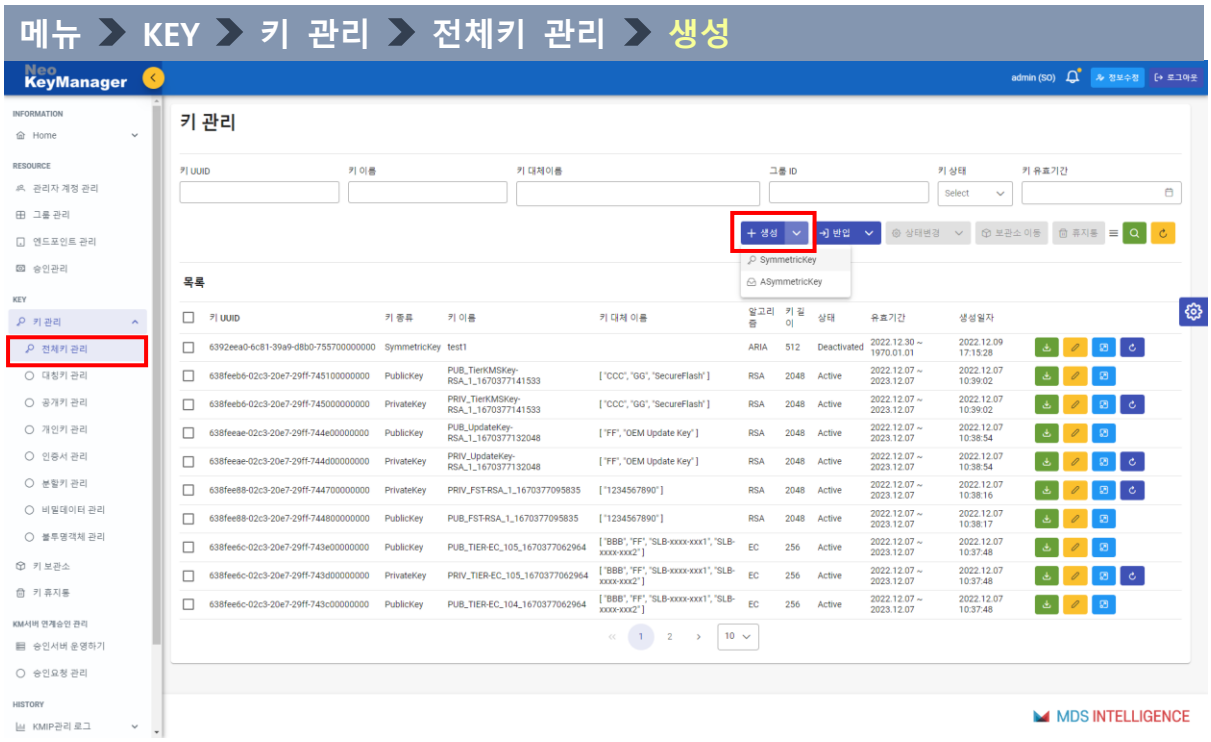


그림 34. 키 생성

- ✓ 암호키 생성 기능
- ✓ 위 그림과 같이 [생성 v] 버튼 클릭 시 대칭, 비대칭 키 선택 후 생성 화면으로 이동

메뉴 > KEY > 키 관리 > 전체키 관리 > 생성(SymmetricKey)

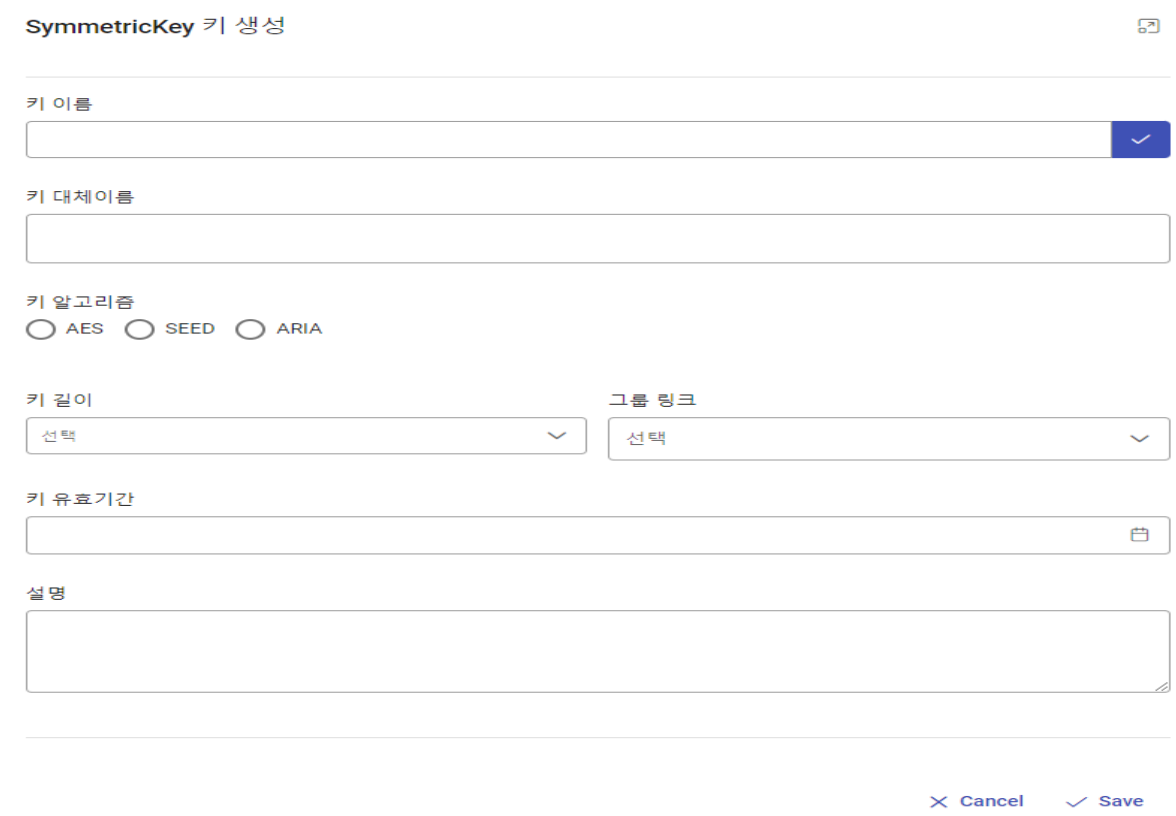


그림 35. 대칭키 생성 화면

✓ 각 항목 별 입력 후 저장	
키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능
키 알고리즘	- 대칭키 : AES[1], ARIA[2], SEED[3] 중 선택
키 길이	- 128, 192, 256, 512 중 선택
그룹 링크	- 생성되는 키를 사용하는 그룹 선택
키 유효기간	- 암호키의 유효기간 선택
설명	- 해당 대칭키에 대한 부가 설명 입력

[1] **AES(Advanced Encryption Standard) :** 미국 표준 기술 연구소(NIST)에 의해 제정된 대칭키 암호화 방식

[2] **ARIA(Academy, Research Institute, Agency) :** 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 국산 범용 블록 암호 알고리즘

[3] **SEED :** 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 02월 한국인터넷진흥원과 국내 암호 전문가들이 국내 기술로 개발한 128비트 블록 암호 알고리즘

그림 36. 비대칭키 생성 화면

✓ 각 항목 별 입력 후 저장	
개인키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
공개키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능

키 알고리즘	- 비대칭키 : RSA[4], EC[5], 중 선택
키 길이	- RSA: 1024, 2048, 3072, 4096 중 선택 - EC: P_224, P_256, P_384, P_521, SECP256K1 중 선택
그룹 링크	- 생성되는 키를 사용하는 그룹 선택
키 유효기간	- 암호키의 유효기간 선택
설명	- 해당 대칭키에 대한 부가 설명 입력

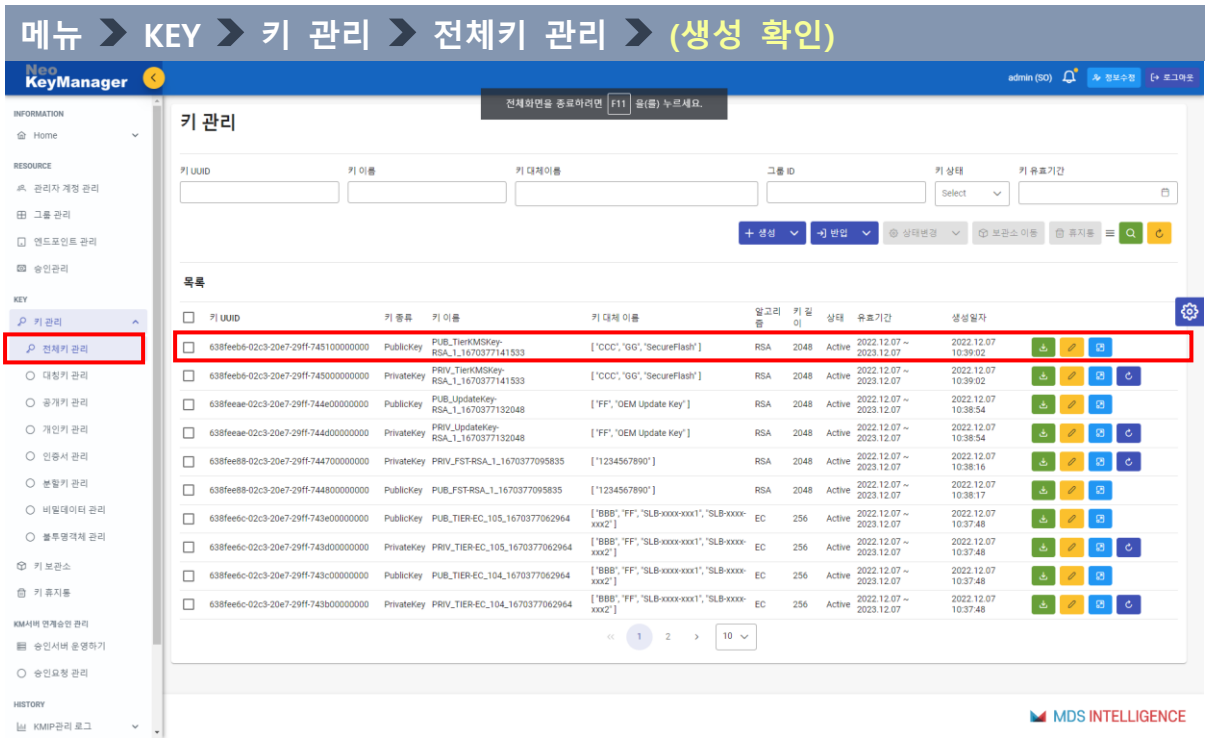


그림 37. 키 생성 확인

✓ 키 생성 확인
✓ 생성된 키에 대한 상세정보 확인 가능

[4] **RSA(Ron Rivest, Adi Shamir and Leonard Adleman) :** 공개키 암호 시스템의 하나로써 암호화 뿐만 아니라 전자서명이 가능한 최초의 알고리즘

[5] **EC(Elliptic curve):** 타원 곡선 암호화 알고리즘을 이용한 공개키 암호 방식
RSA와 같은 기존 공개키 암호 방식에 비해 짧은 키를 사용하면서도 그와 비슷한 수준의 안정성을 제공하는 장점이 있고, 특히 무선 환경과 같이 전송량과 계산량이 상대적으로 열악한 환경에 적합

(2) 키 반입

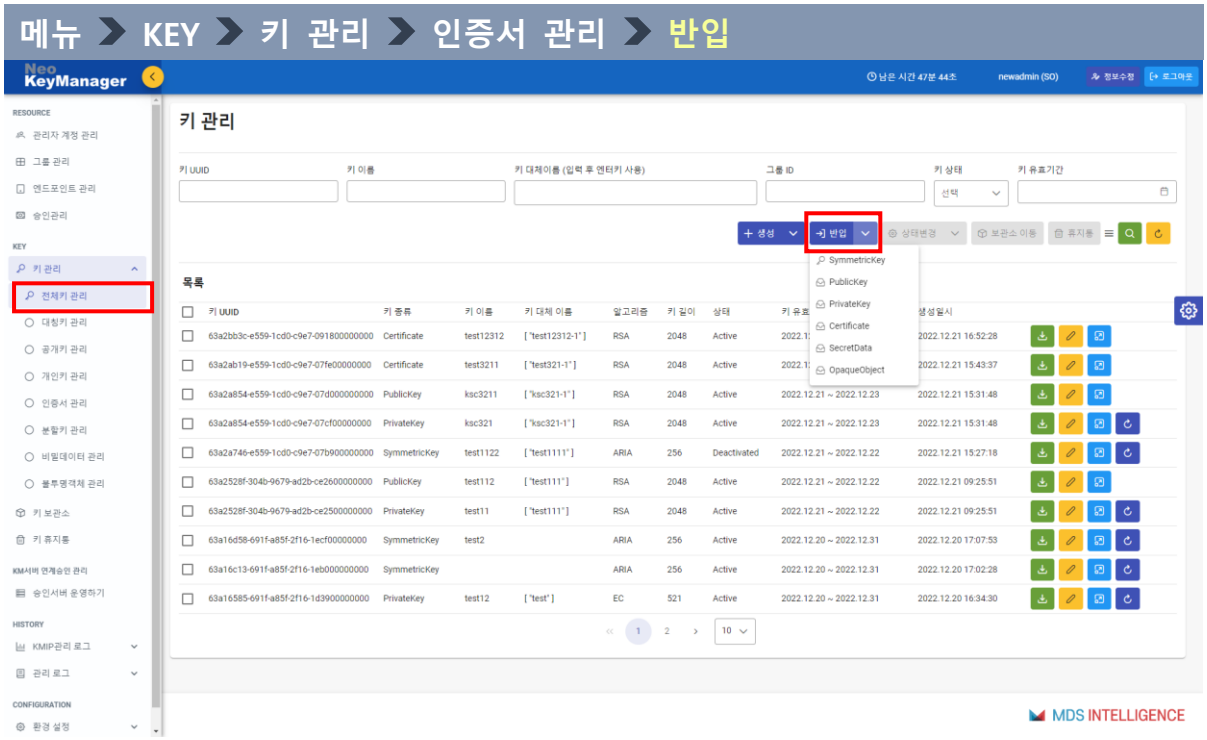


그림 38. 키 반입 화면

- ✓ 기관 간 키 교환 시 외부 키 반입을 위한 기능 제공
- ✓ 대칭키, 비대칭키(개인키, 공개키), 인증서, 비밀 데이터(Password, seed), 불투명객체 반입 가능

① 대칭키(SymmetricKey)

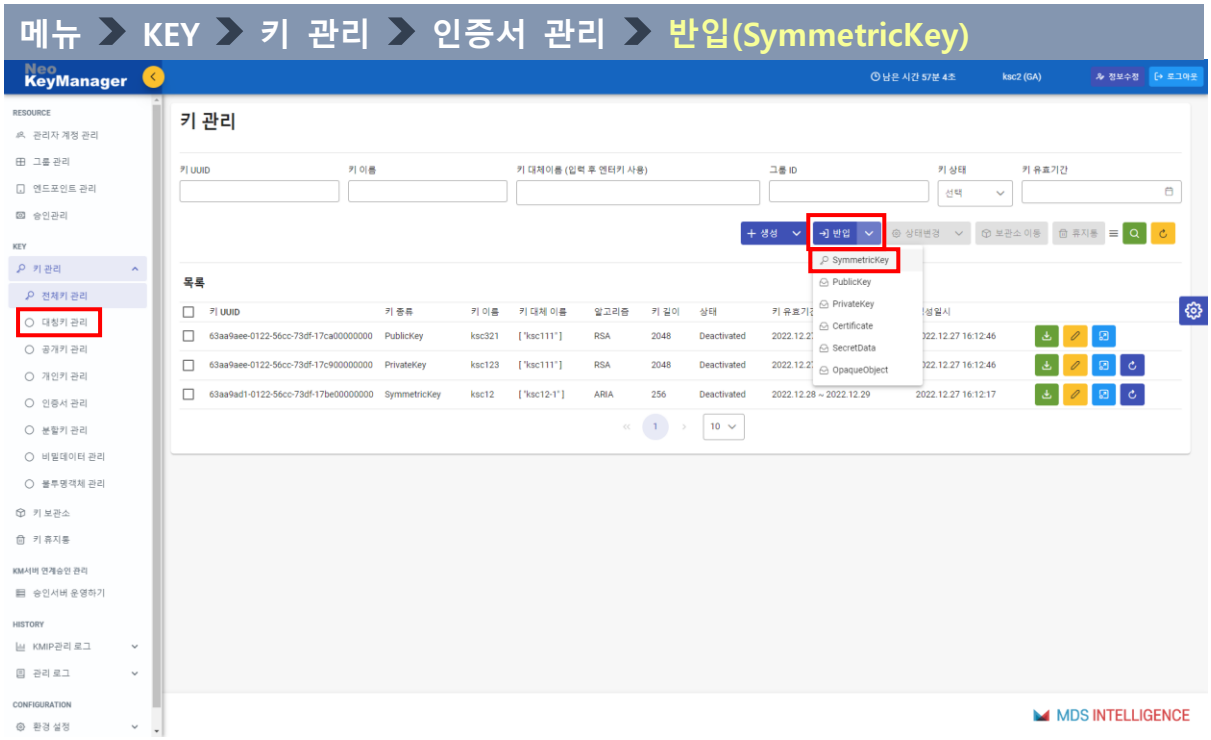


그림 39. 대칭키 반입 선택

- ✓ 대칭키 반입 기능 제공
- ✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 SymmetricKey 선택 후 반입 화면으로 이동

그림 40. 대칭키 반입 화면

✓ 각 항목 정보 입력	
키 이름	- 키 이름 입력
키 대체이름	- 키 대체 이름 입력
그룹 링크	- 반입하고자 하는 대칭키가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
Description	- 반입하고자 하는 대칭키에 대한 부가 설명 입력
키 알고리즘	- AES, SEED, ARIA 선택
키 길이	- 키 길이 선택
키 값(HexString)	- 키 값 입력

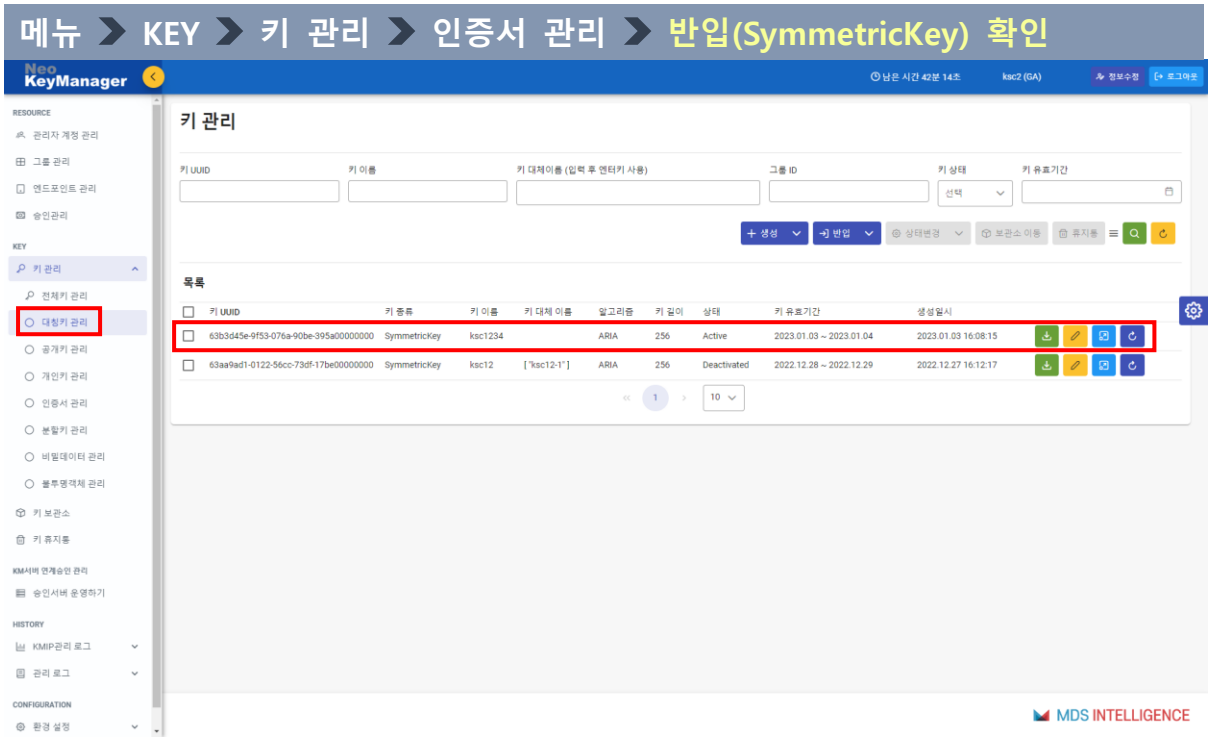


그림 41. 대칭키 반입 확인

✓ 대칭키 반입 확인

② 공개키(PublicKey)

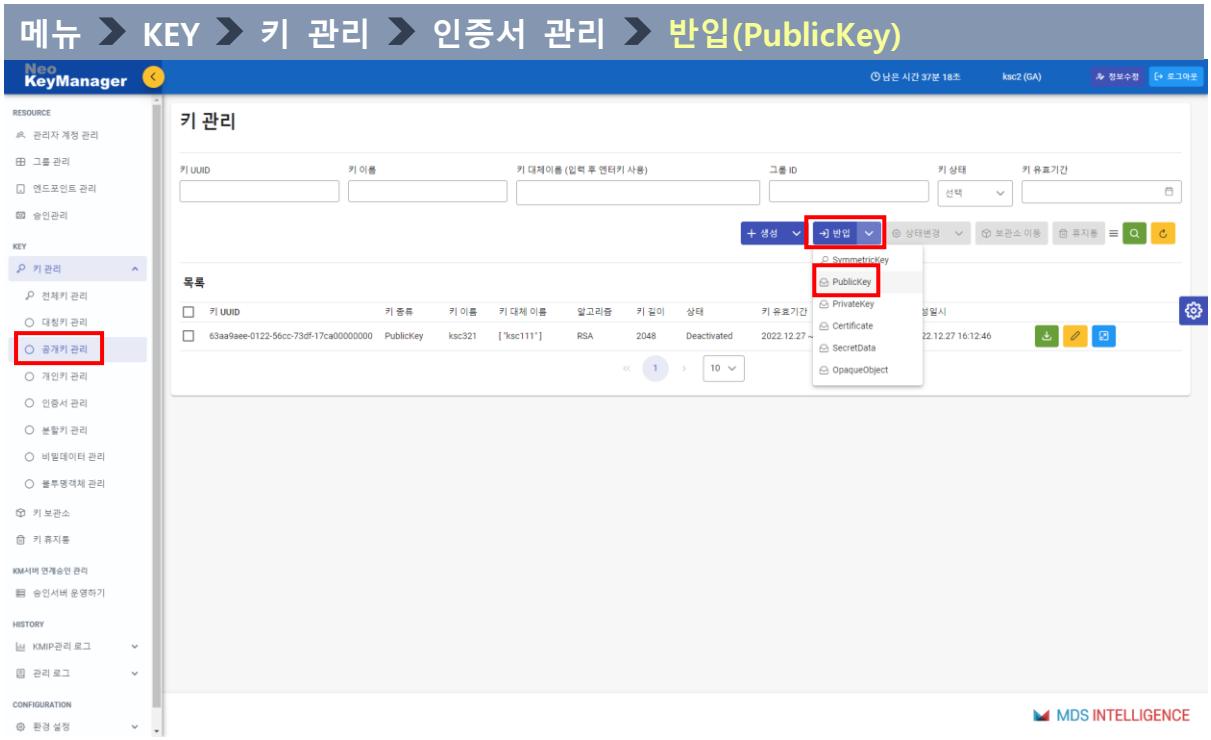


그림 42. 공개키 반입 선택

- ✓ 공개키 반입 기능 제공
- ✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 PublicKey 선택 후 반입 화면으로 이동

그림 43. 공개키 반입 화면

✓ 각 항목 정보 입력	
키 이름	- 키 이름 입력
키 대체이름	- 키 대체 이름 입력
그룹 링크	- 반입하고자 하는 공개키가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
Description	- 반입하고자 하는 공개키에 대한 부가 설명 입력 기능
파일 타입	- DER와 PEM 중 선택
키 파일	- 반입하고자 하는 공개키 파일 선택

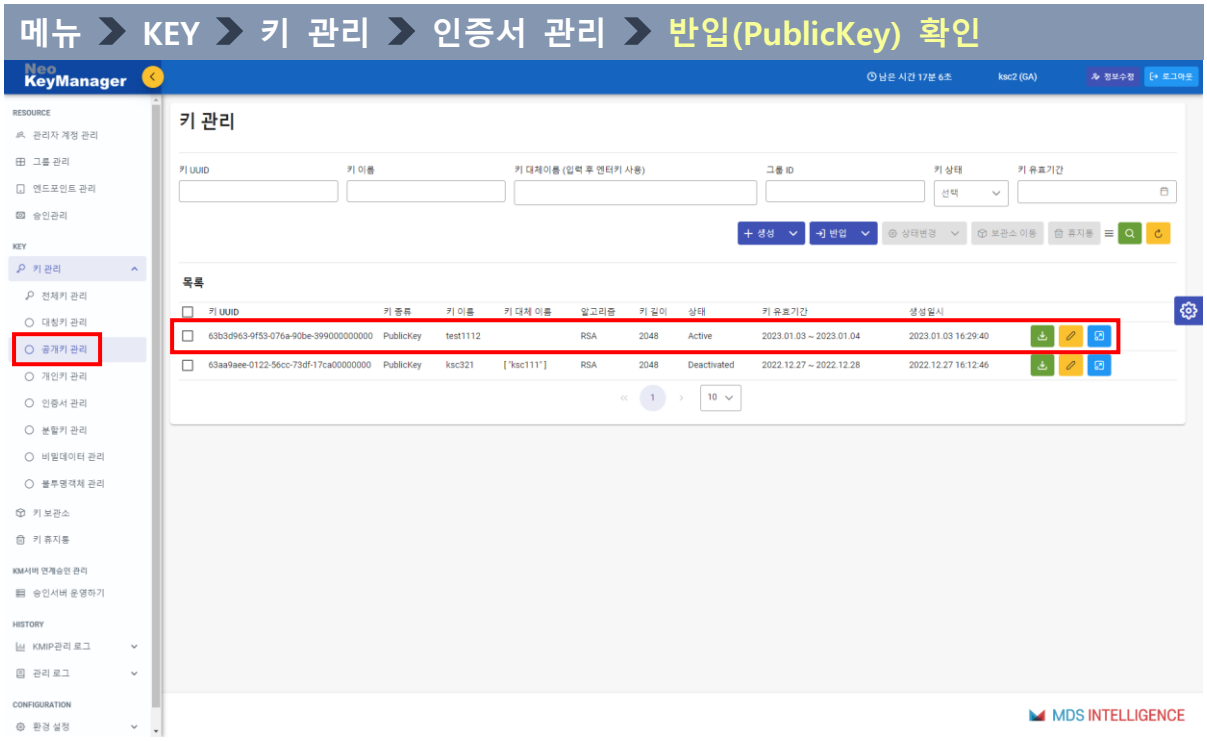


그림 44. 공개키 반입 확인

✓ 공개키 반입 확인

③ 개인키(PrivateKey)

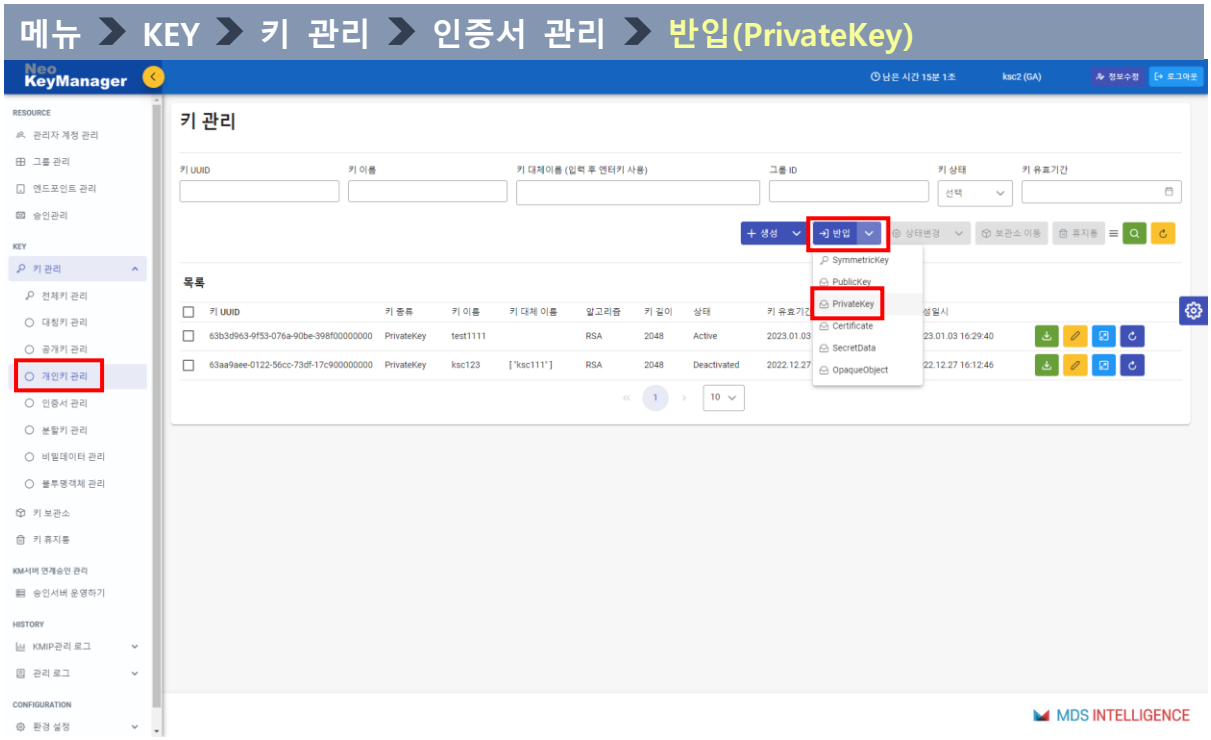


그림 45. 개인키 반입 선택

- ✓ 개인키 반입 기능 제공
- ✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 PrivateKey 선택 후 반입 화면으로 이동

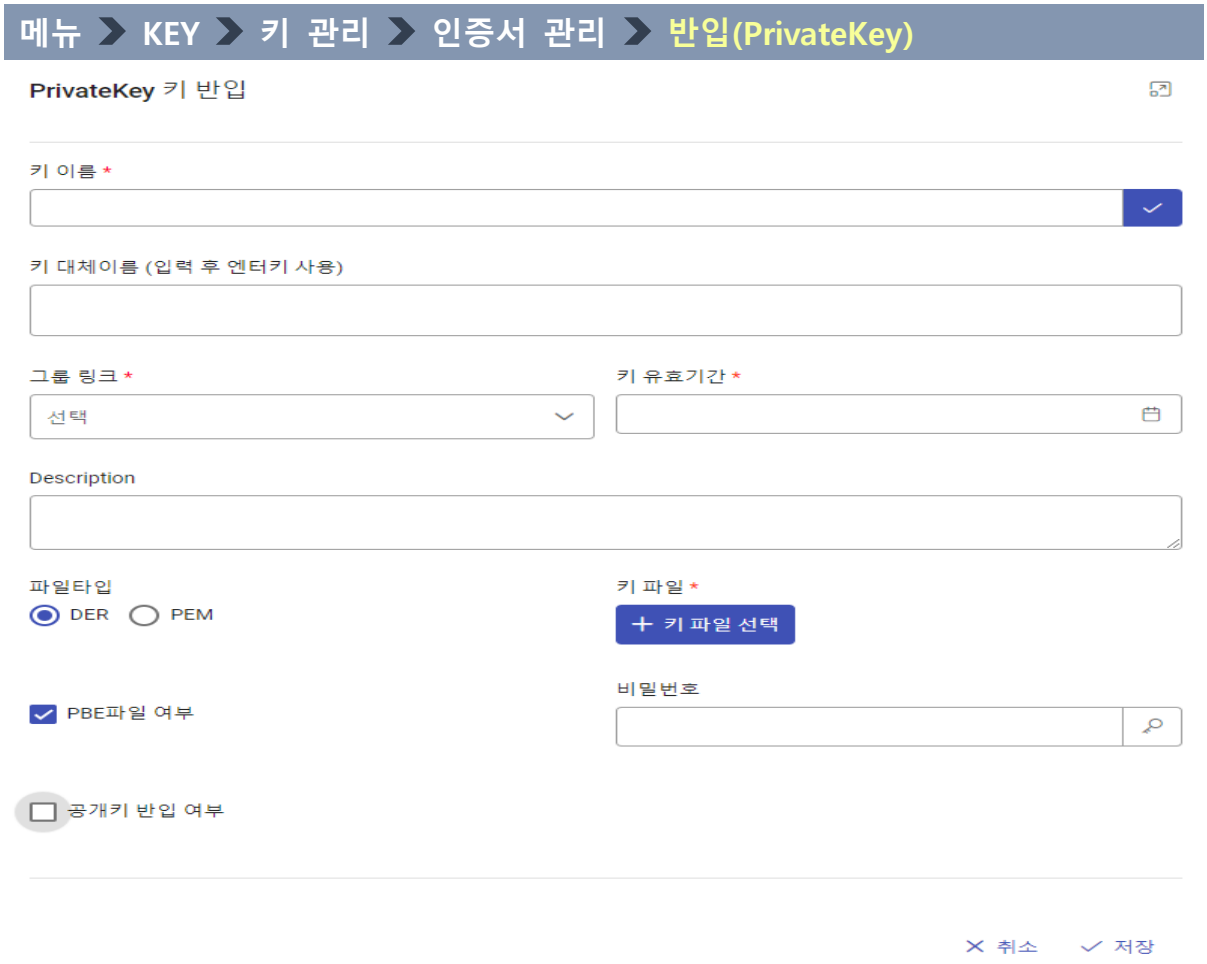


그림 46. 개인키 반입 화면

✓ 각 항목 정보 입력	
키 이름	- 키 이름 입력
키 대체이름	- 키 대체 이름 입력
그룹 링크	- 반입하고자 하는 개인키가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
Description	- 반입하고자 하는 개인키에 대한 부가 설명 입력
파일 타입	- DER와 PEM 중 선택
키 파일	- 반입하고자 하는 개인키 파일 선택
PBE파일 여부	- 필요 시 PBE파일 선택
비밀번호	- PBE파일 비밀번호 입력
공개키 반입 여부	- 공개키 반입 여부 체크

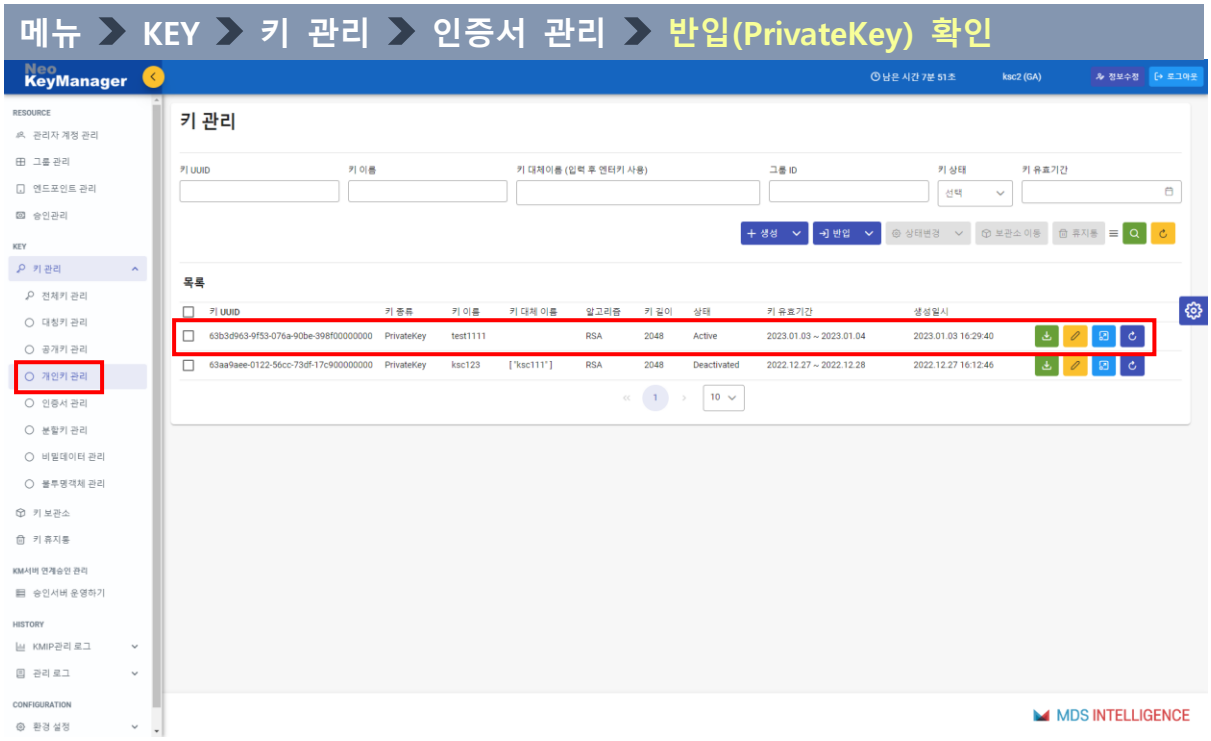


그림 47. 개인키 반입 확인

✓ 개인키 반입 확인

④ 인증서(Certificate)

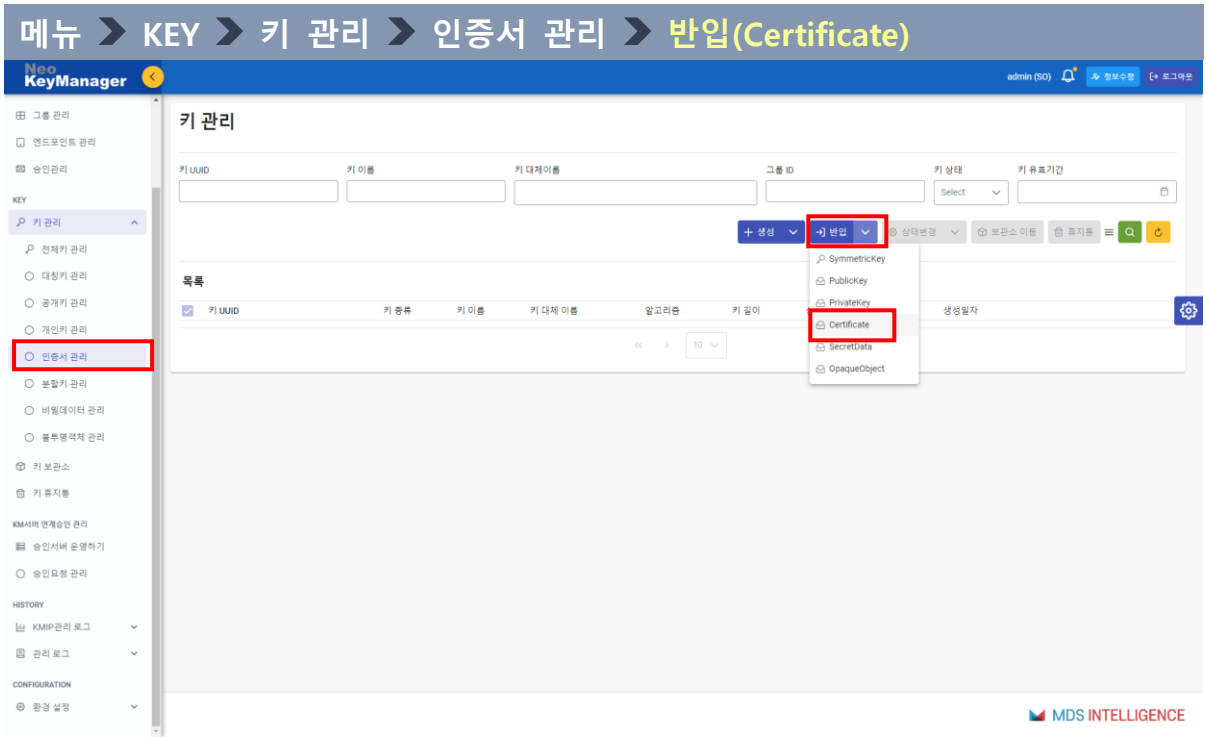


그림 48. 인증서 반입 선택

- ✓ 인증서 반입 기능 제공
- ✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 Certificate 선택 후 반입 화면으로 이동

그림 49. 인증서 반입 화면

✓ 각 항목 별 입력 후 저장	
키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능
그룹 링크	- 반입하고자 하는 인증서가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
설명	- 반입하고자 하는 인증서에 대한 부가 설명 입력
파일 타입	- pem[6], der[7], 중 선택
키 파일	- 반입하고자 하는 인증서 파일 선택

[6] **pem(privacy enhanced mail) :** Base64로 인코딩된 인증서

[7] **der(distinguished encoding representation) :** 바이너리 DER 형식으로 인코딩된 인증서
텍스트 편집기에서 해당 파일을 열었을 때, 읽어 들일 수 없다면 der 인코딩일 확률이 높음

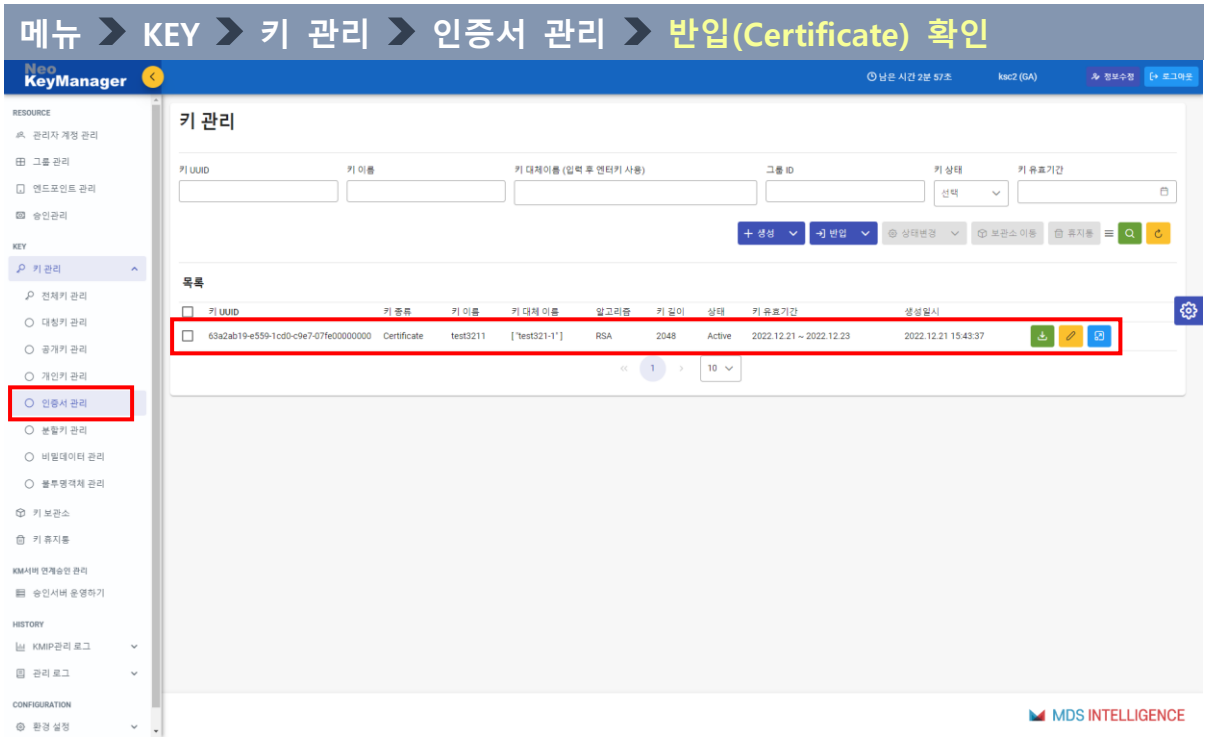


그림 50. 인증서 반입 확인

✓ 인증서 반입 확인

⑤ 비밀데이터(SecretData)

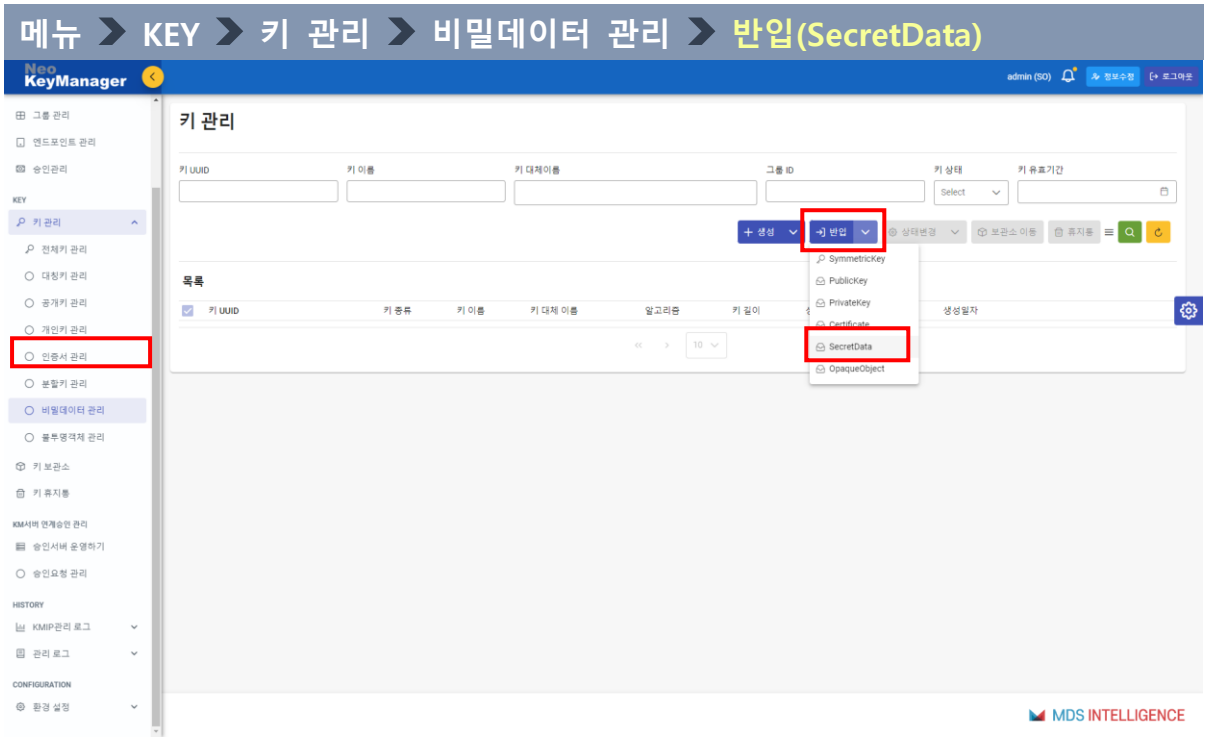


그림 51. 비밀데이터 반입 선택

✓ 비밀데이터 키 반입 기능 제공
✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 SecretData 선택 후 반입 화면으로 이동

메뉴 > KEY > 키 관리 > 비밀데이터 관리 > 반입(SecretData)

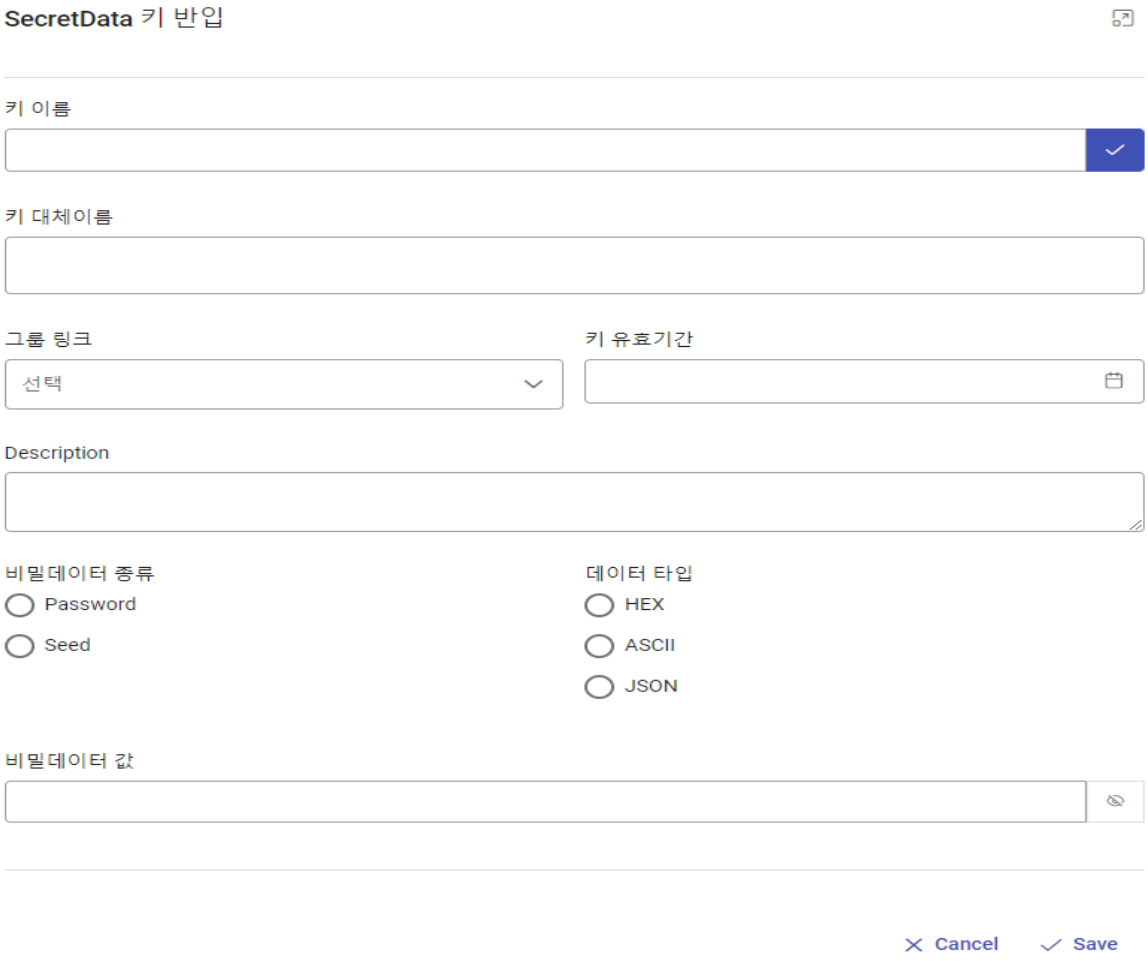


그림 52. 비밀데이터 반입 화면

✓ 각 항목 입력 후 저장	
키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능
그룹 링크	- 반입하고자 하는 비밀데이터가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
설명	- 반입하고자 하는 비밀데이터에 대한 부가 설명 입력
비밀데이터 종류	- Password와 Seed 중 선택
데이터 타입	- HEX, ASCII, JSON 중 선택

비밀데이터 값	- 비밀데이터 값 입력

⑥ 불투명객체(OpaqueObject)

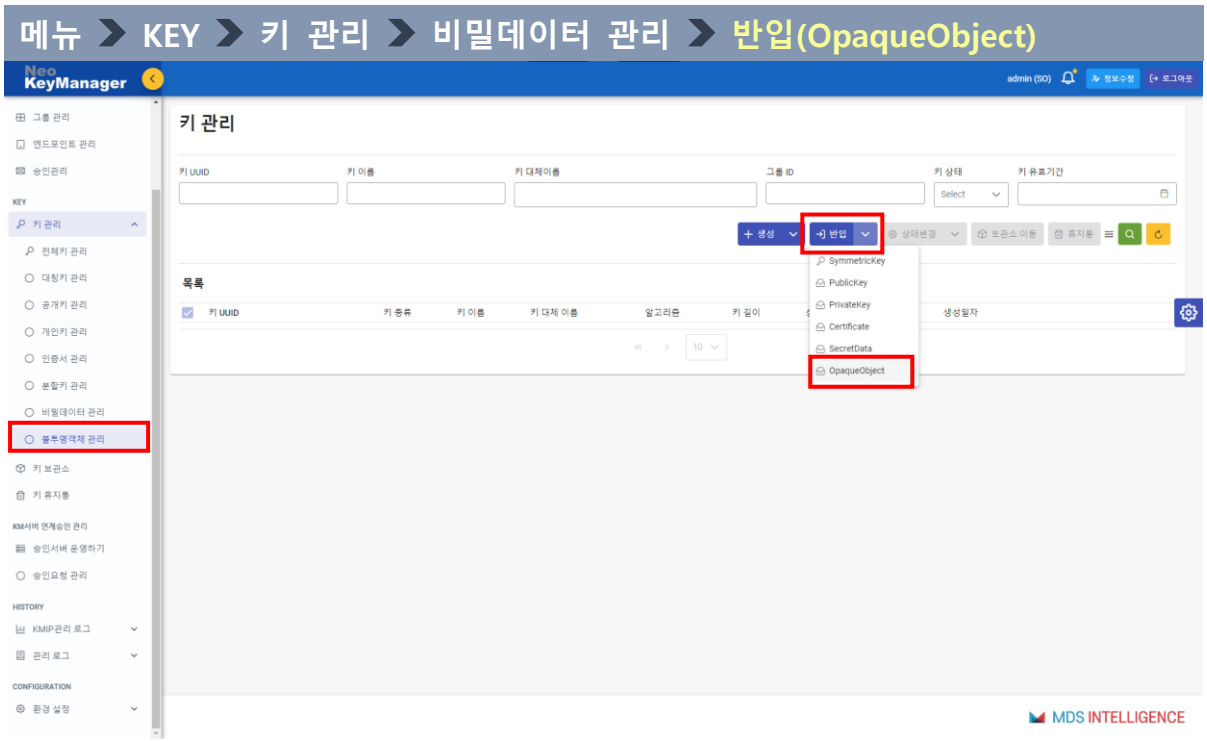


그림 53. 불투명객체 반입 선택

- ✓ 불투명객체 반입 기능 제공
- ✓ 암호키 형식이 아닌 바이너리 파일 자체를 KMS에서 관리하고자 하는 경우, 불투명객체로 반입
- ✓ 위 그림과 같이 [반입 v] 버튼 클릭 시 OpaqueObject 선택 후 반입 화면으로 이동

그림 54. 불투명객체 반입 화면

✓ 각 항목 입력 후 저장	
키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능
그룹 링크	- 반입하고자 하는 불투명객체가 속하는 그룹을 선택
키 유효기간	- 키 유효기간 설정
설명	- 반입하고자 하는 불투명객체에 대한 부가 설명 입력
반입 방법	- File 선택
키 파일	- 반입하고자 하는 불투명객체 파일 선택(1MB 미만)

(3) 상태변경

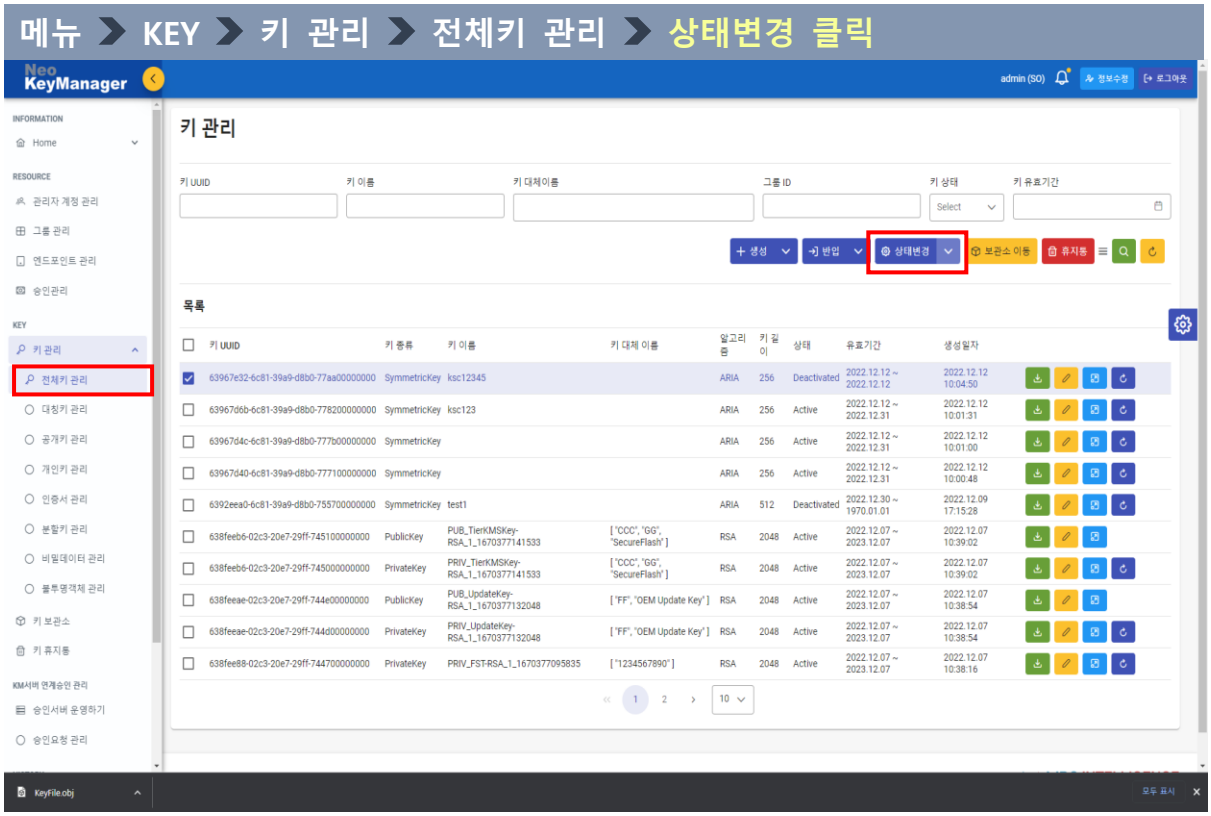


그림 55. 키 상태변경 화면

- ✓ 암호키에 대한 상태변경 기능
- ✓ 위 그림과 같이 [상태변경 v] 버튼 클릭
- ✓ 키 상태가 PreActive 상태인 경우, 활성화 선택 가능
- ✓ 키 상태가 Active 상태인 경우, 비활성화 또는 취소 선택 가능

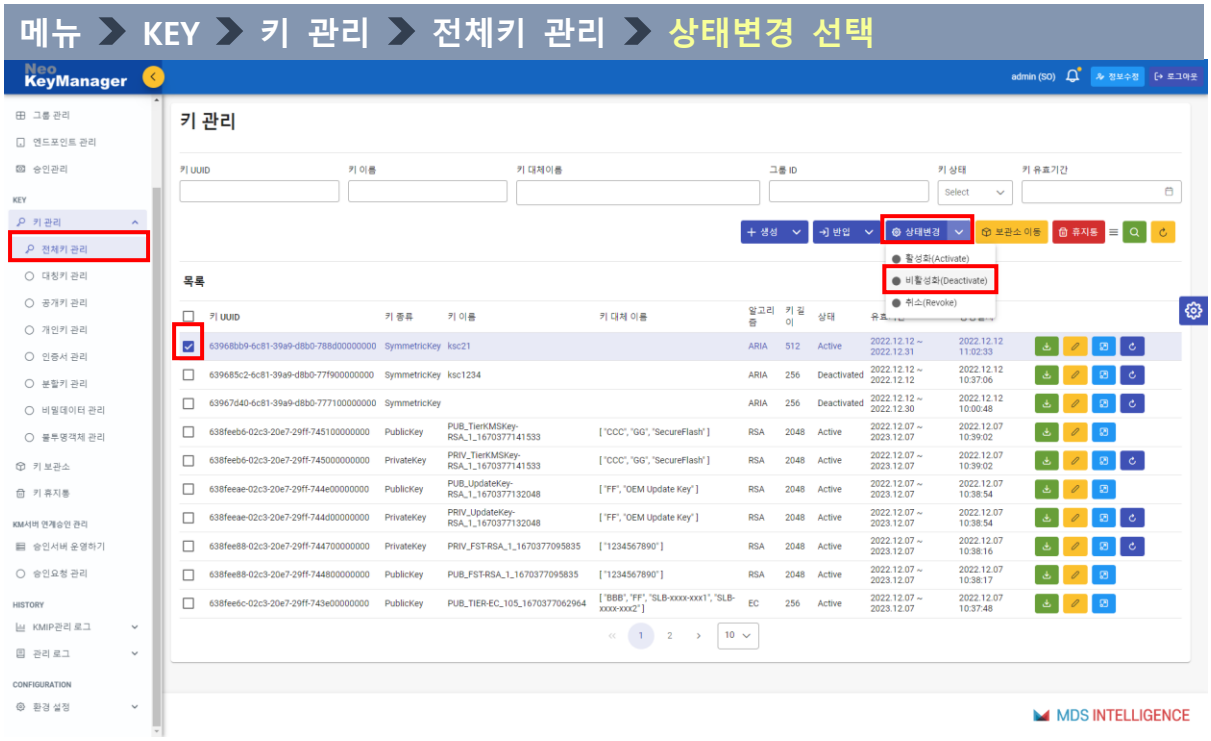


그림 56. 키 비활성화 선택

✓ 위 그림과 같이 활성화(Active)된 키 선택 후 [상태변경 v] 버튼에서 비활성화 클릭
✓ 취소(Revoke)도 동일

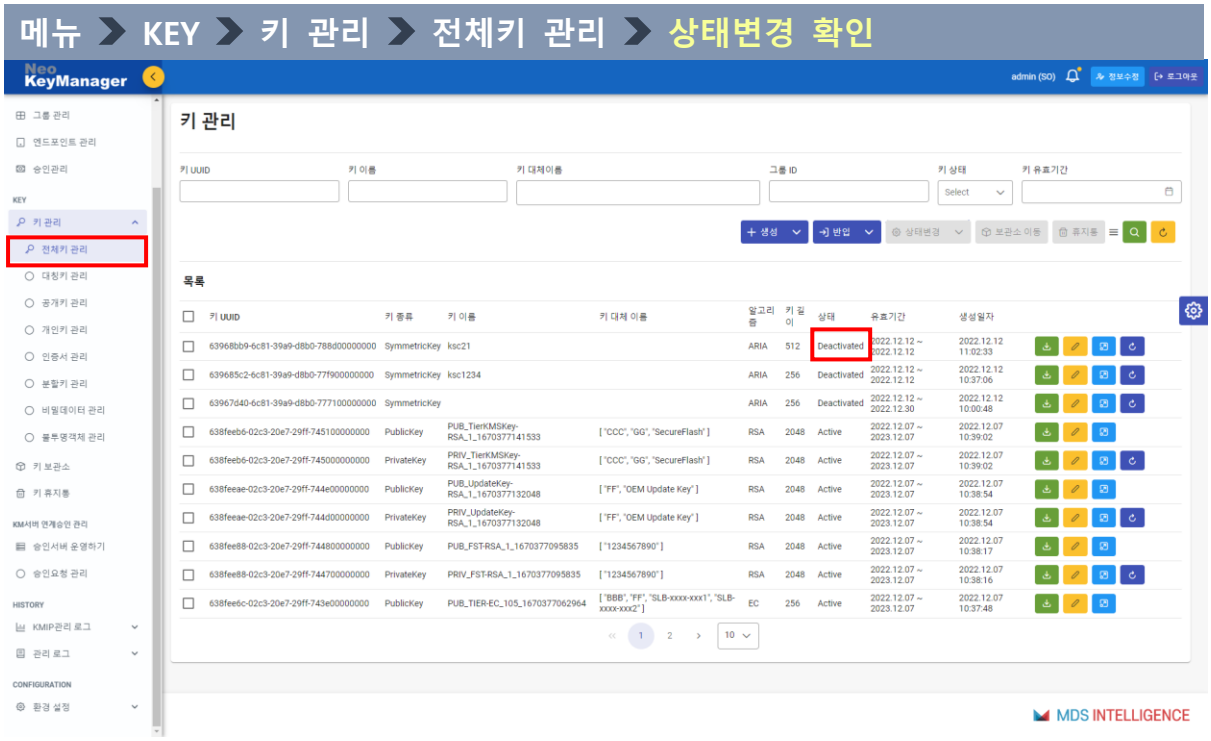


그림 57. 키 상태변경(비활성화) 확인

✓ 위 그림과 같이 키 상태가 비활성화(Deactivated)로 변경 확인

(4) 보관소 이동

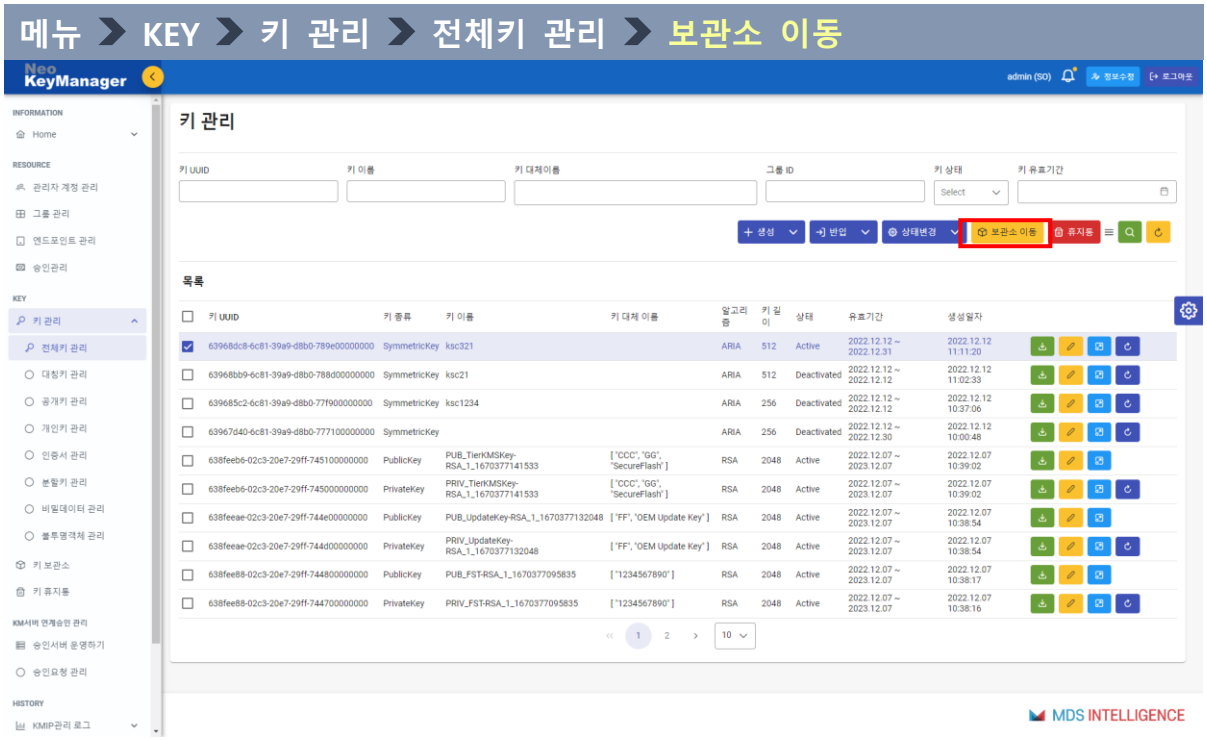


그림 58. 키 보관소 이동

✓ 암호키가 유출되었거나 필요 시 해당 키를 분리 보관할 수 있는 키 보관소를 제공
✓ 암호키가 유출되지 않은 것으로 확인되었거나 필요 시 해당 키를 복구 가능함.
✓ 위 그림과 같이 암호키 선택 후 [보관소 이동] 버튼 클릭 시 키 보관소로 이동함.

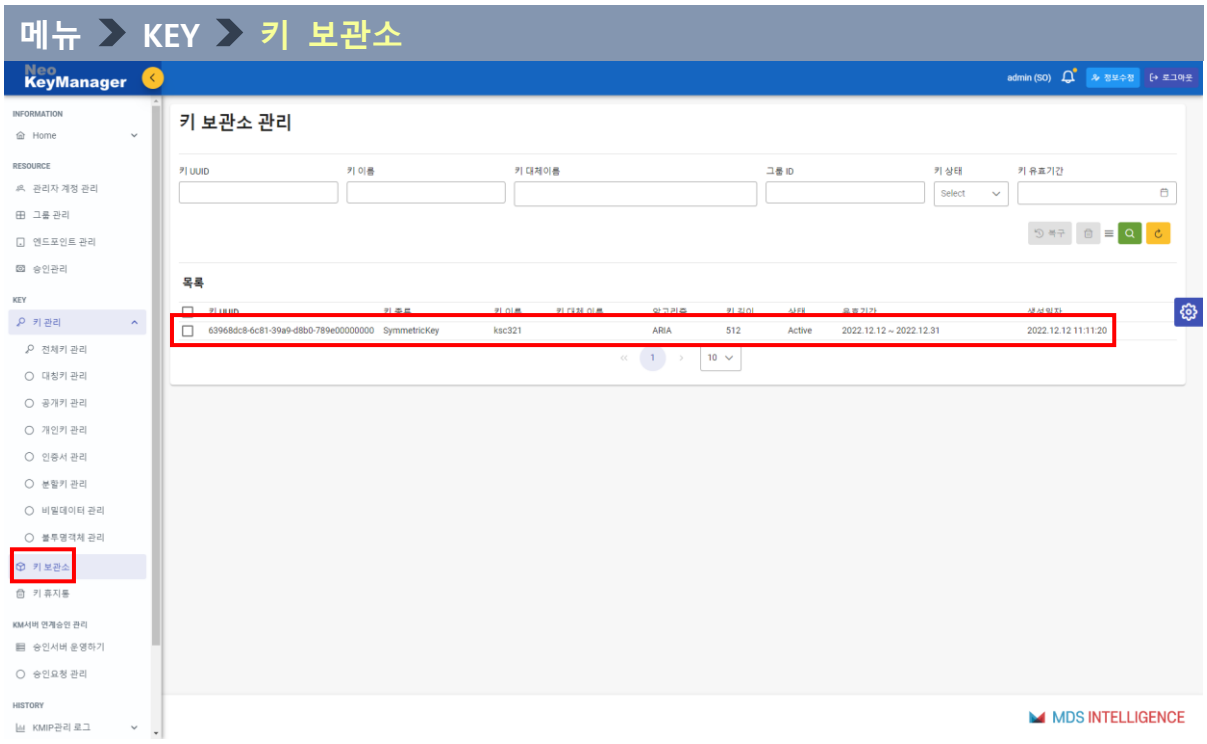


그림 59. 키 보관소에서 해당 암호키 확인

✓ 키 보관소에서 해당 암호키 확인

(5) 키 파기

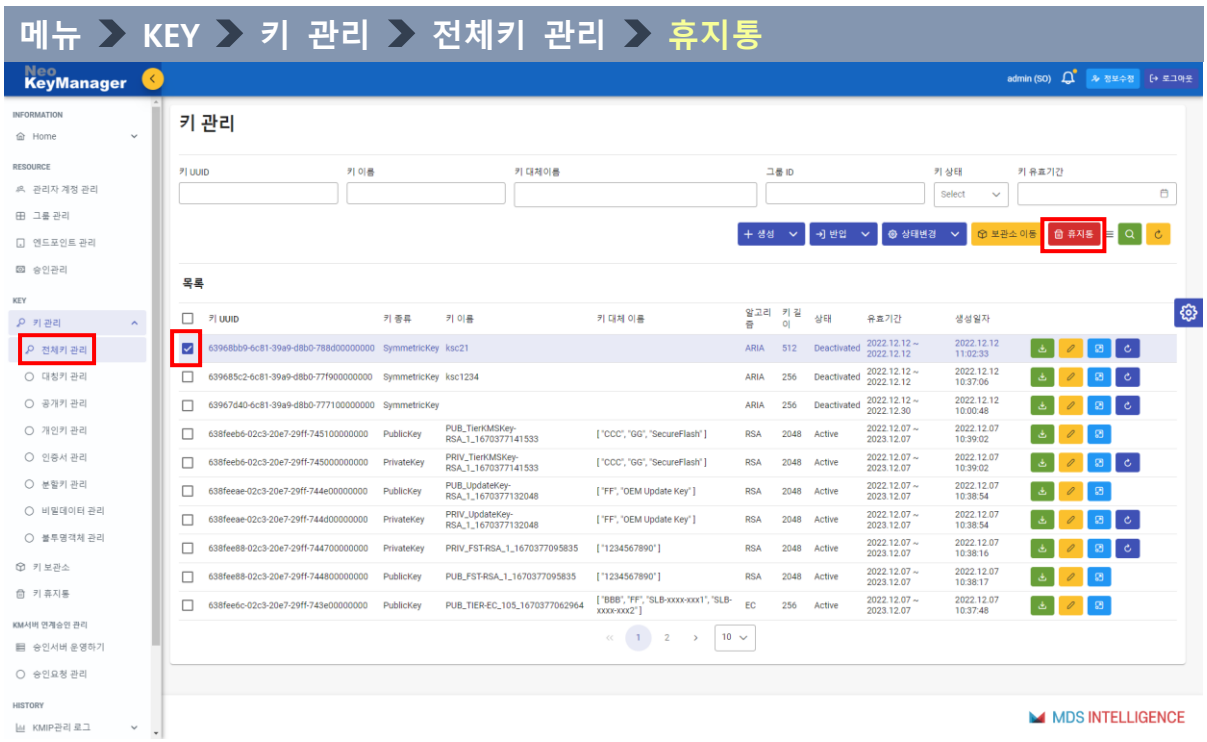


그림 60. 파기할 키 선택

- ✓ 위 그림과 같이 파기할 Deactivated(비활성화) 상태인 키 선택
- ✓ [휴지통] 버튼 클릭하면, 해당 키는 파기(Destroyed) 상태로 변경되어 휴지통으로 이동함.

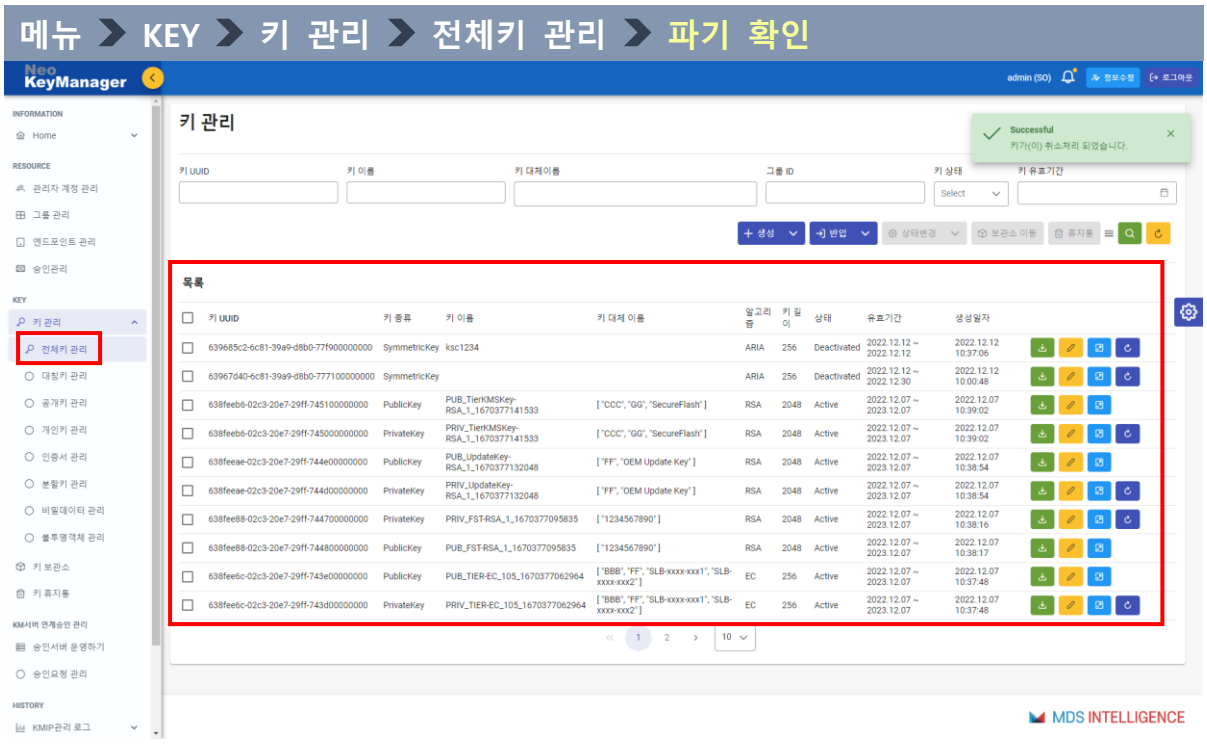


그림 61. 파기 후 키 관리 목록 화면

✓ 파기된 키는 키 휴지통으로 이동하였으므로 키 관리 목록에서 보이지 않음.

(6) 키 반출

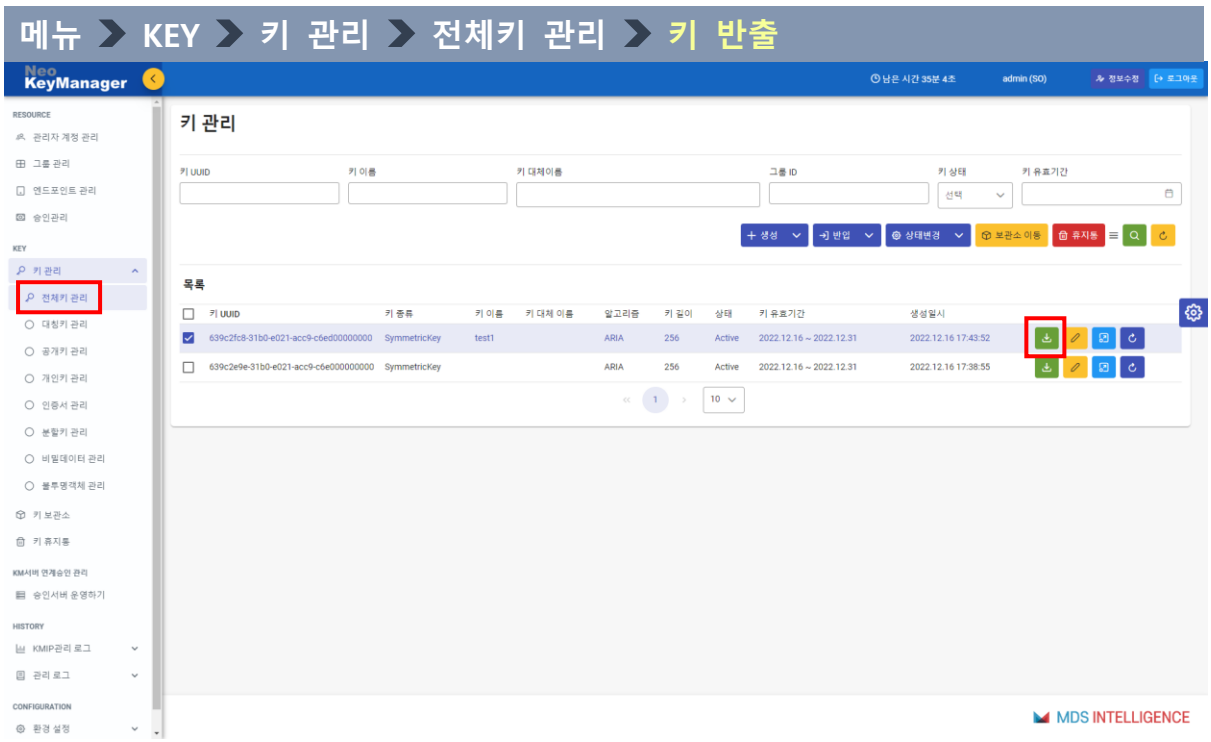


그림 62. 키 반출

- ✓ 기관 간 키 교환 시 내부 키 반출을 위한 기능 제공
- ✓ 위 그림과 같이 반출하고자 하는 키 선택 후 [키 반출] 버튼을 클릭하면, 해당 키가 다운로드됨.

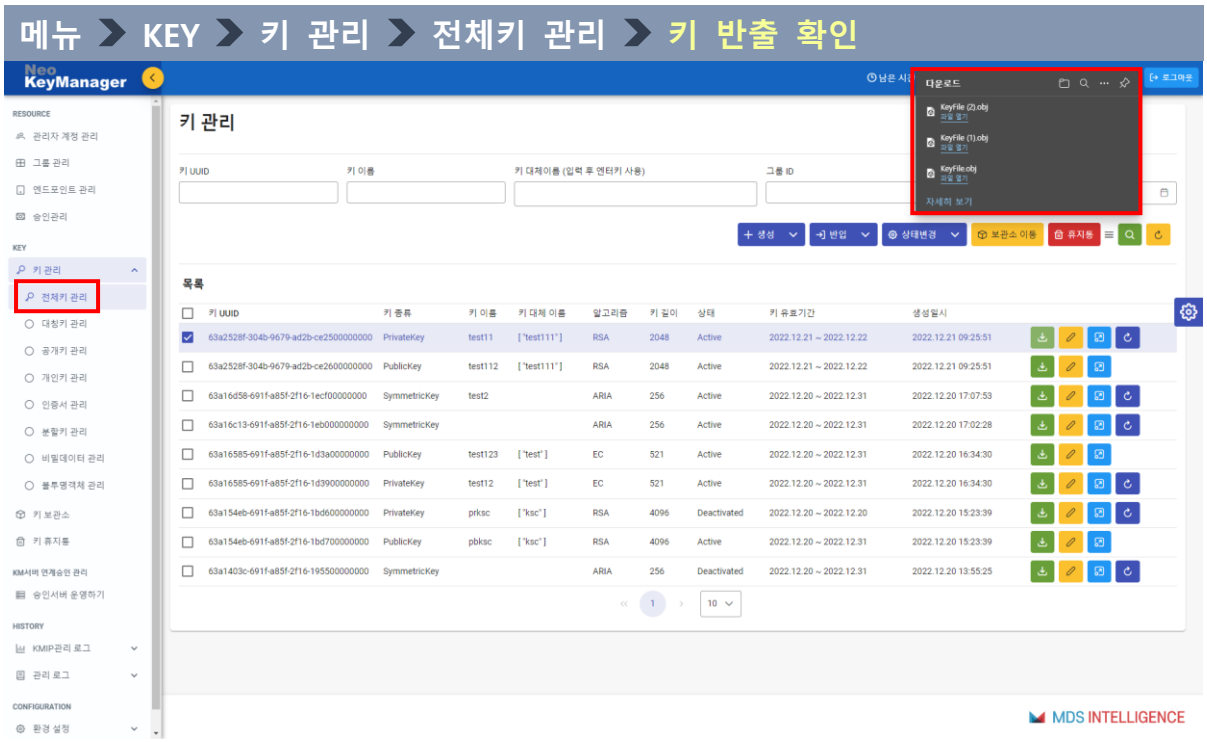


그림 63. 키 다운로드 확인

✓ 반출한 키 다운로드 확인

(7) 키 수정

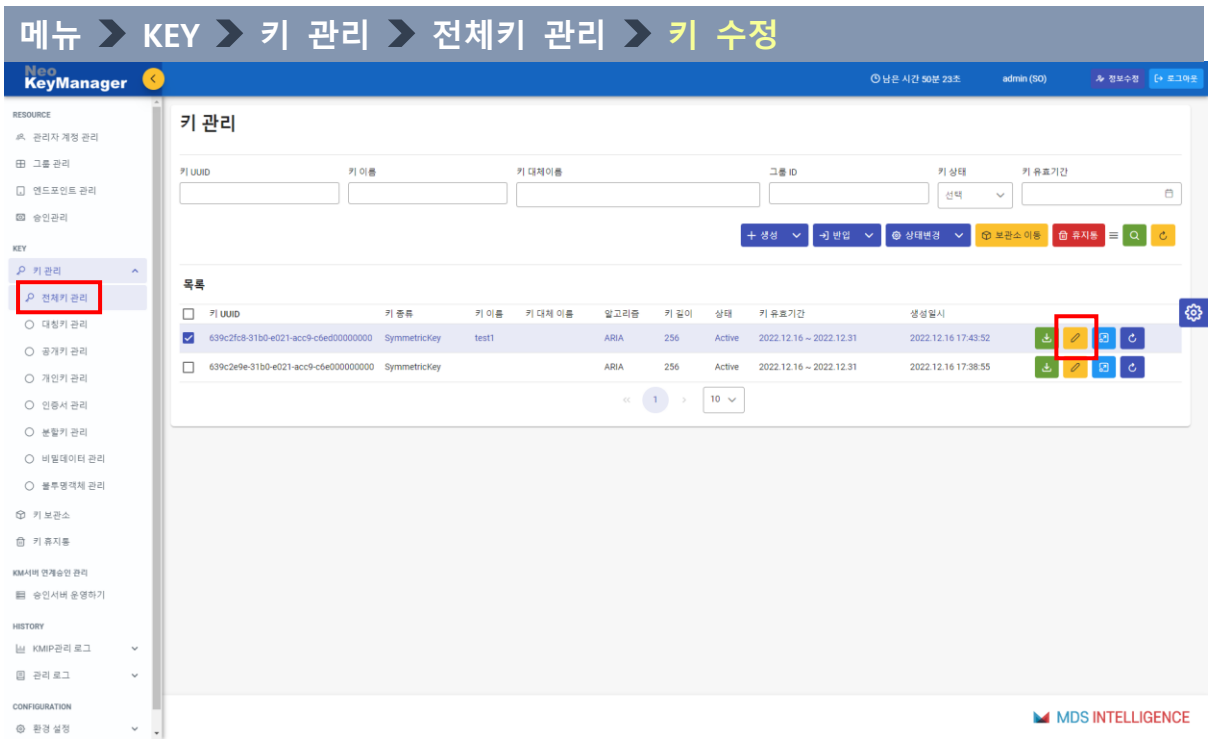


그림 64. 키 수정

✓ 목록에서 해당 키의 수정 버튼 클릭

메뉴 > KEY > 키 관리 > 전체키 관리 > 키 수정 입력화면

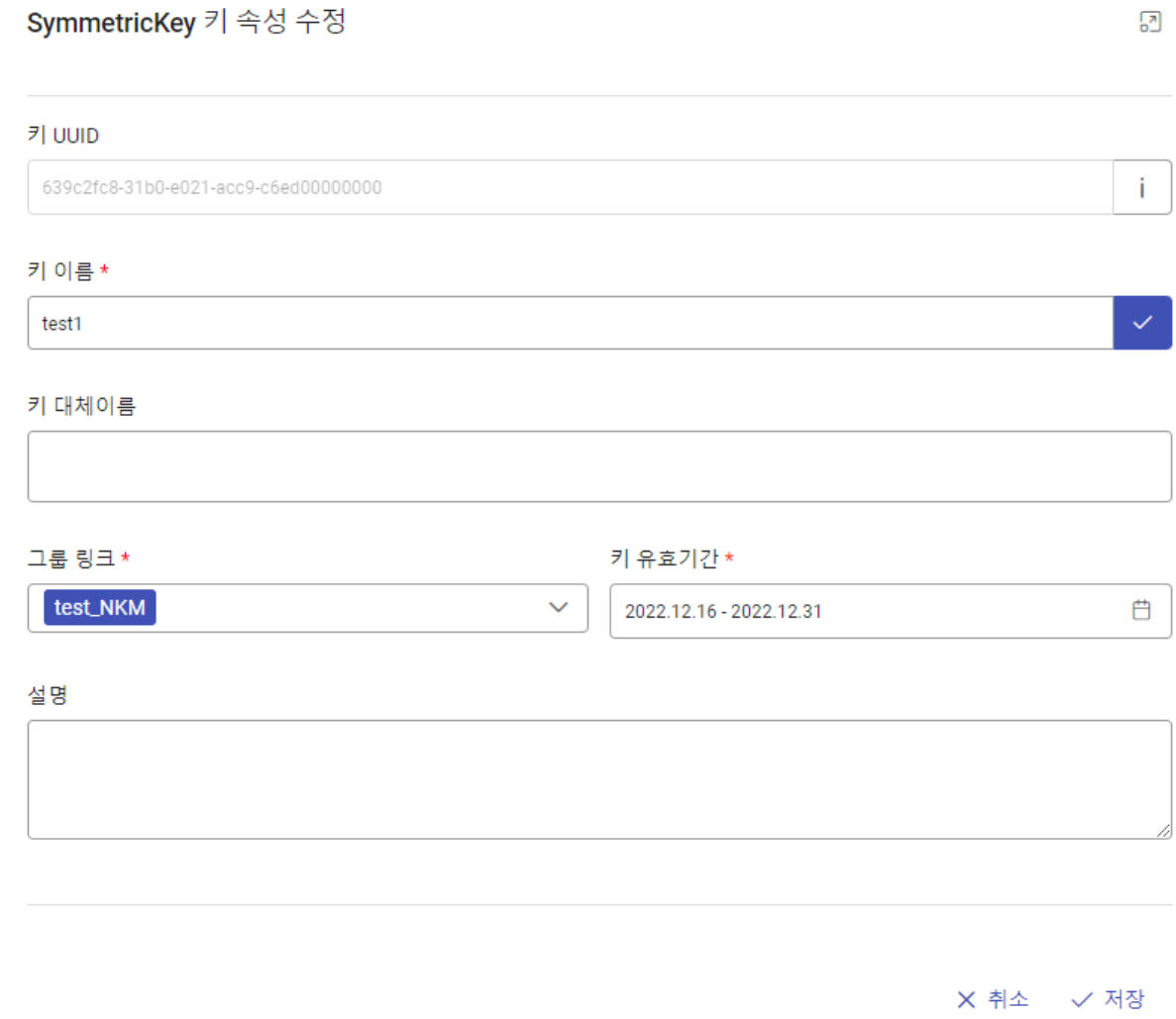


그림 65. 대칭키 수정 화면

✓ 각 항목 입력 후 저장	
키 이름	- 기존 키와 키 이름 중복 불가, 한글 입력 제외
키 대체이름	- 유사한 키 이름의 키 관리를 위한 키 이름 그룹명 예) 키 1 이름 : Test1, 키 2 이름 : Test2, 대체 이름 : Test 대체 이름(Test)으로 키 조회 시 Test1, Test2 조회 가능
그룹 링크	- 키가 속한 그룹을 변경하거나 추가하는 경우, 해당 그룹을 선택
키 유효기간	- 키 유효기간 설정 - [Active] 상태인 키는 활성화 일시 변경 불가 - [비활성화 일시]는 활성화 일시 이전 날짜 선택 불가
설명	- 해당 대칭키에 대한 부가 설명 수정

(8) 키 상세보기

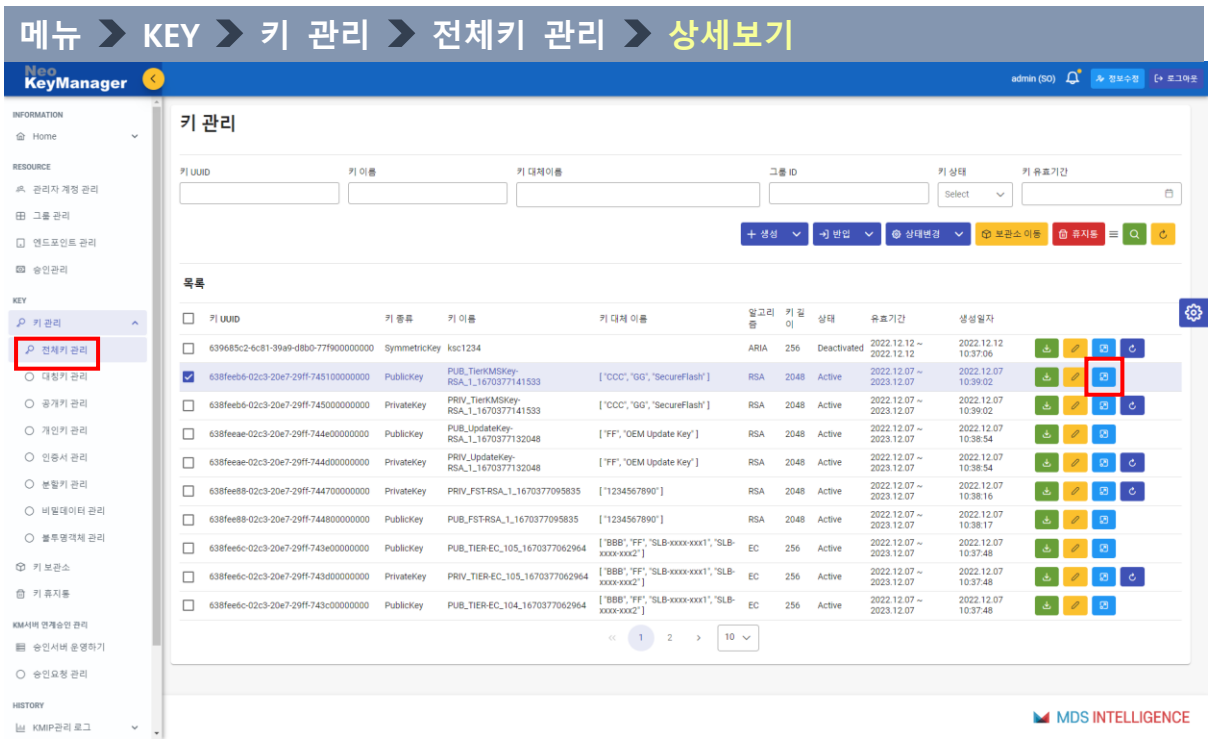


그림 66. 상세보기 클릭 화면

✓ 목록에서 해당 키 상세보기 클릭

메뉴 ➤ KEY ➤ 키 관리 ➤ 전체키 관리 ➤ 상세보기 화면

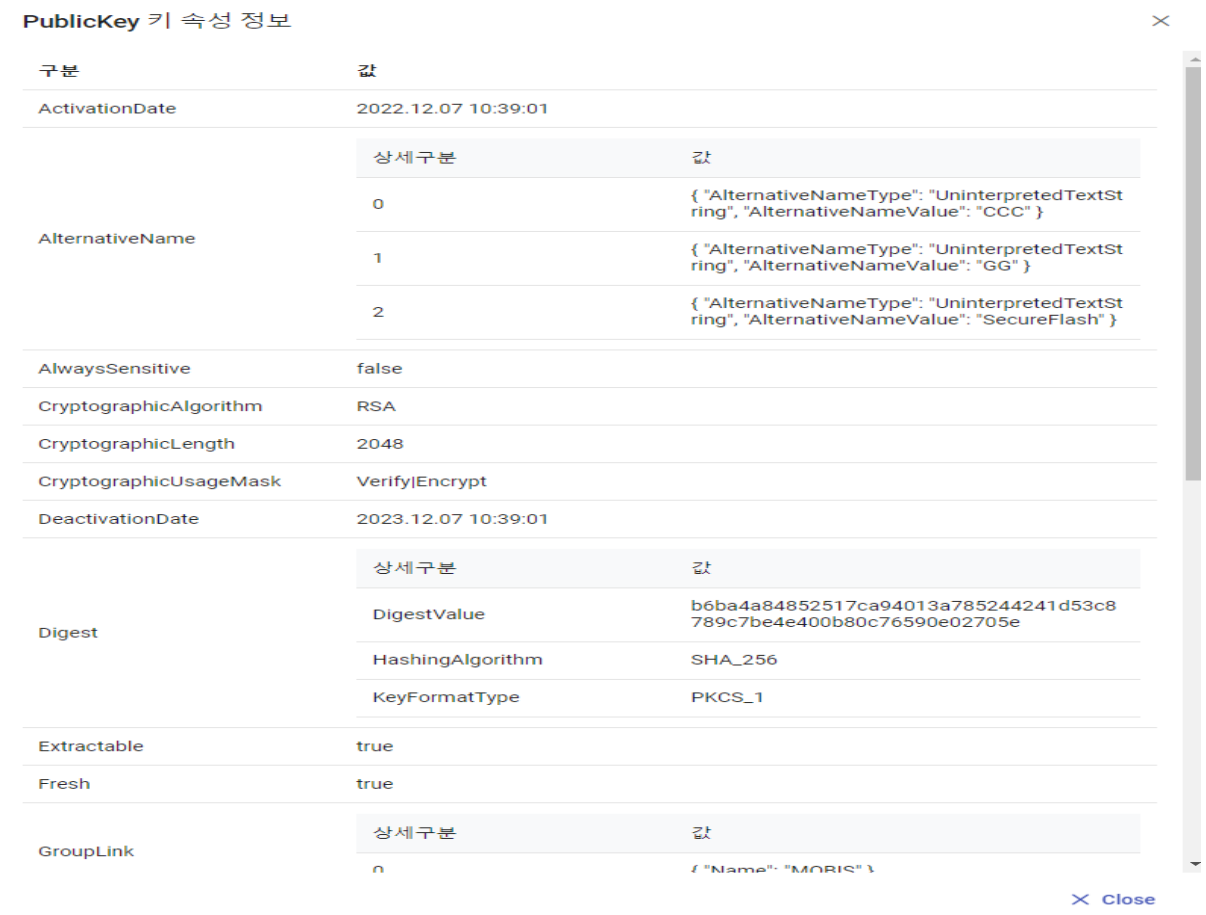


그림 67. 상세보기 화면

✓ 키 속성 정보 확인

(9) 키 갱신

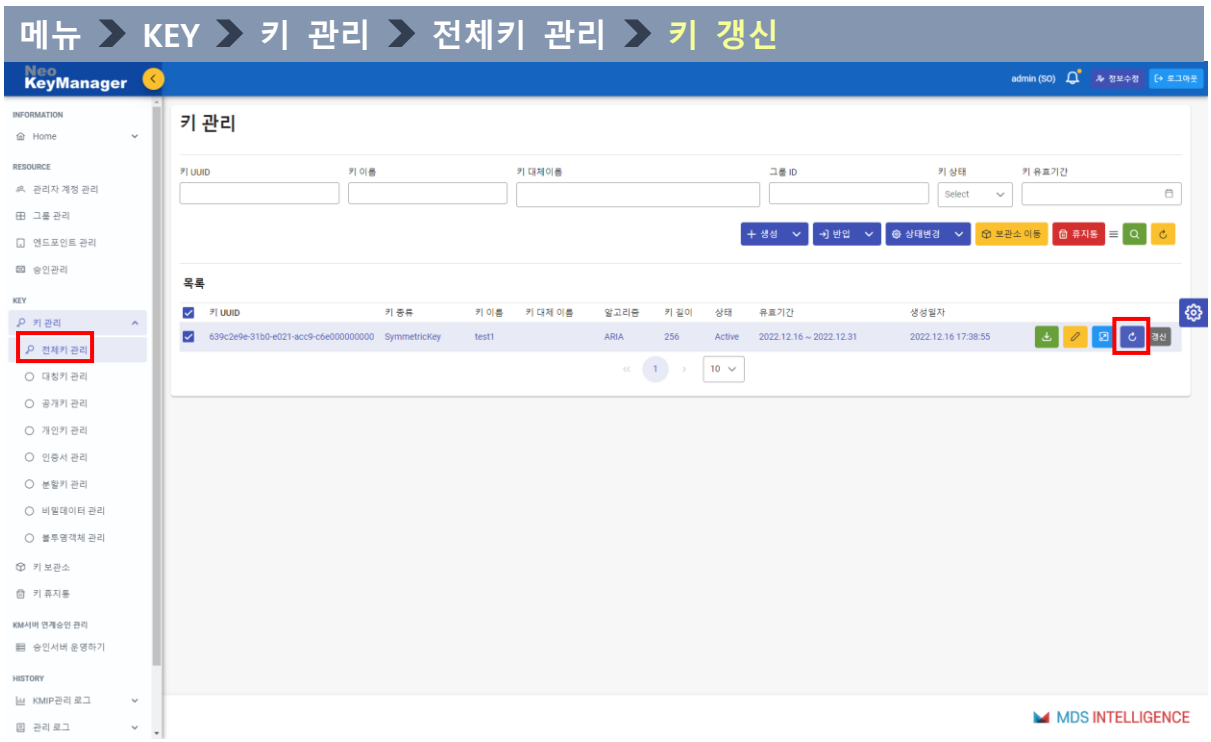


그림 68. 키 갱신 화면

✓ 위 그림과 같이 목록에서 해당 키 갱신 버튼 클릭

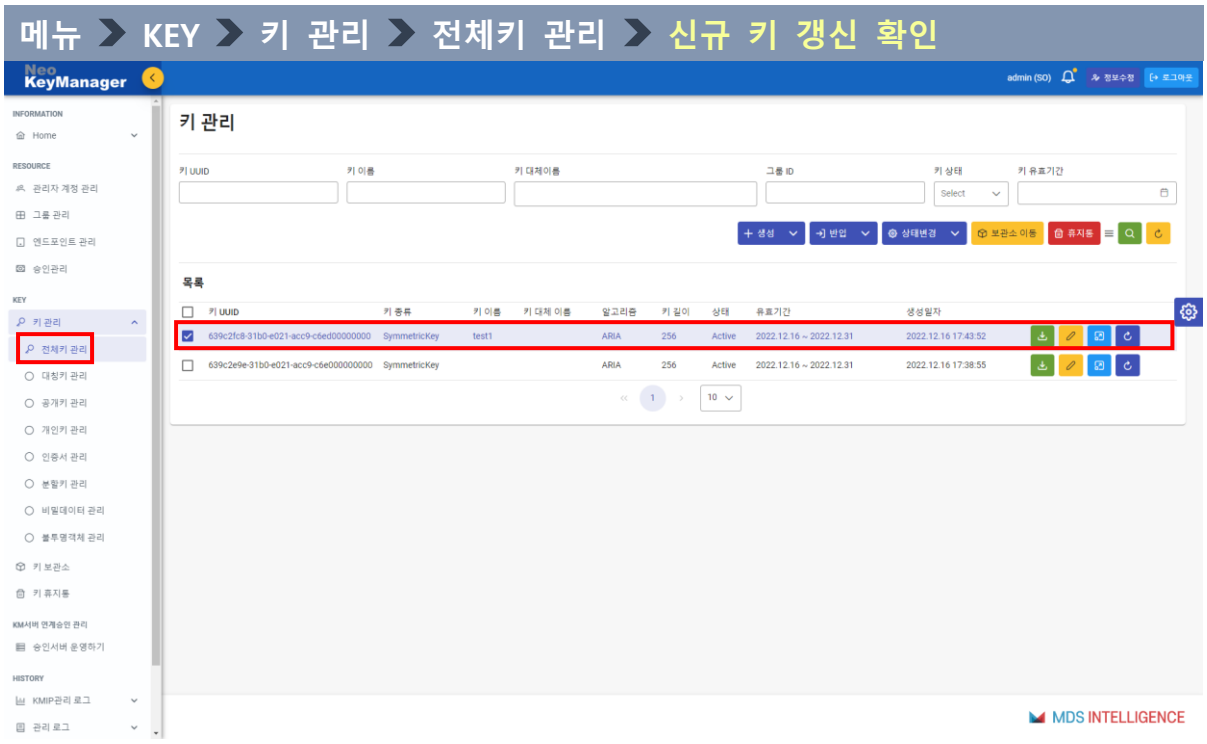


그림 69. 새로운 키 갱신 확인 화면

- ✓ 위 그림과 같이 목록에서 키 갱신 확인
- ✓ 갱신된 키는 기존 키 이름과 키 종류, 유효기간 등의 속성을 그대로 상속받음.
- ✓ 기존 키에서는 키이름이 삭제되나 다른 속성들은 유지됨.

2) 키 보관소

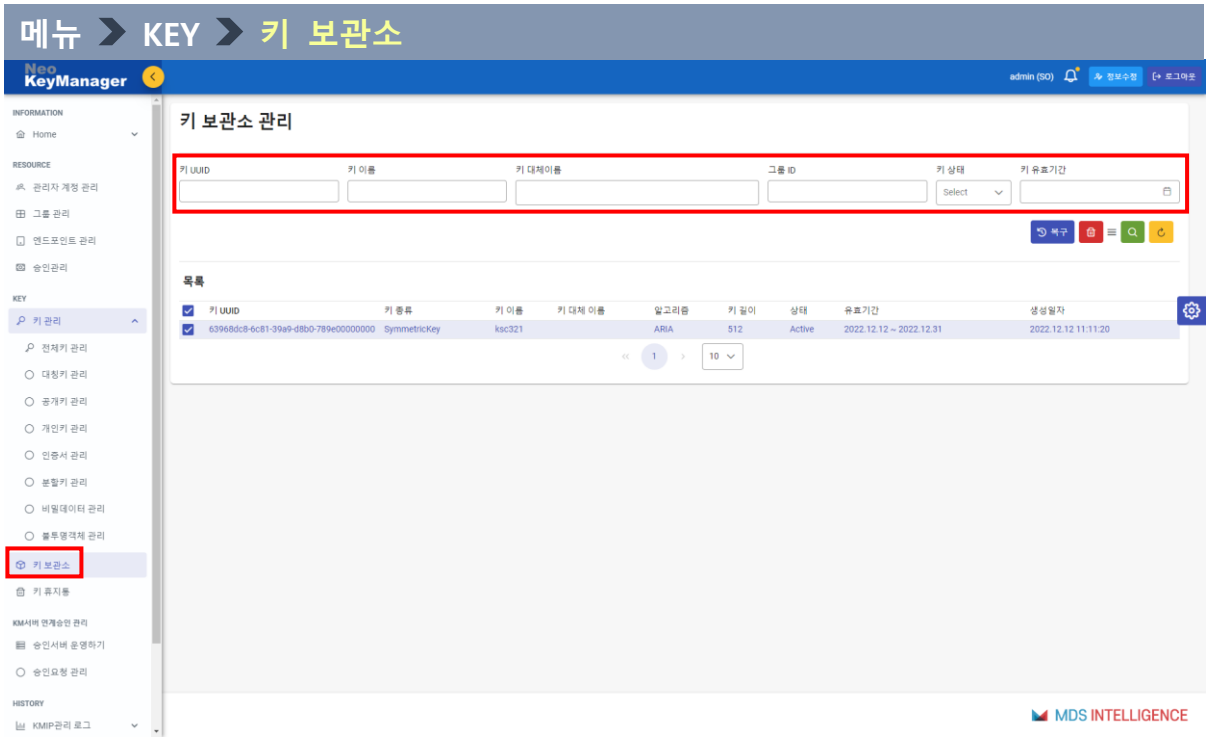


그림 70. 키 보관소 화면

✓ 보관된 키 복구, 삭제 기능 제공	
키 UUID	- 조회하고자 하는 UUID 이름 입력
키 이름	- 조회하고자 하는 키 이름 입력
키 대체이름	- 조회하고자 하는 키 대체이름 입력
그룹 ID	- 조회하고자 하는 그룹 ID 입력
키 상태	- 조회하고자 하는 키 상태 선택 - PreActive, Active, Deactivated 중 선택
키 유효기간	- 키 유효기간 조회 기능

(1) 복구

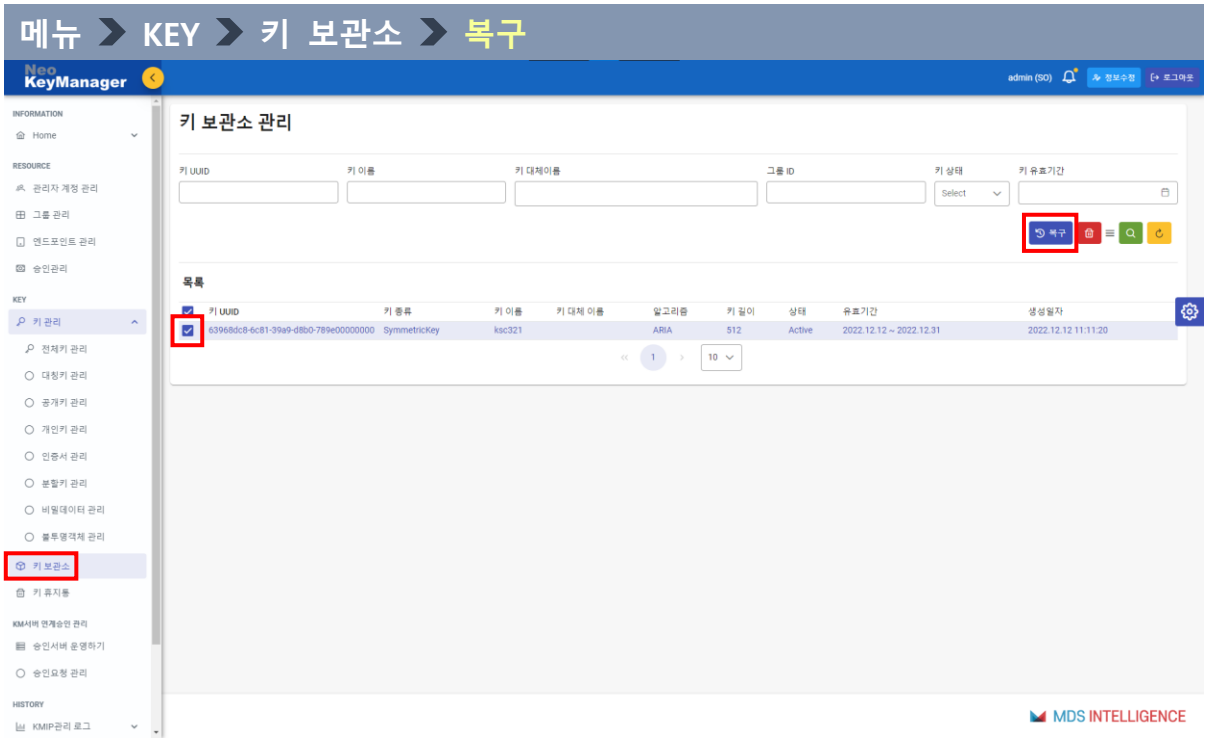


그림 71. 키 보관소 복구 화면

- ✓ 암호키가 유출되지 않은 것으로 판명되었거나 필요 시에 해당 키를 복구 가능
- ✓ 목록에서 복구하고자 하는 키 선택 후 [복구] 클릭

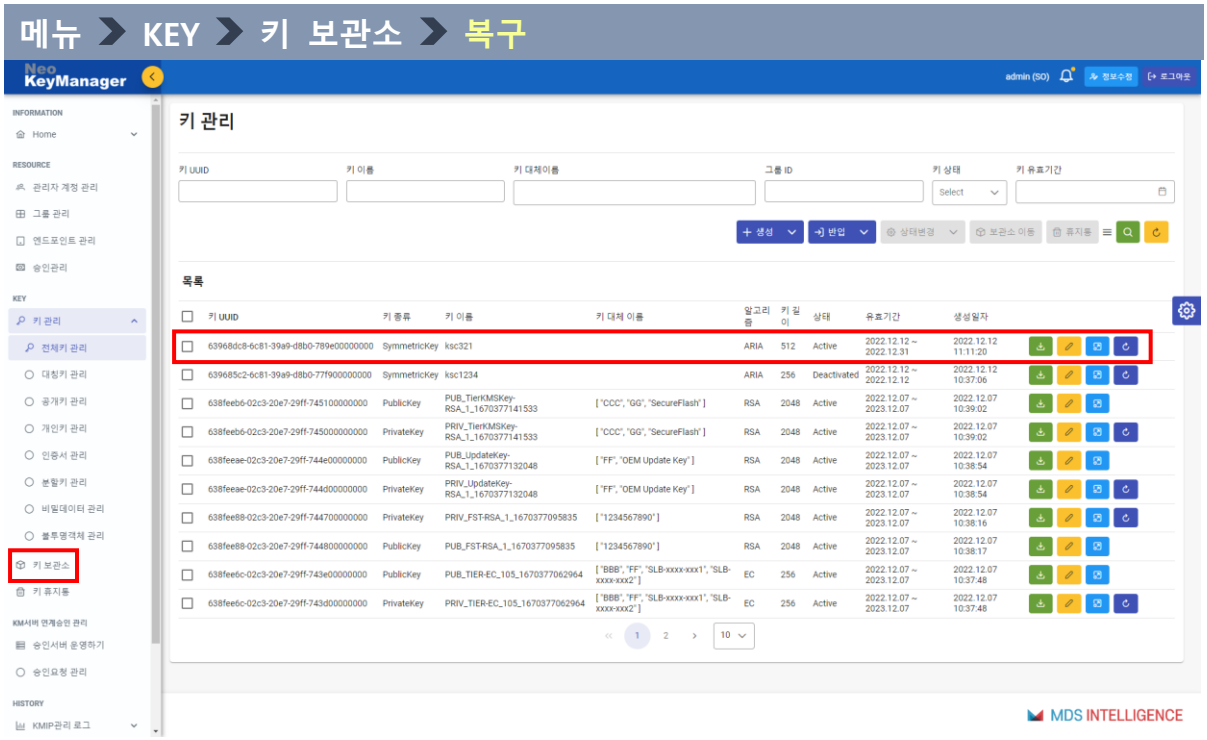


그림 72. 키 관리 목록에서 키 복구 확인

✓ 키 관리 목록에서 키 복구 확인

(2) 삭제

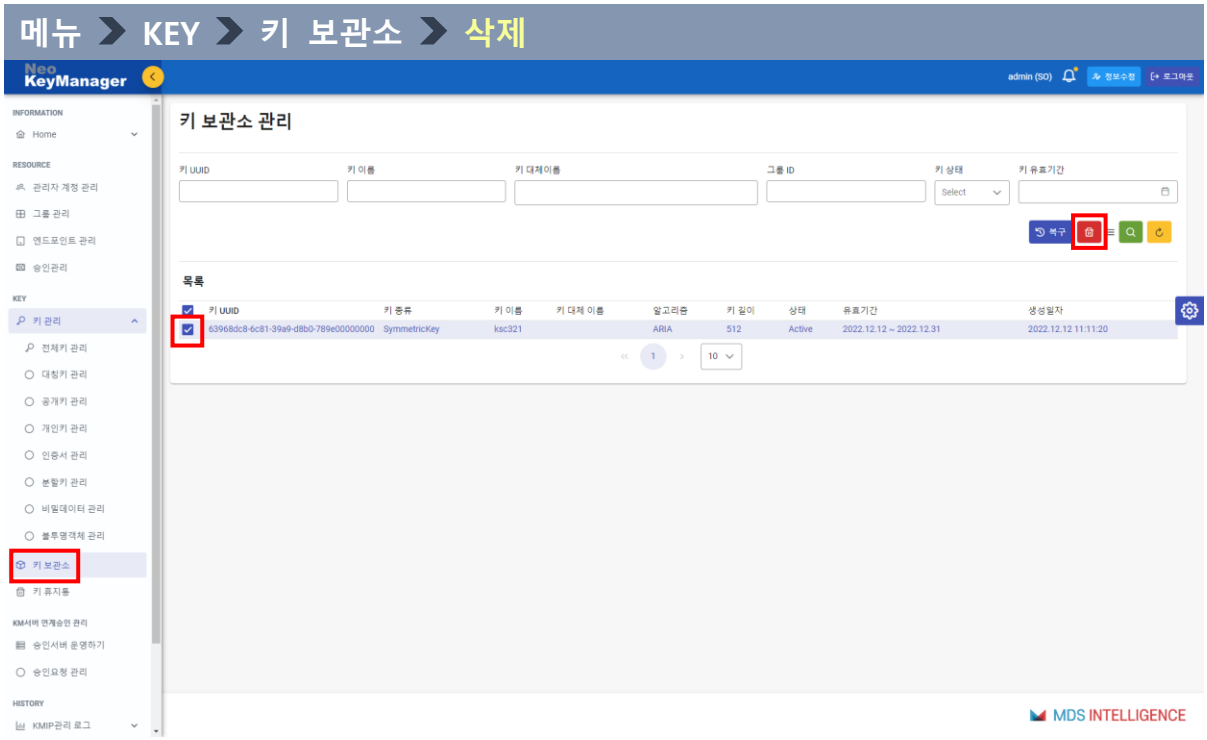


그림 73. 키 보관소의 키 삭제

✓ 키 보관소 관리 목록에서 삭제하고자 하는 키 선택 후 [휴지통] 버튼 클릭

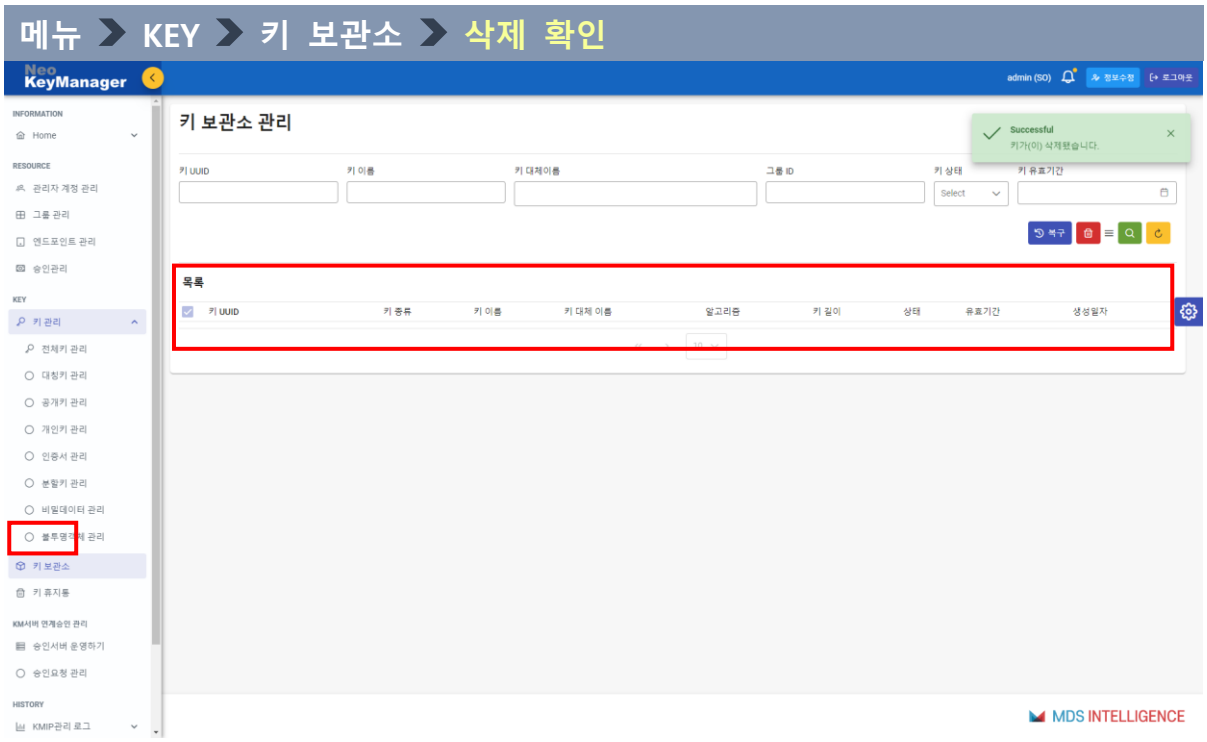


그림 74. 키 삭제 확인

✓ 키 보관소 관리 목록에서 키 삭제 확인

3) 키 휴지통

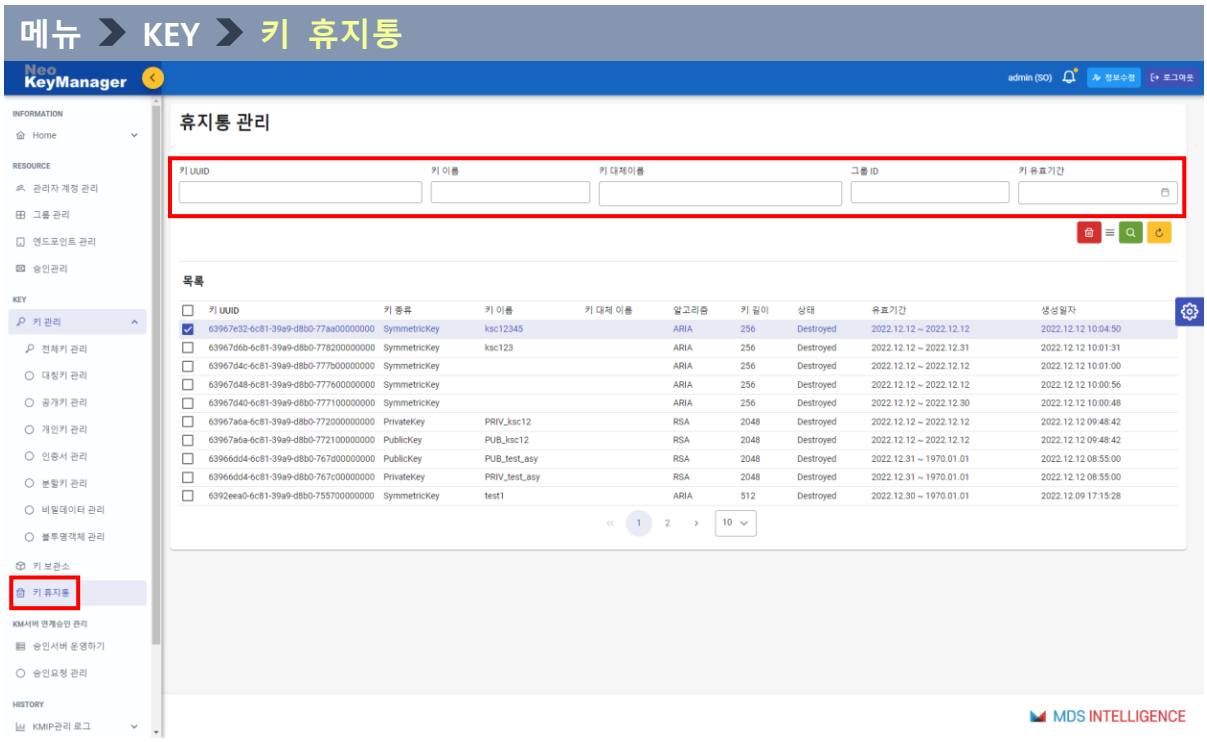


그림 75. 키 휴지통 화면

✓ 파기(Destroyed)된 키에 대한 영구 삭제 기능 ✓ 목록에 있는 키 상태 값은 모두 Destroyed로 되어 있음.	
키 UUID	- 조회하고자 하는 키 UUID 입력
키 이름	- 조회하고자 하는 키 이름 입력
키 대체이름	- 조회하고자 하는 키 대체 이름 입력
그룹 ID	- 조회하고자 하는 그룹 ID 입력
키 유효기간	- 키 유효기간 조회 기능

(1) 키 삭제

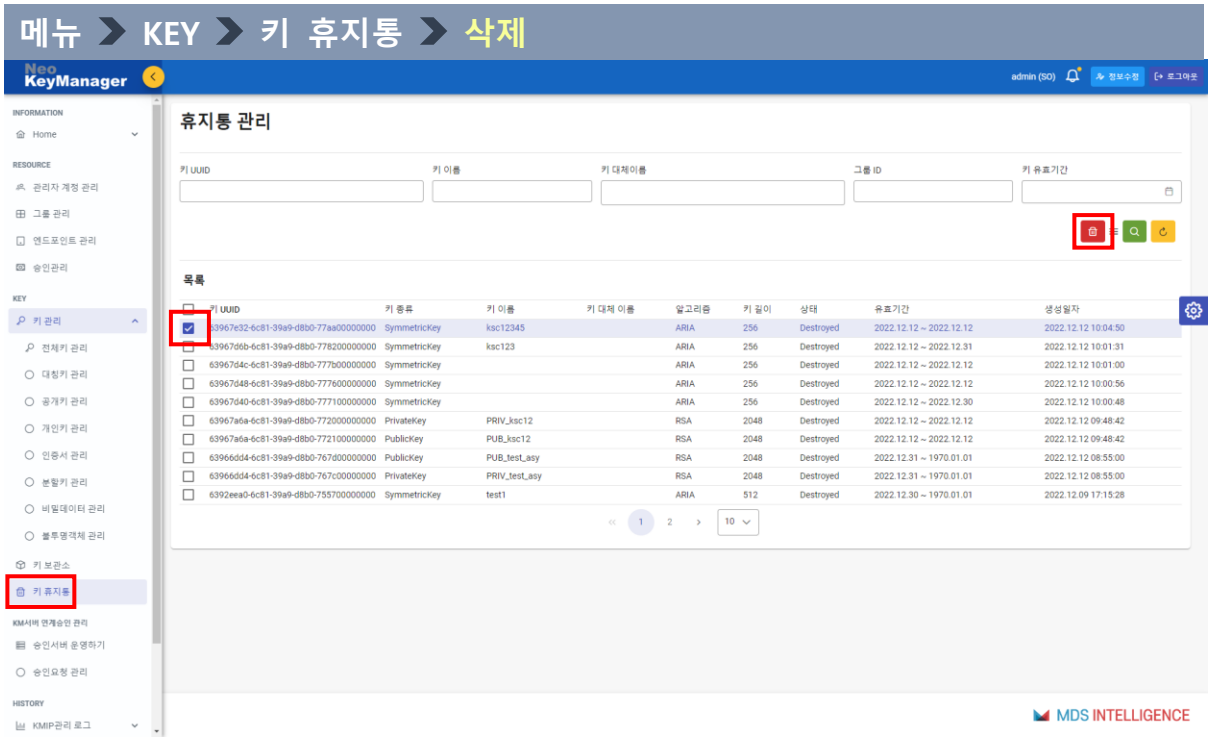


그림 76. 삭제하고자 하는 키 선택

✓ 목록에서 영구 삭제하고자 하는 키 선택 후 [휴지통] 클릭

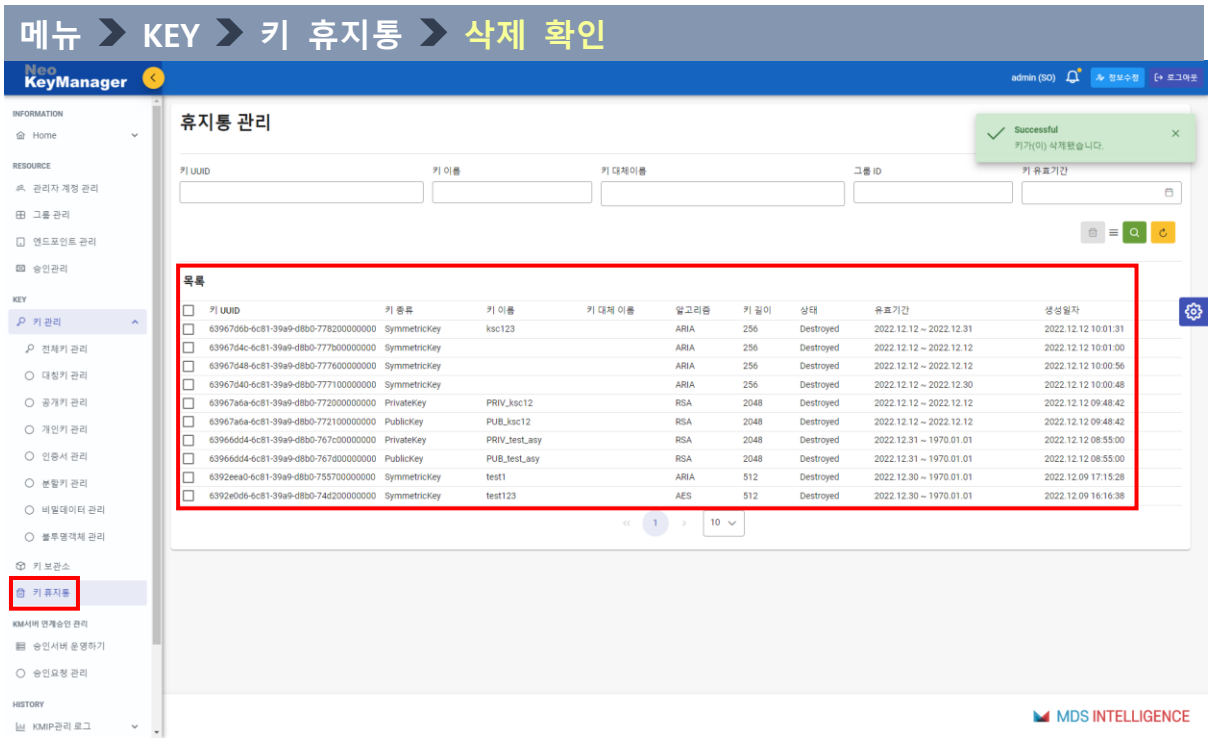


그림 77. 키 삭제 확인

✓ 목록에서 키 삭제 확인

5. HISTORY

1) KMIP연산 로그

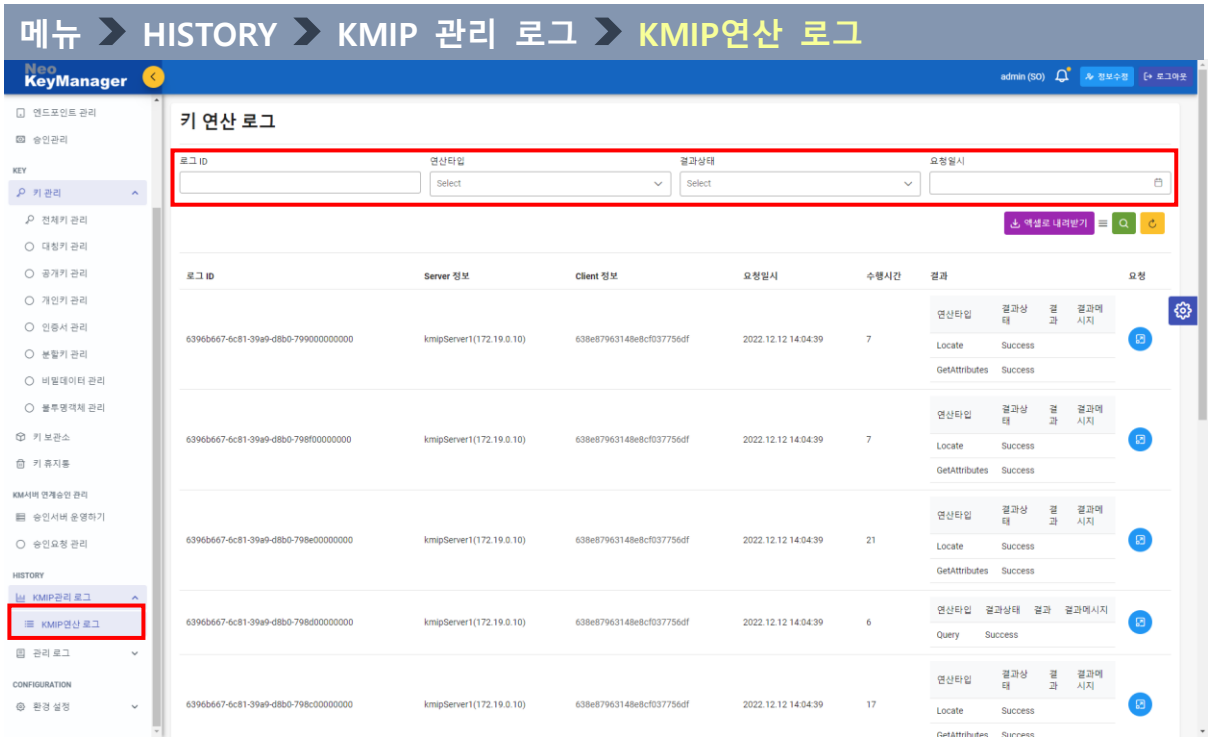


그림 78. KMIP 연산 로그 화면

✓ 로그 ID, 연산타입, 결과상태 등을 입력하여 해당 로그 조회 ✓ [엑셀로 내려받기] 탭을 통해 엑셀 파일로 로그 정보를 내려받기 가능	
로그 ID	- 조회하고자 하는 로그 ID 입력
연산타입	- 조회하고자 하는 연산타입 선택 - Create, CreateKeyPair, Locate, Get 등 연산 중 선택
결과상태	- 키 연산 상태 결과 선택 - Success와 OperationFailed 중 선택
요청일시	- 키 연산 요청일시를 설정하여 해당 기간의 키 연산 로그 조회

(1) 키 연산 로그

그림 79. 키 연산 로그를 엑셀로 내려 받기

✓ [엑셀로 내려받기] 클릭을 통해 로그ID, Client정보, 수행시간 정보 등이 포함된 엑셀파일로 내려받기 가능

2) 관리 로그

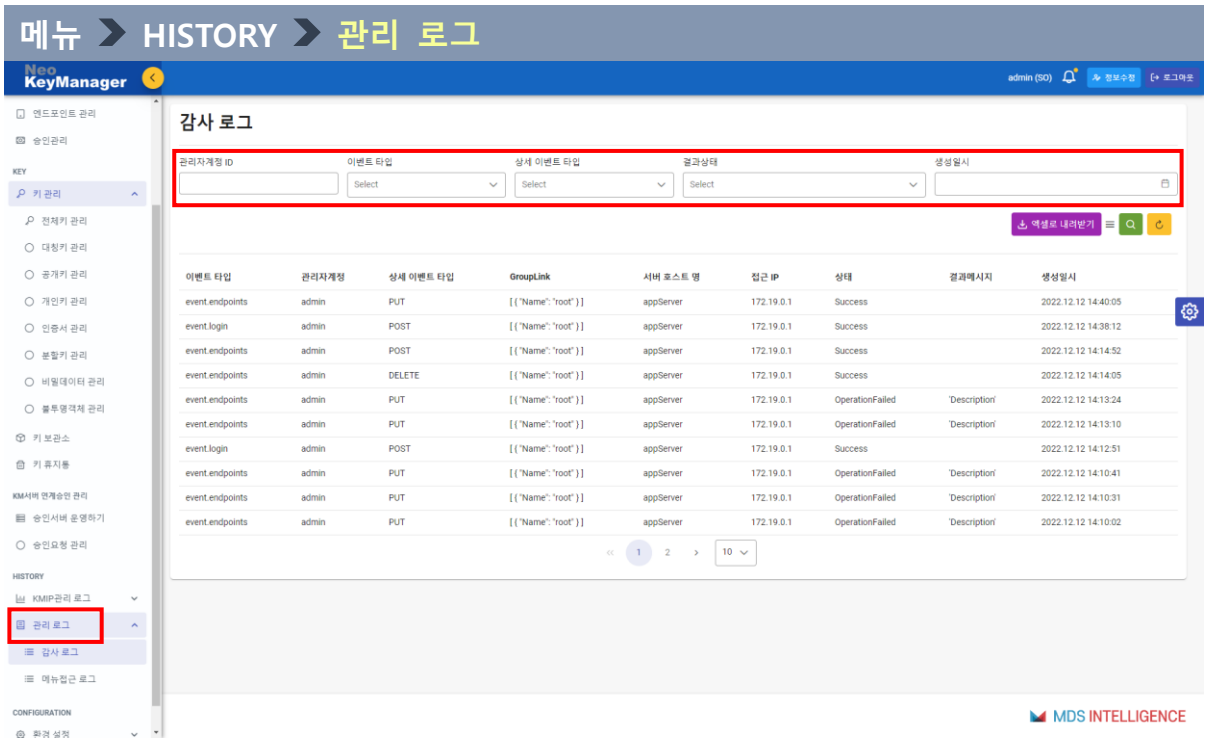


그림 80. 관리 로그 목록 화면

✓ 사용자 별 이벤트 관련 로그 확인 기능 제공 ✓ 관리자계정 ID, 이벤트 타입(관리자계정, 그룹, 엔드포인트 등), 결과 상태 등 확인 가능 ✓ [엑셀로 내려 받기] 탭을 통해 엑셀파일로 로그 정보 제공 기능	
관리자 계정 ID	- 조회하고자 하는 관리자 계정 ID 입력
이벤트 타입	- 관리자계정, 그룹, 엔드포인트, 승인 중 선택
상세 이벤트 타입	- POST, PUT, DELETE 중 선택
결과상태	- Success, OperationFailed 중 선택
생성일시	- 로그 생성일시를 설정하여 해당 기간의 로그 조회

(1) 감사 로그

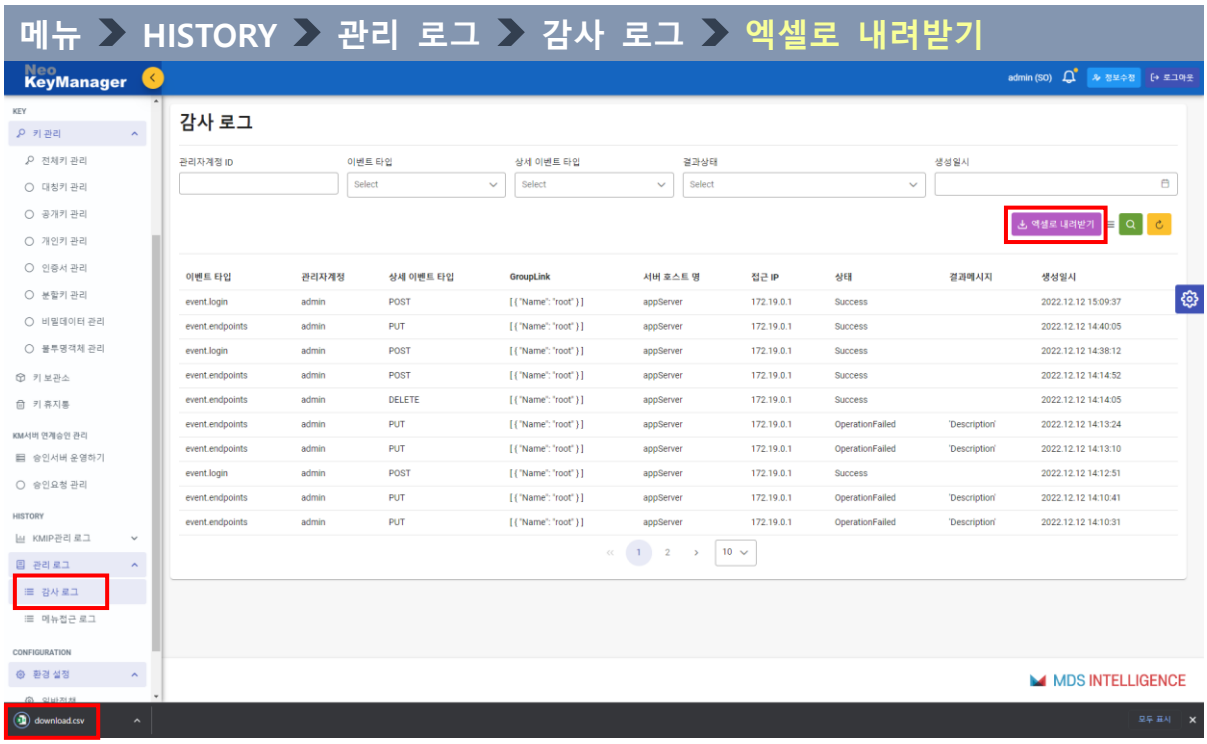


그림 81. 감사 로그 엑셀로 내려 받기 화면

✓ [엑셀로 내려받기] 클릭을 통해 관리자계정, 상세 이벤트, GroupLink 정보 등이 포함된 엑셀파일로 내려받기 가능

(2) 메뉴 접근 로그

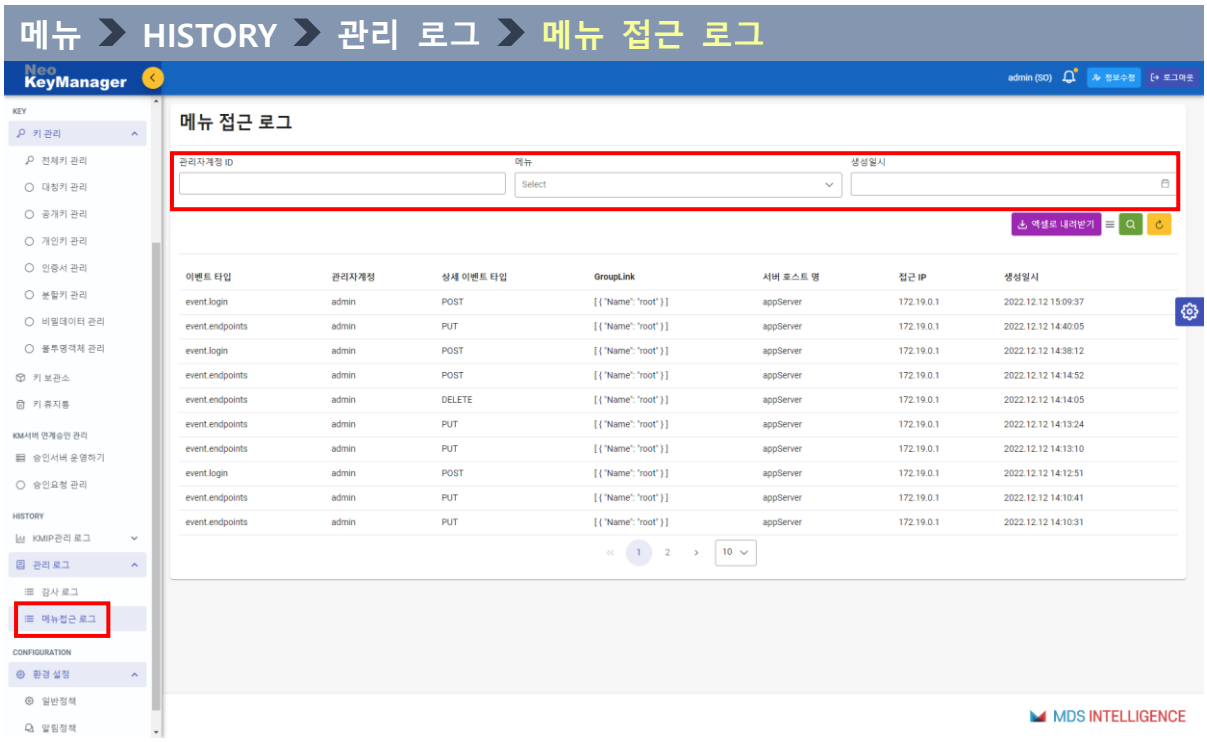


그림 82. 메뉴 접근 로그 화면

✓ 관리자 계정에서 메뉴에 접근한 이력 기능 제공 ✓ 관리자계정 ID, 메뉴, 결과 상태 등을 설정하여 메뉴 접근 로그 확인 ✓ [엑셀로 내려 받기] 탭을 통해 엑셀파일로 로그 정보 제공 기능	
관리자 계정 ID	- 조회하고자 하는 관리자 계정 ID 입력
메뉴	- 계정, 그룹, 엔드포인트, 승인 중 선택
생성 일시	- 로그 생성일시를 설정하여 해당 기간의 메뉴 접근 로그 조회

① 엑셀로 내려받기

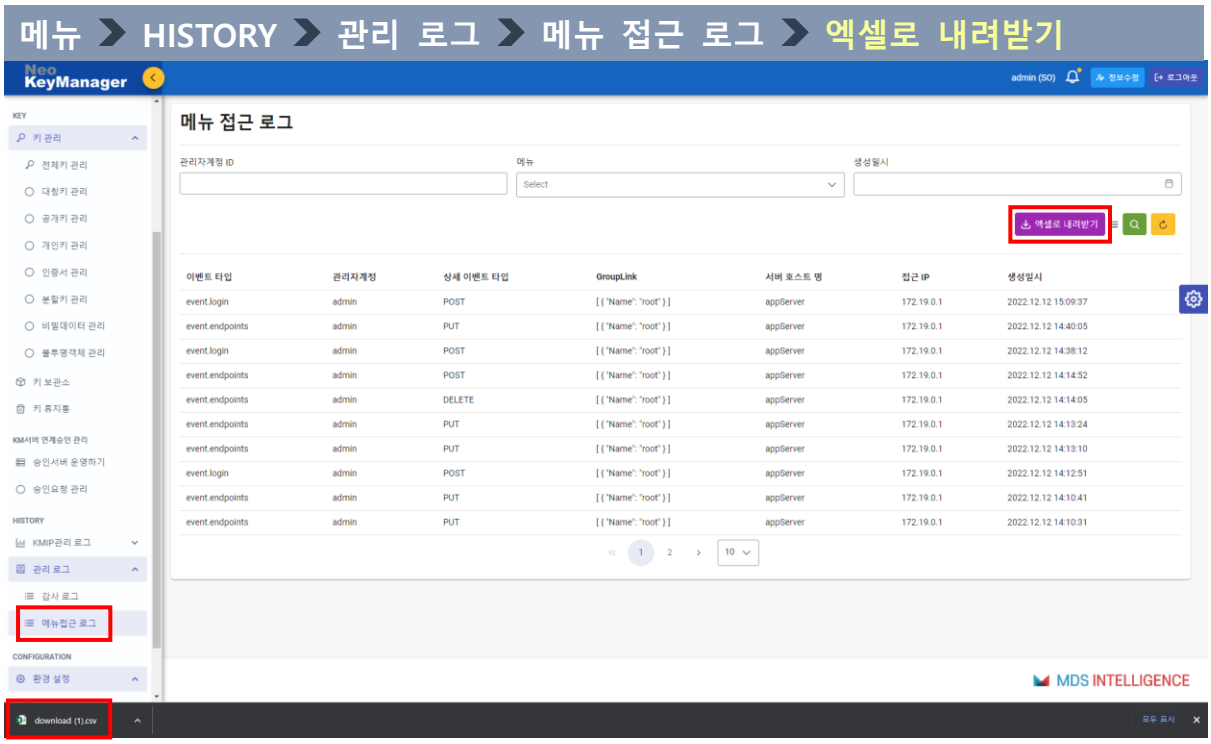


그림 83. 메뉴 접근 로그를 엑셀로 내려 받기

✓ [엑셀로 내려 받기] 클릭을 통해 관리자계정, 상세 이벤트, GroupLink 정보 등이 포함된 엑셀파일로 내려받기 가능

6. CONFIGURATION

1) 환경 설정

(1) 일반 정책

그림 84. 일반정책 화면

- ✓ 관리 웹에 대한 접근 보안 정책 설정
- ✓ 이메일을 통한 알림 전송을 위한 SMTP 서버 설정
- ✓ 라이선스 정보 확인을 위한 라이선스 정책

① 접근 보안 정책

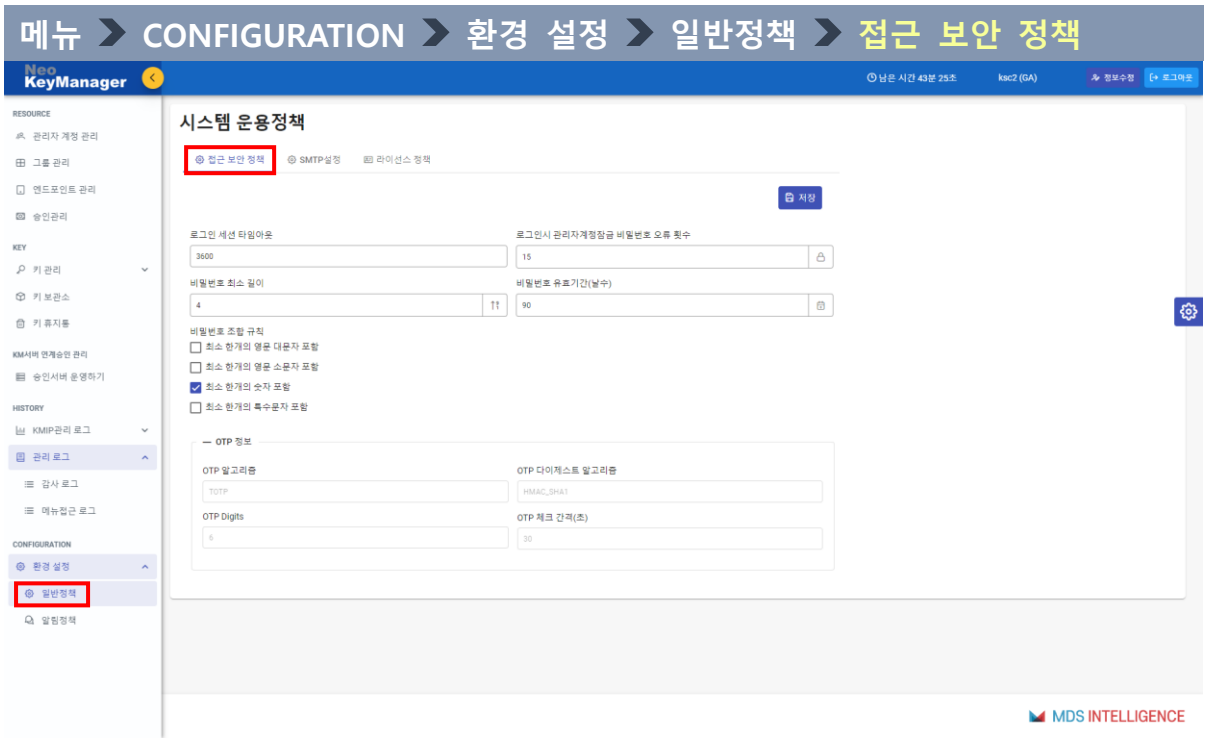


그림 85. 접근 보안 정책 화면

✓ 관리자 계정에 대한 접근 보안 정책 설정	
로그인 세션 타임아웃	- 로그인 세션 타임아웃 시간(초) 설정
로그인 시 관리자계정 잠금 비밀번호 오류 횟수	- 로그인 시 잠금 비밀번호 오류 횟수 설정
비밀번호 최소 길이	- 비밀번호 최소 길이 설정
비밀번호 유효기간(날수)	- 비밀번호 유효기간 설정
비밀번호 조합 규칙	- 비밀번호 조합 규칙 선택 - 영대소문자, 숫자, 특수문자 중 다중 선택 가능

② SMTP설정

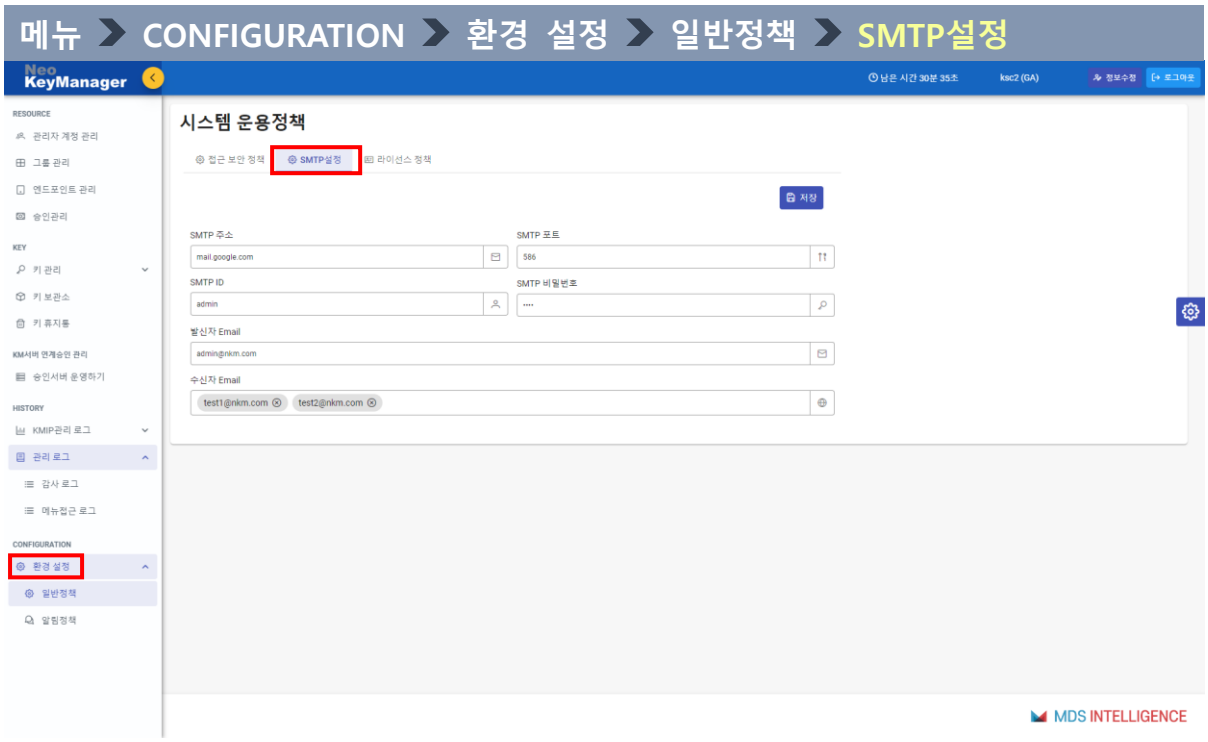


그림 86. SMTP 설정 화면

✓ 이메일을 통한 알림을 전송하기 위한 SMTP 서버 설정	
SMTP 주소	- SMTP 서버 주소 - 자체 보유 SMTP Sever 또는 Public SMTP Server 주소 지정
SMTP 포트	- SMTP 서버 포트
SMTP ID	- 지정된 SMTP 서버에서 사용 가능한 아이디(이메일 주소 입력)
SMTP 비밀번호	- SMTP 사용자 아이디의 패스워드
발신자 Email	- 발신자 Email 입력
수신자 Email	- 수신자 Email 입력

③ 라이선스 정책

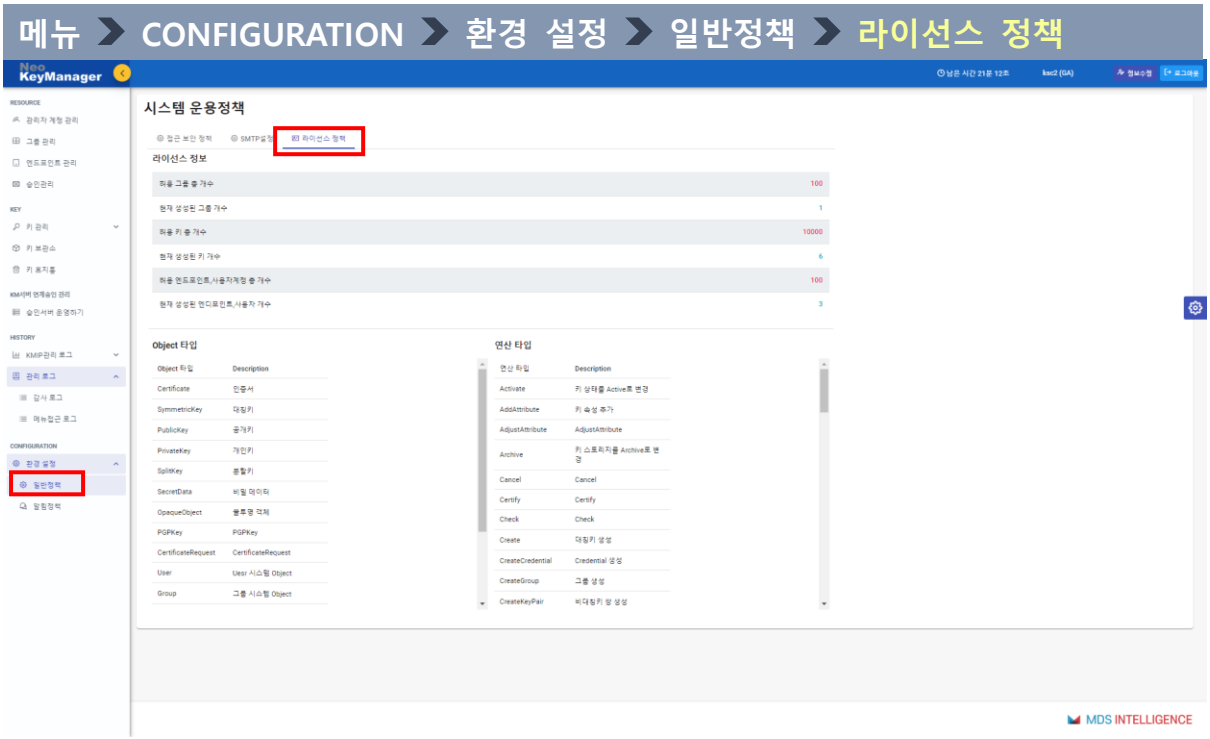


그림 87. 라이선스 정책 화면

- ✓ 허용된 그룹과 키, 엔드포인트의 총 개수 등의 라이선스 정보 확인
- ✓ 현재 생성된 그룹과 키, 엔드포인트 개수 등의 사용현황 확인
- ✓ 지원하고 있는 Object 타입 및 연산 타입 정보

(2) 알림정책

① 알림정책 등록관리

그림 88. 알림 정책 생성 화면

✓ 알림정책 설정을 통해 원하는 알림을 수신할 수 있음.	
알림정책 구분	- 키속성 변경, 키 만료, 연계승인, 내부승인 알림 중 선택
알람정책 명	- 알림정책 명 입력
수신 클라이언트 선택	- 수신 클라이언트 선택 - 알림 수신 클라이언트 등록관리에서 사전 등록 필수
설명	- 해당 알림정책에 대한 부가 설명 입력

② 알림 수신 클라이언트 등록관리

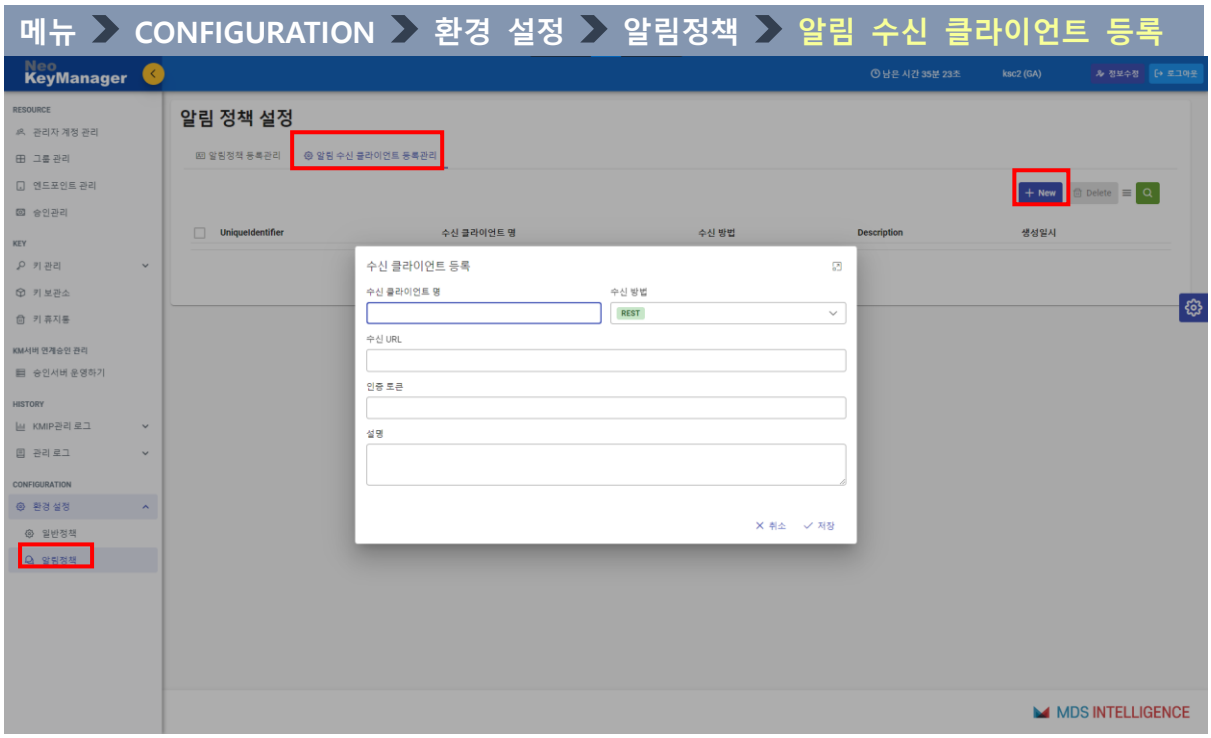


그림 89. 수신 클라이언트 등록 화면

✓ 알림을 수신하고자 하는 클라이언트 등록	
수신 클라이언트 명	- 수신 클라이언트 명 입력
수신 방법	- REST와 EMAIL 중 선택
수신 URL	- 수신 방법으로 REST를 선택한 경우, 수신 URL 입력
수신 Email	- 수신 방법으로 EMAIL을 선택한 경우, 수신 Email 주소를 입력
참조 Email	- 수신 방법으로 EMAIL을 선택한 경우, 참조 Email 주소를 입력
설명	- 수신 클라이언트에 대한 부가 설명 입력

* 약어 및 용어 해설

용어	설명
AES (Advanced Encryption Standard)	미국 표준 기술 연구소(NIST)에 의해 제정된 대칭키 암호화 방식
ARIA (Academy, Research Institute, Agency)	경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 국산 범용 블록 암호 알고리즘
CBC (Cipher Block Chaining Mode)	대칭키 암호의 운용 모드 중 하나로서 순차적으로 암호화하는 구조이며 암호문 블록을 체인처럼 연결시켜 사용
CMS (Cash Management Service)	금융 관리 서비스
DES (Data Encryption Standard)	블록 암호의 일종으로 미국 NBS(National Bureau of Standards, 현재 NIST)에서 국가 표준으로 지정된 대칭키 암호 알고리즘
DES3 (Triple DES)	각 데이터 블록에 데이터 암호화 알고리즘(DES)을 세 번 적용한 삼중 데이터 암호화 알고리즘
DSA (Digital Signature Algorithm)	이산대수 문제에 대한 공용키 암호를 이용하는 ElGamal 알고리즘을 이용하여 NIST(미국립표준기술연구소)에서 개발한 전자서명 방식
EC (Elliptic Curve)	타원 곡선 암호화 알고리즘을 이용한 공개키 암호 방식 RSA와 같은 기존 공개키 암호 방식에 비해 짧은 키를 사용하면서도 그와 비슷한 수준의 안정성을 제공하는 장점이 있고, 특히 무선 환경과 같이 전송량과 계산량이 상대적으로 열악한 환경에 적합
ECB (Electric Code Book Mode)	대칭키 암호의 운용 모드 중 하나로서 블록 단위로 병렬 처리 암·복호화가 가능한 구조
ECDSA (Elliptic Curve Digital Signature Algorithm)	타원 곡선을 이용한 전자서명 알고리즘 공개키의 크기는 DSA의 절반이고, 서명의 크기는 DSA와 동일 (80비트 보안 수준을 위해 160비트의 공개키와 320비트의 서명이 필요)
EMV (Europay, MasterCard, Visa)	유로페이, 마스터카드, 비자카드 등 3대 신용카드 프로세싱 회사가 공동으로 제정한 IC카드 관련 기기 국제기술 표준
HA (High Availability)	고가용성 서버와 네트워크, 프로그램 등의 정보 시스템이 상당히 오랜 기간 동안 지속적으로 정상 운영이 가능한 성질
HSM (Hardware Security Module)	암호화 키 수명 주기 보호를 위해 설계된 하드웨어 보안 모듈
IV (Initialization Vector)	첫 블록을 암호화할 때 사용하는 값
KCV (Key Check Value)	암호키의 무결성 검사를 위한 함수
KEK (Key Encryption Key)	키를 암호화하기 위한 암호키
KMIP (Key Management Interoperability Protocol)	안전한 키 관리를 위하여 국제 표준 단체인 OASIS에 의해 제정된 키 관리 상호 운용성 프로토콜
MAC (Message Authentication Code)	메시지 인증에 사용되는 일련 단위의 정보 (일반적으로 해시 알고리즘을 사용)
OCS (Operation Card Set)	HSM 운용을 위한 스마트카드
PKCS5 (Public Key Cryptography Standard)	RSA PKCS 표준 중 하나로서 8Byte 블록 암호 기반 알고리즘에서 주로 사용 입력이 암호 블록 사이즈인 8Byte(고정 길이)의 배수와 맞지 않으면, 배수에 맞춰 빈 공간을 채워 주는 방법(패딩)

RSA (Ron Rivest, Adi Shamir and Leonard Adleman)	공개키 암호 시스템의 하나로서 암호화 뿐만 아니라 전자서명이 가능한 최초의 알고리즘
SEED	전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 02월 한국인터넷진흥원과 국내 암호 전문가들이 국내 기술로 개발한 128비트 블록 암호 알고리즘
핑거프린트	발급된 인증서에 대한 해시 정보로 인증서 전체 메시지에 대해 해시 값을 생성하여 인증서 중복 사용 검증, 무결성 제공 등의 용도로 사용됨