

SOFTCAMP[□]

Document Security V5.0

사용자설명서(OPE_U)

V 1.0

경기도 성남시 분당구 판교로 228 번길 17,
판교세븐벤처밸리 2 제이렌텍동 2 층 소프트캠프

대표전화: 1644-9366

팩스: 031-697-4599

www.softcamp.co.kr

전체 목차

DOCUMENT SECURITY CLIENT V5.0 5

1. 고객지원..... 5

2. 개요 6

3. 제품 소개 8

4. Document Security Client 시작 8

 4.1. 로그인하기 전 주의사항 9

 4.2. 로그인..... 9

 4.3. 로그아웃..... 17

 4.4. 오프라인 로그인 19

 4.5. 둘러보기..... 20

 4.5.1. 트레이 아이콘 메뉴 21

 4.5.2. 우클릭 메뉴 22

 4.5.3. 권한 변경 알림 22

 4.5.4. 무결성 검증 24

 4.5.5. 사용자 정보 확인 24

 4.5.6. 버전 확인 30

5. Client 사용 31

 5.1. 보안문서 생성..... 32

 5.1.1. 보안문서 생성 경로 34

- 5.1.2. 개인 보안문서 생성 37
- 5.1.3. 공용 보안문서 생성 40
 - 5.1.3.1. 사용자 선택 41
 - 5.1.3.2. 범주 45
 - 5.1.3.3. 등급 49
- 5.2. 보안문서 사용 52
 - 5.2.1. 보안문서의 기본 사용 53
 - 5.2.2. 보안문서의 권한 확인 59
 - 5.2.3. 보안문서의 사용 제어 63
- 5.3. 보안문서 권한 변경 70
- 5.4. 보안문서 해제 74
- 5.5. 보안문서 파기 78
- 6. 환경설정 81
 - 6.1. 서버 환경설정 81
 - 6.2. 비밀번호 변경 85
 - 6.3. 프로그램 실행 확인 91
 - 6.4. 프로그램 보호 기능 93
 - 6.5. 암호화 파일 선택 UI 표시 여부 설정 96
- 7. 소프트웨어 사용권 계약 98

개정 내역

Version	기본 수정 사항	변경자	수정 날짜
V1.0	Document Security V5.0 사용자설명서(OPE_U) 최초 등록	은승현	2018.08.28
	이미지 최신화 및 표준제품으로 내용수정	문정일	2020.03.25

DOCUMENT SECURITY CLIENT V5.0

1. 고객지원

소프트캠프(주)는 기술지원 센터와 홈페이지를 통해 정식 사용자가 제품을 사용하면서 느끼는 의문 사항이나 사용 방법, 프로그램 오류 등에 대하여 접수 받고 있습니다. 상담을 요청하기 전에 운영설명서를 참고하시면 더 빠르고 정확하게 문제를 해결할 수 있습니다.

고객지원센터 연락처

회사홈페이지: www.softcamp.co.kr

이메일: helpsc2@softcamp.co.kr

주소: 13487, 경기도 성남시 분당구 판교로 228 번길 17 판교세븐벤처밸리 2 제이랜텍동 제 2 층 (삼평동 633) 소프트캠프(주)

전화: 1644-9366

팩스: 031-697-4599

2. 개요

문서개요

본 문서는 Document Security V5.0 (이하 "TOE"라 함)의 Client 사용자를 위한 사용자설명서입니다.

용어 설명

본 장은 본 문서에서 사용하는 용어를 설명합니다.

용어	정의
평문	암호화되지 않은 문서를 포함한 모든 형태의 파일로써 임의의 사용자가 열람, 편집, 출력 등이 가능한 파일
암호화	평문을 그냥 보아서는 이해할 수 없는 암호문으로 변환하는 조작
보안문서	암호화 알고리즘을 이용하여 암호화한 전자문서로써 내용이 암호화되고 사용자 권한이 정의된 문서 (암호화 방식에 따라 개인 보안문서, 범주 보안문서, 등급 보안문서로 구분됩니다.)
개인 보안문서	보안문서 중 생성자에 한해 접근 및 사용이 가능한 문서
범주 보안문서	범주 정책을 이용해 생성한 보안문서
등급 보안문서	등급 정책을 이용해 생성한 보안문서
로그	사용자가 보안드라이브 내의 파일을 편집, 인쇄, 반출, 열람 등의 작업을 내역
프린트 마킹	출력물(인쇄물)에 삽입되는 출력자, 출력 경로 로그 및 회사 로고 등의 가독성 마크
문서 사용 권한	읽기, 출력, 암호화 해제, 반출, 접근 대상 변경 등 보안문서를 이용할 수 있는 권한을 변경
온라인	Client PC 와 Server 와의 네트워크가 연결되어 있는 상황
오프라인	Client 와 Server 와의 네트워크가 연결되어 있지 않는 상황

표기 규칙

본 문서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표기 규칙 내용
XXXX 예) 비밀번호	창에서 볼 수 있는 항목 입니다.
<XXXX> 예) <환경설정>	창의 이름 입니다.
[XXXX] 예) [확인]	버튼 이름 입니다.
XX>XXX>XXXXXXX 예) 시작>프로그램>보조프로그램	메뉴 실행의 순서 입니다.
☞ 참고	프로그램 사용 시 참고할 사항 입니다.
※ 주의	프로그램 사용 시 주의해야 할 사항 입니다.

3. 제품 소개

본 장은 Document Security Client V5.0 에 대해 소개하고, 간략히 설명합니다.

Document Security Client V5.0 소개

Document Security Client V5.0(이하 'Client'이라 함)은 TOE 의 사용자 프로그램입니다. 문서 사용자의 사용자 PC 에 설치 되어, Document Security Server V5.0 (이하 'Server' 라고 함)으로부터 배포된 관리자의 정책에 따라 문서 암호화를 수행합니다. Client 의 사용을 위해서는 문서 사용자에게 대한 식별 및 인증 단계를 거쳐야합니다. Client 는 사용자에게 문서 암호화 및 문서 접근, 프린트 마킹, Application 기능 제한 등 관리자가 설정한 정책을 Server 로부터 수신하여 적용합니다.

4. DOCUMENT SECURITY CLIENT 시작

본 장은 Client 를 설치하고 사용자 PC 를 재부팅한 후 Client 를 시작 및 종료하는 과정을 설명합니다.

Client 의 시작 과정은 아래와 같습니다.

가. Client 와 통신할 Server 의 IP 주소와 포트 설정

나. 사용자 ID 및 비밀번호를 입력하여 로그인 시도

- 다. 서버 환경 설정 및 사용자 계정 정보가 올바를 경우, 로그인 성공
- 라. Client 시작

Client 를 종료하는 과정은 아래와 같습니다.

- 가. Client 로그아웃

4.1. 로그인하기 전 주의사항

일반 사용자는 Client 에 로그인하기 전에 다음과 같은 사항은 확인해야 합니다.

- 1) Client 의 원활한 동작을 위해서는 본 제품을 구성하는 각각의 어플리케이션들이 올바르게 설치되어있어야 합니다. 설치 방법은 '설치 지침서'를 참고하시기 바랍니다.
- 2) 일반 사용자는 PC 의 네트워크 연결 상태를 확인합니다. 일반 사용자의 PC 는 Server 와의 원활한 통신을 위해 조직 내의 네트워크에 연결되어 있어야 합니다.
- 3) 일반 사용자는 PC 에 설치된 운영체계를 동작할 수 있는 능력을 포함한 PC 를 조작할 수 있는 기본적인 능력이 요구됩니다. 네트워크 설정 및 사용자 인증 절차에 관한 기본 지식이 요구됩니다.
- 4) 일반 사용자는 아래의 정보를 알고 있어야 합니다. 아래의 정보를 모르는 경우, 관리자에게 해당 정보를 요청합니다.
 - 가. 일반 사용자 계정 정보 (아이디와 비밀번호)
 - 나. Server 의 IP 주소, 포트번호


4.2. 로그인

로그인을 하기 위해서는 Server 의 IP 주소와 포트번호가 올바르게 설정되어 있어야 합니다.

서버 접속 정보를 변경할 필요가 있을 경우, 로그인 환경 설정 기능을 통해 변경할 수 있습니다.

- 1) Client 설치 후 PC 를 재부팅하면 아래와 같이 Client 에 로그인하기 위한 <Log-In> 창이 나타납니다.



 참고 : <Log-In> 창이 보이지 않으면 아래의 그림과 같이 Client 의 트레이아이콘을 우클릭하여 나오는 메뉴에서 '로그인'을 클릭하여 줍니다.



- 2) <Log-In> 창의 하단에 [환경설정]을 클릭하면 아래와 같이 <Setting> 창이 표시됩니다.
아래의 창에서 [서버 환경설정]을 클릭합니다.



- 3) Client 로그인 시 접속을 시도할 Server 의 <Setting>창이 나타납니다. 접속할 Server 의 IP 주소와 포트번호, 응답시간을 입력하고, [확인]을 클릭합니다. 1 차 서버에는 Client 로그인 시 최초로 접속을 시도할 Server 의 정보를 입력합니다. 2 차 서버는 Server 가 이중화 구성된 경우 설정합니다. 1 차로 접속을 시도한 Server 에 접속이 실패할 경우, 자동으로 2 차 서버에 입력된 정보의 Server 에 접속을 시도합니다. 또는, 로그인 시 랜덤으로 접속을 시도합니다.



용어	정의
1 차 서버 / 2 차 서버	로그인 시 접속되는 Server 의 구성에 따라 다르게 나타나며 '1 차 서버'는 'Master Server'를, '2 차 서버'는 'Slave Server'를 나타냅니다. 관리자가 Server 의 '인증 서버 접속 정책'을 설정함에 따라 '2 차 서버'의 표시 여부가 결정됩니다. '1 차 서버'만 표시는 경우는 사용자가 로그인 시 'Master Server'로만 접속하여 인증하는 방식을 선택한 경우이며, 'Slave Server' 접속 설정을 한 경우는 '2 차 서버' 설정부가 표시됩니다. 각각의 설정 값은 해당 관리자에게 문의 바랍니다.
서버 주소	접속할 Server 의 로그인에 사용될 IP 주소를 입력합니다. 기본값은 127.0.0.1 이며, IP 주소는 "###.###.###.###" (###는 0 ~ 255 사이의 아라비아 숫자)의 형태로 입력합니다. 문자와 ".", "\$", "#"을 제외한 특수문자는 입력할 수 없습니다.
포트 번호	접속할 Server 의 포트번호를 입력합니다. 기본값은 62001 이며, 입력 가능한 값은 0 ~ 99999 사이의 아라비아 숫자입니다.
응답 시간	응답시간은 로그인 시 Server 와 접속을 시도하고 응답이 없는 경우 대기 시간을 의미합니다. 기본값은 20 초이며, 입력 가능한 값은 0 ~ 99 사이의 아라비아 숫자입니다. 기본값을 유지하는 것을 권장합니다.

참고 : 관리자의 설정에 따라 2 차 서버를 입력하는 부분이 보이지 않을 수 있습니다. 이 경우, 1 차 서버를 입력하는 부분만 입력하도록 합니다.

4) 아래와 같은 메시지가 출력되면 **[확인]**을 클릭합니다.

알림

수정된 정보는 다음 로그인부터 적용됩니다.

확인

주의 : 잘못된 형태의 IP 주소(예: 125.181.194.999)를 입력하면 아래와 같은 메시지가 출력됩니다.
Server 의 IP 주소를 재확인하여 다시 입력합니다.

알림

잘못된 IP주소입니다. 다시 입력해 주십시오.

확인

5) 아래의 창이 다시 표시되면, **[확인]**을 클릭합니다.

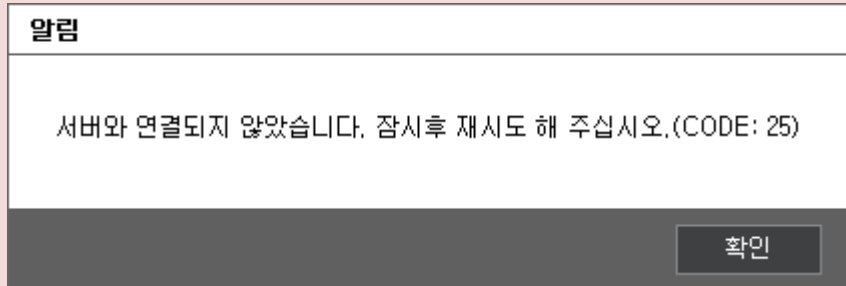


- 6) 다시 <로그인> 창이 표시되면 관리자로부터 부여 받은 아이디와 비밀번호를 각각 '아이디'와 '비밀번호'란에 입력한 후 [확인]을 클릭합니다.



주의 : 로그인에 실패할 경우, 아래와 같은 오류 메시지가 출력될 수 있습니다. 오류의 내용을 확인하시고 다시 로그인을 수행해주시기 바랍니다. 로그인에 계속 실패할 경우, 관리자에게 문의해 주시기 바랍니다.

- 1) Server 의 접속 정보가 잘못 되어 있을 경우, 아래와 같은 오류 메시지가 출력됩니다. [서버 환경설정](#)에서 Server 의 접속 정보가 올바르게 입력되었는지 확인해 주시기 바랍니다. 단, 사용자에게 오프라인 로그인이 가능하도록 설정되어 있다면 오프라인 로그인 상태로 로그인됩니다



- 1) ID 또는 비밀번호가 올바르지 않을 경우, 아래와 같은 오류 메시지가 출력됩니다. ID 또는 비밀번호가 올바른지 확인하시고, 틀린 문자를 입력하지 않도록 주의하여 입력하시기 바랍니다. 관리자에게 부여 받은 아이디와 비밀번호가 올바로 입력되었음에도 불구하고 위와 같은 메시지가 출력된다면, 관리자에게 문의하여 아이디와 비밀번호를 재발급 받도록 합니다

{피드백 메시지 캡처 추가}

아이디나 비밀번호가 틀렸을 경우 위와 같은 메시지가 출력됩니다. 어떤 인증 정보가 틀렸는지 피드백을 제공하지 않습니다.

- 1) 로그인 접속 실패가 관리자가 설정한 회수 이상 계속될 경우, 아래와 같은 오류 메시지가 출력됩니다. 이 경우, 사용자의 계정의 사용이 불가능하게 됩니다. 관리자에게 문의하여 사용자 계정의 재사용을 요청해주시기 바랍니다.

알림

로그인 실패 횟수를 초과하였습니다.
관리자에게 문의하여 주십시오.

2) 사용자의 계정 사용이 중지되어 있는 경우, 아래와 같은 메시지가 출력됩니다. 사용자 계정의 사용을 원할 경우, 관리자에게 요청해주시기 바랍니다.

알림

계정사용이 중지되었습니다.
관리자에게 문의하여 주십시오.

7) 로그인에 성공하면 우측 Client의 **트레이아이콘**이 아래와 같이 로그인 상태로 변경됩니다.



참고 : Client의 트레이아이콘 상태는 아래와 같습니다.

구분	로그인	로그아웃	오프라인 로그인
----	-----	------	----------

아이콘				
-----	---	---	---	--

참고 : 네트워크의 문제로 인하여 서버 접속이 불가능할 경우에도 관리자가 사용자에게 '오프라인 로그인' 권한을 부여한 경우에는 오프라인 로그인에 성공할 수 있습니다. 단, 이전에 정상적인 로그인을 수행한 적이 있는 경우에만 가능하며, 최초 로그인 시에는 불가능합니다. 이 때에도 사용자 ID 와 비밀번호는 올바르게 입력해야 합니다. 오프라인 로그인에 대한 자세한 내용은 [오프라인 로그인](#)을 참조하십시오.

주의 : '오프라인 로그인' 상태에서 '온라인 로그인' 상태로의 전환은 자동적으로 이루어지지 않습니다. 사용자는 네트워크가 정상적으로 동작하게 되면 '로그아웃' 후 재 로그인을 수행해야 합니다.

주의 : '오프라인 로그인' 상태에서는 마지막으로 로그인에 성공하여 Server 로 부터 받은 보안정책을 따르게 됩니다. 단, 사내 조직도와 같이 서버로 접속이 되어야만 받을 수 있는 실시간 정보의 사용 및 그에 따른 작업 내용이 표시되지 않을 수 있습니다.

주의 : 고객사의 환경에 따라 이미 로그인 된 상태에서 다른 아이디로 로그인 하고자 할 경우, 먼저 로그인 되어 있는 사용자는 로그아웃 됩니다.

4.3. 로그아웃

로그아웃은 Client 사용 중 자유롭게 수행할 수 있습니다. 로그아웃을 하면 보안문서를 생성할 수 없으므로, 로그아웃된 상태에서 생성된 문서에 대해서는 보안이 적용되지 않습니다. 또한, 로그아웃된 상태에서는 모든 보안문서에 접근할 수 없어, 열람이 불가능합니다.

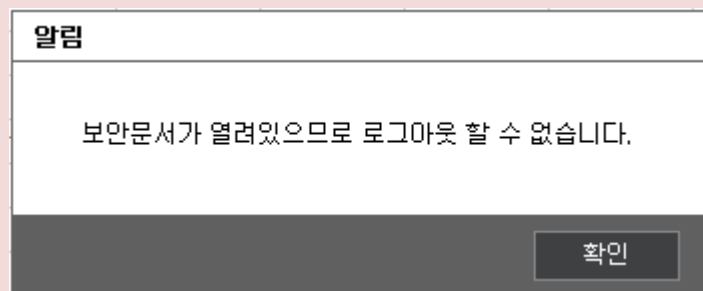
1) Client 트레이아이콘을 우클릭한 후 '로그아웃'을 클릭합니다.



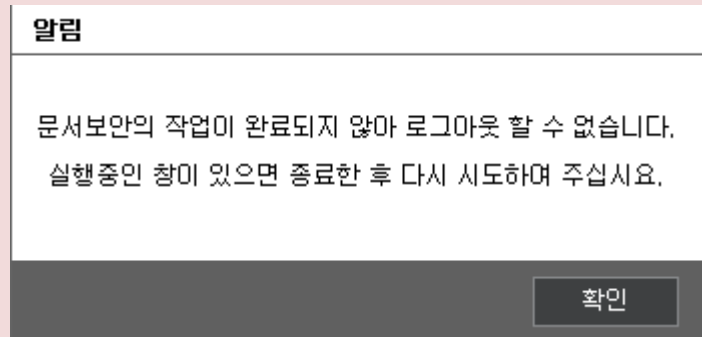
2) 로그아웃이 완료되면 우측 하단의 Client의 트레이아이콘이 아래와 같이 변경됩니다.



⚠ 주의: 보안문서가 열린 상태에서는 로그아웃이 불가능합니다. 아래와 같은 메시지가 출력되면서 로그아웃이 진행되지 않습니다. 작업 중인 보안문서 또는 문서 편집 어플리케이션을 종료하고 다시 로그아웃을 진행하시기 바랍니다.



<환경설정> 창 등 Client 관련 작업창이 열린 상태에서는 아래와 같은 메시지가 출력되며 로그아웃할 수 없습니다. 로그아웃하기 전에 관련 작업창을 모두 닫도록 하십시오.



4.4. 오프라인 로그인

본 장은 오프라인 로그인에 대해 설명합니다. 오프라인 로그인은 Server와의 통신이 연결되지 않은 상태에서 사용자의 ID와 PW를 식별하여 사용자를 인증하는 기능을 의미합니다.

기본적으로 보안문서는 Client에 로그인에 성공해야 사용할 수 있습니다. 이 경우, 네트워크에 문제가 발생하여 로그인을 할 수 없다면 보안문서도 사용할 수 없어지고, 업무상의 불편함을 초래할 수 있습니다. 업무상의 불편을 해소하고자, 네트워크가 정상 동작하지 않을 경우에도, 오프라인 로그인 기능을 활용하여 보안문서를 정상적으로 사용할 수 있습니다.

오프라인 로그인 관련 주의사항

- 1) 오프라인 로그인은 관리자의 설정에 따라 사용자마다 전환될 수 없을 수 있습니다.
- 2) 오프라인 로그인 상태에서는 마지막으로 로그인에 성공하여 Server 로 부터 받은 보안정책을 따르게 되나, 보안문서에 대한 권한이 로그인 시의 권한과 다를 수 있습니다.
- 3) Server 로 접속이 되어 실시간 정보를 사용하고 그에 따른 작업 내용이 표시되는 기능은 정상 동작하지 않습니다.
- 4) 오프라인 로그인 시 Server 와 연결될 경우, 관리자의 설정에 따라 자동으로 온라인으로 전환될 수도 있습니다. 그렇지 않은 경우, 로그아웃한 후 다시 로그인을 시도해야 합니다.

4.5. 둘러보기

본 장은 Client 의 각 메뉴의 위치와 종류를 알아보고, 로그인한 사용자의 정보와 사용자가 가지는 권한에 대해 알아 봅니다. 본 장은 다음과 같이 구성됩니다.

관련링크

- a. [트레이아이콘 메뉴](#)
- b. [우클릭 메뉴](#)
- c. [권한 변경 알림](#)
- d. [무결성 검증](#)
- e. [사용자 정보 확인](#)
- f. [버전 확인](#)

4.5.1. 트레이 아이콘 메뉴

본 장은 Client 의 트레이아이콘에 대해 설명합니다. Client 를 설치하면 트레이에 Client 의 아이콘이 생성됩니다. Client 의 트레이아이콘은 사용자의 로그인/로그아웃/오프라인 로그인 상태에 따라 아래와 같이 색깔이 변경됩니다.

구분	로그인	로그아웃	오프라인 로그인
Client 트레이아이콘			

Client 의 트레이아이콘을 우클릭하면 아래와 같은 메뉴가 표시됩니다. 사용자의 로그인/로그아웃/오프라인 로그인 상태와 관리자가 설정한 권한에 따라 사용이 불가능한 메뉴가 있을 수 있습니다. 사용 불가능한 메뉴는 비활성화되어 회색으로 표시됩니다.

표시되는 메뉴는 다음과 같은 기능을 제공합니다.

용어	정의
환경 설정	접속할 Server 의 접속 정보를 변경하고, 비밀번호를 변경할 수 있습니다.
무결성 검증	Client 실행파일 및 환경설정 파일들에 대한 무결성 검증을 수행합니다.
로그인	Client 에 로그인하기 위한 <로그인> 창을 실행시킬 수 있습니다. 자동 로그인 설정이 되어 있는 경우, 자동으로 로그인 됩니다. 로그아웃 상태에서만 활성화됩니다
로그아웃	Client 에서 로그아웃할 수 있습니다. 로그인이나 오프라인 로그인 상태에서만 활성화됩니다.
사용자 정보	로그인한 사용자의 정보 및 권한 정보를 확인할 수 있습니다. 로그인이나 오프라인 로그인 상태에서만 활성화됩니다.
버전 정보	설치된 Client 의 버전을 확인할 수 있습니다.

4.5.2. 우클릭 메뉴

본 장은 Client 설치 후 파일 우클릭 시 나타나는 메뉴에 대해 설명합니다. 표시되는 메뉴는 Client가 지원하는 문서 편집 어플리케이션에 따라, 문서의 암호화 여부에 따라 다릅니다. 또한 우클릭 메뉴는 관리자가 설정한 권한에 따라 다를 수 있습니다. 우클릭한 파일의 종류에 따라 표시되는 우클릭 메뉴는 아래와 같습니다.

1) Client 에서 지원하는 확장자를 가진 일반문서 우클릭 시

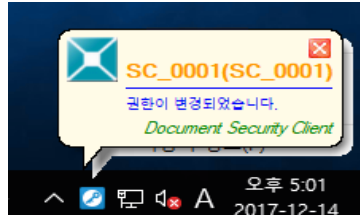
용어	정의
일반 문서 암호화	일반문서를 암호화하여 보안문서를 생성합니다.

2) 보안문서 우클릭 시

용어	정의
보안 문서 파기	보안문서를 복구할 수 없도록 완전 파기합니다.
보안 문서 암호화 해제	암호화를 해제하여 일반문서로 만듭니다.
접근 대상 변경	보안문서의 권한을 변경합니다.

4.5.3. 권한 변경 알림

본 장은 권한 변경 알림에 대해 설명합니다. 관리자가 사용자에게 대해 보안 정책 및 권한을 변경했을 때, Client 의 트레이아이콘은 권한이 변경되었다는 알림 메시지를 표시합니다. 권한 변경 알림 메시지는 사용자에게 변경된 권한이 적용되었을 때 표시됩니다. 알림 메시지는 아래의 그림과 같이, Client 의 트레이아이콘 위에 말풍선 형태로 나타납니다.



말풍선에는 해당 사용자 ID 와 이름과 함께 '권한이 변경되었습니다.'라는 문구를 표시됩니다. 말풍선은 사용자가 말풍선의 노란 부분을 클릭하기 전까지 표시됩니다. 노란 부분을 클릭하면 말풍선은 사라집니다. '권한이 변경되었습니다.'라는 문구 부분을 클릭하면 아래와 같이 <사용자 정보> 창이 표시됩니다. <사용자 정보> 창에 대한 내용은 [사용자 정보 확인](#)을 참고하시기 바랍니다.

User Info

현재 로그인 되어있는 사용자의 정보를 확인할 수 있습니다.

로그인 사용자 정보

성명 : CC인종테스트	PC ID : 201712160000000
아이디 : SC-Test01	PC 소유자 : CC인종테스트 / sc-test0

소속	직위	분류
DS서비스사업부		SECURITYDOMAIN

권한 정보

문서 보안 프로파일

사용자 분류 : SECURITYDOMAIN

범주	읽기	읽기횟수	편집	해제	반출	출력	출력횟수	프린트마킹
SCNET	O	제한없음	X	X	X	X	제한없음	X
외부유입파일	O	제한없음	O	X	X	O	제한없음	O
중역회의 자료	O	제한없음	O	X	X	O	제한없음	O

강제 적용 권한

읽기	읽기횟수	편집	해제	반출	출력	출력횟수	프린트
사용안함	사용안함	사용안함	사용안함	사용안함	사용안함	사용안함	사용안

확인

4.5.4. 무결성 검증

본 장은 사용자가 Client 의 실행 및 설정과 관련된 주요파일들에 대한 무결성 검증을 수행하는 방법을 설명합니다.

- 1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '무결성 검증'을 클릭합니다.



- 2) 무결성 검사가 수행되고 결과는 Server 로 전송됩니다.

4.5.5. 사용자 정보 확인

본 장은 사용자 정보 확인에 대해 설명합니다. 사용자 정보 확인을 통해 사용자는 본인의 계정 및 권한 정보를 확인할 수 있습니다. 사용자는 본인이 속한 분류와 범주 및 해당 범주가 가지는

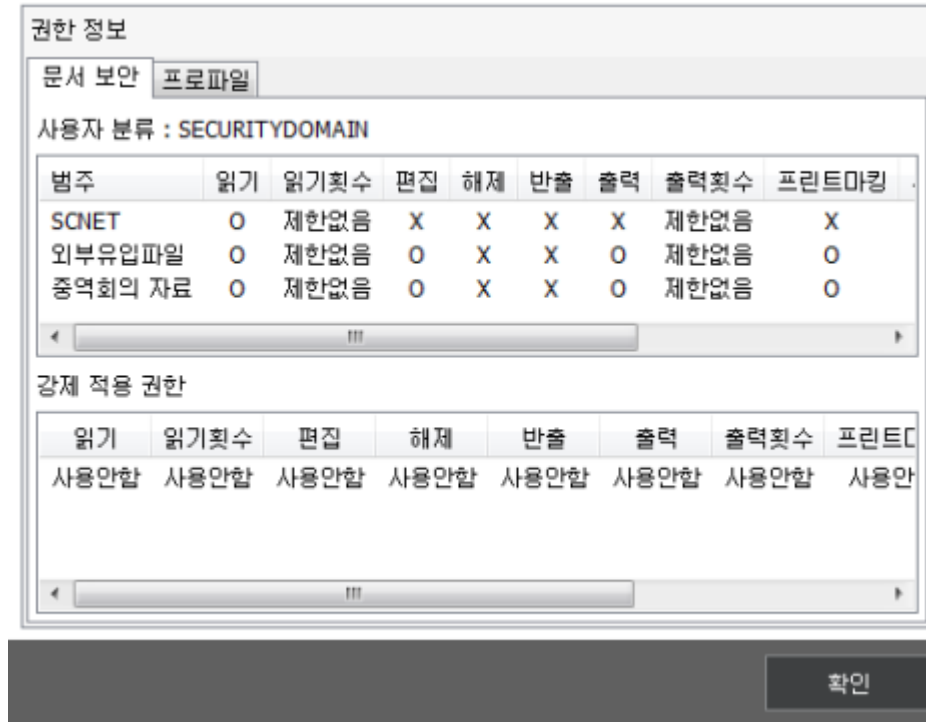
권한, 그리고 프로파일에 관한 권한을 확인할 수 있습니다. 사용자 정보를 확인하기 위해서는 Client 에 로그인되어 있어야 합니다.

1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '**사용자 정보**'를 클릭합니다.



2) 아래와 같이 <**사용자 정보**>창이 출력됩니다. <**사용자 정보**> 창은 다음과 같이 구성됩니다.

[확인]을 클릭하면 창이 닫힙니다.



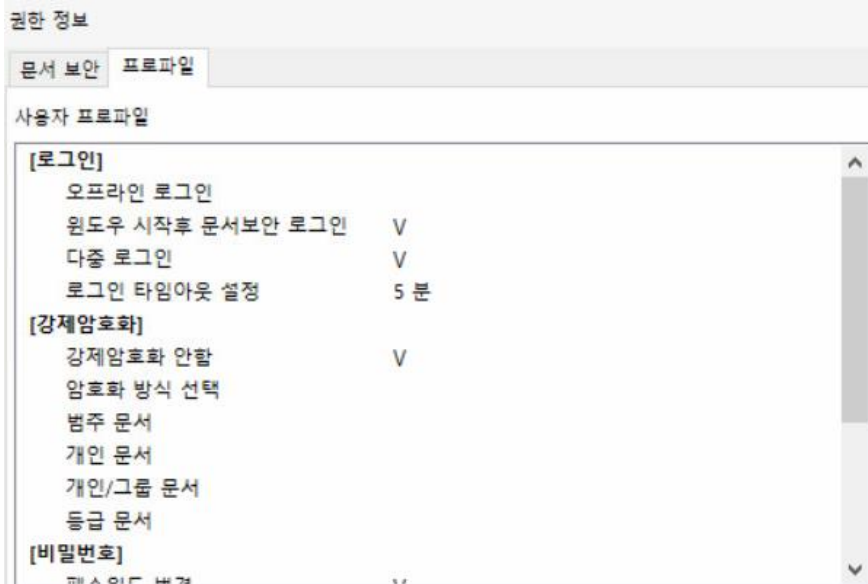
- i. 문서 보안 탭 : 사용자의 문서보안 정책을 나타냅니다.
- 사용자 분류 : 현재 사용자가 속한 분류를 표시합니다.

용어	정의
범주	사용자가 접근 가능한 범주 보안문서의 권한을 표시합니다. 범주에 대한 설명은 범주 를 참고하시기 바랍니다.
읽기	해당 범주 보안문서의 읽기 권한의 유무를 표시합니다.
읽기횟수	해당 범주 보안문서를 열람할 수 있는 최대 횟수를 표시합니다. 제한없음인 경우, 사용자는 해당 범주 보안문서를 제한없이 열람할 수 있습니다.
편집	해당 범주 보안문서의 편집 권한의 유무를 표시합니다.
해제	해당 범주 보안문서의 복호화 권한의 유무를 표시합니다.
출력	해당 범주 보안문서의 출력 권한의 유무를 표시합니다.
출력횟수	해당 범주 보안문서를 출력할 수 있는 최대횟수를 표시합니다. 제한없음인 경우, 사용자는 해당 범주 보안문서를 제한없이 출력할 수 있습니다.
프린트마킹	해당 범주 보안문서의 출력 시 프린트 마킹 삽입 여부를 표시합니다.
유효기간	해당 범주 보안문서를 사용할 수 있는 기간을 표시합니다.
자동파기	읽기 회수, 출력 회수, 유효기간 경과 시 해당 범주 보안문서가 자동파기되는지 여부를 표시합니다.

권한변경	해당 범주 보안문서의 사용 권한의 변경 가능 여부를 표시합니다.
-------------	-------------------------------------

- 강제 적용 권한 : 사용자가 보안문서를 생성했을 때 강제로 적용되는 권한을 표시합니다. 사용안함으로 표시되어 있는 경우, 해당 권한에 대한 강제 적용 권한이 없음을 의미합니다.

용어	정의
읽기	읽기 강제 적용 권한의 유무를 표시합니다.
읽기횟수	읽기횟수 강제 적용 권한의 유무를 표시합니다.
편집	편집 강제 적용 권한의 유무를 표시합니다.
해제	복호화 강제 적용 권한의 유무를 표시합니다
출력	출력 강제 적용 권한의 유무를 표시합니다.
출력횟수	보안문서를 출력할 수 있는 강제 적용된 최대횟수를 표시합니다. 제한없음인 경우, 사용자는 보안문서를 제한없이 출력할 수 있습니다.
프린트마킹	프린트 마킹 삽입 강제 적용 권한을 표시합니다.
유효기간	보안문서의 사용 유효기간 강제 적용 권한을 표시합니다.
자동파기	보안문서 자동파기 강제 적용 권한을 표시합니다.
권한변경	보안문서 권한변경 강제 적용 권한을 표시합니다.



- ii. 프로파일 : 사용자가 보안문서를 생성했을 때 강제로 적용되는 권한을 표시합니다. 사용안함으로 표시되어 있는 경우, 해당 권한에 대한 강제 적용 권한이 없음을 의미합니다.

- 로그인

용어	정의
오프라인 로그인	사외, 재택 등 사내 네트워크에 연결되지 않은 상태에서 Client 을 사용할 수 있습니다.
윈도우 시작 후 문서보안 로그인 실행	PC 부팅과 동시에 Client 로그인 창이 실행됩니다.
다중 로그인	하나의 사용자 아이디로 복수의 PC 가 동시에 문서보안 로그인이 가능합니다.

- 강제암호화 : 사용자에게 적용된 강제 암호화 정책에 ' V '가 표시됩니다. 강제암호화 정책이 적용되지 않은 사용자에게는 아래의 항목이 표시되지 않습니다.

용어	정의
강제암호화 안함	문서에 대해 강제로 암호화를 하지 않습니다.
암호화 방식 선택	문서 생성 시 암호화 방식을 선택하도록 강제합니다.
범주 문서	문서 생성 시 범주 보안문서를 생성하도록 강제합니다. 범주에 대한 설명은 범주 를 참고하시기 바랍니다.
개인 문서	문서 생성 시 개인 보안문서를 생성하도록 강제합니다.
개인/그룹 문서	문서 생성 시 관리자가 설정한 사용자에게 접근 권한이 있는 보안문서를 생성하도록 강제합니다.
등급문서	문서 생성 시 등급 보안문서를 생성하도록 강제합니다. 등급에 대한 설명은 등급 을 참고하시기 바랍니다.

- 비밀번호

용어	정의
비밀번호 변경	사용자가 비밀번호를 변경할 수 있습니다.
변경주기	관리자가 설정한 월 단위의 주기마다 비밀번호를 변경해야 합니다.
비밀번호 변경 시 패턴 제한	비밀번호 변경 시 관리자가 설정한 길이 이상으로 비밀번호를 변경해야 합니다. 또한, 연속적인 영문 또는 숫자로 비밀번호를 변경할 수 없습니다. 비밀번호의 최소 길이는 <사용자 정보>에 표시됩니다.

최초 로그인시 비밀번호 변경	사용자가 Client 에 최초 로그인 시 비밀번호를 변경하도록 강제합니다.
-----------------	---

- 기타

용어	정의
프로그램 삭제	프로그램 삭제 권한이 허용된 사용자는 Client 를 삭제할 수 있습니다.

4.5.6. 버전 확인

본 장은 사용자가 설치한 Client 의 버전을 확인하는 방법을 설명합니다. 올바른 버전을 설치했는지 확인할 수 있습니다.

- 1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '버전 정보'를 클릭합니다.



- 2) 아래와 같이 <Product Info> 창에서 사용자 프로그램의 버전을 확인할 수 있습니다.

표시되는 내용은 아래와 같습니다. 첫 번째는 Major 버전, 두 번째는 Minor 버전, 세 번째는 빌드 버전을 의미합니다. [확인]을 클릭하면 창이 닫힙니다.



용어	정의
제품명	제품의 이름입니다. “문서보안” 으로 표기됩니다.
설명	제품의 간략한 설명 입니다. “문서를 암호화하고 사용 권한을 제어하여 정보 유출을 방지하는 문서보안 솔루션” 으로 표기됩니다.
버전	Client 의 버전입니다. 버전은 숫자로 '#.#.#.#'와 같이 이루어집니다. 첫번째 숫자는 Major 버전, 두번째 숫자는 Minor 버전, 세번째 숫자는 빌드 버전, 네번째 숫자는 revisoin 을 의미합니다.

5. CLIENT 사용

본 장에서는 Client 를 이용해 보안문서를 생성/사용/공유/권한 변경/해제/파기하는 일련의 과정에 대해 설명합니다.

관련링크

- a. [보안문서 생성](#)
- b. [보안문서 사용](#)
- c. [보안문서 공유](#)
- d. [보안문서 권한 변경](#)
- e. [보안문서 해제](#)
- f. [보안문서 파기](#)
- g. [기타](#)

© 2017 SoftCamp Co.,Ltd. All rights reserved. Made in Korea.



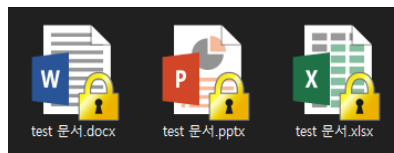
5.1. 보안문서 생성


Client 는 사용자가 Client 가 지원하는 문서 편집 어플리케이션을 통해 생성한 문서가 자동으로 암호화 되거나 Client 가 지원하는 문서에 대해 사용자가 수동으로 암호화를 할 수 있습니다. 사용자는 문서를 저장 시점이나 문서 편집 어플리케이션의 종료 시점에 암호화할 수 있습니다. 관리자의 설정에 따라 개인 보안문서나 공용 보안문서로 자동으로 암호화되거나, 사용자가 선택할 수 있습니다.

- a. 개인 보안문서는 해당 문서에 대한 접근 권한을 보안문서를 생성한 사용자로 한정됩니다. 개인 보안문서라고 할지라도 관리자가 사용자에게 부여한 권한에 따라 암호화되므로 개인 보안문서에 대한 생성자의 사용권한이 제한됩니다.

b. 공용 보안문서는 개인 보안문서와 달리 사용자가 암호화된 문서를 타사용자가 사용이 가능합니다. 사용자는 전자문서의 암호화 시 해당 문서에 대한 접근 권한을 부여할 사용자를 지정하거나 특정 범주 또는 등급을 지정합니다. 해당 범주 또는 등급에 속한 타사용자는 자신이 가진 권한에 따라 해당 문서를 사용할 수 있습니다. 해당 보안문서에 대해 접근 권한이 없는 사용자는 사용이 불가능합니다.

암호화된 문서는 모두 별도의 아이콘으로 표시됩니다. 아이콘은 기존의 문서 편집 어플리케이션에서 생성된 파일의 아이콘에 자물쇠가 얹어진 형태입니다. Microsoft Words 에서 생성된 문서를 암호화할 경우, 아래와 같이 아이콘이 변경됩니다.

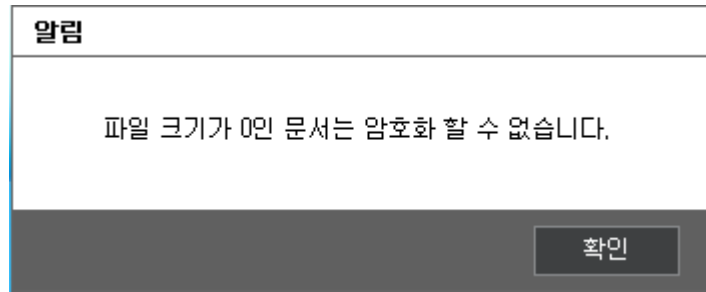


 참고 : Client 가 설치되지 않은 경우, 보안문서도 일반문서와 동일한 아이콘으로 표시됩니다.

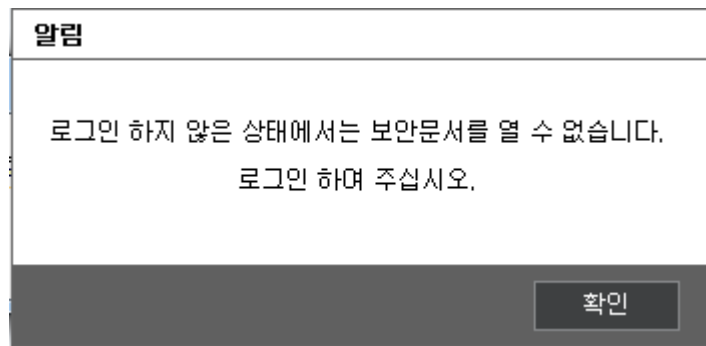
문서 암호화 및 보안문서 사용 시 주의 사항

문서를 암호화할 때 아래의 사항에 대해 주의하도록 합니다.

아무 내용도 작성되지 않은 빈문서는 암호화되지 않습니다. 빈문서에 대한 암호화를 시도하면 아래와 같은 메시지가 출력되며 암호화가 불가능합니다. 사용자에게 강제 암호화가 적용된 경우, 빈문서라도 생성되면 암호화됩니다. 암호화된 빈문서를 실행하면 아래와 같은 메시지가 출력되며 사용할 수 없습니다.



암호화된 문서는 Client 에 로그인한 상태에서만 사용이 가능합니다. 로그아웃 상태에서 보안문서 사용을 시도하면 다음과 같은 메시지가 출력됩니다.

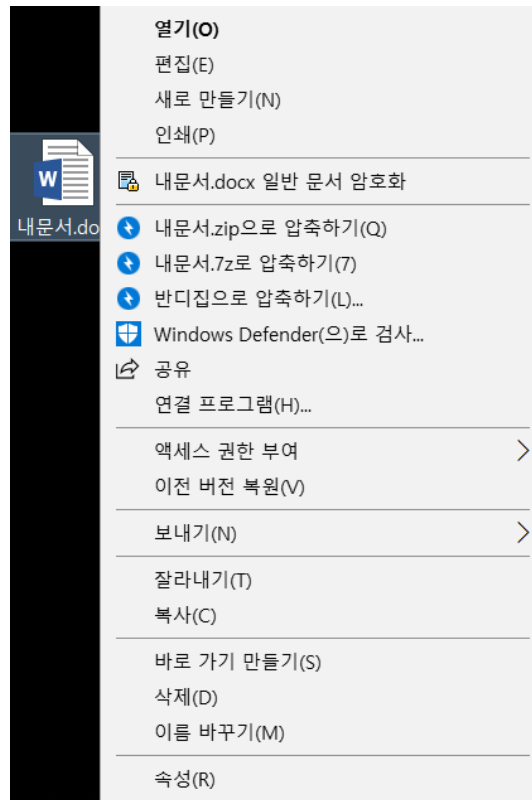


5.1.1.1. 보안문서 생성 경로

본 장은 보안문서 생성 경로에 대해 설명합니다. 보안문서는 아래와 같이 다양한 경로에 생성할 수 있습니다.

생성된 일반문서 우클릭

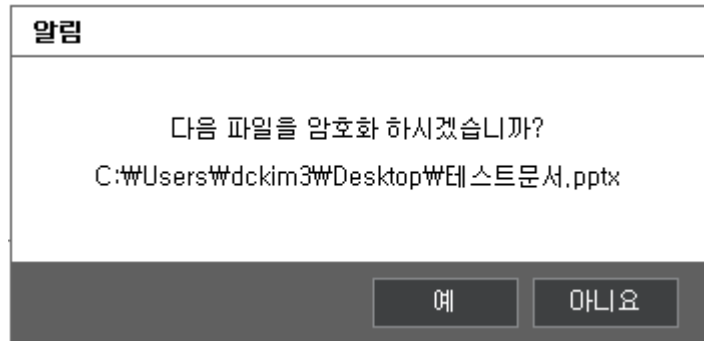
일반문서 파일의 아이콘을 우클릭하여 출력되는 메뉴에서 '{파일명}.{확장자} 일반 문서 암호화'를 클릭하여 보안문서를 생성할 수 있습니다. 아래의 그림과 같이 파일명이 '내문서'이고 확장자가 'docx'라면, 메뉴 항목은 '내문서.docx 일반 문서 암호화'라고 출력됩니다.




사용자는 다수의 문서를 선택하여 암호화할 수 있습니다. 다수의 문서를 선택할 경우, 우클릭 메뉴에서 '**일반 문서 암호화**'를 클릭하면 아래와 같이 선택한 문서 중에서 암호화할 문서를 선택할 수 있는 창이 표시됩니다. 암호화할 문서만 체크하고 [확인]을 클릭하면 암호화할 수 있습니다. 체크 해제된 문서를 암호화할 대상에서 제외됩니다. 체크된 문서 중에 가장 상위에 표시된 문서부터 암호화가 진행됩니다.

문서 작업 중 저장 시

문서 편집 어플리케이션에서 작성한 문서를 저장할 때, 아래의 그림과 같이 문서 암호화 여부를 묻는 메시지가 출력됩니다. [예]를 클릭하면 보안문서를 생성할 수 있습니다.



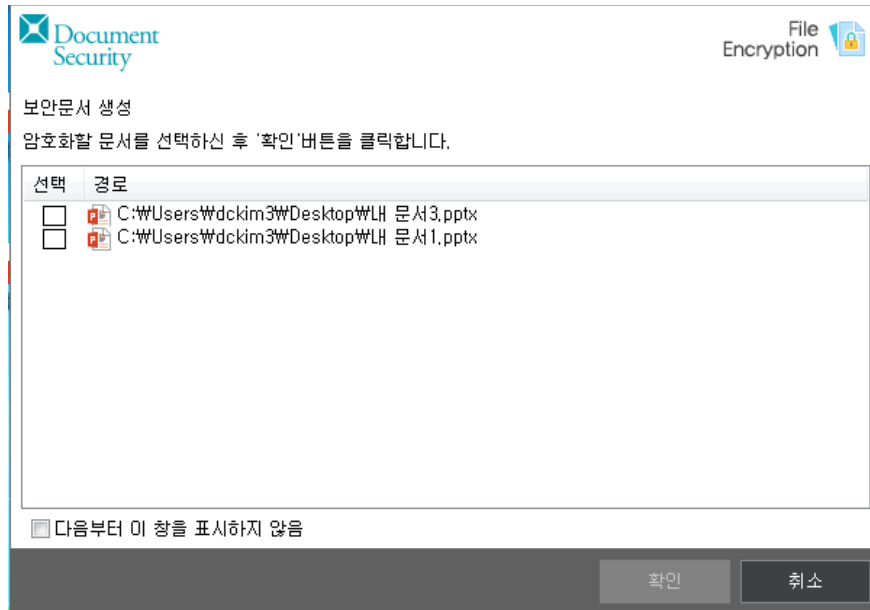
 참고 : 지원하는 문서 편집 어플리케이션 중에 저장 시 암호화 기능을 지원하는 어플리케이션은 아래와 같습니다.

- a. Microsoft Word 2010/2013/2016/2019/365 용 MS Office 호환팩
 - b. Microsoft Excel 2010/2013/2016/2019/365 용 MS Office 호환팩
 - c. Microsoft PoerPoint 2010/2013/2016/2019/365 용 MS Office 호환팩
- 기타 어플리케이션은 어플리케이션 종료 시 암호화 기능만 제공합니다.

문서 작업 후 종료 시

문서 편집 어플리케이션에서 작성한 문서를 종료할 때, 아래의 그림과 같이 문서 암호화 여부를 묻는 메시지가 출력됩니다. 문서 편집 어플리케이션에서 다수의 문서 작업을 한 후 종료했을

경우, 아래와 같이 작업한 문서가 모두 표시됩니다. 암호화하지 않을 문서를 체크 해제하고 **[확인]**를 클릭하면 체크된 문서를 암호화할 수 있습니다. 체크된 문서 중에 가장 상위에 표시된 문서부터 암호화가 진행됩니다.



강제 암호화

관리자가 사용자가 생성한 문서에 대해 강제 암호화를 설정한 경우, 사용자는 문서를 무조건 암호화해야 합니다. 문서 저장 시나 문서 편집 어플리케이션 종료 시 문서가 자동으로 암호화되거나 관리자가 설정한 암호화 방식(개인 보안문서, 범주문서, 등급문서 등)으로만 암호화할 수 있습니다.

5.1.2. 개인 보안문서 생성

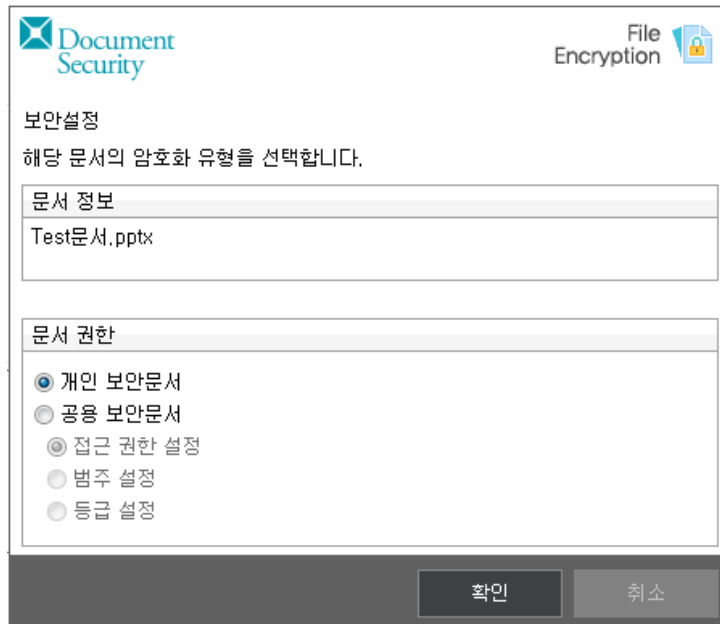
본 장은 개인 보안문서를 생성하는 방법을 설명합니다. 개인 보안문서는 생성한 개인 또한 관리자가 지정한 보안정책에 의해 해당문서의 열람, 편집, 해제(복호화) 등의 사용 가능 여부가 결정됩니다.


개인 보안문서 생성 및 사용 시 주의사항

- 1) 개인 보안문서는 타사용자가 사용할 수 없습니다. 타사용자와 보안문서를 공유하고자 할 때는, 공용 보안문서나, 외부전송용 보안문서를 생성하십시오.
- 2) 개인 보안문서라고 할 지라도 관리자가 설정한 권한에 따라, 해당 문서의 사용이 제한될 수 있습니다. 예를 들어, 열람은 가능하나 편집이 불가능하거나, 열람/편집은 가능하나 해제를 할 수 없을 수 있습니다.

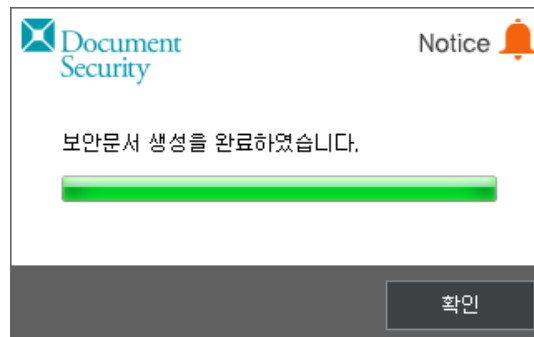
개인 보안문서 생성 방법

- 1) 각각의 [보안문서 생성 경로](#)를 통하면 아래와 같은 메시지 출력됩니다. 개인 보안문서를 생성하려면 '개인 보안문서'를 클릭하고 공용 보안문서를 생성하려면 '공용 보안문서'를 선택합니다. 개인 보안문서 생성하려면 '개인 보안문서'를 클릭하고 [다음]을 클릭합니다. 암호화를 취소하려면 [취소]를 클릭합니다. (공용 보안문서 생성 방법은 [공용 보안문서 생성](#)을 참조하십시오.)

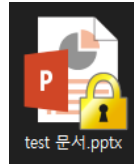


 참고 : 다수의 문서를 암호화하는 경우, 위의 메시지가 암호화할 문서의 갯수대로 표시됩니다.
 각각 다른 방식으로 암호화할 수 있습니다.

- 2) 해당 문서의 암호화가 진행되고, 암호화 진행 과정이 완료되면 아래와 같은 메시지가 출력됩니다. **[확인]**을 클릭하여 암호화를 종료합니다.



- 3) 암호화된 문서의 아이콘이 아래와 같이 변경되었는지 확인합니다.



⚠ 주의: Client 를 설치 및 로그인을 하고 나서, 아래아 한글이나 Acrobat Reader 를 설치하고 관련 문서를 암호화하면, 문서의 아이콘이 변경되지 않을 수 있습니다. 재로그인하거나 컴퓨터를 재부팅하면, 보안문서의 아이콘이 정상적으로 변경됩니다.

⚠ 주의: Windows 7 에서는 바탕화면, 탐색기 내 문서 생성/변경 시 자동으로 Refresh 되지 않아, 보안문서의 아이콘이 갱신되지 않을 수 있습니다. 이 때 바탕화면, 탐색기의 빈 공간을 우클릭하여 나오는 메뉴에서 '새로고침'을 클릭하거나, 'F5'를 누르면 정상적으로 아이콘이 변경됩니다.

5.1.3. 공용 보안문서 생성

본 장은 공용 보안문서를 생성하는 방법을 설명합니다. 공용 보안문서는 생성자, 생성자가 지정한 타사용자 및 부서, 생성자가 선택한 범주 및 등급에 해당하는 타사용자에 의해 접근이 가능합니다. 개인 보안문서와 마찬가지로, 생성자 또한 관리자가 지정한 보안정책에 의해 해당문서의 열람, 편집, 복호화 등의 사용 가능 여부가 결정됩니다. 공용 보안문서는 아래의 3 가지로 구분됩니다.

- 1) **사용자 선택** : 사용자가 해당 공용보안문서에 접근 가능한 사용자 및 부서를 선택하고 권한을 부여할 수 있습니다. 해당 문서에 대한 접근 권한은 생성자를 포함하여 생성자가 선택한 사용자 및 부서에 있습니다. 생성자의 해당 문서에 대한 권한은 생성자가 설정하지 못하며, 관리자가 설정한 권한을 따릅니다.

- 2) **범주** : 해당 보안문서에 대한 접근 권한을 선택한 분류에 속한 사용자 및 그룹마다 다르게 설정합니다. 생성자는 자신에게 설정된 범주만을 선택할 수 있습니다.
- 3) **등급** : 문서 등급별 정책 / 사용자 기준 정책의 혼용방식의 이슈를 해결하고 등급에 따른 사용자/그룹의 추가, 삭제 등이 가능하도록 하는 방식입니다.

관련링크

- a. [사용자 선택](#)
- b. [범주](#)
- c. [등급](#)

5.1.3.1. 사용자 선택

본 장은 사용자 선택을 통한 공용 보안문서 생성 방법에 대해 설명합니다.

사용자 선택 보안문서 생성 시 주의사항

- 1) 생성자는 접근 대상자에게 보안문서의 사용 권한을 설정할 수 있습니다. 이 때, 생성자는 자신이 가진 개인 보안문서 권한에 한해서만 타사용자에게 권한을 부여할 수 있습니다. 예를 들어, 개인 보안문서를 생성했을 때, 문서를 편집이나 출력할 수 없었다면, 사용자 선택 보안문서의 접근 대상자에게 해당 권한을 부여할 수 없습니다.

- 2) 사용자 선택을 통한 공용 보안문서를 생성하기 위해서는 반드시 온라인 상태여야 합니다.
로그아웃이나 오프라인 로그인 상태에서는 사용자 선택을 통한 공용 보안문서를 생성이 불가능합니다.

사용자 선택 보안문서 방법

- 1) 각각의 [보안문서 생성 경로](#)를 통하면 아래와 같은 메시지 출력됩니다. 공용 보안문서를 생성하려면 '공용 보안문서'를 클릭하고 개인 보안문서를 생성하려면 '개인 보안문서'를 선택합니다. 사용자 선택 공용 보안문서 생성하려면 '공용 보안문서'를 클릭하고, '접근 권한 설정'을 선택하고 [다음]을 클릭합니다. 암호화를 취소하려면 [취소]를 클릭합니다. (개인 보안문서 생성 방법은 [개인 보안문서 생성](#)을 참조하십시오.)

Document Security File Encryption

보안설정
해당 문서의 암호화 유형을 선택합니다.

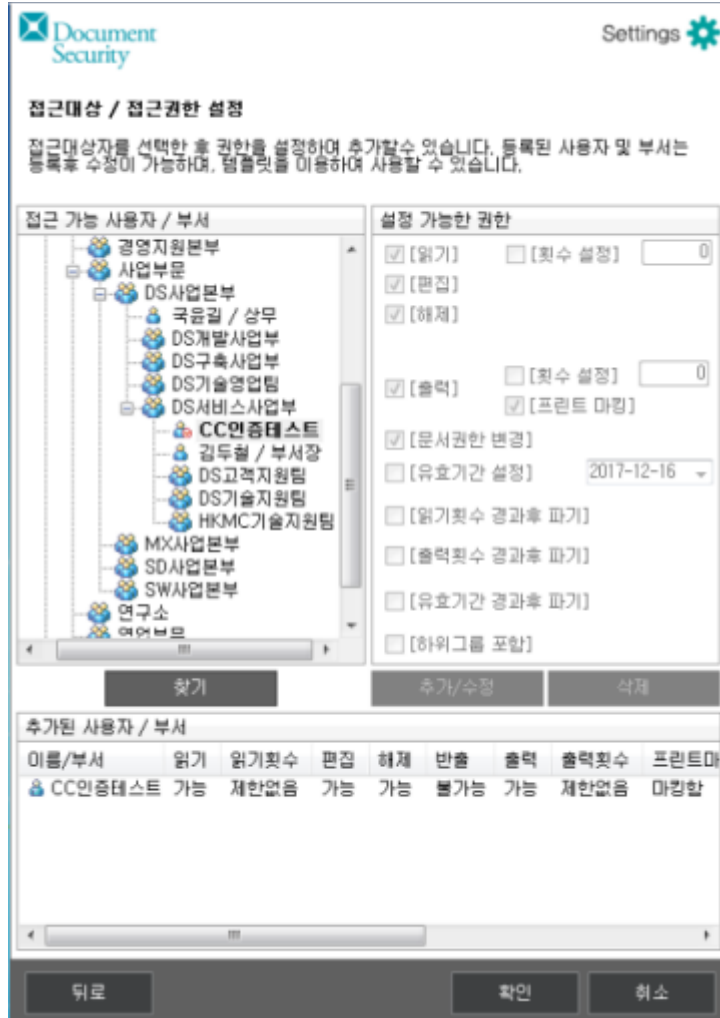
문서 정보
새 Microsoft PowerPoint 프레젠테이션.pptx

문서 권한

- 개인 보안문서
- 공용 보안문서
- 접근 권한 설정
- 범주 설정
- 등급 설정

다음 취소

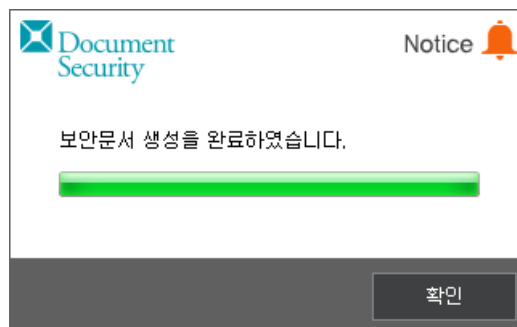
- 2) 아래와 같은 창이 표시되면 '접근 가능 사용자 / 부서'의 조직도에서 해당 보안문서에 접근을 가능하게 할 사용자 및 부서를 선택합니다. 우측의 '설정 가능한 권한'이 활성화 되고 접근 가능한 사용자 및 부서의 문서 권한을 설정합니다. 각 항목의 기능은 아래와 같습니다.



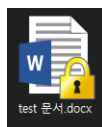
용어	정의
읽기	보안문서에 대하여 열람 권한을 부여 하며 읽기 횟수를 제한/지정할 수 있습니다. [읽기 횟수 설정]을 체크하지 않으면 읽기 횟수는 제한이 없습니다. [읽기 횟수 설정]을 체크하면 읽기 횟수를 설정할 수 있는 창이 활성화되고, 읽기 횟수를 지정할 수 있습니다. [읽기 횟수 설정]을 체크하면 [읽기 횟수 경과 후 파기]가 활성화되고, 읽기 횟수가 경과한 경우, 자동 파기되도록 설정할 수 있습니다.

<p>편집</p>	<p>보안문서에 편집하여 저장 권한을 부여 합니다. [편집]을 선택하게 되면 자동으로 [읽기]의 [Hits 설정]과 [읽기Hits 경과후 파기]이 비활성화됩니다. 즉 열람에는 무제한의 권한이 부여됩니다. [편집]을 비활성화하면 [편집] 기능과 연관된 있는 [해제]와 [문서관한 변경]이 자동으로 비활성화(체크가 안된 상태) 됩니다.</p>
<p>해제</p>	<p>보안문서를 복호화할 수 있는 권한을 부여합니다. [해제]이 체크되면 [편집]이 자동으로 체크 상태가 되면서 [읽기]의 [Hits 설정]과 [읽기Hits 경과후 파기]가 비활성화됩니다. 즉, 해제가 가능하면 편집이 가지는 모든 기능을 가지게 됩니다. 또한 [출력]이 자동 체크 상태가 되고 [출력]의 [Hits 설정]과 [프린트 마킹], [읽기Hits 경과후 파기]가 비활성화됩니다. 즉 해제가 가능하면 출력은 항상 가능하며 출력 Hits는 제한이 없으며 프린트 마킹은 항상 하게 됨을 의미합니다. 그리고 [유효기간 설정] 및 [유효기간 경과 후 파기]가 자동으로 비활성화됩니다.</p>
<p>출력</p>	<p>보안문서를 프린트 출력 권한을 부여 하며 출력 Hits, 프린트 마킹을 지정할 수 있습니다. [출력]이 체크되면 [Hits 설정]과 [프린트마킹]이 활성화가 되게 됩니다. 출력의 [Hits 설정]이 체크하지 않으면 출력이 무제한으로 가능합니다. [Hits 설정]을 체크하면 Hits를 설정할 수 있는 창이 활성화되고, 출력 Hits를 지정할 수 있습니다. [Hits 설정]을 체크하면 [출력Hits 경과후 파기]가 활성화가 됩니다. 이 항목을 체크한 경우 출력Hits 경과 후 문서가 자동으로 파기됩니다. [프린트마킹]은 보안문서의 출력 시 프린트 마킹을 포함시킬 것인지 여부를 나타냅니다. 체크 시 보안문서는 마킹이 되어 출력되게 됩니다. [출력]을 비활성화하면 [출력] 기능과 연관된 있는 [해제]와 [문서관한 변경]이 자동으로 비활성화(체크가 안된 상태) 됩니다.</p>
<p>문서관한변경</p>	<p>보안문서의 접근대상자 변경 권한을 부여합니다. [문서관한 변경] 이 체크되면 [편집]이 자동으로 활성화되어 모든 편집 권한을 가지게 됩니다. 또한 [출력]이 자동으로 활성화되며 출력 Hits의 제한 없이 출력할 수 있으며 프린트 마킹은 항상 포함되게 됩니다. 그리고 자동으로 [유효기간 설정]이 비활성화됩니다.</p>
<p>유효기간 설정</p>	<p>보안문서의 열람 가능 기간을 설정 할 수 있습니다. [유효기간 설정]이 체크되면 일자를 선택할 수 있는 창과 [유효기간 경과후 파기]가 자동으로 활성화되어 유효기간을 설정할 수 있으며 필요 시에 자동파기 기능을 선택할 수 있습니다.</p>
<p>읽기Hits 경과 후 자동 파기</p>	<p>설정한 읽기 Hits를 경과한 경우, 문서가 자동차기 되도록 설정할 수 있습니다.</p>
<p>출력Hits 경과 후 자동 파기</p>	<p>설정한 출력 Hits를 경과한 경우, 문서가 자동차기 되도록 설정할 수 있습니다.</p>
<p>유효기간 경과 후 자동 파기</p>	<p>설정한 유효기간을 경과한 경우, 문서가 자동차기 되도록 설정할 수 있습니다.</p>

- 3) 아래의 예시와 같이 사용자를 선택하고, **[추가/수정]**을 클릭하면 **'추가된 사용자 / 부서'**에 선택한 사용자 또는 부서가 추가됩니다. 추가된 사용자 또는 부서를 해당 보안문서에 대한 접근 대상에서 제외하려면 **'추가된 사용자 / 부서'**에서 제외하고자 하는 사용자 또는 그룹을 선택하고 **[삭제]**를 클릭합니다. 추가된 사용자 또는 부서의 접근권한을 변경하려면, **'추가된 사용자 / 부서'**에서 권한을 변경하고자 하는 사용자 또는 그룹을 선택하고 **'설정 가능한 권한'**에서 권한을 변경한 뒤 **[추가/수정]**을 클릭하면 변경된 권한이 적용됩니다. 접근 대상의 설정을 마쳤으면 **[확인]**을 클릭합니다. **[뒤로]**를 클릭하면 전단계로 되돌아 갑니다. **[취소]**를 클릭하면 보안문서 생성을 취소합니다.
- 4) 아래와 같은 메시지가 출력되고 **[확인]**을 클릭하면 작업이 완료됩니다.



- 5) 아래와 같이 보안문서가 정상적으로 생성되었는지 확인합니다.



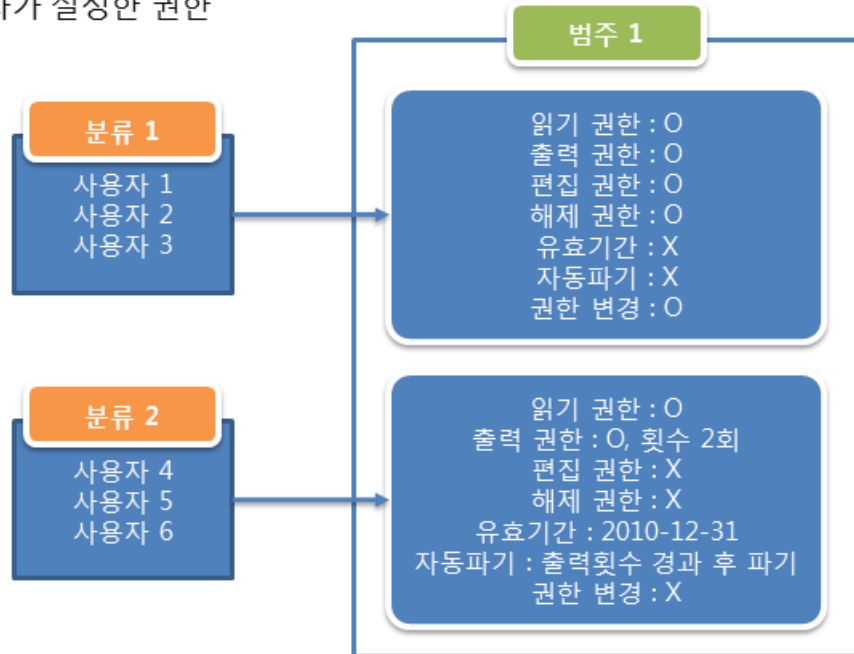
5.1.3.2. 범주

본 장은 범주를 통한 공용 보안문서 생성 방법에 대해 설명합니다.

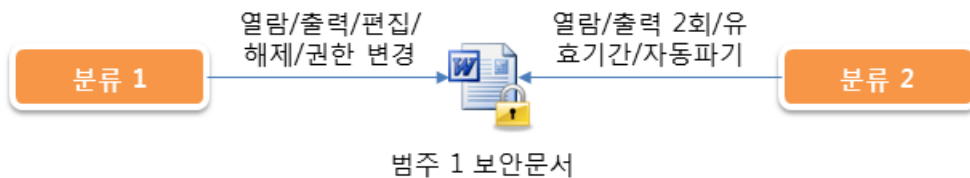
범주란?

범주 정책은 사용자의 분류마다 해당 범주로 암호화된 문서의 사용 권한을 다르게 설정하여, 사용자의 지위나 업무에 따라 필요한 수준의 사용 권한을 부여하는 정책을 의미합니다. 아래의 예시와 같이 각각의 분류마다 같은 범주로 암호화된 문서의 사용 권한이 상이하게 적용됩니다.

관리자가 설정한 권한



범주 1 보안문서 사용 권한



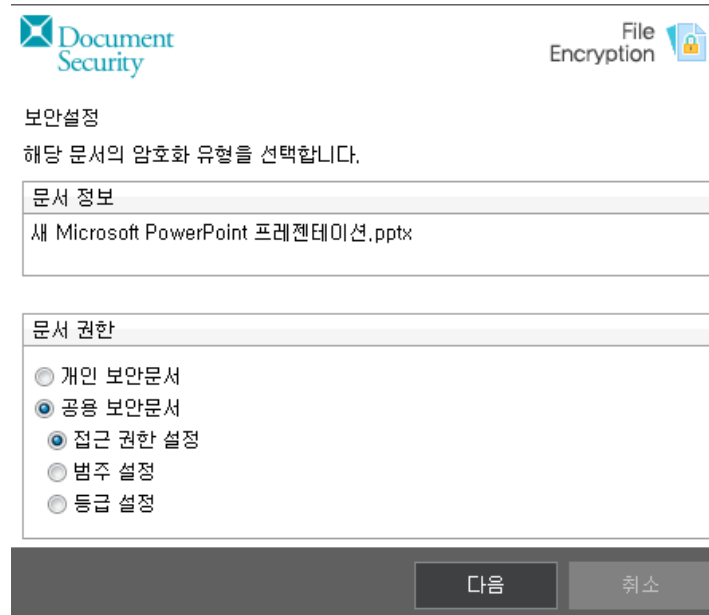
'분류 1'에 속한 '사용자 1'이 '범주 1'로 보안문서를 생성했을 경우, '분류 1'에 속한 '사용자 2'나 '사용자 3'은 해당 보안문서에 대해 열람/출력/편집/해제/권한 변경이 가능하나, '분류 2'에 속한 '사용자 4, 5, 6'은 열람 및 출력 2 회만 가능하고, 유효기간(2010 년 12 월 31 일)이 지나면 사용이 불가능합니다. 또한 출력 횟수가 경과하면 자동 파기됩니다. 사용자는 각각의 범주에 대한 권한을 [사용자 정보 확인](#)에서 확인할 수 있습니다.

범주 보안문서 생성 시 주의사항

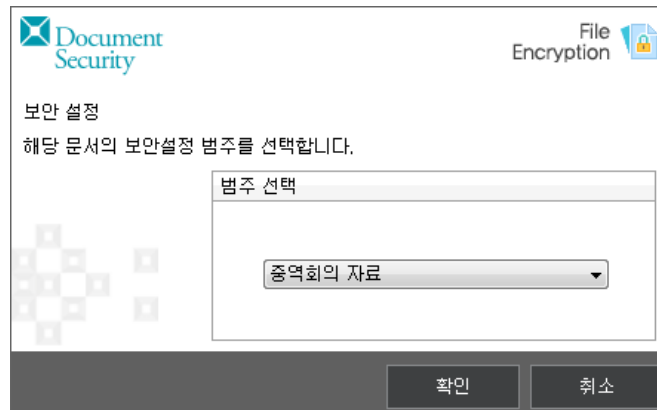
- 1) 사용자가 선택 가능한 범주는 관리자에 의해 설정됩니다. 사용자는 임의로 범주를 추가/변경/삭제할 수 없습니다.

범주 보안문서 방법

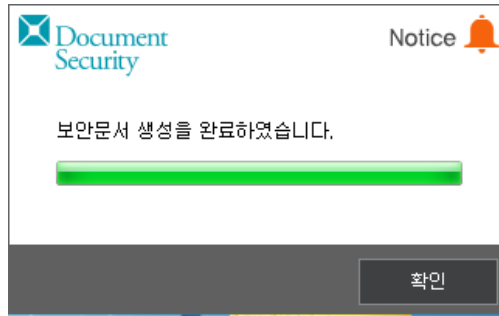
- 1) 각각의 [보안문서 생성 경로](#)를 통하면 아래와 같은 메시지 출력됩니다. 공용 보안문서를 생성하려면 '공용 보안문서'를 클릭하고 개인 보안문서를 생성하려면 '개인 보안문서'를 선택합니다. 사용자 선택 공용 보안문서 생성하려면 '공용 보안문서'를 클릭하고, '범주 설정'을 선택하고 [다음]을 클릭합니다. 암호화를 취소하려면 [취소]를 클릭합니다. (개인 보안문서 생성 방법은 [개인 보안문서 생성](#)을 참조하십시오.)



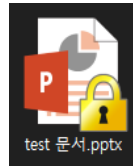
- 2) 아래와 같은 창이 표시되면 '범주 선택'의 드롭다운 메뉴에서 범주를 선택하고 [확인]을 클릭합니다. [뒤로]를 클릭하면 전단계로 되돌아 갑니다. [취소]를 클릭하면 보안문서 생성을 취소합니다.



- 3) 아래와 같은 메시지가 출력되고 [확인]을 클릭하면 작업이 완료됩니다.



4) 아래와 같이 보안문서가 정상적으로 생성되었는지 확인합니다.



5.1.3.3. 등급

본 장은 등급을 통한 공용 보안문서 생성 방법에 대해 설명합니다.

등급이란?

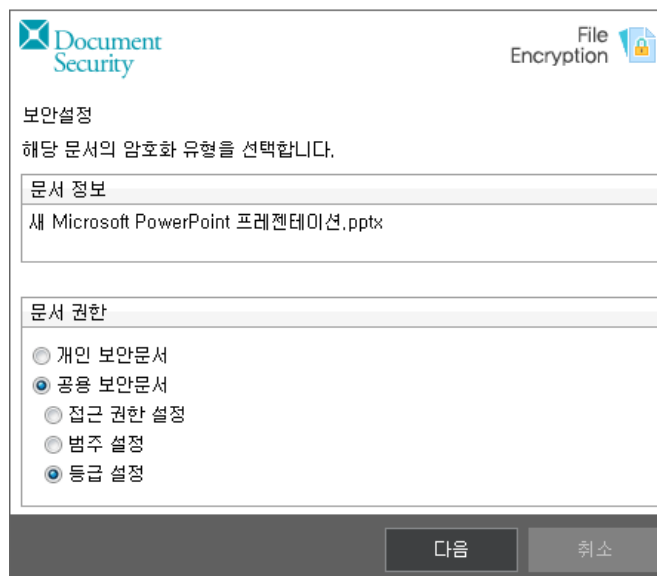
등급은 사용자 선택과 범주를 결합한 형태의 암호화 정책입니다. 범주와 같이 분류에 따라 등급 보안문서에 대한 사용 권한이 상이하게 적용됩니다. 또한, 사용자 선택 기능이 추가되어, 암호화 시 접근 대상자를 선택할 수 있고, 권한을 설정할 수 있습니다.

등급 보안문서 생성 시 주의사항

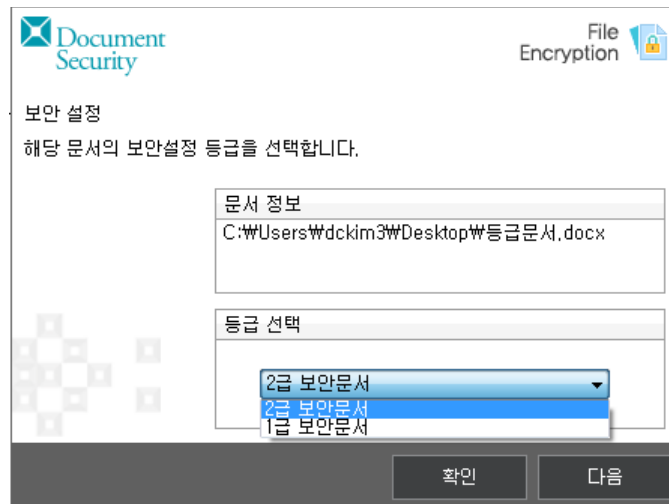
- 1) 사용자는 선택 가능한 등급은 관리자에 의해 설정됩니다. 사용자는 임의로 등급을 추가/변경/삭제할 수 없습니다.

등급 보안문서 방법

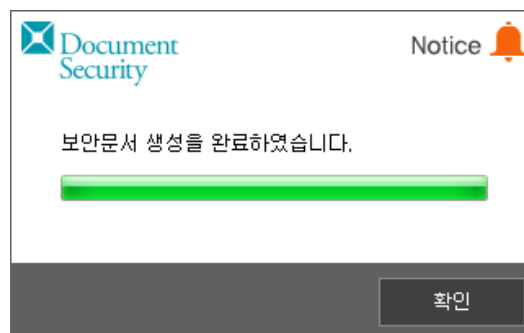
- 1) 각각의 [보안문서 생성 경로](#)를 통하면 아래와 같은 메시지 출력됩니다. 공용 보안문서를 생성하려면 '공용 보안문서'를 클릭하고 개인 보안문서를 생성하려면 '개인 보안문서'를 선택합니다. 사용자 선택 공용 보안문서 생성하려면 '공용 보안문서'를 클릭하고, '등급 설정'을 선택하고 [다음]을 클릭합니다. 암호화를 취소하려면 [취소]를 클릭합니다. (개인 보안문서 생성 방법은 [개인 보안문서 생성](#)을 참조하십시오.)



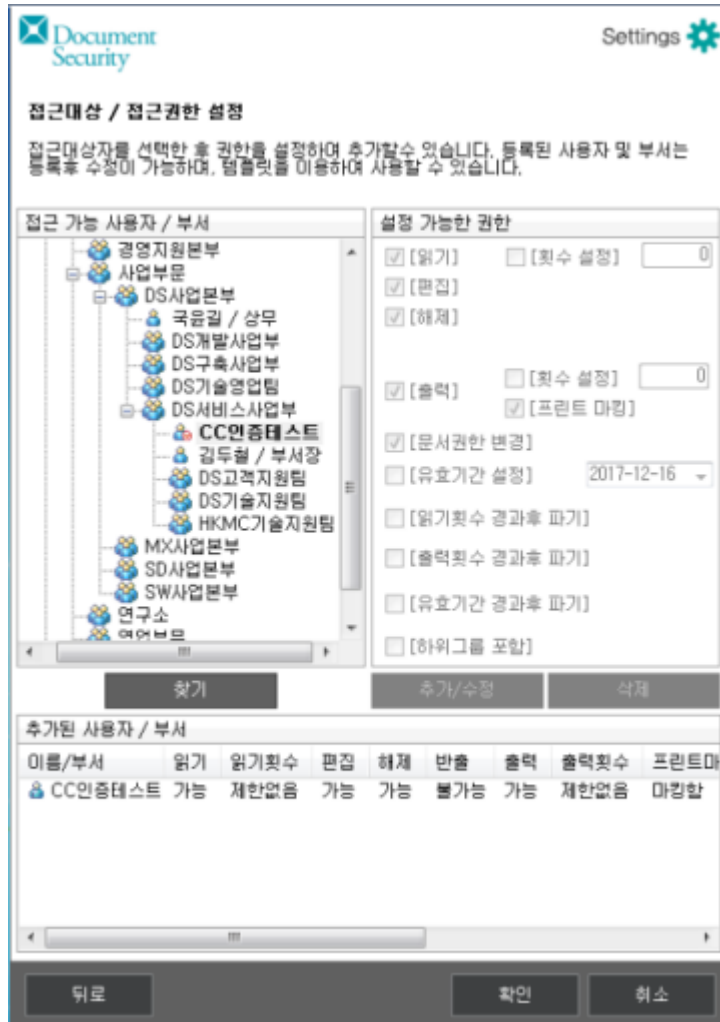
- 2) 아래와 같은 창이 표시되면 '등급 선택'의 드롭다운 메뉴에서 등급을 선택하고 **[확인]**을 클릭하면 보안문서가 생성됩니다. **[뒤로]**를 클릭하면 전단계로 되돌아 갑니다. **[다음]**를 클릭하면 사용자를 선택할 수 있습니다.



- 3) 위의 메시지에서 **[확인]**을 클릭한 경우, 아래와 같은 메시지가 출력되고 **[확인]**을 클릭하면 작업이 완료됩니다. **[다음]**을 클릭한 경우, 아래와 같이 사용자를 선택할 수 있습니다. **[다음]**을 클릭한 경우, [사용자 선택](#)을 참조하시기 바랍니다.

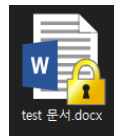


[확인]을 클릭한 경우



[다음]을 클릭한 경우

4) 아래와 같이 보안문서가 정상적으로 생성되었는지 확인합니다.



5.2. 보안문서 사용

본 장은 보안문서의 사용에 대해 설명합니다.

관련링크

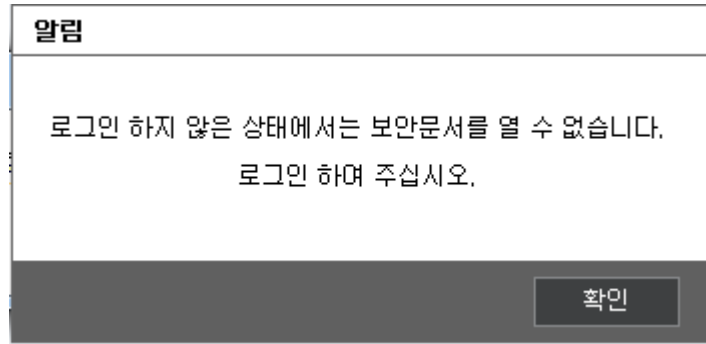
- a. [보안문서의 기본 사용](#)
- b. [보안문서의 권한 확인](#)
- c. [보안문서의 사용 제어](#)

5.2.1. 보안문서의 기본 사용

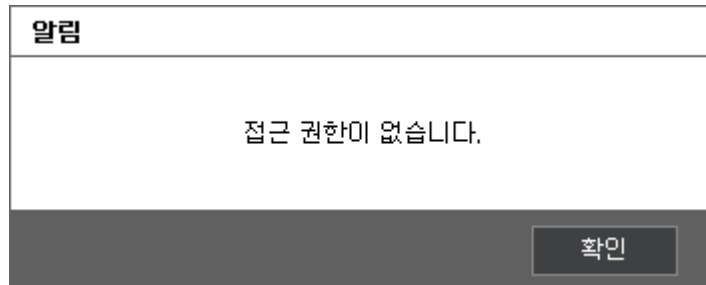
본 장은 보안문서의 사용에 대해 설명합니다. 보안문서를 사용하는 방법은 일반문서와 동일합니다. 하지만 사용자마다 보안문서를 사용할 수 있는 권한이 설정되어 있어, 일반문서와 같이 자유롭게 열람/편집/출력 등을 하지 못할 수 있습니다. 또한, 유효기간이 설정된 보안문서는 유효기간이 지나면 사용할 수 없습니다.

보안문서 열람, 열람횟수 제한, 자동파기

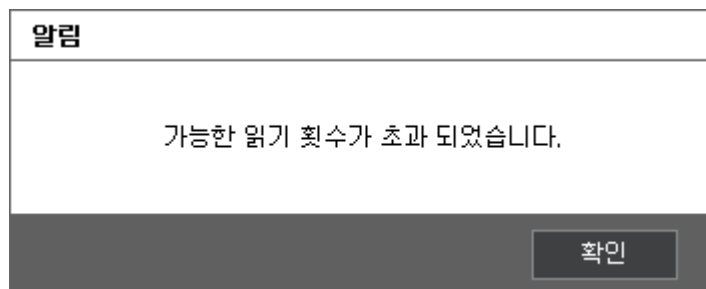
보안문서를 열람하는 방법은 일반문서와 동일합니다. 문서의 아이콘을 더블클릭하여 실행하거나, 문서 편집 어플리케이션을 실행한 후 불러오기를 통해 열람할 수 있습니다. 보안문서는 반드시 Client 에 로그인/오프라인 로그인 상태에서만 열람이 가능합니다. 로그아웃 상태에서 보안문서의 열람을 시도하면 아래와 같은 메시지가 출력됩니다.



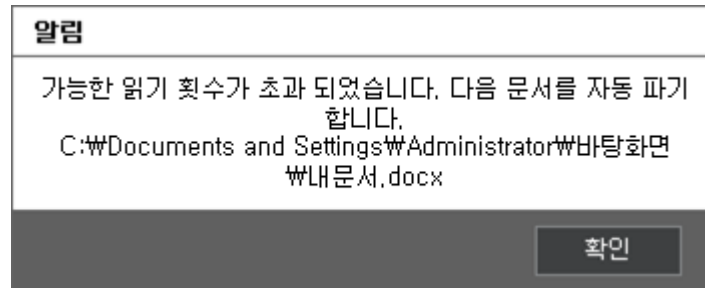
열람할 수 있는 권한이 없는 사용자의 경우, 아래와 같은 메시지가 표시되며 열람이 불가능합니다.



보안문서에 열람 횟수가 제한된 경우, 해당 횟수가 경과하면 더 이상 보안문서를 열람할 수 없습니다. 열람 횟수가 경과하면 아래와 같은 메시지가 출력됩니다.

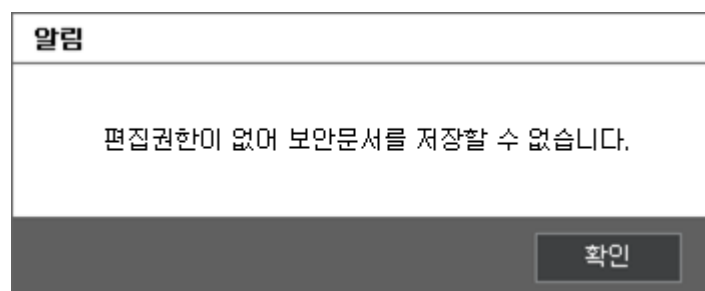



보안문서에 열람 횟수가 경과하면 자동으로 파기되는 경우, 아래와 같은 메시지가 출력되며, 보안문서가 자동으로 파기됩니다.



보안문서 편집

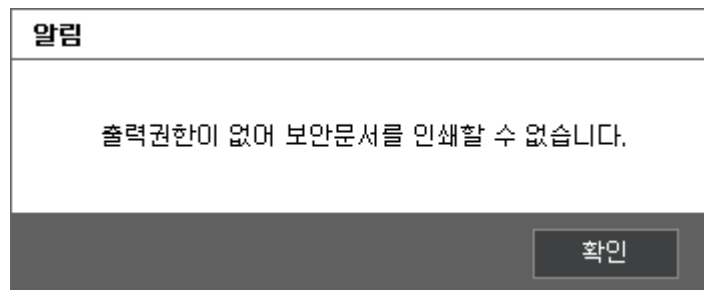
보안문서를 편집하는 방법은 일반문서와 동일합니다. 문서 편집 어플리케이션에 보안문서를 불러온 후, 내용을 변경하고 저장하면 됩니다. 보안문서의 편집 권한이 있는 사용자는 열람 권한 또한 자연스럽게 가집니다. 보안문서의 편집 권한이 있는 사용자는 일반문서와 마찬가지로, 변경된 내용이 저장됩니다. 편집 권한이 없는 사용자가 내용을 변경하고 저장을 시도하는 경우, 아래와 같은 메시지가 표시되며 편집이 불가능합니다.



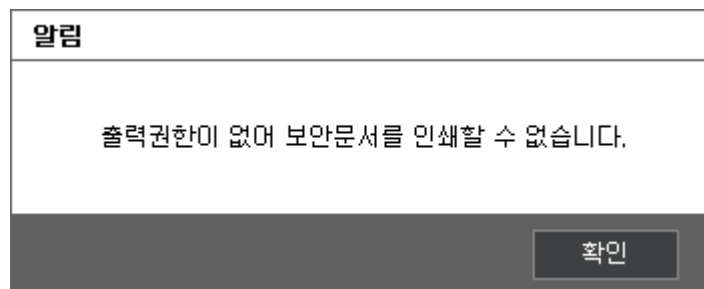
 참고 : 관리자의 설정에 따라, 저장시점에 암호화 여부를 묻는 창이 표시되거나, 자동으로 암호화될 수 있습니다. [보안문서 생성 경로](#)를 참고하십시오.

보안문서 출력, 출력횟수 제한, 자동파기

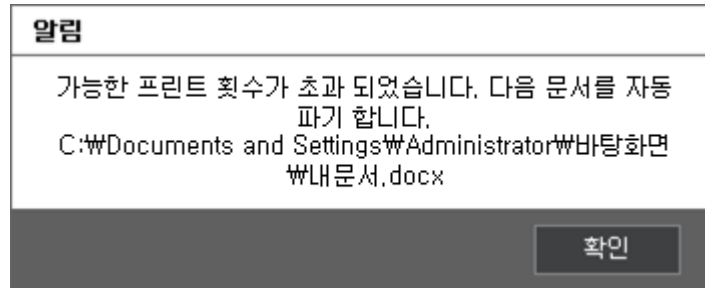
보안문서를 출력하는 방법은 일반문서와 동일합니다. 문서 편집 어플리케이션에 보안문서를 불러온 후, 인쇄를 하면 됩니다. 보안문서의 출력 권한이 있는 사용자는 열람 권한 또한 자연스럽게 가집니다. 출력 권한이 없는 사용자가 출력을 시도하는 경우, 아래와 같은 메시지가 표시되며 출력이 불가능합니다.



보안문서에 출력 횟수가 제한된 경우, 해당 횟수가 경과하면 더 이상 보안문서를 출력할 수 없습니다. 출력 횟수가 경과하면 아래와 같은 메시지가 출력됩니다.

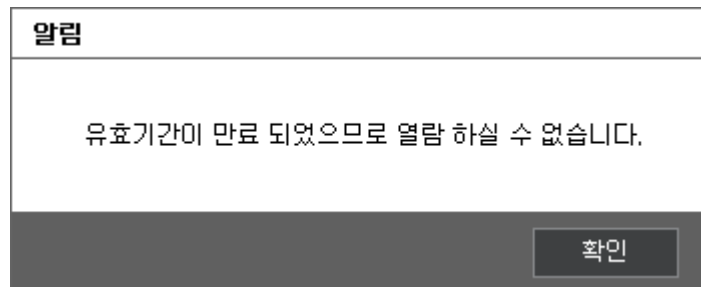


보안문서에 출력 횟수가 경과하면 자동으로 파기되는 경우, 아래와 같은 메시지가 출력되며, 보안문서가 자동으로 파기 됩니다.

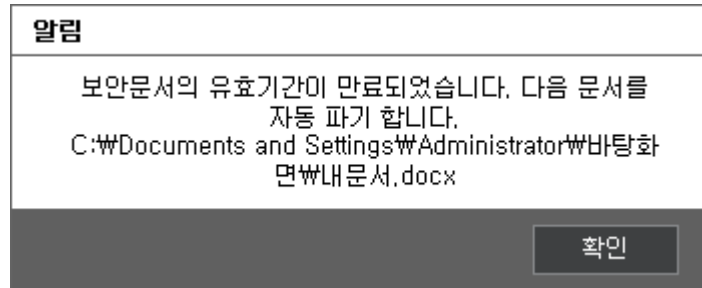


보안문서 유효기간 및 자동파기

보안문서에 유효기간이 설정될 수 있습니다. 유효기간이 설정되면 유효기간 내에는 권한에 따라 보안문서를 사용할 수 있지만, 유효기간이 경과하면 더이상 보안문서를 열람조차 할 수 없습니다. 유효기간이 경과한 보안문서의 열람을 시도하면 아래와 같은 메시지가 표시되면 열람이 불가능합니다.



유효기간 경과 후 자동파기되도록 설정된 보안문서의 열람을 시도하면 아래와 같은 메시지가 표시되며 파기됩니다.



보내기, 게시 기능 제어

Microsoft Office 에서 생성된 보안문서의 경우, Microsoft Office 에서 제공하는 '보내기'와 '게시' 기능이 차단됩니다. 보안문서에서 차단되는 기능은 아래와 같습니다.

Microsoft Office (Word, Excel, PowerPoint) 공통

- 1) 보내기>전자 메일
- 2) 보내기>PDF 첨부 파일로 전자 메일 보내기
- 3) 보내기>XPS 첨부 파일로 전자 메일 보내기
- 4) 보내기>인터넷 팩스
- 5) 게시>문서 관리 서버
- 6) 게시>문서 작업 영역 만들기

Microsoft Office Word

- 1) 게시>블로그

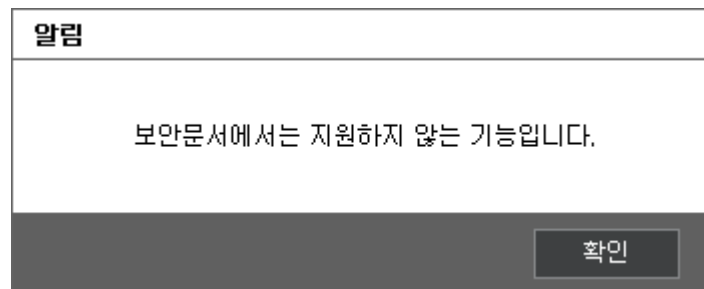
Microsoft Office Excel

- 1) Excel 서비스

Microsoft Office PowerPoint

- 1) 게시>CD 용 패키지
- 2) 게시>슬라이드 게시
- 3) 게시>Microsoft Office Word 에서 유인물 만들기

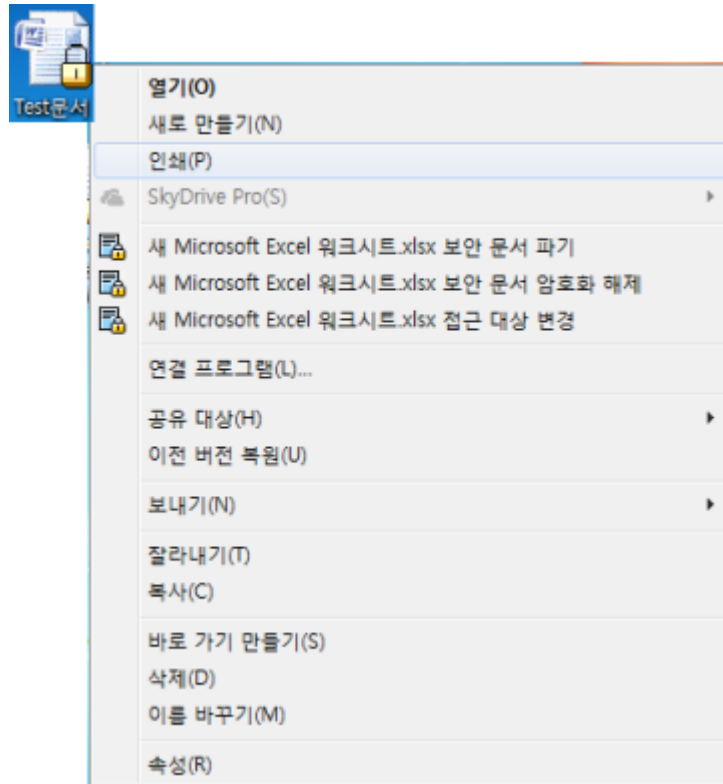
보안문서를 열고, '보내기' 또는 '게시' 기능을 시도할 경우, 아래와 같은 메시지가 출력됩니다.



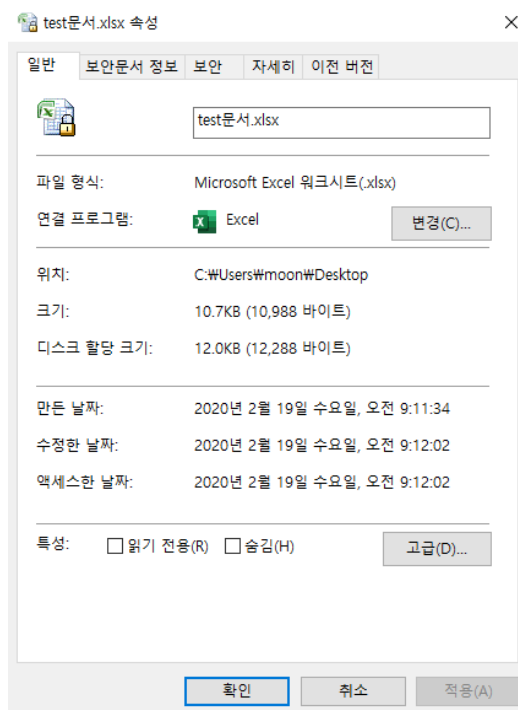
5.2.2. 보안문서의 권한 확인

본 장은 보안문서의 권한 확인에 대해 설명합니다. 사용자는 보안문서에 대한 본인의 접근 권한을 확인하여 열람, 편집, 출력, 해제, 권한 변경 등의 가능 여부를 확인할 수 있습니다.

- 1) 권한을 확인하고자 하는 보안문서를 우클릭하여, 표시되는 메뉴에서 '속성'을 클릭합니다.



2) 아래의 창이 표시되면 창의 상단 탭 중에 '보안문서 정보'를 클릭합니다.



3) 아래와 같은 창이 표시되고 보안문서에 대한 정보, 접근 대상자 정보, 현재 PC 에 로그인한 사용자의 문서 권한을 볼 수 있습니다. 각각의 내용은 아래와 같습니다. **[확인]**을 클릭하면 창이 닫힙니다.



a. **일반 정보** : 보안문서에 대한 일반적인 정보를 표시합니다.

용어	정의
원본 문서 이름	해당 문서의 경로를 포함한 파일명을 표시합니다. 경로가 길 경우, 경로와 파일명을 확인하지 못할 수도 있습니다.
최초 생성자 / 일시	해당 문서의 최초생성자의 ID 와 해당 문서를 생성한 일시를 나타냅니다.
최근 문서 사용자	가장 최근에 사용한 사용자의 ID 를 나타냅니다.
문서 등급	등급 보안문서일 경우, 해당 문서의 등급을 표시합니다. 다른 형식의 보안문서일 경우 '없음'이 표시됩니다.

b. **접근 대상자 정보** : 해당 문서의 접근 대상자 정보를 표시합니다.

용어	정의
범주	범주 보안문서일 경우, 해당 문서의 범주를 표시합니다. 다른 형식의 보안문서일 경우 '없음'이 표시됩니다
이름	현재 PC 에 로그인한 사용자의 이름을 출력합니다.
읽기	보안문서의 열람 가능 여부를 나타냅니다.
읽기횟수	보안문서를 열람할 수 있는 횟수를 나타냅니다. 횟수의 제한이 없으면 '제한없음'이 표시됩니다.
편집	보안문서의 편집 가능 여부를 나타냅니다.
해제	보안문서의 복호화 가능 여부를 나타냅니다.
출력	보안문서의 출력 가능 여부를 나타냅니다.
출력횟수	보안문서를 출력할 수 있는 횟수를 나타냅니다. 횟수의 제한이 없으면 '제한없음'이 표시됩니다.
프린트마킹	보안문서를 출력 시 관리자가 지정한 프린트 마킹의 삽입 여부를 나타냅니다.
유효기간	보안문서를 사용할 수 있는 기간을 나타냅니다.
자동파기	읽기횟수 및 출력횟수 초과 시, 보안문서 유효기간 경과 시 자동파기 여부를 나타냅니다.
권한변경	보안문서의 접근 대상 변경 가능 여부를 나타냅니다.

- c. **로그인한 사용자 문서 권한** : 현재 PC 에 로그인한 사용자의 해당 보안문서에 대한 사용 권한을 표시합니다.

용어	정의
이름	현재 PC 에 로그인한 사용자의 이름을 출력합니다.
읽기	보안문서의 열람 가능 여부를 나타냅니다.
읽기횟수	보안문서를 열람할 수 있는 횟수를 나타냅니다. 횟수의 제한이 없으면 '제한없음'이 표시됩니다.
편집	보안문서의 편집 가능 여부를 나타냅니다.
해제	보안문서의 복호화 가능 여부를 나타냅니다.
출력	보안문서의 출력 가능 여부를 나타냅니다.
출력횟수	보안문서를 출력할 수 있는 횟수를 나타냅니다. 횟수의 제한이 없으면 '제한없음'이 표시됩니다.
프린트마킹	보안문서를 출력 시 관리자가 지정한 프린트 마킹의 삽입 여부를 나타냅니다.
유효기간	보안문서를 사용할 수 있는 기간을 나타냅니다.
자동파기	읽기횟수 및 출력횟수 초과 시, 보안문서 유효기간 경과 시 자동파기 여부를 나타냅니다.
권한변경	보안문서의 접근 대상 변경 가능 여부를 나타냅니다.

5.2.3. 보안문서의 사용 제어

본 장은 보안문서의 사용 제어에 대해 설명합니다. Client 가 설치된 사용자의 PC 에서 보안문서가 가지는 내용의 유출을 방지하기 위한 보안기능이 동작합니다.

복사 / 붙여넣기 제어

Client 에 로그인/오프라인 로그인 상태에서는 문서 편집 어플리케이션에서 작업 중인 내용을 복사하여 다른 어플리케이션으로 붙여넣기하는 것이 차단될 수 있습니다. 이는 복사&붙여넣기에 대한 보안 정책 설정에 따른 것입니다.

복사 / 붙여넣기에 대한 제한이 없을 경우 문서 편집 어플리케이션에서 작업 중인 내용을 자유롭게 복사하여 다른 문서에 붙여넣을 수 있으나, 정책적으로 제한한 경우(예, 편집권한 이상 있는 문서에 한하여 보안문서로 저장 허용), 복사하고 붙여넣기 대상 파일의 권한에 따라서 붙여넣기가 되지 않을 수 있습니다. 이 경우 별도의 알림 메시지는 제공되지 않습니다.



참고 : 복사 / 붙여넣기의 제한은 다음과 같이 보안문서의 사용 권한에 따라 다르게 적용될 수 있습니다. .

- 1) 복사 / 붙여넣기 전면 차단 : 보안문서 내의 내용에 대한 복사 / 붙여넣기가 전부 차단됩니다.
- 2) 복사 / 붙여넣기 전면 허용 : 보안문서 내의 내용에 대한 복사 / 붙여넣기가 자유롭게 허용됩니다.

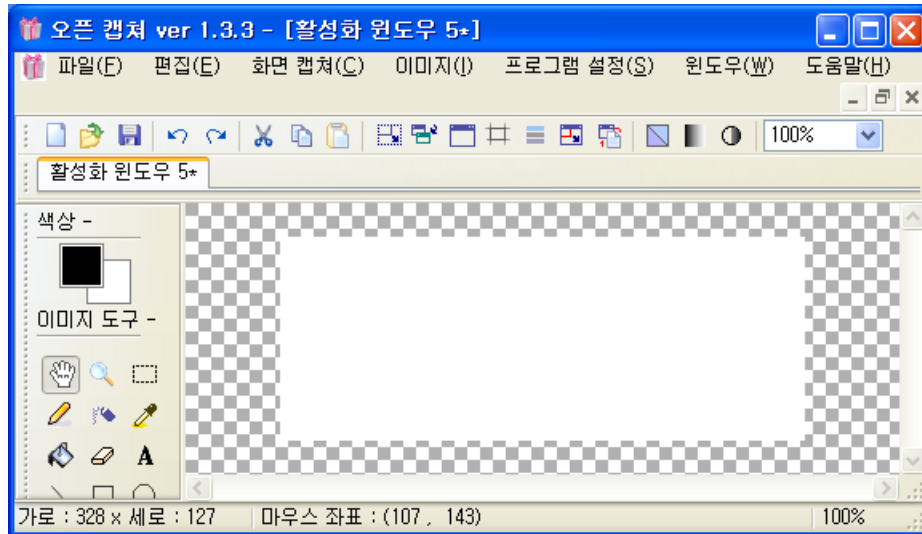
- 3) 편집 가능한 보안문서에서 보안문서로 복사 / 붙여넣기 허용 : 편집/해제 가능한 보안문서 내의 내용에 대한 복사 / 붙여넣기가 보안문서에 한해 허용됩니다. 일반문서로는 붙여넣기할 수 없습니다.


프린트 마킹

Client 에 로그인/오프라인 로그인 상태에서는 문서 편집 어플리케이션에서 작업 중인 내용을 출력할 경우, 출력물에 사용자의 이름 및 부서, 보안문서의 범주 또는 등급 등이 같이 출력될 수 있습니다. 프린트 마킹은 관리자가 설정하는 것으로, 설정에 따라 프린트 마킹 이미지나 문자열의 내용/위치/농도 등이 다를 수 있으며, 실제 프린터 드라이버의 특성에 따라 다르게 출력될 수 있습니다(PCL 6 이상 권장합니다.).

화면캡처 제어

Client 는 프린트 스크린 키(Print Screen)이나 화면 캡처툴을 이용한 화면 캡처를 제어할 수 있습니다. 관리자의 설정에 따라 프린트 스크린이나 화면 캡처툴을 이용한 화면 캡처가 불가능할 수 있습니다. 관리자가 화면 캡처를 제어한 경우, 프린트 스크린 키를 눌러 화면을 캡처되지 않아 붙여넣기를 할 수 없고, 화면 캡처툴로 캡처를 시도한 경우 아래의 그림과 같이 흰색 또는 블랙의 아무 내용이 없는 화면만 표시됩니다.



 참고 : 특정 화면 캡처틀의 경우는 프로그램 실행 자체가 차단될 수 있습니다.

Microsoft Office 슬라이드 및 파일 메뉴 제어

MS Office 의 슬라이드 및 파일 메뉴가 일부 제어됩니다. 제어되는 기능은 아래와 같습니다.

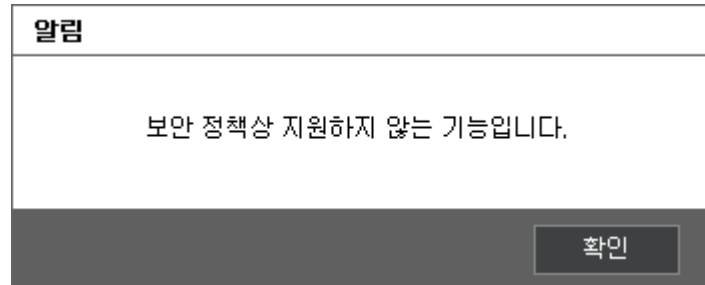
Microsoft Office Word

- 1) 삽입>개체>파일 텍스트
- 2) 편지 (관련 모든 기능)
- 3) 검토>비교

Microsoft Office PowerPoint

- 1) 홈>새 슬라이드>슬라이드 다시 사용
- 2) 삽입>사진 앨범

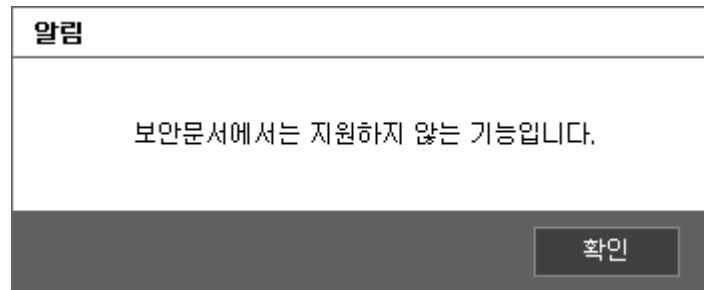
위의 기능을 실행을 시도하면 아래와 같은 메시지가 출력됩니다.



매크로 제어

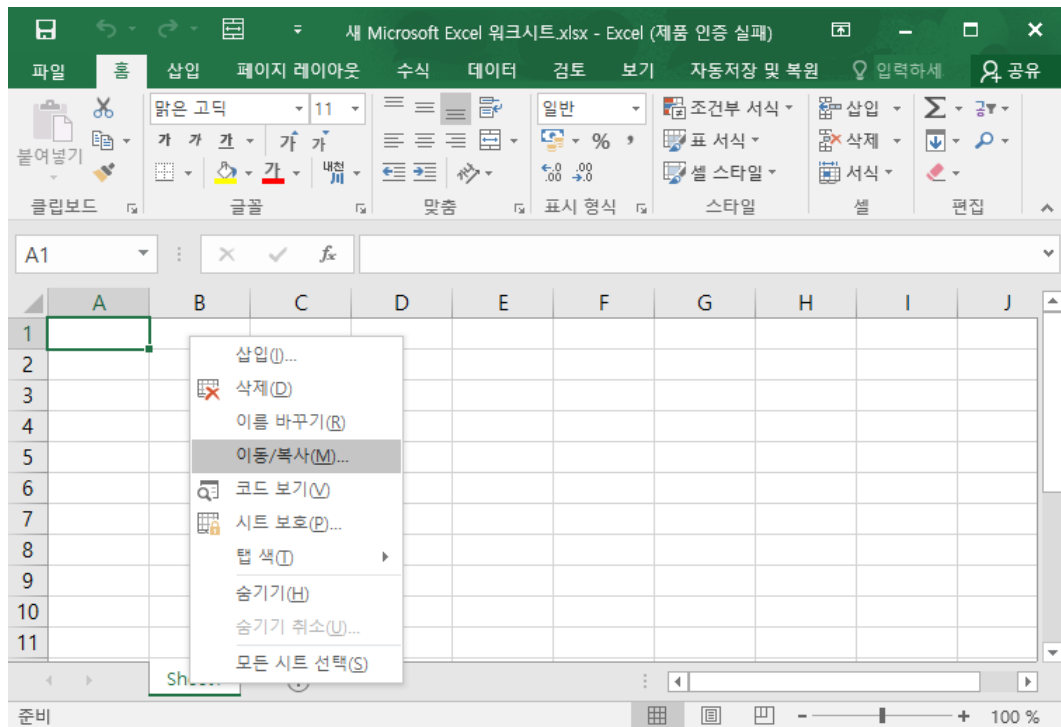
Microsoft Office 에서 제공하는 매크로 기능을 제어합니다. 매크로는 매크로 명령어(macro instruction)의 줄임말로 프로그램 내에서 1 개 이상의 문장으로 이루어진 프로그램의 한 블록이 프로그램 곳곳에 반복적으로 쓰일 때 이러한 프로그램 작성상의 불편을 없애기 위해 반복적으로 사용되는 부분을 약자로 따로 정의하여 사용 할 수 있도록 정의한 명령어 집합입니다. 매크로 기능은 사용자의 능력에 따라 여러 문서의 데이터를 조합 하여 새로운 문서 생성 및 문서간의 병합기능을 자유자재로 이용을 할 수 있으므로 보안문서의 내용과 일반문서의 내용을 병합하여 새로운 일반문서 생성이 가능하며, 정보 유출의 위험이 있습니다. 이에 관리자의 설정에 의해 보안문서에서 매크로 사용이 차단될 수 있습니다.

관리자가 매크로를 차단한 경우, Microsoft Office 의 보안문서에서 **보기>매크로**를 실행하면 아래와 같은 메시지가 출력되면 사용이 차단됩니다.

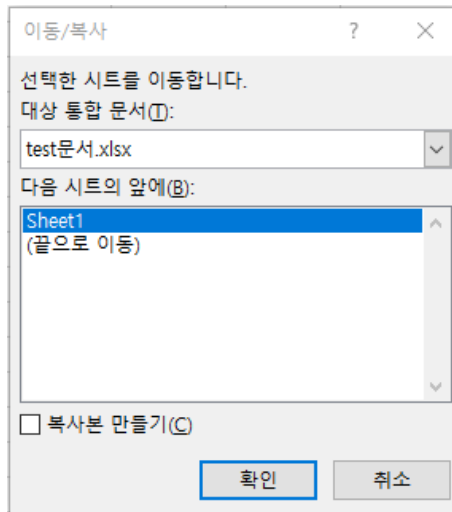


Microsoft Office Excel 시트 이동 / 복사 제어

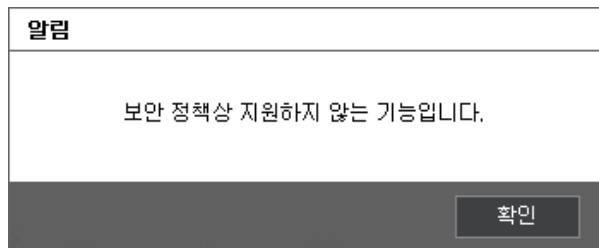
Client 는 MS Office Excel 의 보안문서에 대해 시트의 이동 및 복사를 제어합니다. 관리자의 권한에 따라 암호화된 엑셀 문서의 시트를 다른 엑셀 문서로 이동 및 복사하는 것이 차단됩니다. 아래의 그림과 같이 시트 이동 및 복사를 수행할 경우 드롭다운 메뉴가 비활성화되어, 다른 엑셀문서를 선택할 수 없습니다.



엑셀 시트 아래의 탭을 우클릭하여 나오는 메뉴에서 '이동/복사' 클릭

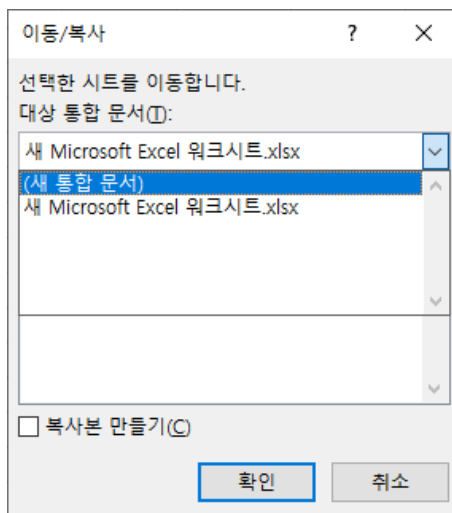


드롭다운 메뉴를 사용할 경우



알림 메시지가 나타나고 드롭다운 메뉴는 사용할수 없습니다.

관리자가 허용한 경우, 아래의 그림과 같이 자유롭게 엑셀 시트를 이동 및 복사할 수 있습니다.



드롭다운 메뉴에서 엑셀문서 선택 가능

보내기, 게시 기능 제어

Client 는 Microsoft Office 에서 제공하는 '보내기'와 '게시' 기능을 제어할 수 있습니다.

관리자의 설정에 따라, Microsoft Office 에서 제공하는 기능인 작성한 문서를 바로 메일에 첨부하거나, 인터넷 팩스를 보내거나, 블로그에 게시하는 등의 기능이 차단됩니다. 차단되는 기능은 아래와 같습니다.

Microsoft Office (Word, Excel, PowerPoint) 공통

- 1) 보내기>전자 메일
- 2) 보내기>PDF 첨부 파일로 전자 메일 보내기
- 3) 보내기>XPS 첨부 파일로 전자 메일 보내기
- 4) 보내기>인터넷 팩스
- 5) 게시>문서 관리 서버
- 6) 게시>문서 작업 영역 만들기

Microsoft Office Word

- 1) 게시>블로그


Microsoft Office Excel

- 1) Excel 서비스

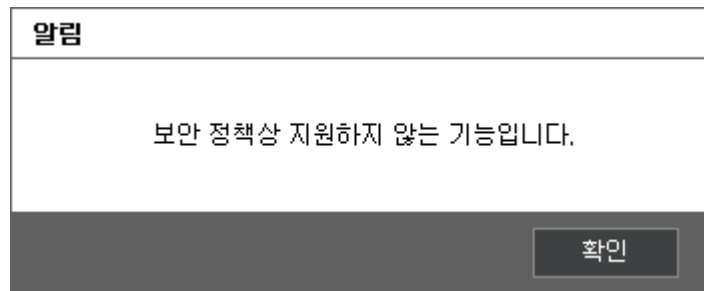
Microsoft Office PowerPoint

- 1) 게시>CD 용 패키지

- 2) 게시>슬라이드 게시
- 3) 게시>Microsoft Office Word 에서 유인물 만들기

 참고 : 보안문서의 경우, 위의 기능은 관리자의 설정과 관계없이 차단됩니다.

위의 기능들이 시도될 경우, 아래와 같은 메시지가 출력됩니다.



5.3. 보안문서 권한 변경

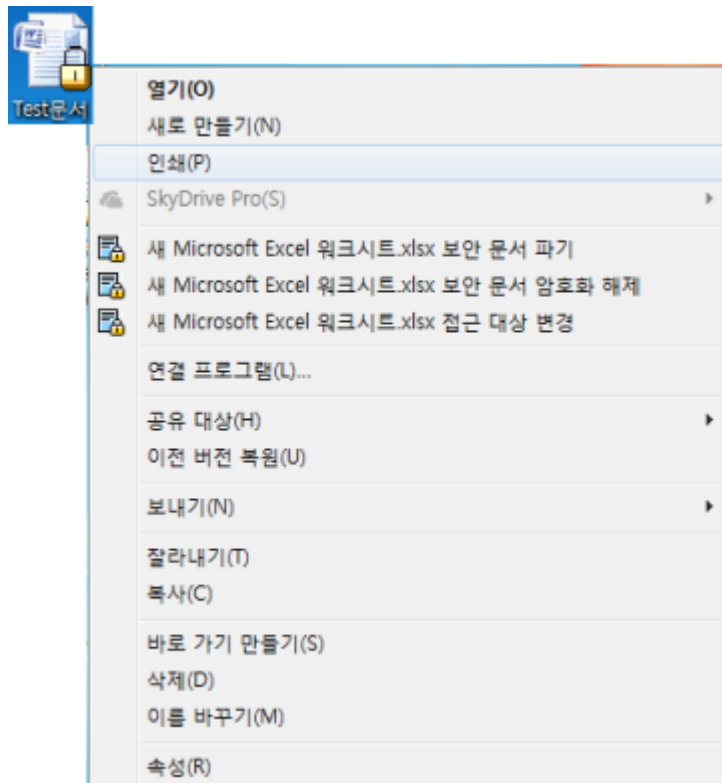
본 장은 보안문서의 권한 변경에 대해 설명합니다. 보안문서를 업무 상의 이유로 접근 권한이 없는 사용자가 사용해야할 경우, 보안문서에 설정된 접근 대상을 변경하거나 다른 범주나 등급으로 설정하여 해당 문서에 대한 접근 권한이 없는 사용자가 접근할 수 있도록 할 수 있습니다.

보안문서 권한 변경 시 주의사항

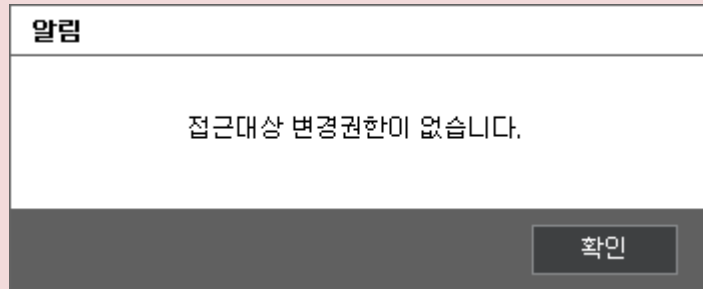
- 1) 해당 보안문서에 대해 권한 변경을 할 수 있는 권한이 있는 사용자만 권한을 변경할 수 있습니다.
- 2) 보안문서의 암호화 방식에 따라 권한 변경을 할 수 없을 수 있습니다.
- 3) 보안문서의 암호화 방식은 변경할 수 없습니다. 예를 들어, 사용자 선택 보안문서를 범주 보안문서나 등급 보안문서로 변경할 수 없습니다.

보안문서 권한 변경 방법

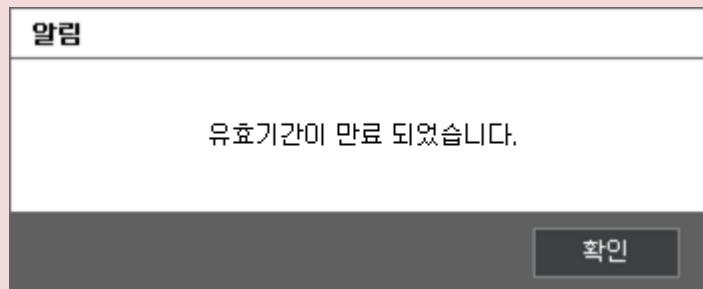
- 1) 권한 변경하려는 보안문서를 우클릭하여 나오는 메뉴에서 '{파일명}.{확장자} 접근 대상 변경'을 클릭합니다. 보안문서의 파일명이 '내문서', 확장자가 'docx'일 경우, '내문서.docx 접근 대상 변경'이라고 표시됩니다.



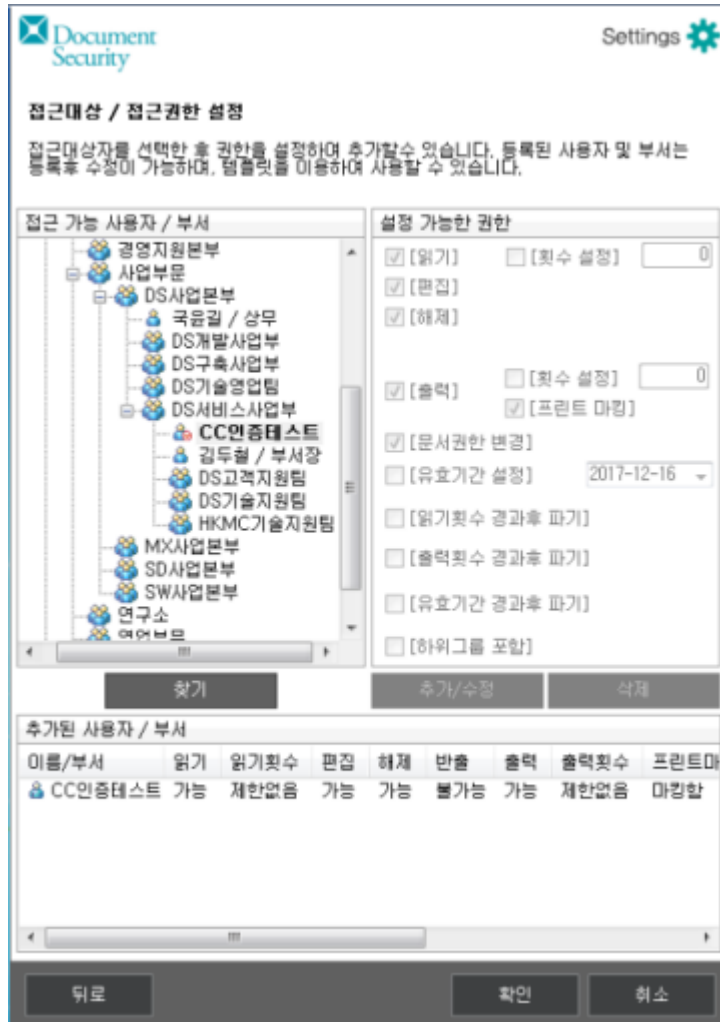
⚠ 주의: 접근 대상 변경을 할 수 없는 사용자는 아래와 같은 메시지가 출력됩니다. 관리자에 의해 부여된 권한에 암호화된 문서에 대한 접근 대상을 변경 권한이 차단된 경우입니다. 접근 대상 변경 권한이 필요하다면, 관리자에게 요청하여 해당 권한을 부여받도록 합니다.



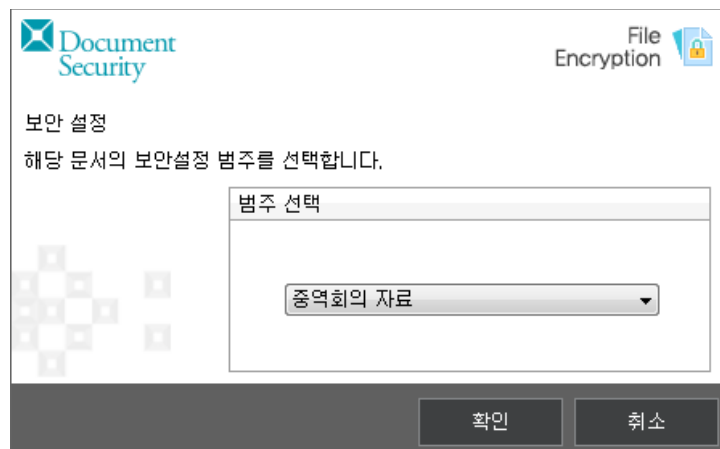
유효기간이 만료된 보안문서를 권한 변경할 경우, 아래와 같은 메시지가 출력되며 권한 변경에 실패합니다. [확인]을 클릭하여 창을 종료합니다.



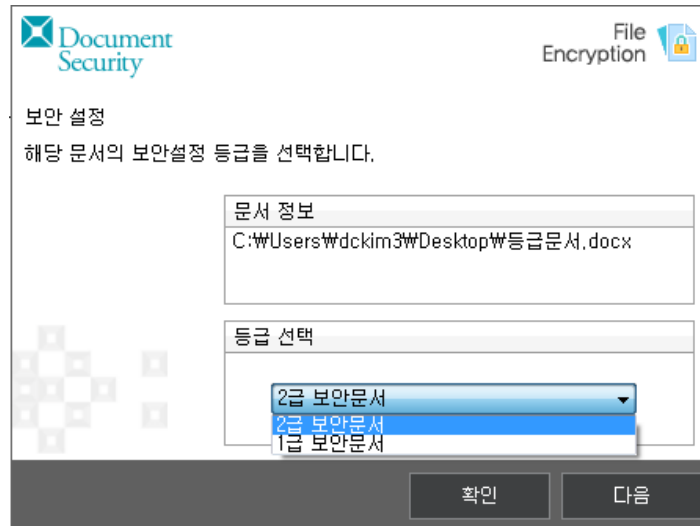
2) 해당 보안문서에 대해 권한 변경을 할 수 있는 사용자는 아래와 같은 창이 출력됩니다. 해당 보안문서가 어떤 방식으로 암호화되었는 지에 따라 다음과 같은 창이 출력됩니다.



개인 보안문서나 사용자 선택 보안문서의 권한 변경을 시도한 경우

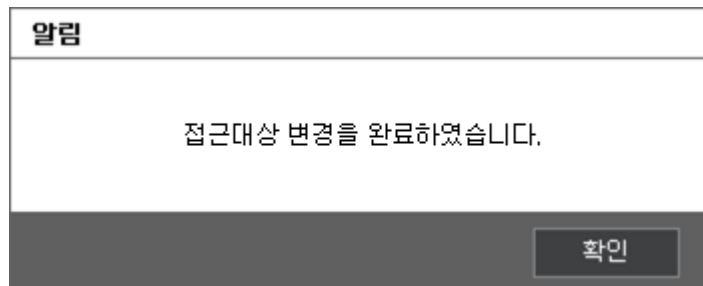


범주 보안문서의 권한 변경을 시도한 경우



등급 보안문서의 권한 변경을 시도한 경우

- 3) 이후 권한 변경은 공용 보안문서 생성 과정과 동일합니다. [공용 보안문서 생성](#)을 참고하시기 바랍니다.
- 4) 접근 대상을 성공적으로 변경하면 아래와 같은 메시지가 출력됩니다. 작업이 완료하려면 **[확인]**을 클릭합니다.



5.4. 보안문서 해제

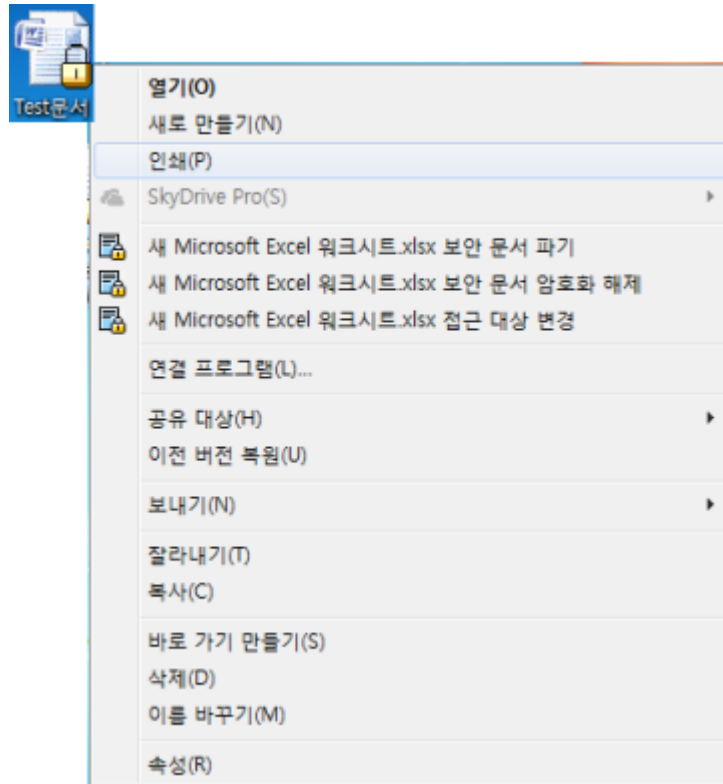
본 장은 보안문서의 해제(복호화) 과정을 설명합니다. 복호화된 보안문서는 암호화되기 전의 일반문서로 돌아갑니다.

보안문서 해제 시 주의사항

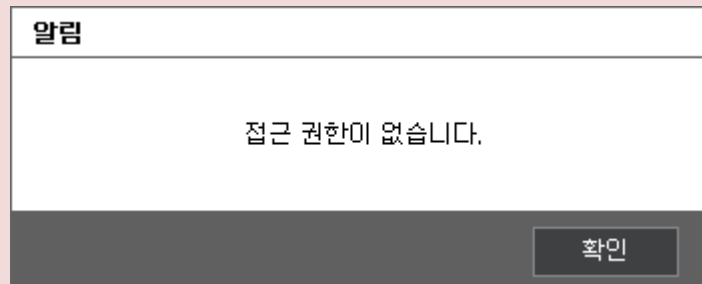
- 1) 보안문서 해제는 해당 보안문서에 대해 해제 권한이 있어야만 가능합니다. 권한은 관리자에 의해 설정됩니다. 보안문서의 복호화 권한이 필요한 경우 관리자에게 문의하시기 바랍니다.
- 2) 해제된 보안문서는 일반문서입니다. 임의의 사용자로 인해 아무 제한없이 사용될 수 있으므로, 조직의 중요자료가 외부로 유출될 수 있습니다.
- 3) 작업 중인 문서는 해제할 수 없습니다.
- 4) 다수의 파일을 선택하고 일괄적으로 복호화할 수 없습니다.

보안문서 해제 방법

- 1) 보안문서를 우클릭하여 나오는 메뉴에서 '**{파일명}.{확장자} 보안 문서 암호화 해제**'을 클릭합니다. 보안문서의 파일명이 '**내문서**', 확장자가 '**docx**'일 경우, '**내문서.docx 보안 문서 암호화 해제**'라고 표시됩니다.



⚠ 주의 : 해당 보안문서에 대한 복호화 권한이 없는 경우는 아래와 같은 메시지가 출력됩니다.
 [확인]을 클릭하여 창을 종료합니다. 보안문서에 대한 복호화 권한이 필요한 경우, 관리자에게 문의하시기 바랍니다.



유효기간이 만료된 보안문서를 해제할 경우, 아래와 같은 메시지가 출력되며 해제에 실패합니다.
 [확인]을 클릭하여 창을 종료합니다.

알림

유효기간이 만료 되었습니다.

확인


현재 작업 중인 보안문서는 복호화할 수 없습니다. 작업 중인 보안문서의 복호화를 시도할 경우 아래와 같은 메시지가 출력됩니다.


알림

보안문서가 열려있으므로 로그아웃 할 수 없습니다.


확인

2) 아래와 같이 선택한 보안문서가 복호화됩니다.



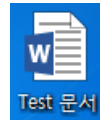
Notice 


보안문서 암호화 해제를 완료하였습니다.



확인

3) 복호화된 문서는 아래와 같이 아이콘이 암호화하기 전으로 변경됩니다.



 주의: Windows 7에서는 바탕화면, 탐색기 내 문서 생성/변경 시 자동으로 Refresh 되지 않아, 복호화된 일반문서의 아이콘이 갱신되지 않을 수 있습니다. 이 때 바탕화면, 탐색기의 빈 공간을 우클릭하여 나오는 메뉴에서 '새로고침'을 클릭하거나, 'F5'를 누르면 정상적으로 아이콘이 변경됩니다.

5.5. 보안문서 파기

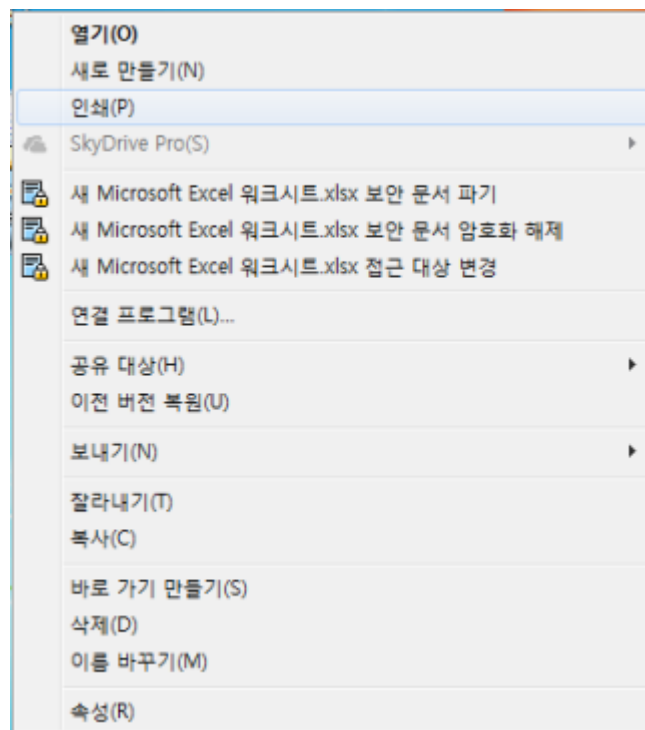
본 장은 보안문서의 파기 과정을 설명합니다. 사용자는 보안문서가 더 이상 필요없거나 필요없는 보안문서가 유출 시 중요 정보가 유출될 위험이 있는 경우, 보안문서를 파기할 수 있습니다.

보안문서 파기 시 주의사항

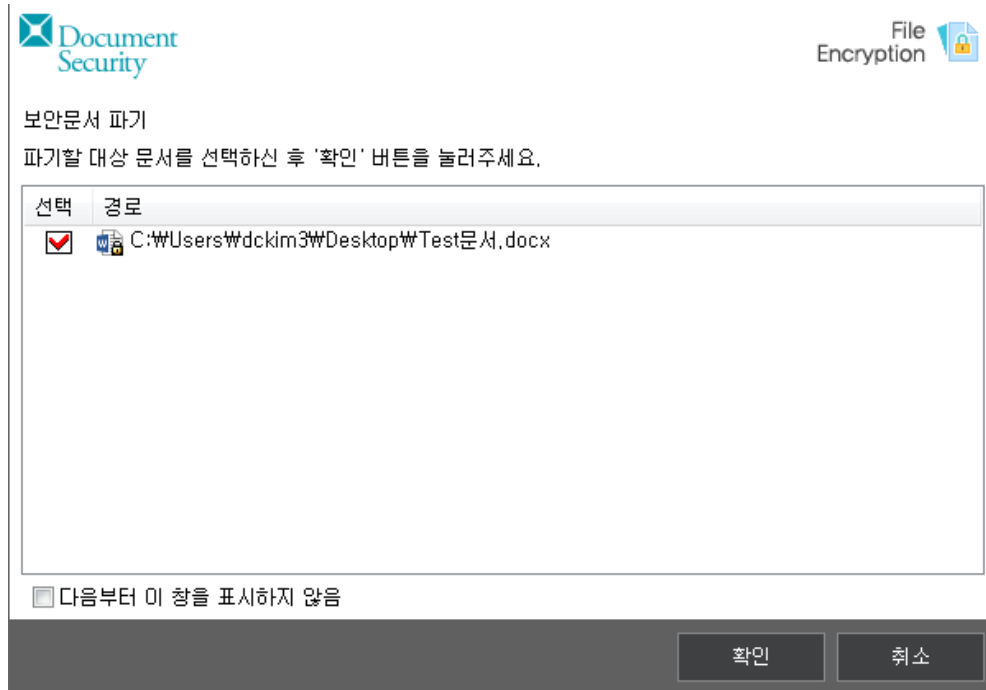
- 1) 파기된 보안문서는 복구가 불가능합니다.
- 2) 작업 중인 보안문서는 파기할 수 없습니다. 보안문서를 파기하려면 문서를 닫고 파기하도록 합니다.

보안문서 파기 방법

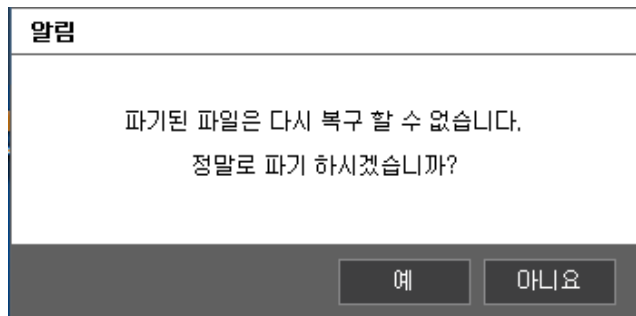
- 1) 보안문서를 우클릭하여 나오는 메뉴에서 '{파일명},{확장자} 보안 문서 파기'를 선택합니다.
보안문서의 파일명이 '내문서', 확장자가 'docx'일 경우, '내문서.docx 보안 문서 파기'라고 표시됩니다.



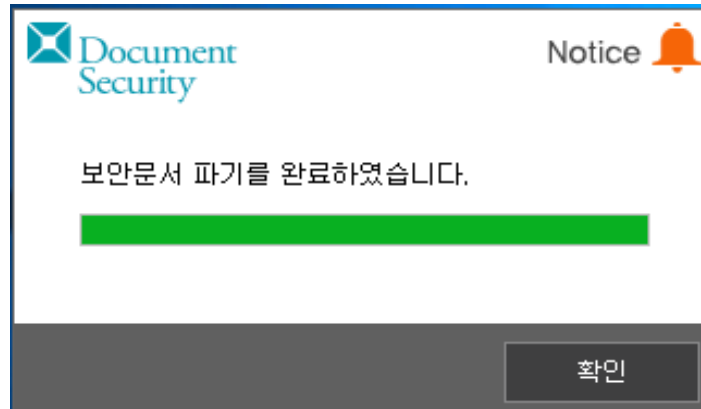
- 2) 아래와 같은 창이 출력됩니다. 체크된 항목은 파기될 대상입니다. 파기를 계속하려면 **[확인]**을 클릭합니다. 작업을 취소하려면 **[취소]**를 클릭합니다. 다수의 보안문서를 선택하고 파기를 시도했다면 선택한 모든 보안문서가 아래의 창에 표시됩니다.



3) 아래의 창이 출력되고 파기를 계속하려면 **[확인]**을 클릭합니다. 작업을 취소하려면 **[취소]**를 클릭합니다.



4)아래와 같이 보안문서의 파기가 진행되고, 완료되었다는 메시지가 출력됩니다. **[확인]**을 클릭하여 작업을 종료합니다.



6. 환경설정

본 장은 환경 설정하는 방법을 설명합니다.

관련링크

- a. [서버 환경설정](#)
- b. [비밀번호 변경](#)
- c. [프로그램 실행 확인](#)
- d. [프로그램 보호 기능](#)
- e. [암호화 파일 선택 UI 표시 여부 설정](#)

6.1. 서버 환경설정

본 장은 서버 환경설정에 대해 설명합니다. 사용자는 접속할 Server 의 접속 주소를 변경할 수 있습니다.

서버 환경설정 시 주의 사항

- 1) 서버 환경설정은 로그아웃 상태에서만 가능합니다.
- 2) 서버 환경설정이 잘못된 서버 접속 정보를 입력하면, 로그인이 정상적으로 이루어지지 않습니다.
- 3) 서버 접속 정보(IP 와 PORT) 입력 시 올바른 형식의 번호를 입력해야 합니다.
 - a. **IP** : ###.###.###.### 형태의 0 ~ 255 사이의 숫자
 - b. **PORT** : 0 ~ 65535 사이의 숫자
 - c. **응답시간** : 0 ~ 60 사이의 숫자

서버 환경설정 방법

- 1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '**환경 설정**'을 클릭합니다.




2) 아래의 창이 표시되면 **[서버 환경설정]**을 클릭합니다.

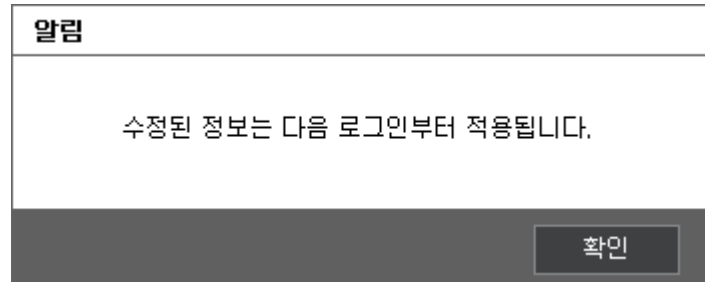


3) Client 로그인 시 접속을 시도할 Server 의 <서버 환경 설정>창이 나타납니다. <서버 환경 설정>창에는 설치 시 입력한 Server 접속 정보가 나타납니다. 내용을 확인 후 **[확인]**을 클릭합니다.

- a. **1 차 서버 / 2 차 서버** : 로그인 시 접속되는 Server 의 구성에 따라 다르게 나타나며 '1 차 서버'는 'Master Server'를, '2 차 서버'는 'Slave Server'를 나타냅니다. 관리자가 Server 의 '인증 서버 접속 정책'을 설정함에 따라 '2 차 서버'의 표시 여부가 결정됩니다. '1 차 서버'만 표시는 사용자가 로그인 시 'Master Server'로만 접속하여 인증하는 방식을 선택한 경우이며, 'Slave Server' 접속 설정을 한 경우는 '2 차 서버' 설정부가 표시됩니다. 각각의 설정 값은 해당 관리자에게 문의 바랍니다.
- b. **서버 주소** : 접속할 Server 의 로그인에 사용될 IP 주소를 입력합니다.
- c. **포트번호** : 접속할 Server 의 로그인에 사용될 포트번호를 입력합니다.
- d. **응답시간** : 응답시간은 로그인 시 Server 와 접속을 시도하고 응답이 없는 경우 대기 시간을 의미합니다.

 참고 : 관리자의 설정에 따라 2 차 서버를 입력하는 부분이 보이지 않을 수 있습니다. 이 경우, 1 차 서버를 입력하는 부분만 입력하도록 합니다.

4) 아래와 같은 메시지가 출력되면 **[확인]**을 클릭합니다.



6.2. 비밀번호 변경

본 장은 비밀번호 변경에 대해 설명합니다. 비밀번호 변경 페이지는 인가된 관리자에게 최초로 생성된 문서 암호화 사용자 (Client 사용자)가 Client 로 최초 접속 시도를 하거나 아이디와 비밀번호가 인가된 관리자에 의하여 갱신된 후 최초 접속 시 표시됩니다. 이 때 사용자는 비밀번호를 반드시 변경해야 합니다.

비밀번호 변경 시 주의 사항

- 1) 관리자의 설정에 따라 사용자가 임의로 비밀번호를 변경하지 못할 수 있습니다. 비밀번호 변경을 원하면 관리자에게 문의하십시오.
- 2) 비밀번호 변경은 로그인에 성공한 상태에서만 가능합니다.

3) 관리자가 비밀번호 최소 길이 및 조합 규칙을 설정한 경우, 사용자는 관리자가 설정한 최소 길이와 조합 규칙에 만족하는 비밀번호를 생성해야 합니다. 관리자가 설정할 수 있는 비밀번호 관련 정책은 아래와 같습니다.

- a. 관리자는 비밀번호의 최소 길이를 지정할 수 있습니다. 이 경우, 사용자는 반드시 해당 최소 길이보다 긴 비밀번호를 설정해야 합니다. 비밀번호 최소 길이의 기본 값은 9 자 이상 15 자 이하입니다.
- b. 관리자는 비밀번호의 조합 규칙을 설정할 수 있습니다. 이 경우, 사용자는 반드시 해당 조합 규칙을 만족하는 비밀번호를 설정해야 합니다. 조합 규칙은 영문자 + 숫자 또는 영문자 + 특수문자 또는 영문자 + 숫자 + 특수문자일 수 있습니다. 인가된 관리자의 별도 설정이 없을 경우 영문자 + 숫자 + 특수문자가 기본 설정입니다.
- c. 관리자는 사용자가 동일한 비밀번호로 변경하지 못하도록 설정할 수 있습니다. 이 경우, 사용자는 반드시 현재 사용하고 있는 것과 다른 비밀번호를 설정해야 합니다.
- d. 관리자는 비밀번호 변경주기를 설정할 수 있습니다. 이 경우, 변경주기가 지나면 사용자는 반드시 비밀번호를 재설정해야 합니다. 변경주기는 월단위로 설정됩니다.
- e. 관리자는 비밀번호가 3 글자 이상 반복된 글자 또는 3 글자 이상의 오름/내림차순의 연속된 글자가 포함되지 못하도록 설정할 수 있습니다. 이 경우, 사용자는 동일한 글자가 반복되거나 연속된 패턴을 가지지 않은 비밀번호를 설정해야 합니다.
- f. 사용자는 계정 생성 이후 최초 인증 정보로 로그인 시에 로그인 후 반드시 비밀번호를 변경해야 Client 에 접속할 수 있습니다.

4) 비밀번호 관련 정책은 사용자마다 다를 수 있습니다.

비밀번호 변경 방법

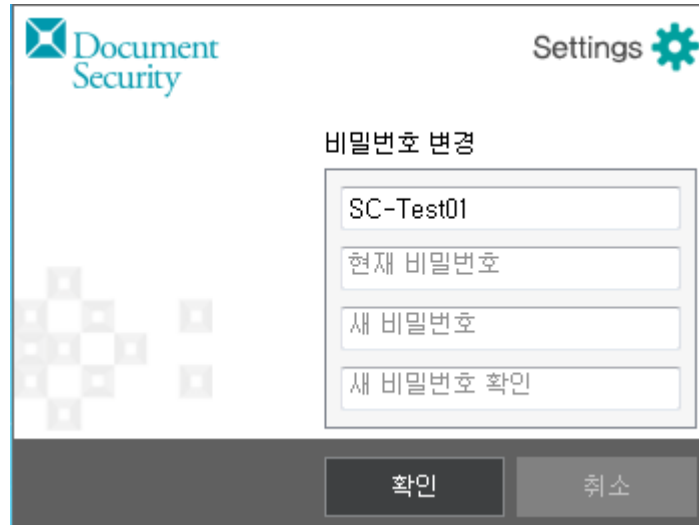
1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '환경 설정'을 클릭합니다.




2) 아래의 창이 출력되면 **[비밀번호 변경]**을 클릭합니다.



3) 아래의 창이 출력되면 다음을 순서대로 입력하고, **[확인]**을 클릭합니다. **[취소]**를 클릭하면 작업이 취소되고, 비밀번호는 유지됩니다.



- a. **아이디** : 사용자의 아이디를 표시합니다. 아이디는 변경할 수 없습니다.
- b. **현재 비밀번호** : 현재 사용 중인 비밀번호를 입력합니다.
- c. **새 비밀번호** : 변경하려는 새로운 비밀번호를 입력합니다. 새로운 비밀번호는 최소길이 및 조합 규칙을 만족해야 합니다.
- d. **새 비밀번호 확인** : 변경하려는 비밀번호를 다시 한번 입력합니다.

 참고: 비밀번호 관련 정책

비밀번호 최소 길이 및 조합 규칙 등 비밀번호 관련 정책에 어긋난 새 비밀번호를 입력하거나, 올바르게 입력하지 않은 경우 아래와 같은 메시지가 출력됩니다.

- 1) 관리자가 설정한 비밀번호의 최소 길이가 9 자이고 새 비밀번호의 길이가 이에 미치지 못할 경우, 아래와 같은 메시지가 출력됩니다.

알림
9자리 이상의 비밀번호를 입력해 주십시오.
<input type="button" value="확인"/>

2) 새 비밀번호가 특정 글자의 반복으로 이루어진 경우, 아래와 같은 메시지가 출력됩니다.

알림
반복되는 패스워드는 사용 할 수 없습니다. 다시 시도해 주십시오.
<input type="button" value="확인"/>

3) 관리자가 설정한 조합 규칙이 영문+숫자+특수문자의 조합이고, 새 비밀번호가 관리자가 설정한 조합 규칙에 어긋난 경우, 아래와 같은 메시지가 출력됩니다.

알림
잘못된 비밀번호입니다. 영문과 숫자와 특수문자를 조합해 주십시오.
<input type="button" value="확인"/>

4) 관리자가 설정한 조합 규칙이 영문+숫자의 조합이고, 새 비밀번호가 관리자가 설정한 조합 규칙에 어긋난 경우, 아래와 같은 메시지가 출력됩니다.

알림
잘못된 비밀번호입니다. 영문과 숫자를 조합해 주십시오.
<input type="button" value="확인"/>

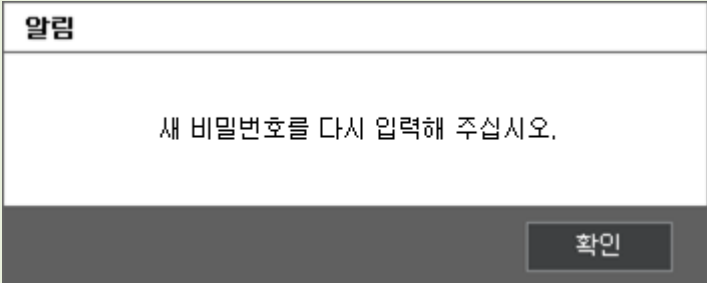
- 5) 관리자가 설정한 조합 규칙이 영문+특수문자의 조합이고, 새 비밀번호가 관리자가 설정한 조합 규칙에 어긋난 경우, 아래와 같은 메시지가 출력됩니다.

알림
잘못된 비밀번호입니다. 영문과 특수문자를 조합해 주십시오.
<input type="button" value="확인"/>

- 6) 새 비밀번호가 현재 비밀번호와 동일할 경우 아래와 같은 메시지가 출력됩니다.

알림
이전과 동일한 패스워드는 사용 할 수 없습니다. 다시 시도해 주십시오.
<input type="button" value="확인"/>

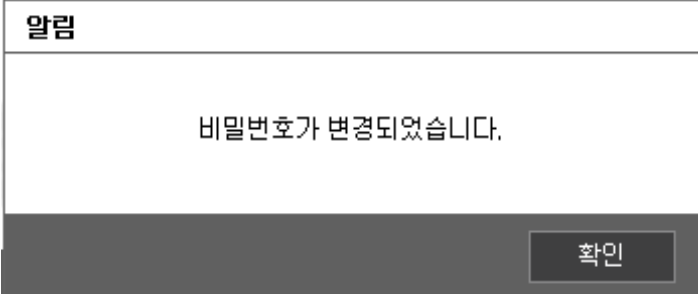
- 7) 새 비밀번호와 새 비밀번호 확인에 입력한 값이 일치하지 않을 경우 아래와 같은 메시지가 출력됩니다.



The image shows a modal dialog box with a title bar labeled '알림' (Alert). The main content area contains the text '새 비밀번호를 다시 입력해 주십시오.' (Please re-enter your new password.). At the bottom right, there is a button labeled '확인' (Confirm).

8) 비밀번호의 최대 길이는 15 자입니다.

- 1) 새롭게 입력한 비밀번호가 정상적으로 적용되면 아래와 같은 메시지가 표시됩니다. 다음 로그인 시부터 변경한 비밀번호를 입력해야 합니다.



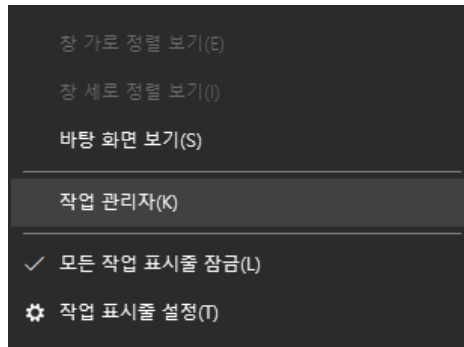
The image shows a modal dialog box with a title bar labeled '알림' (Alert). The main content area contains the text '비밀번호가 변경되었습니다.' (The password has been changed.). At the bottom right, there is a button labeled '확인' (Confirm).

6.3. 프로그램 실행 확인

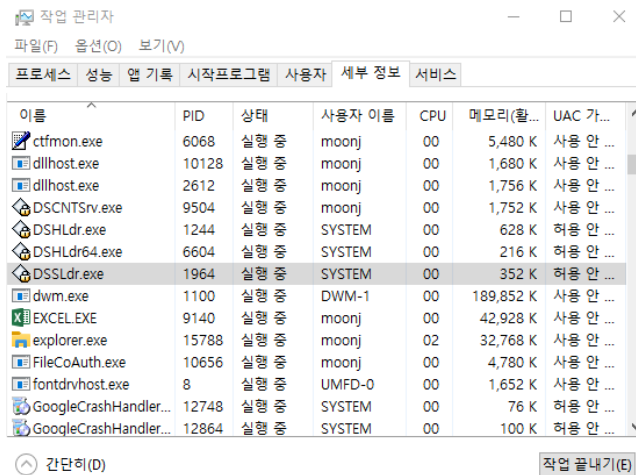
본 장은 프로그램 실행 확인에 대해 설명합니다. 사용자는 윈도우 작업관리자를 통해 Client 가 실행되고 있음을 확인할 수 있습니다.

프로그램 실행 확인 방법

- 1) 윈도우의 작업 표시줄에서 마우스 우클릭을 실행 합니다.
- 2) 쉘 메뉴 중 "작업 관리자 시작"을 클릭 합니다.



- 3) "Windows 작업 관리자" 창에서 [프로세스] 탭을 클릭 합니다.



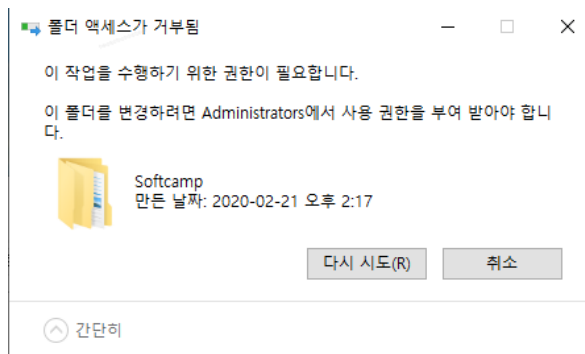
- 4) Client 의 "DSSLdr.exe *32"가 자동 실행되어 있음을 확인할 수 있습니다.

6.4. 프로그램 보호 기능

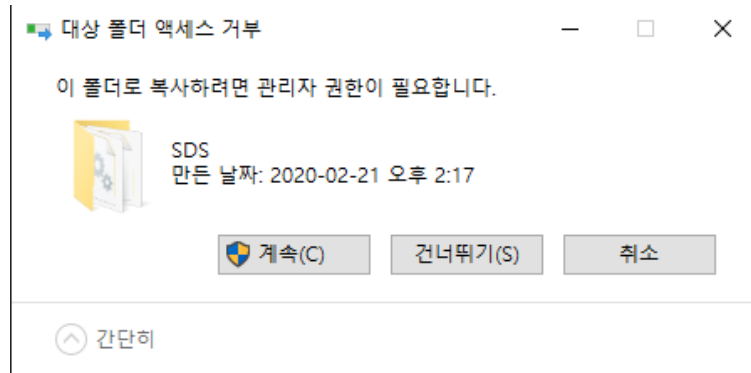
본 장은 프로그램 보호 기능에 대해 설명합니다. 사용자는 Client 가 설치된 폴더 및 제품과 관련된 파일에 대해서 삭제, 이동, 변경, 복사 붙여넣기를 할 수 없습니다. 본 기능은 제품의 정책을 통한 제어를 받지 않는 제품 자체의 보호 기능 입니다.

프로그램 보호 기능 확인 방법

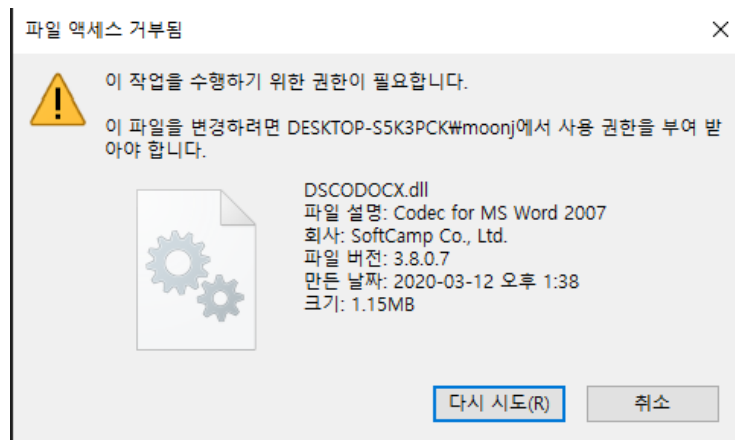
- 1) 윈도우 탐색기를 통해 Client 가 설치된 C:\Windows\softcamp 경로로 이동 합니다.
- 2) 해당 경로의 파일, 폴더 등에 대해 윈도우 우클릭 메뉴 또는 키보드 단축키를 사용하여 삭제, 이동, 변경, 복사 붙여넣기 등의 행위를 할 경우 아래와 같은 윈도우 메시지가 표출되며 해당 실행이 차단됩니다.
 - Client 의 설치 경로에 다른 파일이나 폴더를 복사 붙여넣기 등을 시도할 경우 표출되는 메시지 입니다.



- Client 가 설치된 경로의 파일을 이동, 변경, 복사 등을 시도할 경우 표출되는 메시지 입니다.

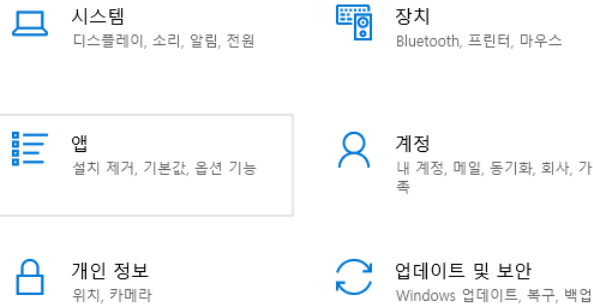


- Client 가 설치된 경로의 파일 이름을 변경 시도할 경우 표출되는 메시지 입니다



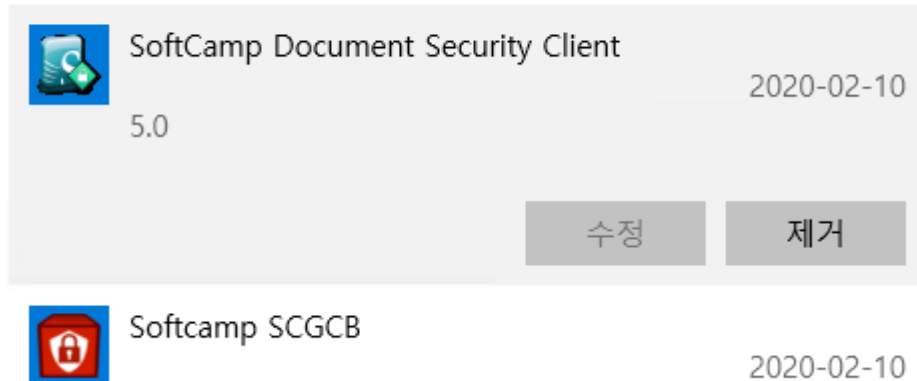
프로그램 삭제 권한 관리

- 1) 윈도우의 제어판으로 이동하여 "앱"을 실행합니다.

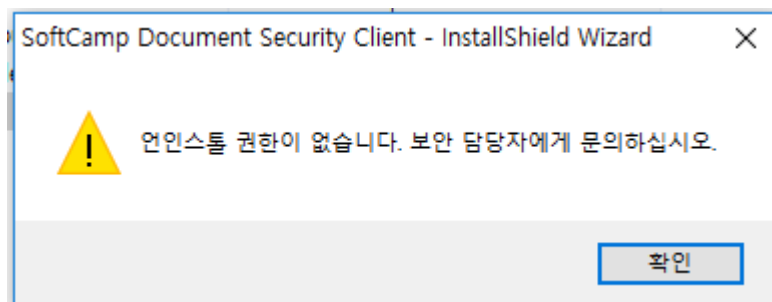


2) 프로그램 설치 목록에서 "Softcamp Client" 를 선택하여 "제거"를 실행 합니다.

앱 및 기능



3) 아래 메시지가 표출되며 프로그램 삭제가 차단됩니다.

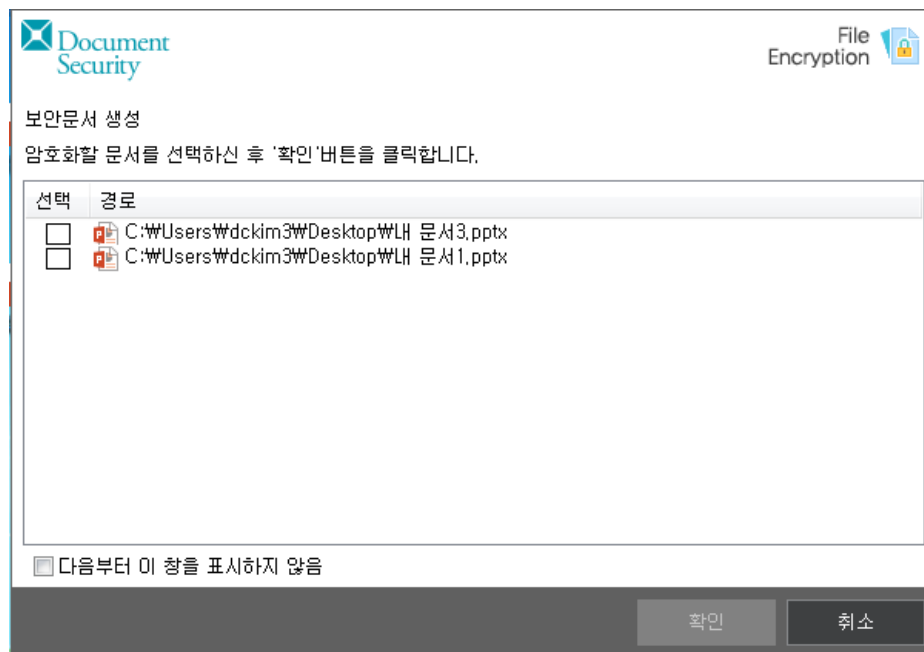


- 4) 사용자의 임의 삭제를 차단하기 위해 프로그램의 삭제 기능은 삭제 권한 여부를 통해 제어됩니다.

6.5. 암호화 파일 선택 UI 표시 여부 설정

본 장은 암호화 파일 선택 UI 표시 여부 설정에 대해 설명합니다.

암호화 파일 선택 UI 는 아래의 그림과 같이 일반문서를 작업하고, 문서 어플리케이션을 종료 시에 표시됩니다. 사용자는 아래의 UI 가 표시되지 않도록 설정할 수 있습니다.



암호화 파일 선택 UI 표시

1) Client 트레이아이콘을 우클릭을 하여 출력되는 메뉴에서 '환경 설정'을 클릭합니다.




2) 아래의 창이 표시됩니다. UI가 표시되도록 하려면 '문서작업 종료시 창을 표시하지 않음'을 체크 해제하고, 표시되지 않게 하려면 체크하도록 합니다. [확인]을 클릭하여 변경한 내용을 저장합니다. [취소]를 클릭하면 변경한 내용이 저장되지 않습니다.

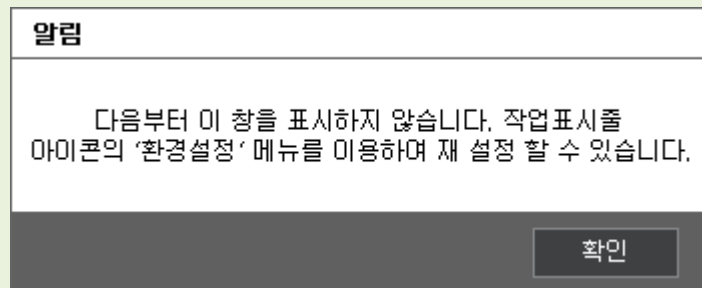


암호화 파일 선택 UI가 표시되지 않음



암호화 파일 선택 UI 가 표시됨

 참고 : 암호화 파일 선택 UI 의 하단에 '다음부터 이 창을 표시하지 않음'을 선택하면 아래와 같은 메시지가 나오며 UI 가 표시되지 않습니다. 단, 체크박스가 관리자의 설정에 따라, 비활성화되어 있을 수 있습니다. 다시 UI 를 표시하도록 하려면 '환경 설정'에서 '문서작업 종료시 창을 표시하지 않음'을 체크 해제하도록 합니다.



7. 소프트웨어 사용권 계약

본 계약은 소프트캠프(주) (SoftCamp Co.,Ltd.)와 사용자 사이에 체결되는 계약입니다.

공급자명

소프트캠프(주) (SoftCamp Co.,Ltd.)

제품명

Document Security Client V5.0 (5.0.0.1)

사용권의 효력

귀하는 본 제품을 설치, 복사 또는 사용함과 동시에, 본 사용 계약서에 동의함을 인정하는 것입니다. 귀하가 본 계약서에 동의하지 않을 경우 소프트캠프(주) (SoftCamp Co.,Ltd.)는 귀하에게 본 제품의 사용을 허가하지 않습니다. 그 경우, 귀하는 본 제품을 사용 또는 복사할 수 없으며, 환불을 위한 제품 반환에 대해서는 즉시 제조 업체나 판매 업체에 문의해야 합니다.

사용권 허가

귀하는 1 개의 소프트웨어 제품 복사본을 컴퓨터에 설치하여 사용할 수 있습니다.

귀하는 본 소프트웨어를 PC 에 설치하여 사용할 수 있으나, 전체 혹은 일부 파일을 네트워크나 파일서버에 저장하여 사용할 수 없습니다. 본 소프트웨어가 컴퓨터의 주기억장치에 실려 있거나 기타 기억장치에 저장되어 있는 경우, 본 소프트웨어를 '사용하고 있는' 것으로 간주합니다. 본 소프트웨어가 네트워크 서버에 설치되어 있는 경우에는 그 서버의 사용자 수만큼 본 소프트웨어를 구입해야 합니다. 또 사용자는 구입한 제품의 일련 번호(Serial Number)나 등록 번호가 다른 사람에게 알려지지 않도록 주의할 의무가 있습니다.

사용권의 이전

귀하는 본 제품을 임대 또는 배포할 수 없습니다.

귀하가 본 제품을 타인에게 양도 시 모든 소프트웨어 제품(모든 구성요소, 매체, 인쇄물, 업그레이드, 정품 인증서를 포함한)을 양도해야 하며, 양수인이 본 계약서의 모든 조항에 동의해야 합니다.

구 Version 에서 신 Version 으로 Upgrade 한 경우에는, 구 Version 의 사용권은 신 Version 으로 옮겨지지만, 구 Version 을 신 Version 과 동일한 시간에 실행하지 않는다는 전제하에서 구 Version 을 사용할 수 있습니다.

저작권

본 소프트웨어의 모든 부속물에 대한 저작권과 지적소유권은 소프트캠프(주) (SoftCamp Co.,Ltd.)에 있으며, 이 권리는 대한민국의 저작권법과 국제 저작권 조약에 의하여 보호 됩니다. 귀하는 소프트웨어 제품에 동봉된 인쇄물을 복사할 수 없습니다. 본 계약서에 의하여 명시적으로 허용되지 않은 모든 권리는 소프트캠프(주) (SoftCamp Co.,Ltd.)가 보유합니다.

보증의 한계

소프트캠프(주) (SoftCamp Co.,Ltd.)는 본 제품을 구입한 날로부터 90 일간 설치 CD 를 비롯한 패키지 내용에 대해 물리적인 결함이 없을 것을 보증합니다. 이 기간 중 제품 제작상의 실수로 결함이 발생한 경우에는 무료로 교환해드립니다.

교환 대상은 구입 일로부터 90 일이 지나지 않았다는 것을 증명해야 하며, 사용자의 부주의나 실수, 취급 소홀에 의한 손상일 경우에는 교환해 드리지 않습니다. 또, 소프트캠프(주) (SoftCamp Co.,Ltd.)는 본 소프트웨어에 포함된 기능이 특정 목적에 적합할 것이라는 보증은 하지 않으며, 본 제품의 사용으로 인해 초래된 모든 결과에 대한 책임을 지지 않습니다.

계약의 인정

귀하는 본 계약서의 내용을 모두 읽고 이해하며, 동의함을 인정합니다. 동시에 이 내용이 과거의 모든 주문이나 약속, 광고, 고지, 서면 합의 사항에 우선하는 것임을 인정합니다.