비정형데이터 암호솔루션

# CryptoSwell 매뉴얼

Blueswell (주)블루쉘
www.blueswell.kr

# 목 차

제 1 장. CryptoSwell 개요

제 2 장. CryptoSwell 실행

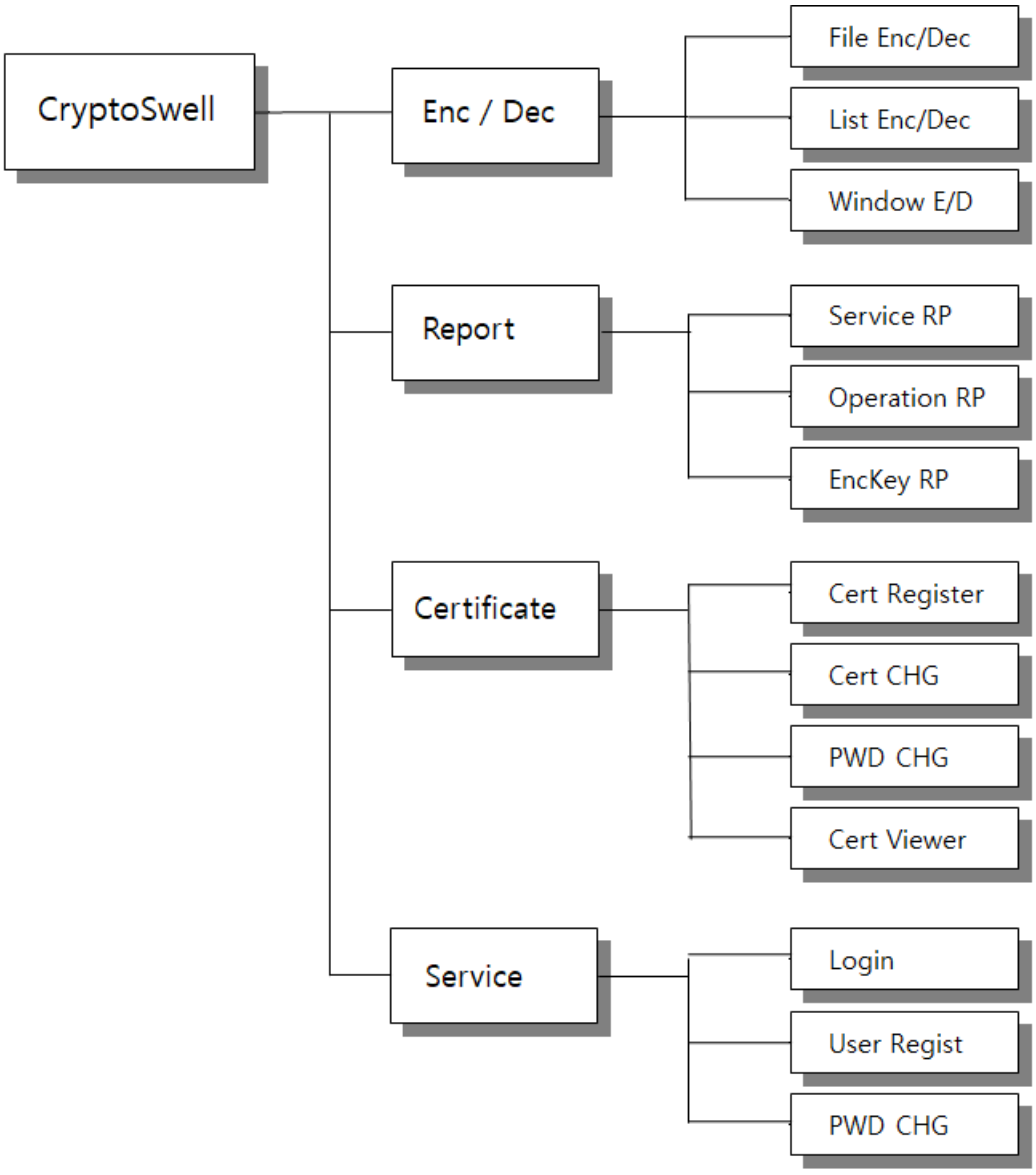
제 3 장. Log File

제 4 장. 메뉴 상세 설명

# 제 1 장 CryptoSwell 개요

CryptoSwell은 client와 Server로 구성되어 있으며, 비정형데이터(문서파일, 이미지, 동영상 등)를 암호하는 솔루션입니다. 암호에 사용되는 암호키를 관리하고, 서비스 이력과 관리자의 운영을 모두 로그로 저장합다.

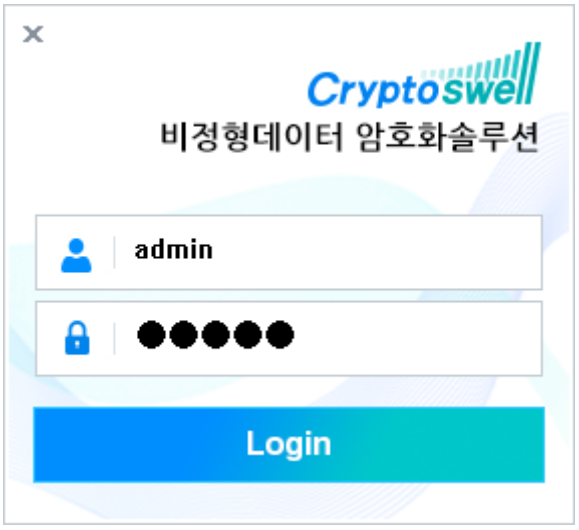
## ▪ 메뉴구성



# 제 2 장 CryptoSwell 실행

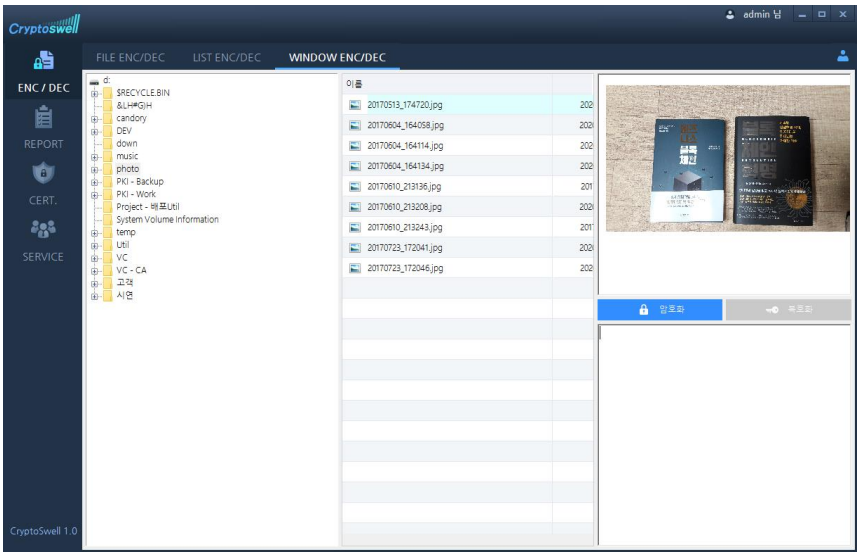
## 1. CryptoSwell 실행

가. 윈도우의 시작->프로그램-> CryptoSwell ->CryptoSwell Client를 클릭합니다.




나. ID와 Password를 입력합니다.

다. Login 버튼을 클릭합니다.



## 2. CryptoSwell Server 실행

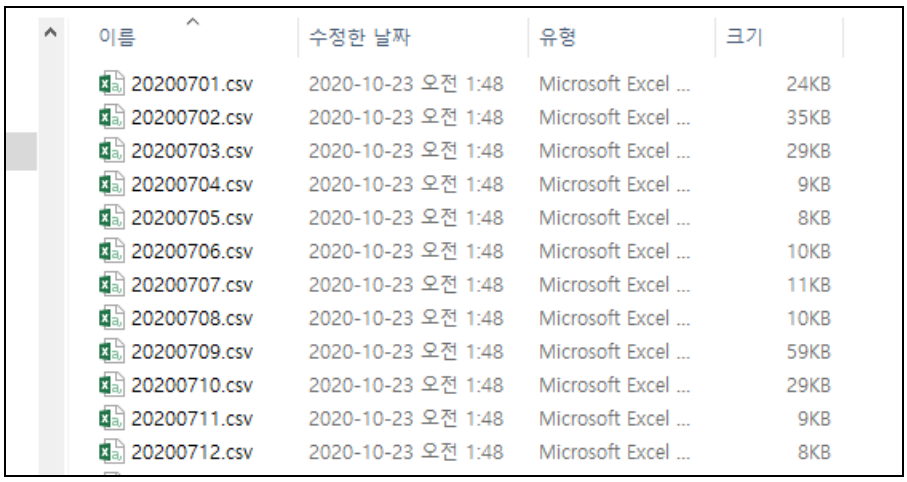
가. 프로그램을 설치하면 CryptoSwell Server는 자동실행 됨

나. 버튼을 누르면 “TrayIcon”으로 동작

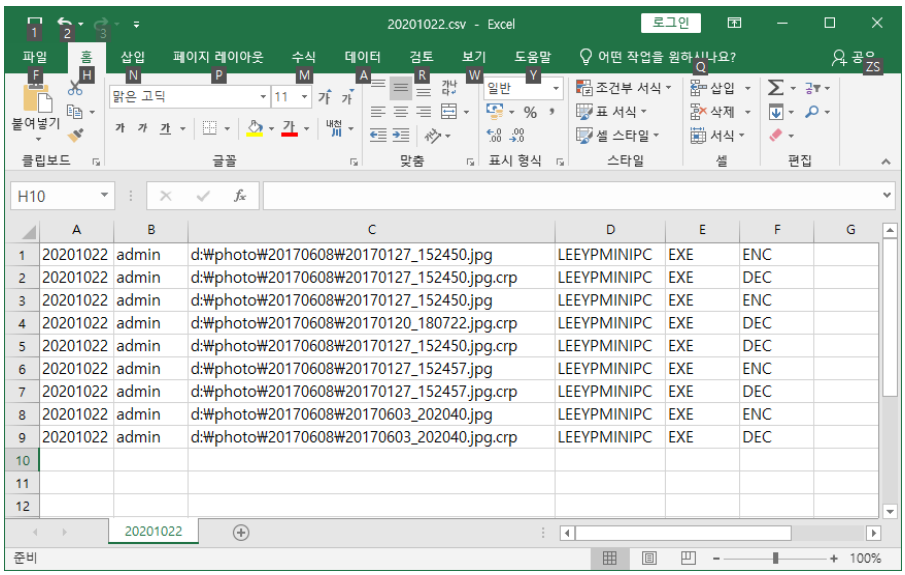
# 제 3 장 LOG File

## 1. Service Log

- 이름 : “년월일.csv” 예) “20201022.csv”
- 위치 : Server 설치된 폴더 밑에 “log”라는 디렉토리에 있음
- 용도 : 암호, 복호한 내역을 저장
- 생성 : Client에서 비정형데이터를 암호, 복호할 때마다 생성
- 내용 : Time, file name, Client, Type(Enc, Dec), Tool(API, exe), PC Name



| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| 20200701.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 24KB |
| 20200702.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 35KB |
| 20200703.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 29KB |
| 20200704.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 9KB |
| 20200705.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 8KB |
| 20200706.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200707.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 11KB |
| 20200708.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200709.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 59KB |
| 20200710.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 29KB |
| 20200711.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 9KB |
| 20200712.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 8KB |

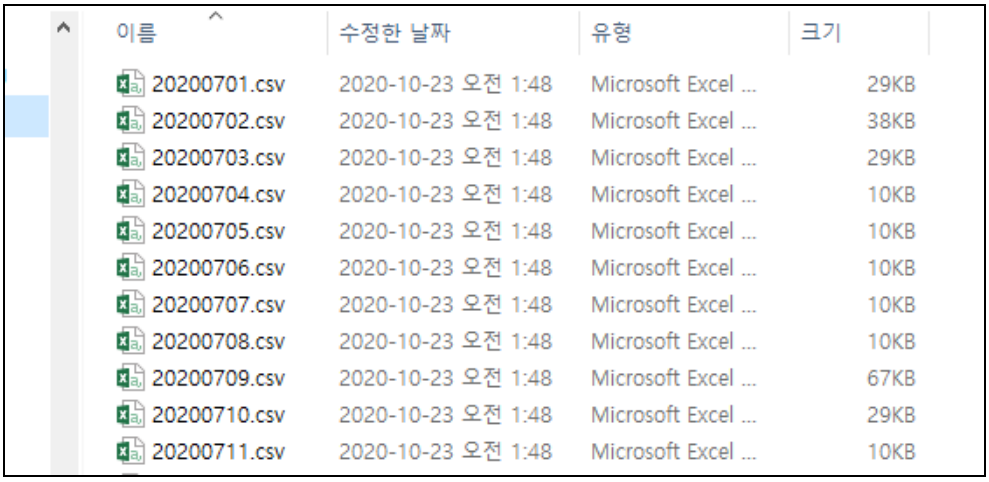


20201022.csv - Excel

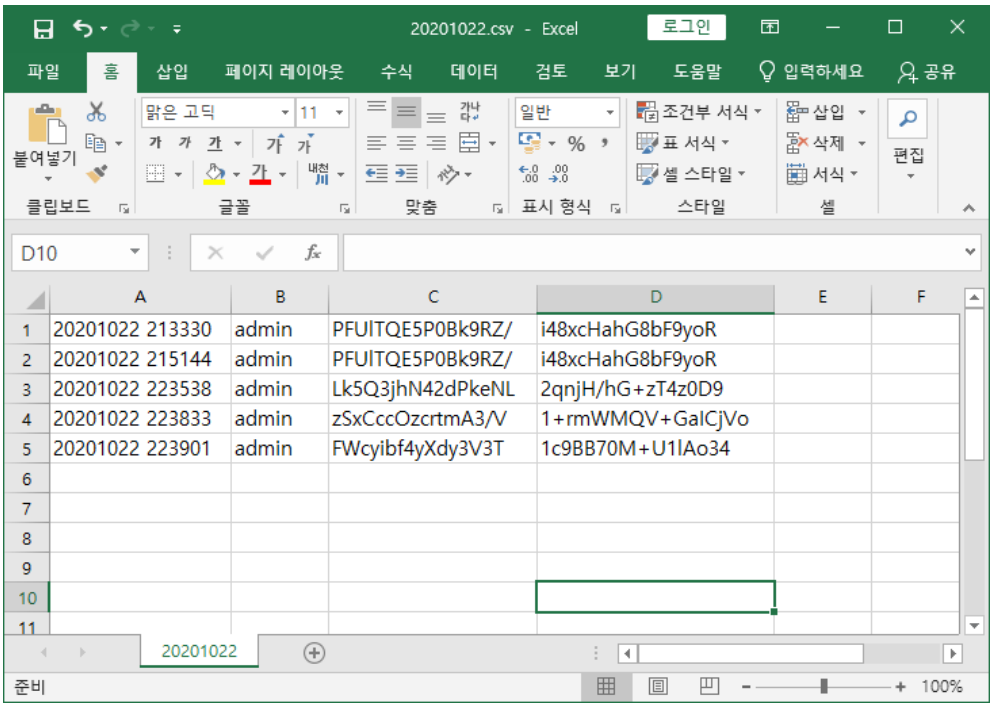
| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | 20201022 | admin | d:₩photo₩20170608₩20170127_152450.jpg | LEEYPMINIPC | EXE | ENC | |
| 2 | 20201022 | admin | d:₩photo₩20170608₩20170127_152450.jpg.crp | LEEYPMINIPC | EXE | DEC | |
| 3 | 20201022 | admin | d:₩photo₩20170608₩20170127_152450.jpg | LEEYPMINIPC | EXE | ENC | |
| 4 | 20201022 | admin | d:₩photo₩20170608₩20170120_180722.jpg.crp | LEEYPMINIPC | EXE | DEC | |
| 5 | 20201022 | admin | d:₩photo₩20170608₩20170127_152450.jpg.crp | LEEYPMINIPC | EXE | DEC | |
| 6 | 20201022 | admin | d:₩photo₩20170608₩20170127_152457.jpg | LEEYPMINIPC | EXE | ENC | |
| 7 | 20201022 | admin | d:₩photo₩20170608₩20170127_152457.jpg.crp | LEEYPMINIPC | EXE | DEC | |
| 8 | 20201022 | admin | d:₩photo₩20170608₩20170603_202040.jpg | LEEYPMINIPC | EXE | ENC | |
| 9 | 20201022 | admin | d:₩photo₩20170608₩20170603_202040.jpg.crp | LEEYPMINIPC | EXE | DEC | |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |

## 2. Crypt Key Log

- 이름 : “년월일.csv” 예) “20201022.csv”
- 위치 : Server 설치된 폴더 밑에 “key”라는 디렉토리에 있음
- 용도 : Server가 Client에 내려 보낸 암호키를 저장
- 생성 : Client에서 암호키를 요청할 때 키를 보내고, 로그 저장
- 내용 : Time, Client, Encrypted CryptKey and Vector



| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| 20200701.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 29KB |
| 20200702.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 38KB |
| 20200703.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 29KB |
| 20200704.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200705.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200706.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200707.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200708.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |
| 20200709.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 67KB |
| 20200710.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 29KB |
| 20200711.csv | 2020-10-23 오전 1:48 | Microsoft Excel ... | 10KB |

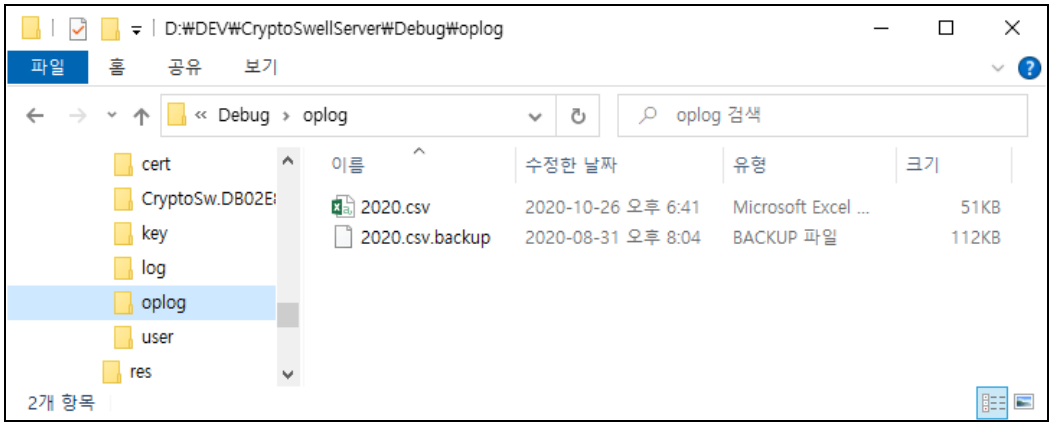


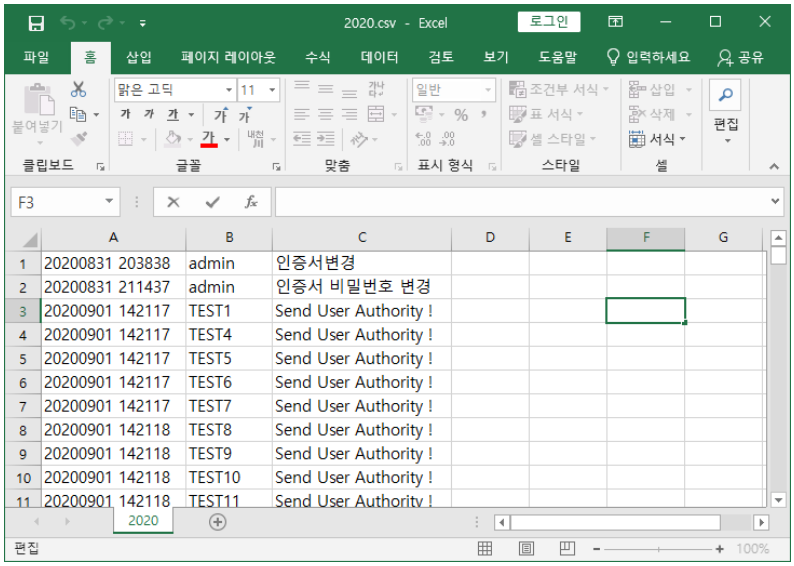
20201022.csv - Excel

| | A | B | C | D |
|---|---|---|---|---|
| 1 | 20201022 213330 | admin | PFUlTQE5P0Bk9RZ/ | i48xcHahG8bF9yoR |
| 2 | 20201022 215144 | admin | PFUlTQE5P0Bk9RZ/ | i48xcHahG8bF9yoR |
| 3 | 20201022 223538 | admin | Lk5Q3jhN42dPkeNL | 2qnjH/hG+zT4z0D9 |
| 4 | 20201022 223833 | admin | zSxCccOzcrtmA3/V | 1+rmWMQV+GaICjVo |
| 5 | 20201022 223901 | admin | FWcyibf4yXdy3V3T | 1c9BB70M+U1lAo34 |

## 3. Operation Log

- 이름 : “년.csv” 예) “2020.csv”
- 위치 : Server 설치된 폴더 밑에 “oplog”라는 디렉토리에 있음
- 용도 : 운영자가 운영한 내역을 저장
- 생성 : CryptoSwell을 운영할 때 생성 예) 로그온, 인증서 변경 등
- 저장되는 내용
  1) 운영 : 로그온, 로그오프, 비밀번호변경
  2) 인증서 : 인증서 등록, 변경, 조회, 비밀번호변경
  3) 암호키 : 암호키 생성, 변경, 조회
  4) 사용자 : 등록, 삭제, 변경
  5) 서비스 : 파일 암호/복호, 리스트 암호/복호, 윈도우 암호/복호

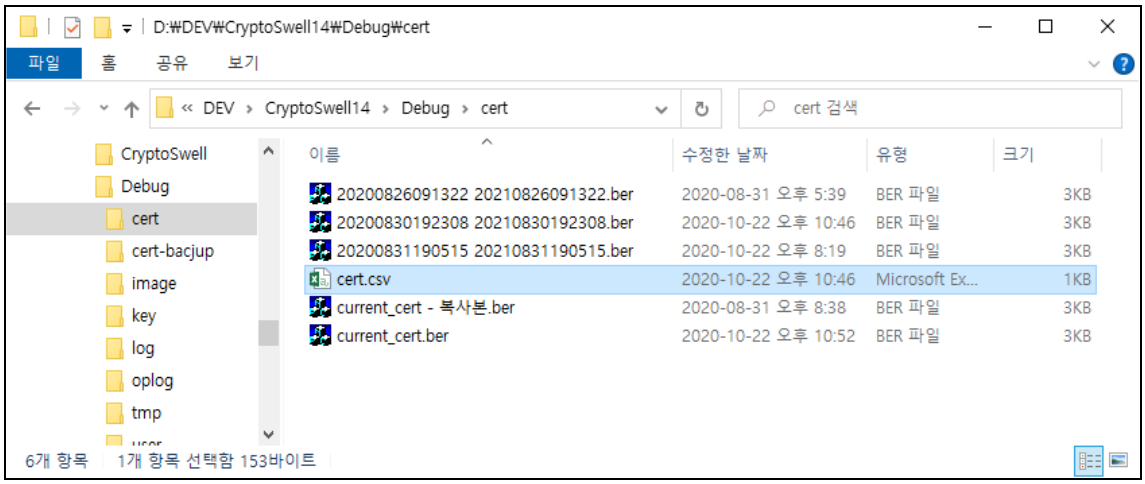


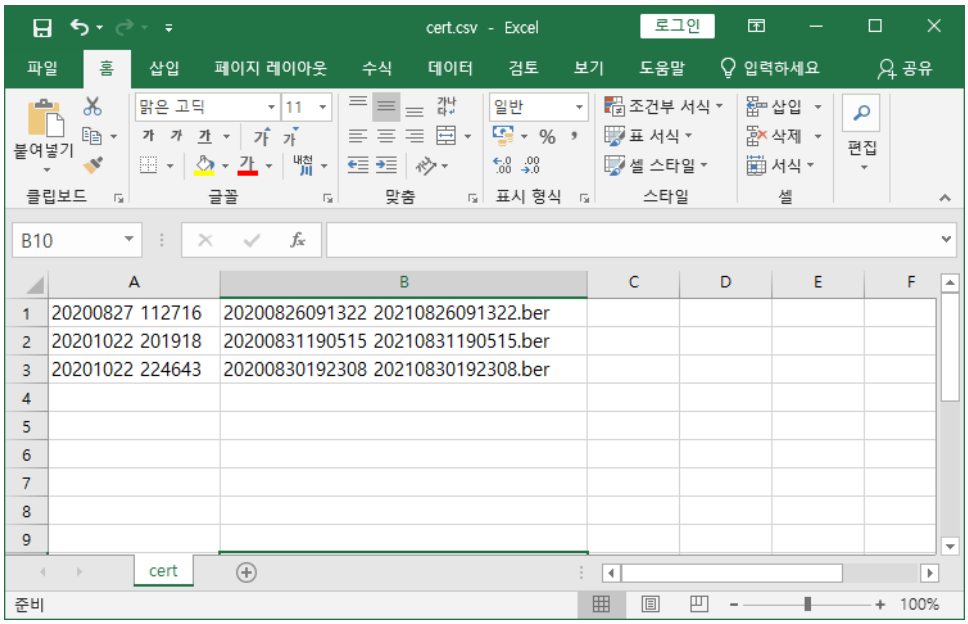



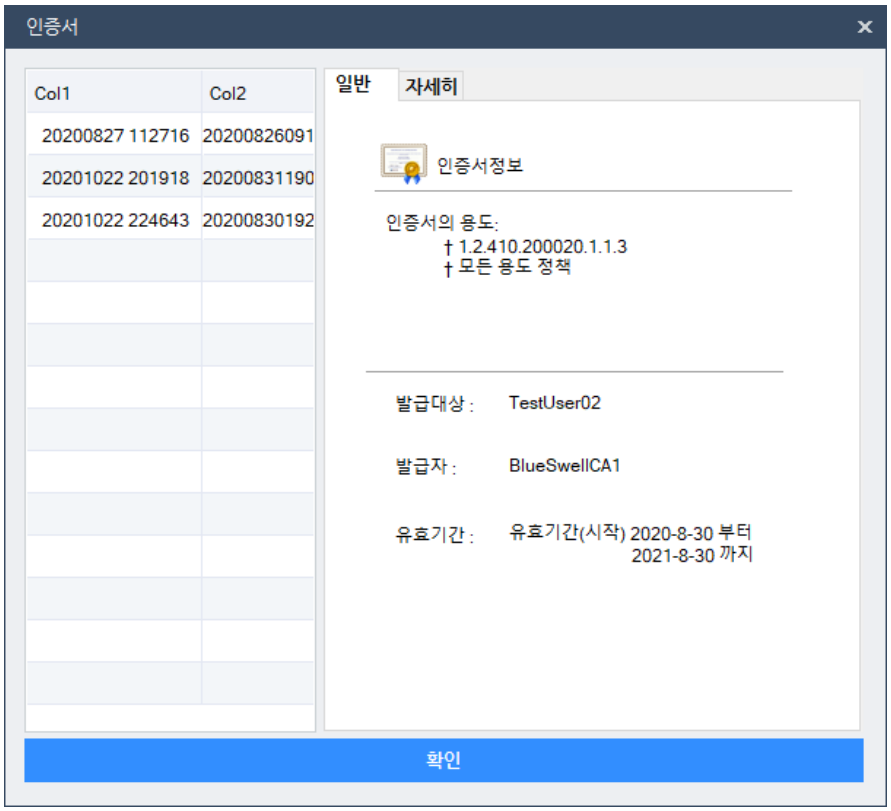

| | A | B | C |
|---|---|---|---|
| 1 | 20200831 203838 | admin | 인증서변경 |
| 2 | 20200831 211437 | admin | 인증서 비밀번호 변경 |
| 3 | 20200901 142117 | TEST1 | Send User Authority ! |
| 4 | 20200901 142117 | TEST4 | Send User Authority ! |
| 5 | 20200901 142117 | TEST5 | Send User Authority ! |
| 6 | 20200901 142117 | TEST6 | Send User Authority ! |
| 7 | 20200901 142117 | TEST7 | Send User Authority ! |
| 8 | 20200901 142118 | TEST8 | Send User Authority ! |
| 9 | 20200901 142118 | TEST9 | Send User Authority ! |
| 10 | 20200901 142118 | TEST10 | Send User Authority ! |
| 11 | 20200901 142118 | TEST11 | Send User Authority ! |

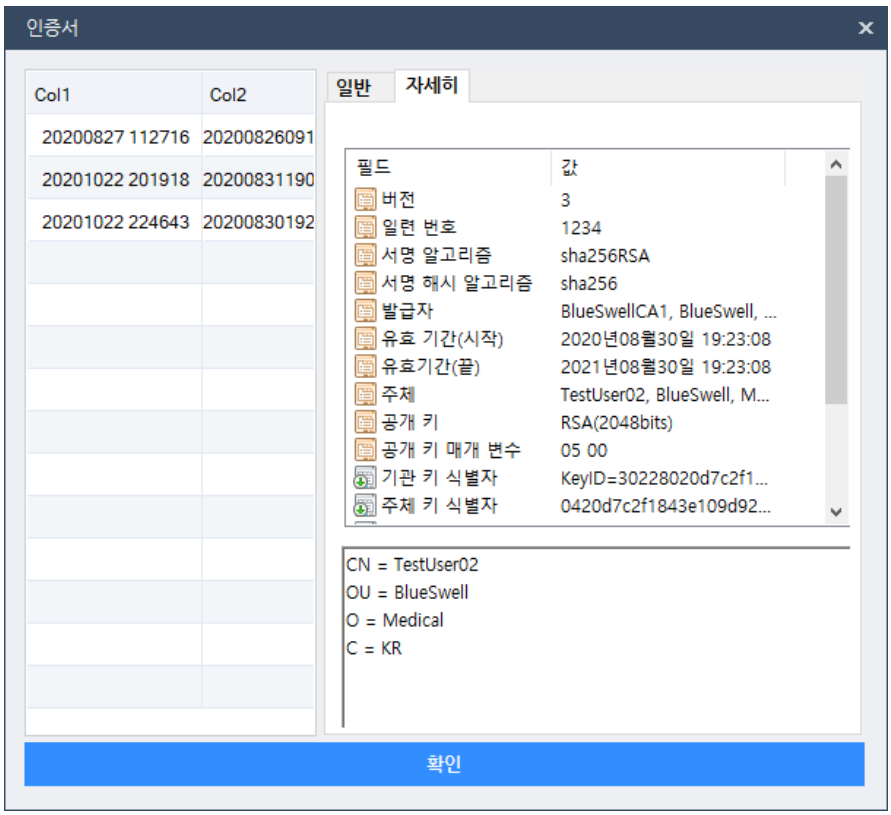
## 4. Certification Log

- 이름
  1) 인증서 변경 이력 : “Cert.csv”
  2) 현재 인증서 : “current_cert.ber
  3) 지난 인증서 : “유효기간시작일_유효기간종료일.ber”
     예) 20200831190515 20210831190515.ber
- 위치 : Server 설치된 폴더 밑에 “cert”라는 디렉토리에 있음
- 용도 : 운영자가 인증서를 변경한 내역을 저장
- 생성 : 인증서를 변경할 때마다 로그와 새로운 인증서 파일이 생성



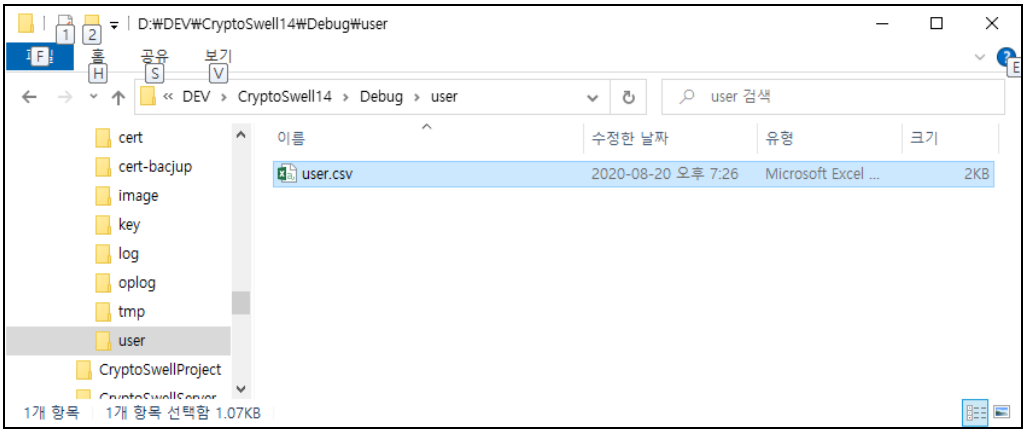



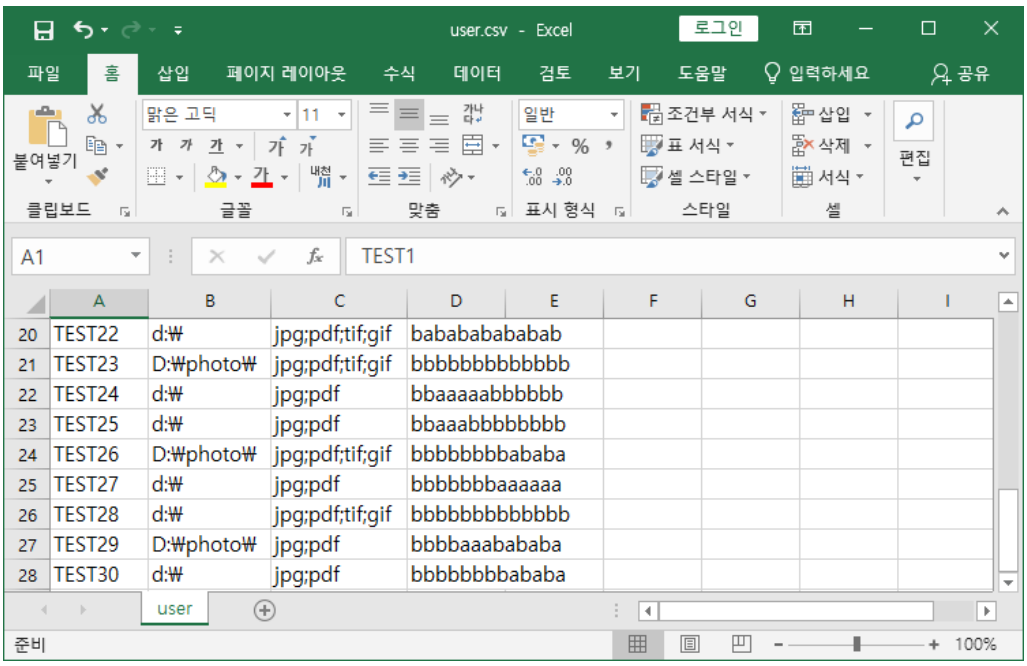

인증서
Col1
Col2
20200827 112716
20200826091
20201022 201918
20200831190
20201022 224643
20200830192
일반
자세히
인증서정보
인증서의 용도:
† 1.2.410.200020.1.1.3
† 모든 용도 정책
발급대상 : TestUser02
발급자 : BlueSwellCA1
유효기간 : 유효기간(시작) 2020-8-30 부터
2021-8-30 까지
확인


인증서
Col1
Col2
20200827 112716
20200826091
20201022 201918
20200831190
20201022 224643
20200830192
일반
자세히
필드
값
버전
3
일련 번호
1234
서명 알고리즘
sha256RSA
서명 해시 알고리즘
sha256
발급자
BlueSwellCA1, BlueSwell, ...
유효 기간(시작)
2020년08월30일 19:23:08
유효기간(끝)
2021년08월30일 19:23:08
주체
TestUser02, BlueSwell, M...
공개 키
RSA(2048bits)
공개 키 매개 변수
05 00
기관 키 식별자
KeyID=30228020d7c2f1...
주체 키 식별자
0420d7c2f1843e109d92...
CN = TestUser02
OU = BlueSwell
O = Medical
C = KR
확인

## 5. User File

- 이름 : “년.csv” 예) “2020.csv”
- 위치 : Server 설치된 폴더 밑에 “oplog”라는 디렉토리에 있음
- 용도 : 운영자가 운영한 내역을 저장
- 생성 : CryptoSwell을 운영할 때 생성 예) 로그온, 인증서 변경 등
- 저장되는 내용




| | A | B | C | D |
|---|---|---|---|---|
| 20 | TEST22 | d:₩ | jpg;pdf;tif;gif | babababababab |
| 21 | TEST23 | D:₩photo₩ | jpg;pdf;tif;gif | bbbbbbbbbbbbb |
| 22 | TEST24 | d:₩ | jpg;pdf | bbaaaaabbbbbb |
| 23 | TEST25 | d:₩ | jpg;pdf | bbaaabbbbbbbb |
| 24 | TEST26 | D:₩photo₩ | jpg;pdf;tif;gif | bbbbbbbbababa |
| 25 | TEST27 | d:₩ | jpg;pdf | bbbbbbbaaaaaa |
| 26 | TEST28 | d:₩ | jpg;pdf;tif;gif | bbbbbbbbbbbbb |
| 27 | TEST29 | D:₩photo₩ | jpg;pdf | bbbbaaabababa |
| 28 | TEST30 | d:₩ | jpg;pdf | bbbbbbbbababa |

# 제 4 장 메뉴 상세 설명

## 1. REPORT

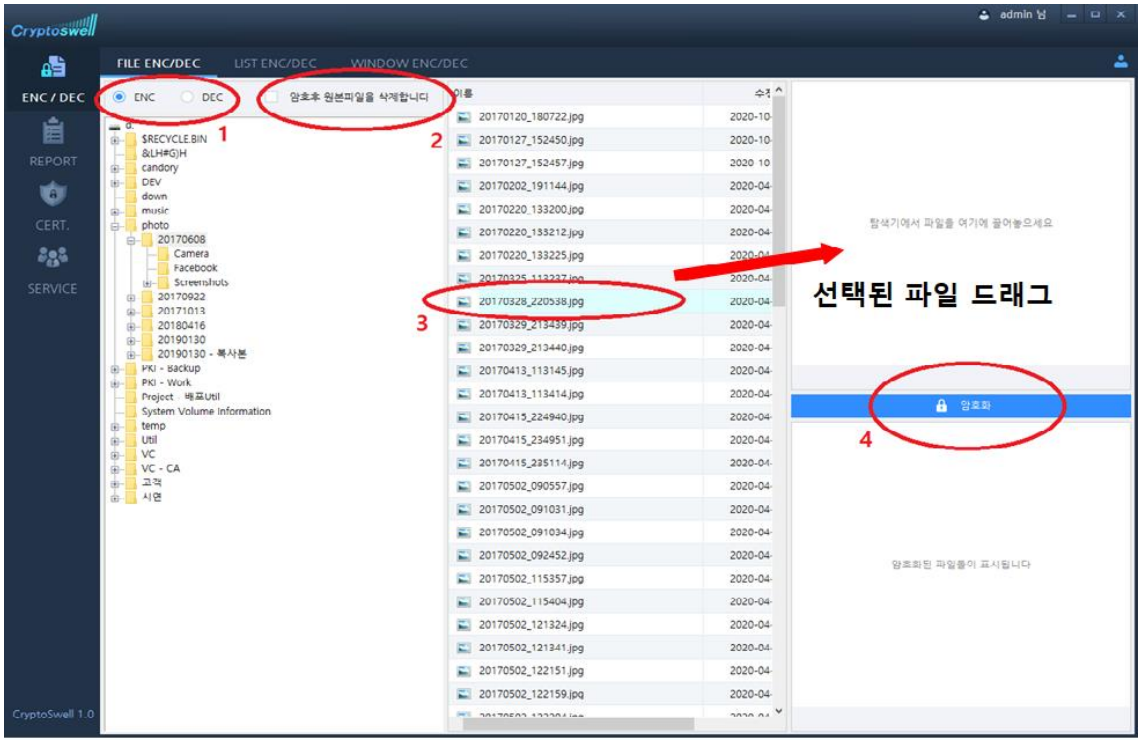
### 1) FILE ENC/DEC

선택한 파일을 암호, 복호합니다.

화면에 CryptoSwell 탐색기에서 파일을 선택하여 암호 또는 복호하면 됩니다.

서비스로그, 암호키로그를 남깁니다.

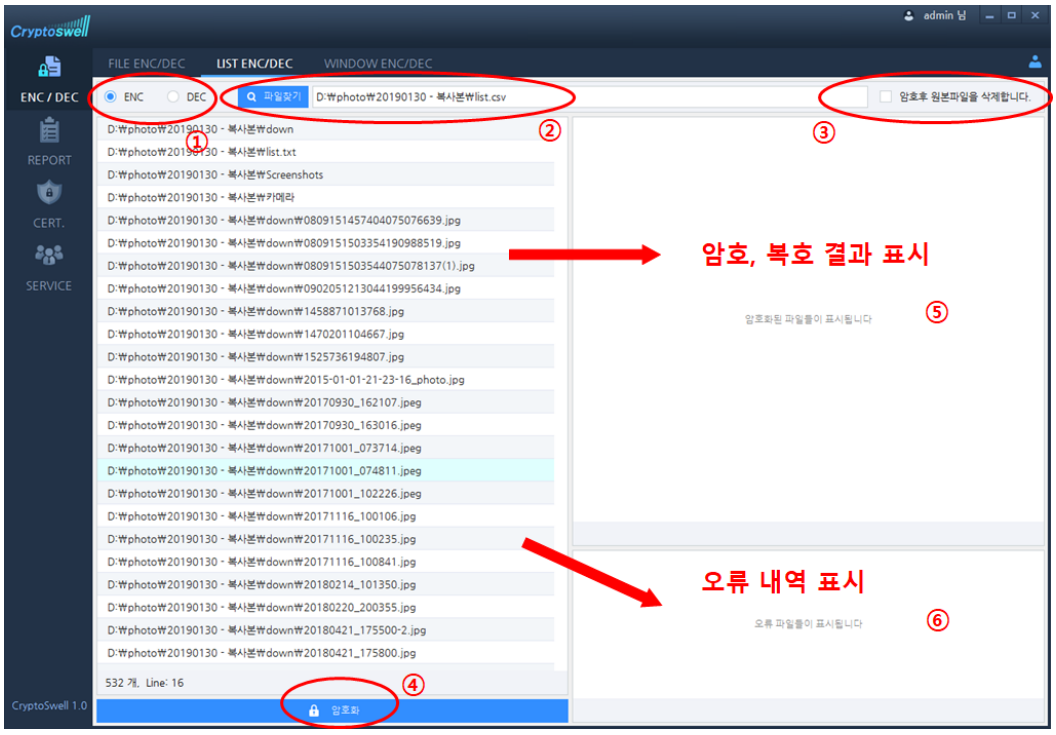
① 암호, 복호 선택
② 암호/복호 후 원본 삭제 선택
③ 선택된 파일 드래그
④ 암호/복호 버튼 클릭 (버튼의 글자는 1번의 선택에 따라 바뀜)



## 2) LIST ENC / DEC

파일리스트를 만들어 파일을 암호, 복호 합니다.
파일은 “.csv” 타입으로 만들어 드래그 하면 됩니다.
서비스로그와 암호키로그를 남깁니다.

① 암호, 복호 선택
② 리스트파일( 예 list.csv ) 선택
③ 원본 삭제 선택
④ 암호, 복호 버튼 클릭




* 리스트 파일 샘플 “list.csv”

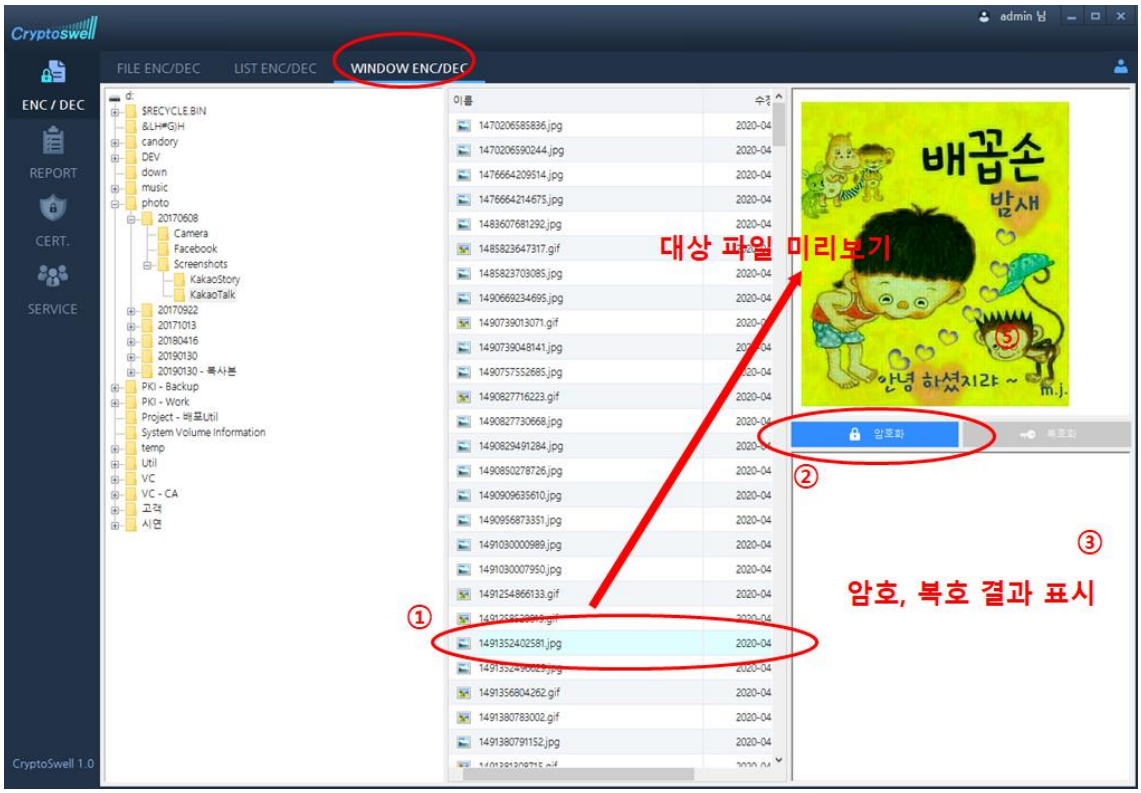
| | A | B |
|---|---|---|
| 1 | 1 | D:₩photo₩20190130 - 복사본₩down |
| 2 | 2 | D:₩photo₩20190130 - 복사본₩list.txt |
| 3 | 3 | D:₩photo₩20190130 - 복사본₩Screenshots |
| 4 | 4 | D:₩photo₩20190130 - 복사본₩카메라 |
| 5 | 5 | D:₩photo₩20190130 - 복사본₩down₩080915145740407507663 9.jpg |
| 6 | 6 | D:₩photo₩20190130 - 복사본₩down₩080915150335419098851 9.jpg |
| 7 | 7 | D:₩photo₩20190130 - 복사본₩down₩080915150354407507813 7(1).jpg |
| 8 | 8 | D:₩photo₩20190130 - 복사본₩down₩090205121304419995643 4.jpg |
| 9 | 9 | D:₩photo₩20190130 - 복사본₩down₩1458871013768.jpg |
| 10 | 10 | D:₩photo₩20190130 - 복사본₩down₩1470201104667.jpg |
| 11 | 11 | D:₩photo₩20190130 - 복사본₩down₩1525736194807.jpg |
| 12 | 12 | D:₩photo₩20190130 - 복사본₩down₩2015-01-01-21-23-16_photo.jpg |

list

## 3) WINDOW ENC / DEC

파일리스트를 만들어 파일을 암호, 복호 합니다.
파일은 “.csv” 타입으로 만들어 드래그 하면 됩니다.
서비스로그와 암호키로그를 남깁니다.

① 파일을 선택. 파일에 따라 암호, 복호가 결정
예) 확장자 “.crp” -> 복호, 나머지 확장자는 암호
② 미리보기에서 확인
③ 암호/복호 버튼 클릭



# 2. REPORT

: 운영 내역을 조회하는 서비스

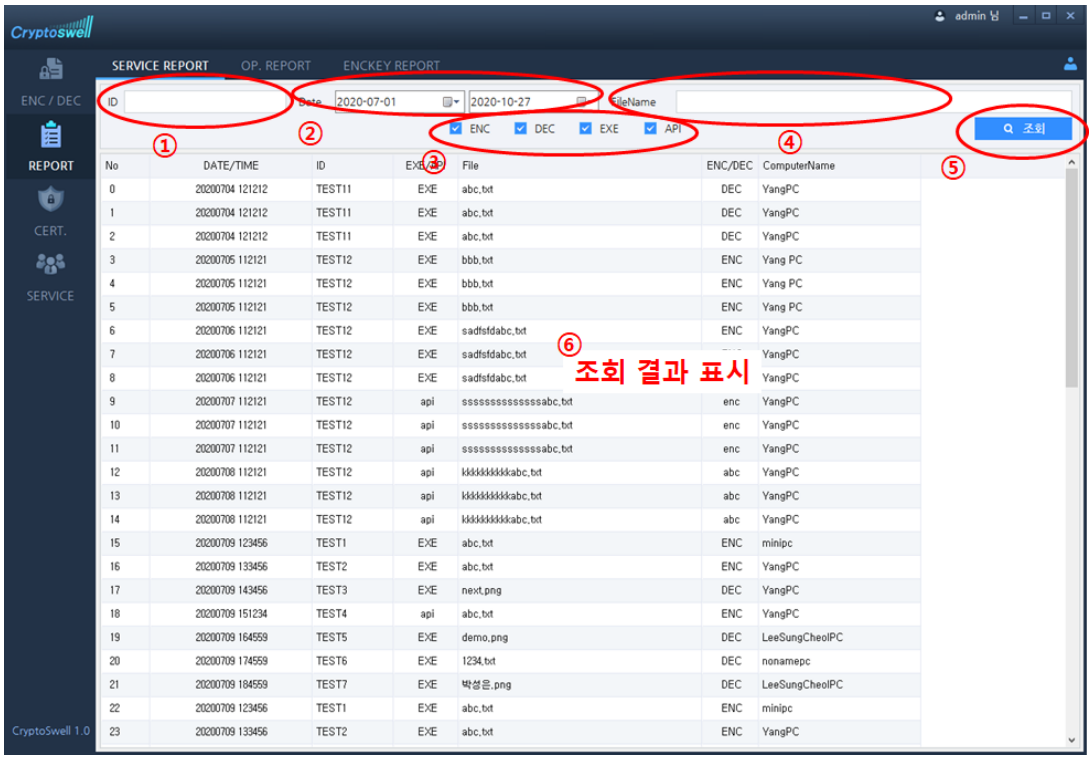
## 1) SERVICE REPORT

암호, 복호 내역을 조회합니다.

검색 조건은 OR 또는 AND 방식으로 추가됩니다.

로그는 “log”디렉토리 밑에 저장되어 있습니다.

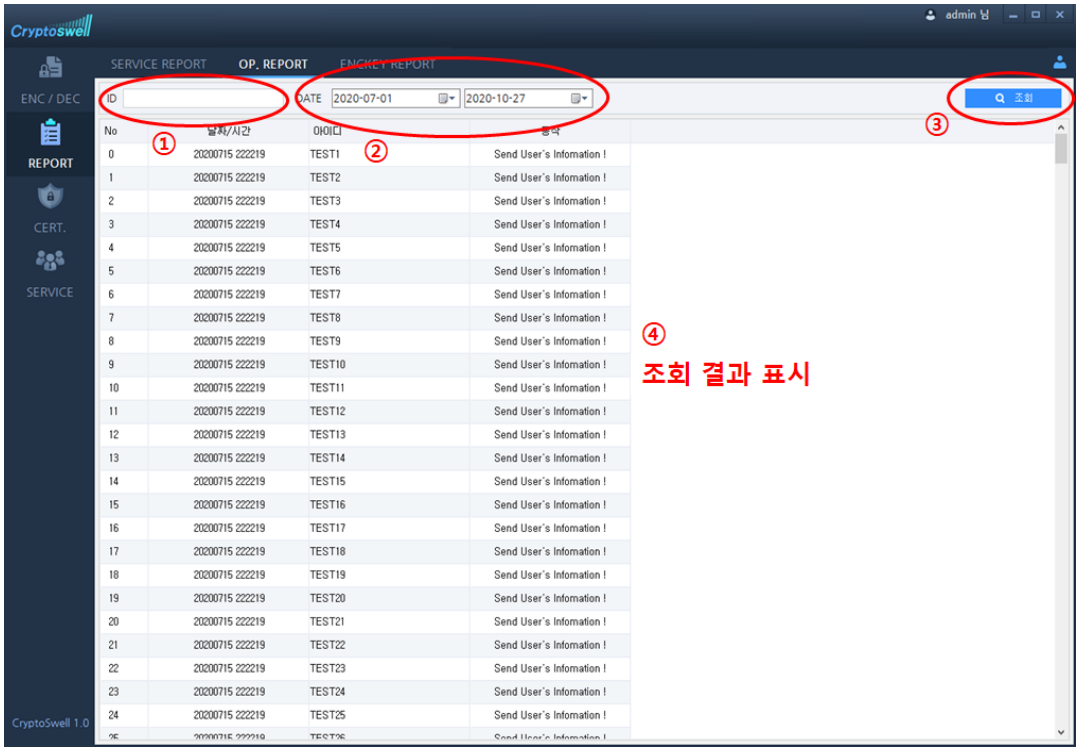
① ID로 암호, 복호 내역 검색
② 날짜로 암호, 복호 내역 검색
③ 검색 조건 선택 : 암호, 복호, EXE, API
④ 파일 이름으로 암호, 복호 내역 검색



## 2) OP. REPORT

Admin 또는 User가 운영한 내역을 조회합니다.
검색 조건은 OR 또는 AND 방식으로 추가됩니다.
로그는 “oplog”디렉토리 밑에 저장되어 있습니다.

① ID로 운영 내역 조회
② 날짜로 운영 내역 조회



## 3) ENCKEY REPORT

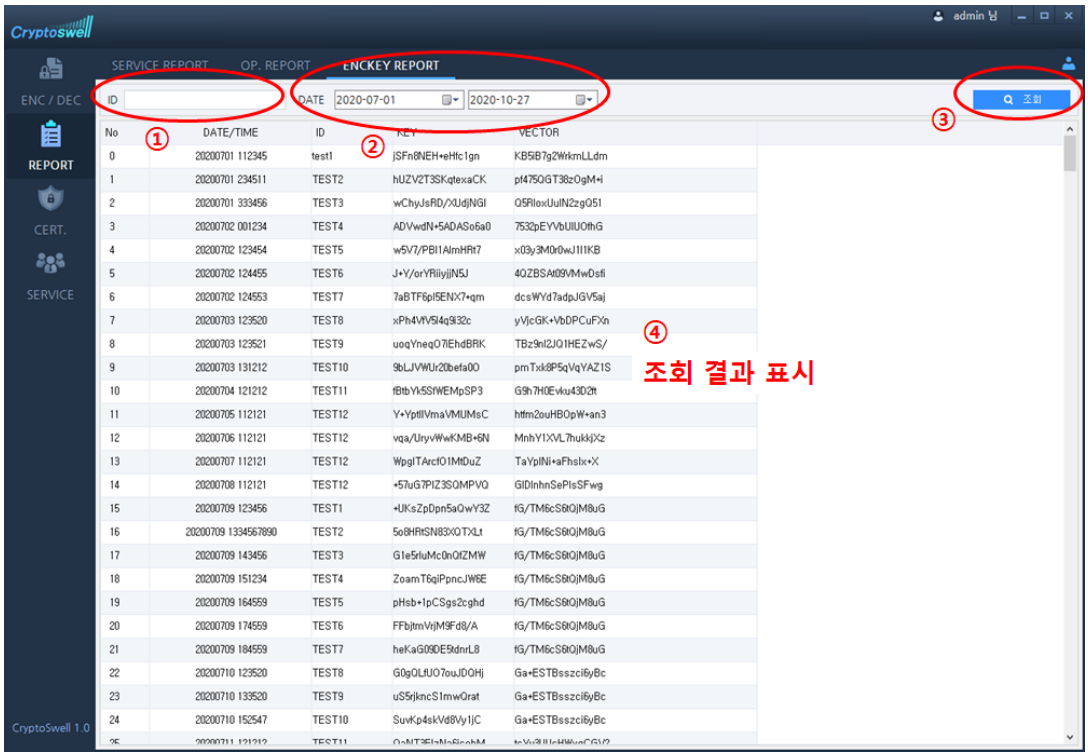
암호키를 조회합니다.

암호키는 client가 암호를 할 때마다 생성 됩니다.

로그는 “key”디렉토리 밑에 저장되어 있습니다.

① ID로 암호키 조회

② 날짜로 운영 내역 조회

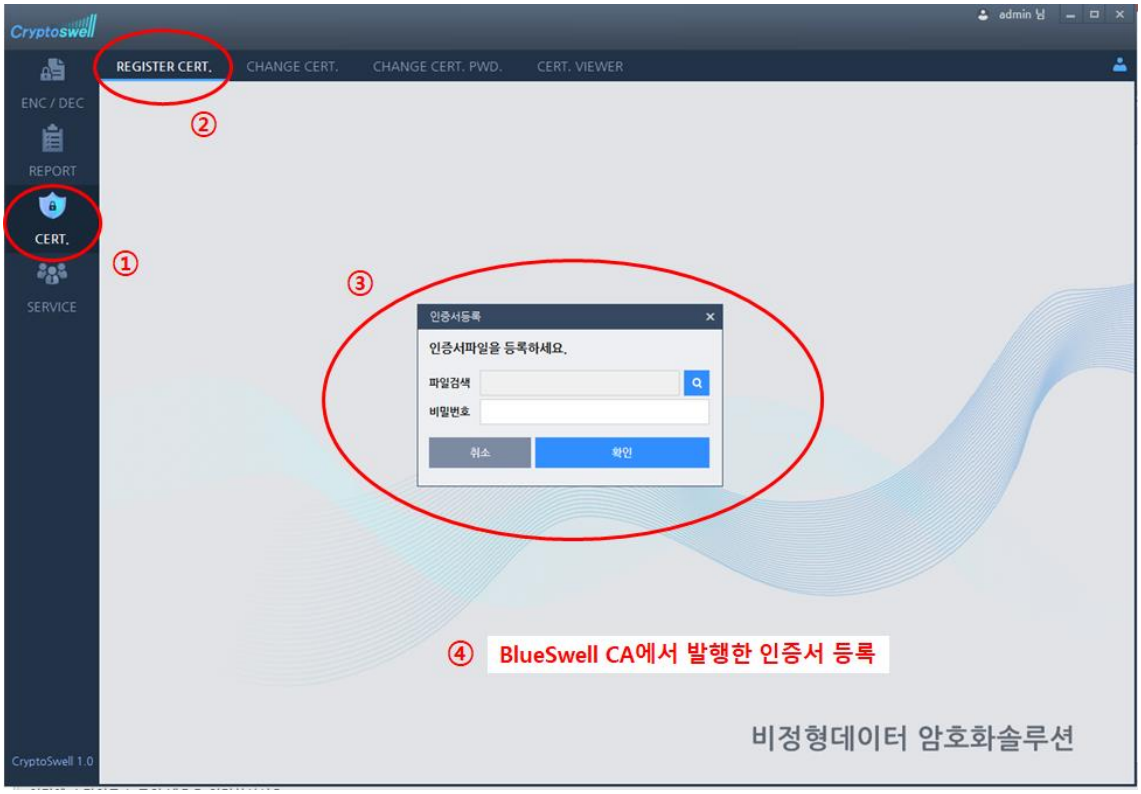


# 3. CERTIFICATE

## 1) REGISTER CERT.

인증서를 등록합니다.
인증서가 등록되지 않으면 “SERVICE” 매뉴를 이용할 수 없습니다.
인증서는 “cert” 디렉토리에 저장됩니다.
사용가능한 인증정책은 “1.2.410.200020.1.1.3” 입니다.

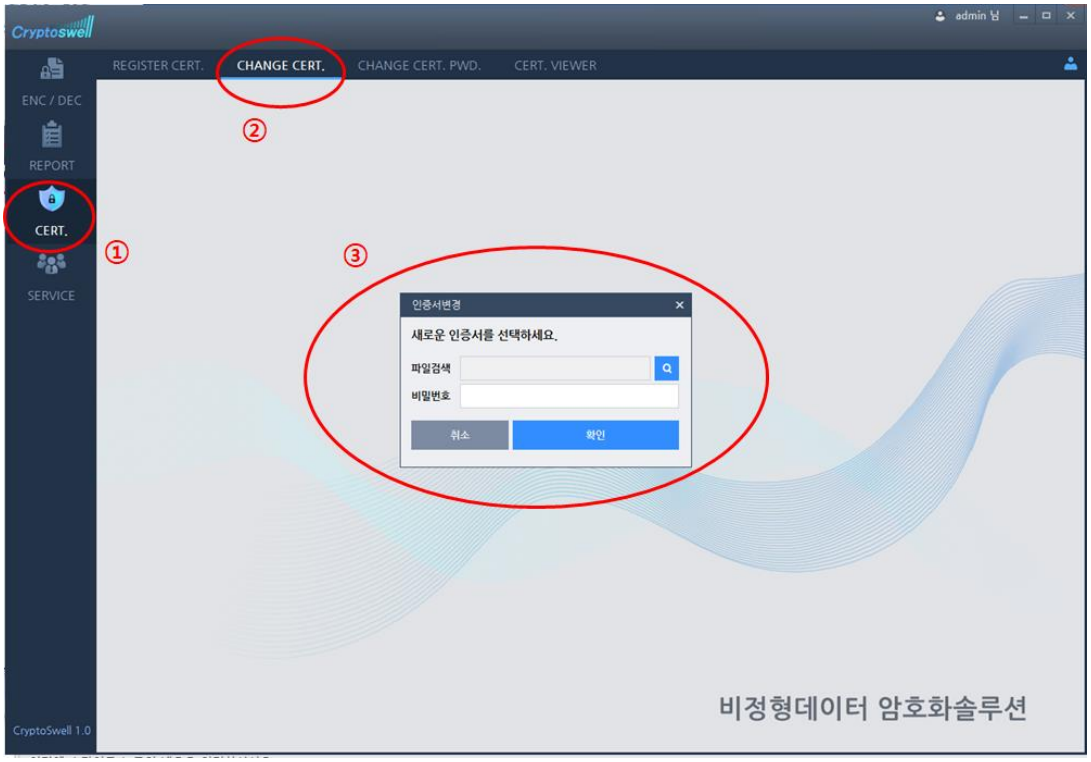
① “CERT” -> “REGISTER” 를 선택
② BlueSwell에서 발급한 인증서를 입력
③ 인증서 비밀번호를 입력



## 2) CHANGE CERT.

인증서의 유효기간이 지나면 갱신해야 합니다.
인증서를 갱신하지 않으면 서비스를 이용할 수 없습니다.
갱신한 인증서는 “cert” 디렉토리에 저장되고, 이력도 “cert.csv”에 기록 됩니다.
사용가능한 인증정책은 “1.2.410.200020.1.1.3” 입니다.

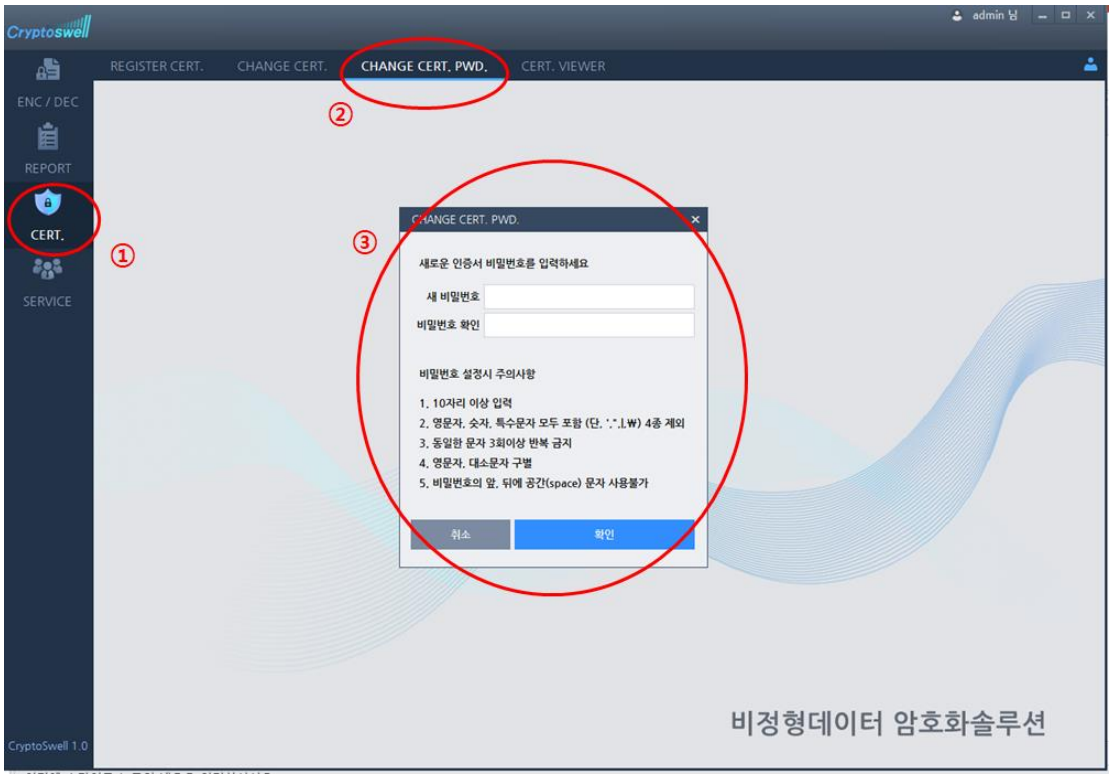
① “CERT” -> “CHANGE CERT.” 를 선택
② BlueSwell에서 발급한 인증서를 입력
③ 인증서 비밀번호를 입력



## 3) CHANGE CERT. PWD.

인증서의 비밀번호는 변경할 수 있습니다.
비밀번호를 변경하면 “current_cert.ber”에 변경된 비밀번호가 반영 됩니다.

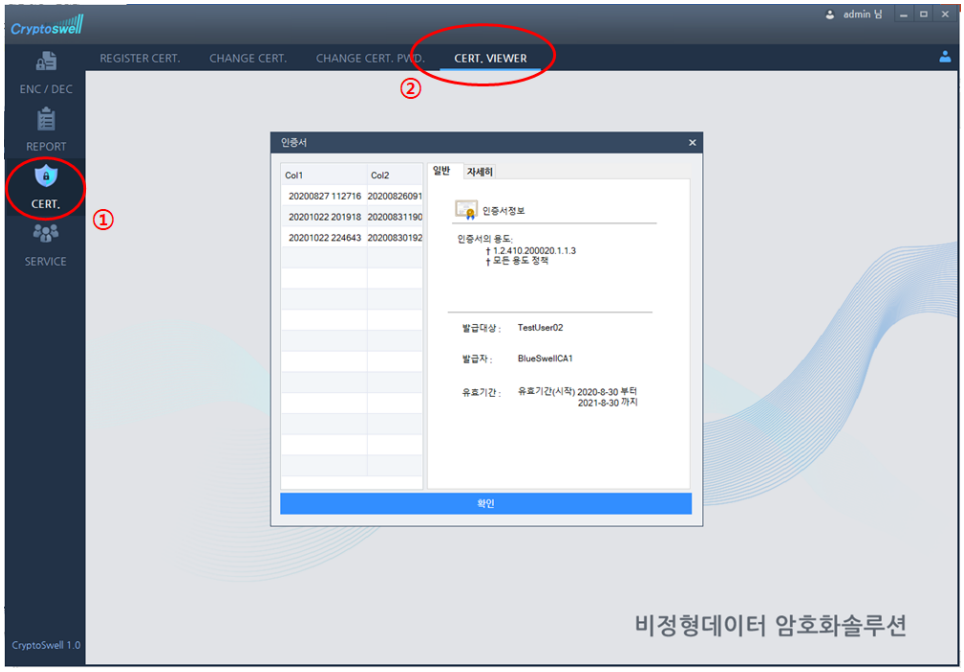
① “CERT” -> “CHANGE CERT. PWD” 를 선택
② 새로운 인증서 비밀번호를 입력

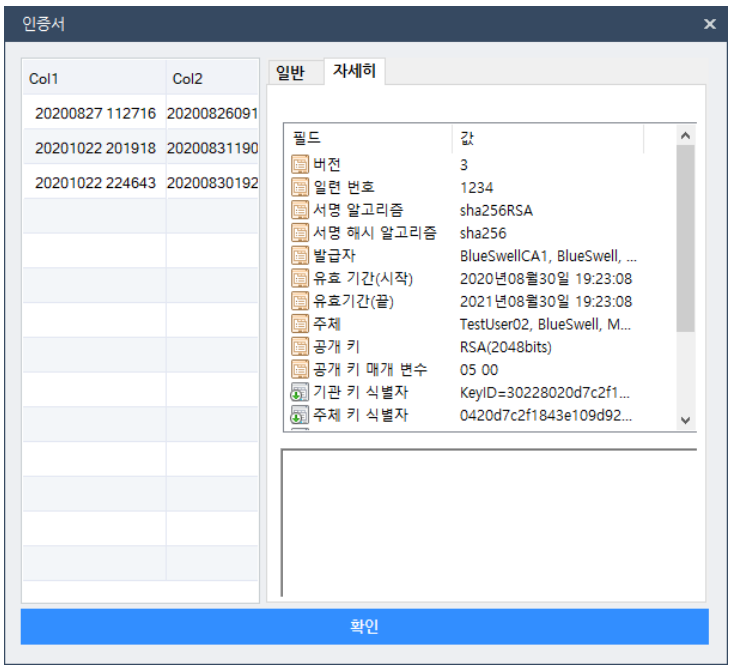


## 4) CERT. VIEWER

현재 사용하고 있는 인증서 정보를 볼 수 있습니다.
유증서의 유효기간은 인증서보기 메뉴를 통해 확인합니다.

① “CERT” -> “CERT. VIEWER” 를 선택
② 인증서의 유효기간 등을 확인



# 4. SERVICE

: 운영자가 CryptoSwell 을 관리하는 메뉴 입니다.

## 1) LOGIN

CryptoSwell을 사용하기 위해서는 login을 해야 합니다.
로그인 정보는 user_login.ini 에 저장 됩니다.

① “SERVIDE” -> “LOGIN” 선택
② ID 와 Password를 입력

: user_login.ini 샘플
[USER]
id = admin
EncID = hQLMIdv/Se+iBPr1DIzIFLjy2dyVzfCi/dJAZvDx+1/3J7nvZejzJgbFQOStuB
EncPWD = hQLMIdv/Se+iBPr1DIzIFLjy2eHdyVzfCi/Dx+1/3J7nvZejzJgbFQOStuB

## 2) REGISTER USER

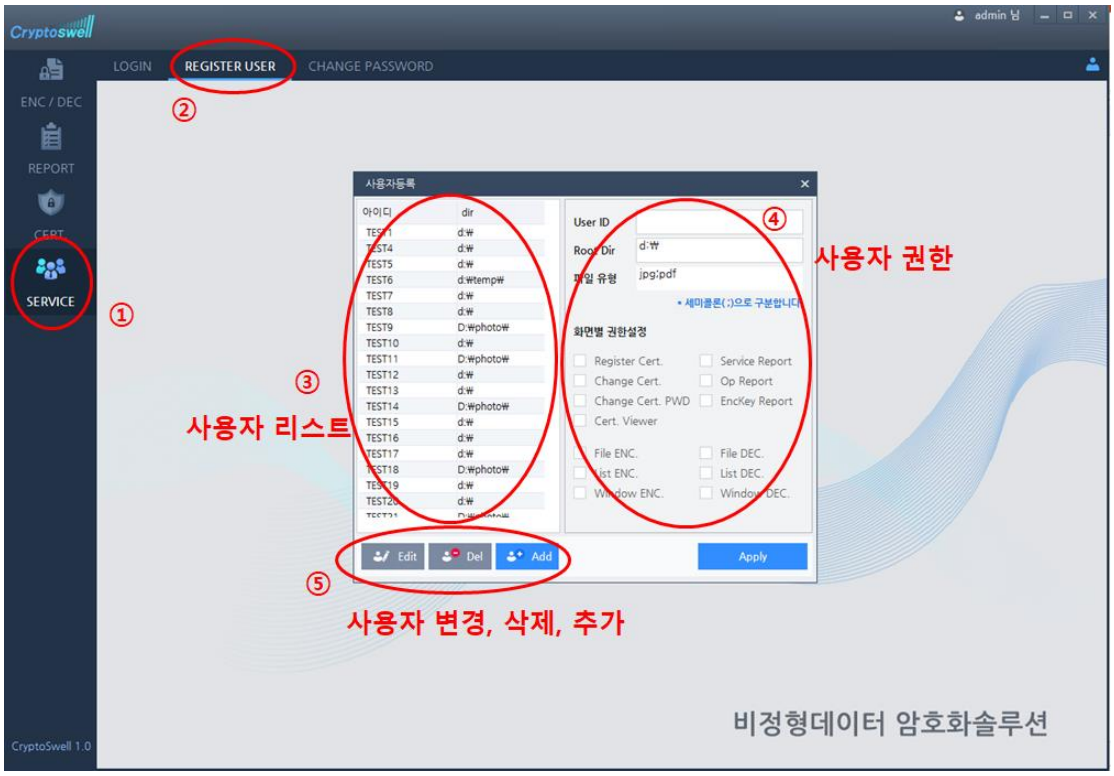
Admin 기능 입니다.

Admin는 Client를 등록할 수 있습니다.

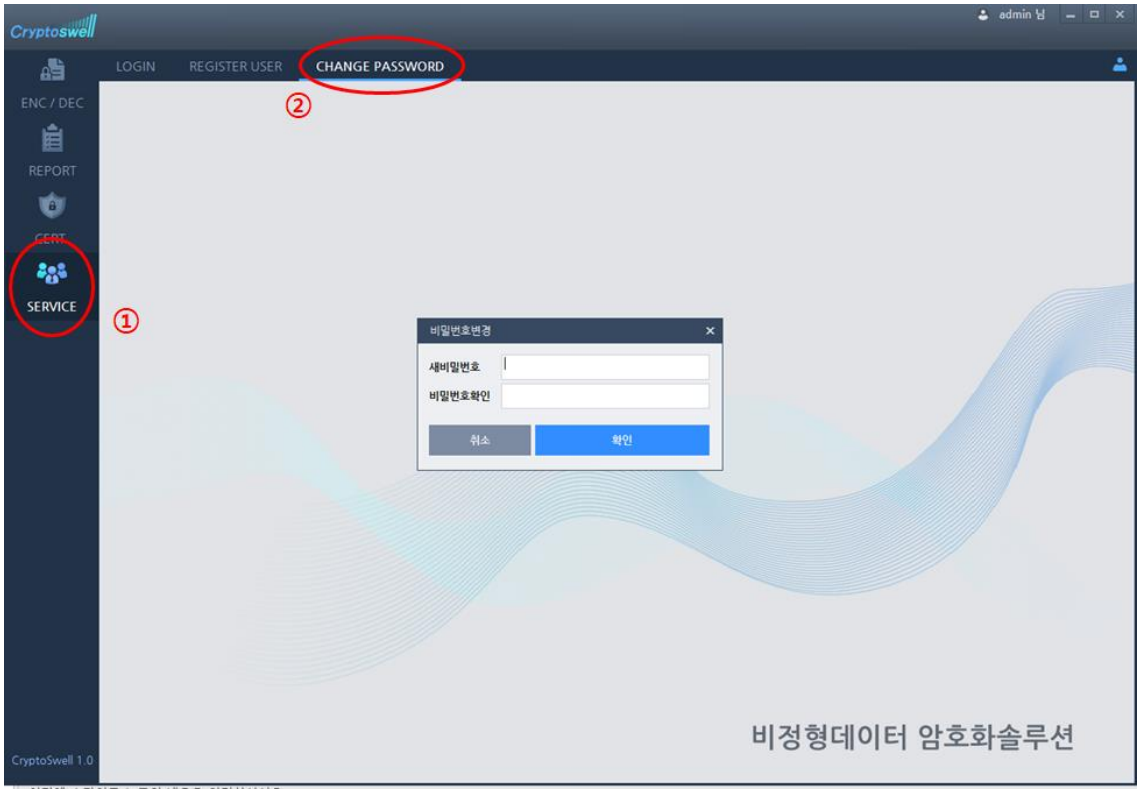
등록된 Client만 CryptoSwell을 사용할 수 있습니다.

User정보는 “user”디렉토리에 저장 됩니다.

① “SERIVCE” -> “REGISTER” 선택
② 사용자 리스트에서 사용자를 선택
③ 사용자를 추가할 경우는 “user id”에 새로운 id를 입력하면 됨
④ 사용자 권한 부분에 필요한 권한을 부여
⑤ “edit”, “Del”, “Add” 버튼을 상황에 맞게 사용



## 3) CHANGE PASSWORD

CryptoSwell을 Client의 비밀번호를 변경할 수 있습니다.
변경된 비밀번호는 user_login.ini 에 저장 됩니다.

① “SERVIDE” -> “CHANGE PASSWORD” 선택
② 새로운 Password를 입력