SOFTCAMP

Document Security V5.0

관리자설명서(OPE_A)

V 1.0

경기도 성남시 분당구 판교로 228 번길 17,

판교세븐벤쳐밸리 2 제이렌텍동 2 층 소프트캠프

대표전화: 1644-9366

팩스: 031-697-4599

www.softcamp.co.kr

전체 목차

개정 내역

Version	기본 수정 사항	변경자	수정 날짜
V1.0	Document Security V5.0 관리자설명서(OPE_A) 최초 등록	은승현	2018.09.11

DOCUMENT SECURITY CONSOLE V5.0

1. 고객지원

소프트캠프㈜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㈜

전화: 1644-9366

팩스: 031-697-4599

2. 개요

문서개요

본 문서는 Document Security V5.0 (이하 "TOE"라 함)의 관리자를 위한 관리자설명서 입니다.

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	사용자 PC 와 Document Security Server 와의 네트워크가 연결되어 있는 상황
오프라인	사용자 PC 와 Document Security Server 와의 네트워크가 연결되어 있지 않는 상황
최고 보안 관리자	TOE 의 최상위 관리자로써, Document Security Console 이 제공하는 모든 보안 및 관리기능을 수행할 수 있는 관리자.
중간 관리자	최고 보안 관리자가 Manager Console 에서 추가한 관리자로서, 최고 보안 관리자가 설정한 범위 내에서 Manager Console 을 사용하는 관리자
하위 관리자	일반 사용자 중 자신이 속한 그룹 내의 일반 사용자의 개인 그룹별 강제 권한 및 암호화 정책, 보안 정책 등을 변경할 수 있는 관리자

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>XXXXXX 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 Console V5.0 에 대해 소개하고, 간략히 설명합니다.

Document Security Console V5.0 소개

Document Security Console V5.0(이하 'Console'이라 함)은 TOE 의 관리자 프로그램입니다. 관리자의 PC 에 설치되어, 문서 암호화 사용자 계정을 생성하고 문서 암호화 정책을 설정합니다. 또한, 사용자에 대해 화면 캡쳐 및 복사/붙여넣기 제한, 프린트 마킹에 대한 정책 및 권한을 설정합니다.

4. CONSOLE 사용 시 주의사항

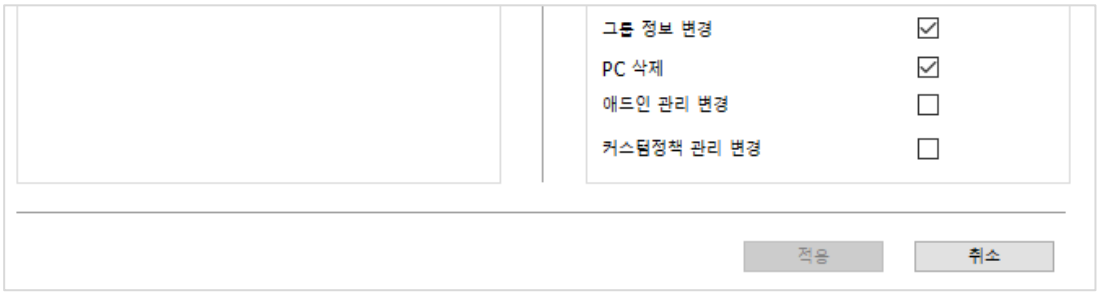
본 장은 Console 사용 시 주의사항에 대해 설명합니다.

변경한 보안 정책 적용

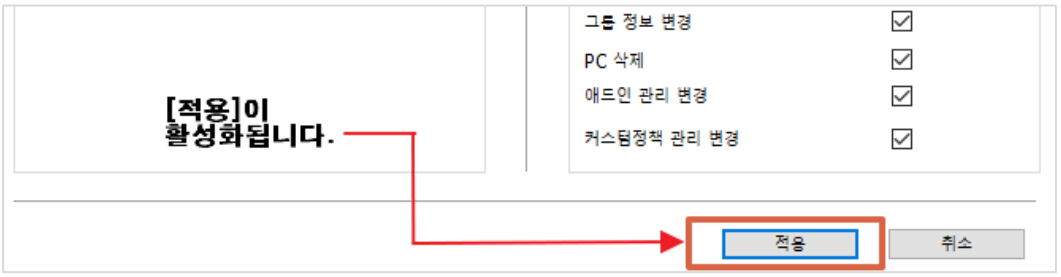
Console 을 이용해 조직, 개인 및 그룹별 보안 정책을 변경할 경우, 변경한 보안 정책을 적용해야 합니다. 변경한 보안 정책을 적용하지 않으면, 변경된 내용이 Document Security Server V5.0(이하 'Server' 라고 함)으로 전송되지 않아 사용자 클라이언트 프로그램인 Document Security Client V5.0 (이하 'Client' 라고 함)에 반영되지 않습니다. 보안 정책을 적용하는 방법은 아래와 같습니다.

1) 보안 정책을 변경하면 작업창 하단의 **[적용]**이 활성화됩니다. 변경한 보안 정책을 적용하려면 **[적용]**을 클릭합니다.

Console 의 정책관리>로그정책 (변경 전)

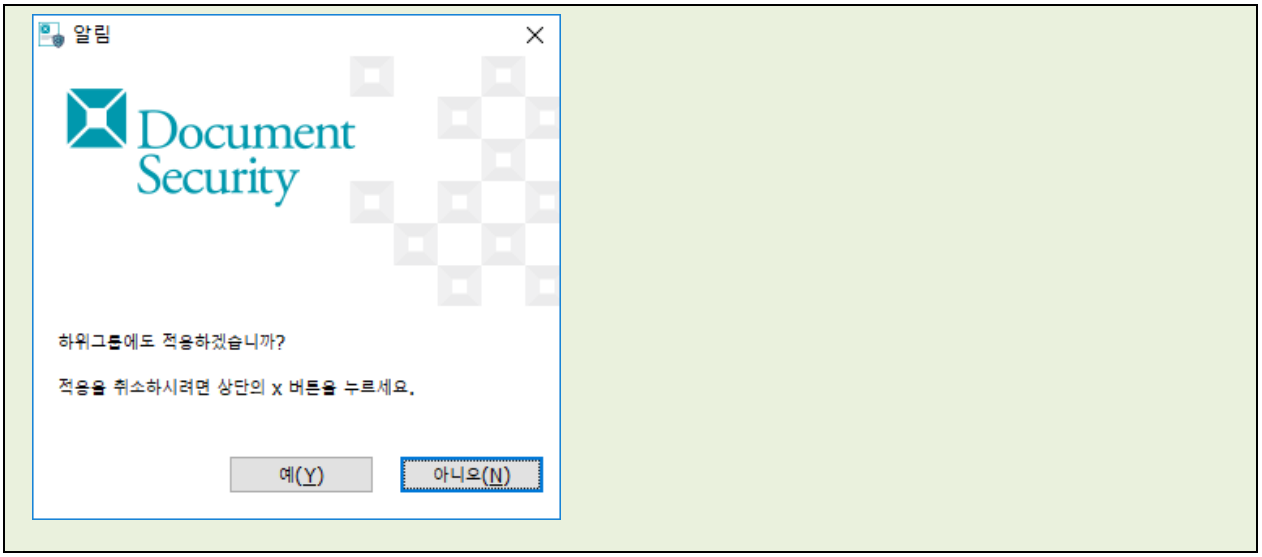


Console 의 정책관리>로그정책 (변경 후)

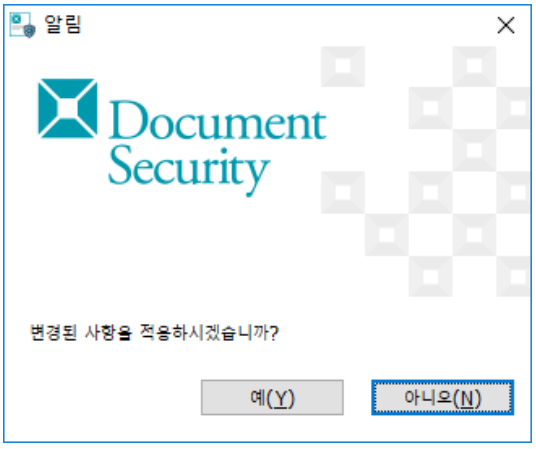


2) **[적용]**을 클릭하면 아래와 같은 창이 출력되면서, 변경한 보안 정책이 적용됩니다. 변경된 보안 정책은 서버로 전송되고, 사용자 프로그램에 전달되어 적용되게 됩니다. **[확인]**을 누르면 창이 닫힙니다.

참고 : 그룹을 대상으로 보안정책을 변경한 경우, 아래와 같은 메시지가 표시됩니다. [예]를 클릭하면 해당 그룹의 사용자 뿐만 아니라 하위 그룹의 모든 사용자에게도 동일하게 보안 정책이 적용됩니다.



3) 보안 정책을 변경한 후에 다른 메뉴나 다른 그룹이나 사용자를 선택하면 아래와 같은 창이 표시되면서, 변경한 보안 정책의 적용 여부를 묻습니다. 이 때 **[예]**를 클릭하면 변경된 보안정책이 적용되고, **[아니오]**를 클릭하면 변경된 보안정책이 적용되지 않고, 취소됩니다.



4) 변경된 보안 정책이 정상적으로 적용되면 아래와 같은 메시지가 표시됩니다. **[확인]**을 클릭하여 창을 닫습니다.

주의 : TOE 에서 다루어지는 데이터 중 문서 암호화 및 TSF 데이터 암호화를 위해 사용되는 DEK 와 계정 접속 정보, 관리자 및 사용자의 비밀번호, 암호화 대상 문서 등은 보호 대상 데이터 입니다. 해당 데이터는 암호화 되어 안전하게 보호됩니다.

5. CONSOLE 시작

본 장은 Console 의 실행과 관련된 로그인 및 매뉴의 구성에 대해 설명합니다.

관련링크

a. 실행

b. 메뉴 구성

c. 메뉴탐색창

d. 프로그램 정보 확인

e. 종료

5.1. 실행

본 장은 Console 을 실행하는 과정을 설명합니다.

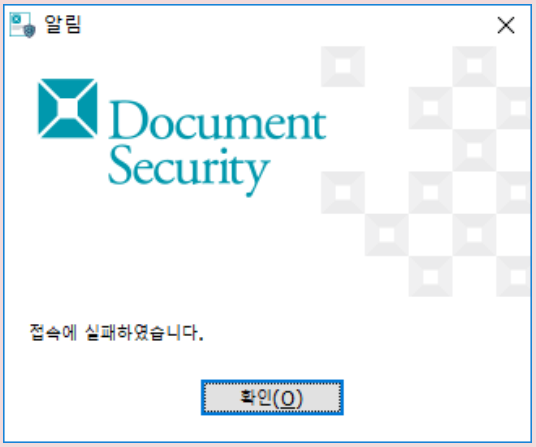
1) Console 의 설치를 마친 후 바탕화면의 **'Document Security Console'** 아이콘을 더블 클릭하여 실행합니다.

2) 아래와 같이 관리자 로그인 창이 실행됩니다. 다음의 정보를 입력하고 **[확인]**을 클릭합니다.

표기 규칙	표기 규칙 내용
서버	Server 가 설치된 장비의 IP 주소를 입력합니다. 설치 후 기본값은 '**127.0.0.1**'입니다. 각각의 필드는 0 ~ 255 까지의 숫자만 입력할 수 있습니다.
아이디	관리자의 아이디를 입력합니다. 기본값은 document 입니다. 해당 필드는 영문 기준 20 자까지 입력할 수 있습니다.
비밀번호	관리자의 비밀번호를 입력합니다. 해당 필드는 영문기준 15 자까지 입력할 수 있습니다.
통신포트	Console 과 Server 가 통신하는 포트번호를 입력합니다. Server 설치 시 설정한 PMS 의 서버 베이스 포트 번호와 동일한 번호를 입력합니다. 설치 후 기본값은 '**62004**'입니다. 해당 필드는 0 ~ 65535 까지 숫자만 입력할 수 있습니다.

주의: <로그인>창에 값을 올바르게 입력하지 않으면 다음과 같은 메시지들이 출력될 수 있습니다.

아래의 메시지는 입력한 주소를 가진 서버가 동작하지 않거나 입력한 서버의 IP 주소가 틀렸을 경우에 출력됩니다. 서버의 IP 주소를 확인하고 IP 주소가 올바름에도 접속이 되지 않는다면 서버가 동작하고 있는지 확인합니다.



아래의 메시지는 입력한 비밀번호가 올바르지 않은 경우에 출력됩니다. 비밀번호를 확인하고 재입력합니다.

아래의 메시지는 입력한 아이디가 올바르지 않은 경우에 출력됩니다. 아이디를 확인하고 재입력합니다. 아이디와 비밀번호가 틀렸을 경우 제공되는 메시지는 동일합니다.

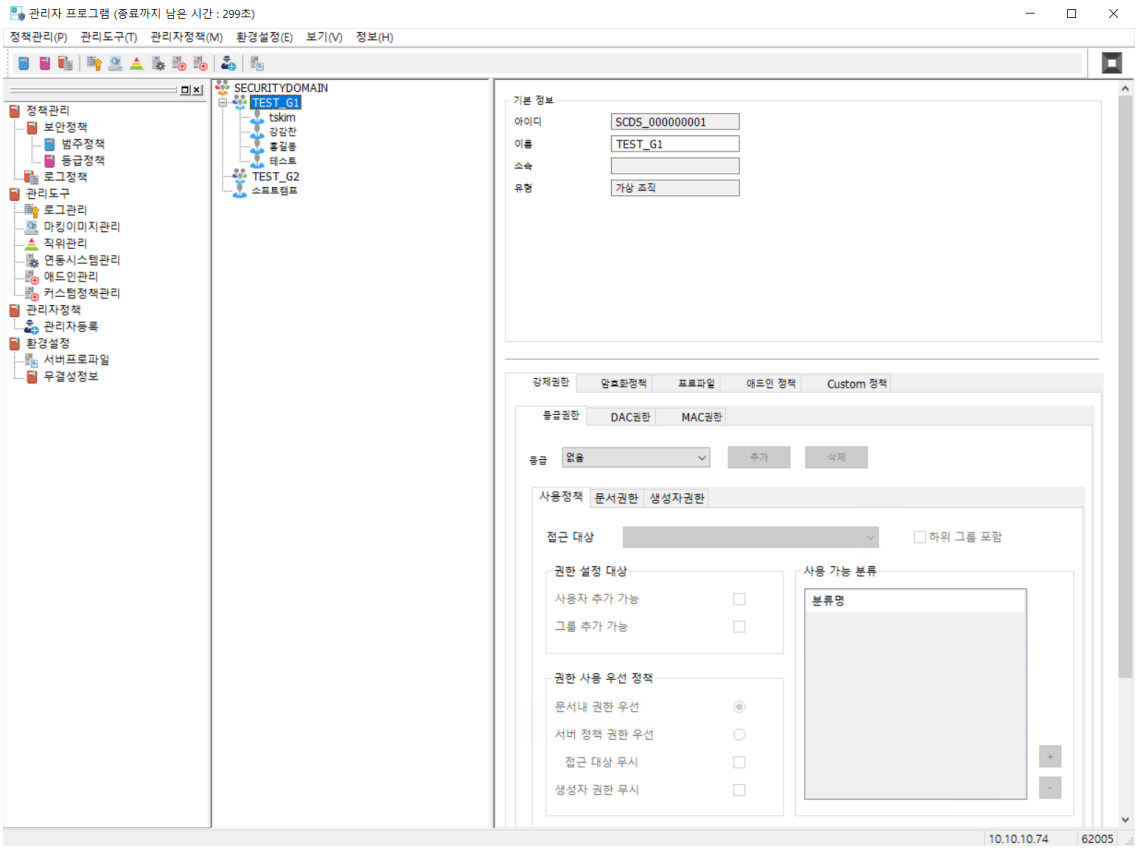
관리자 인증 시도 시 5 번 연속으로 인증에 실패하면 10 분간 해당 계정의 인증이 제한됩니다.

참고: 인증 방식 및 인증정보의 재사용 방지

인가된 관리자에 대한 식별 및 인증은 비밀번호 기반 인증방식을 사용하고 있습니다.

인증정보의 재사용을 방지하기 위하여 타임스탬프 값을 Salt 값으로 적용합니다.

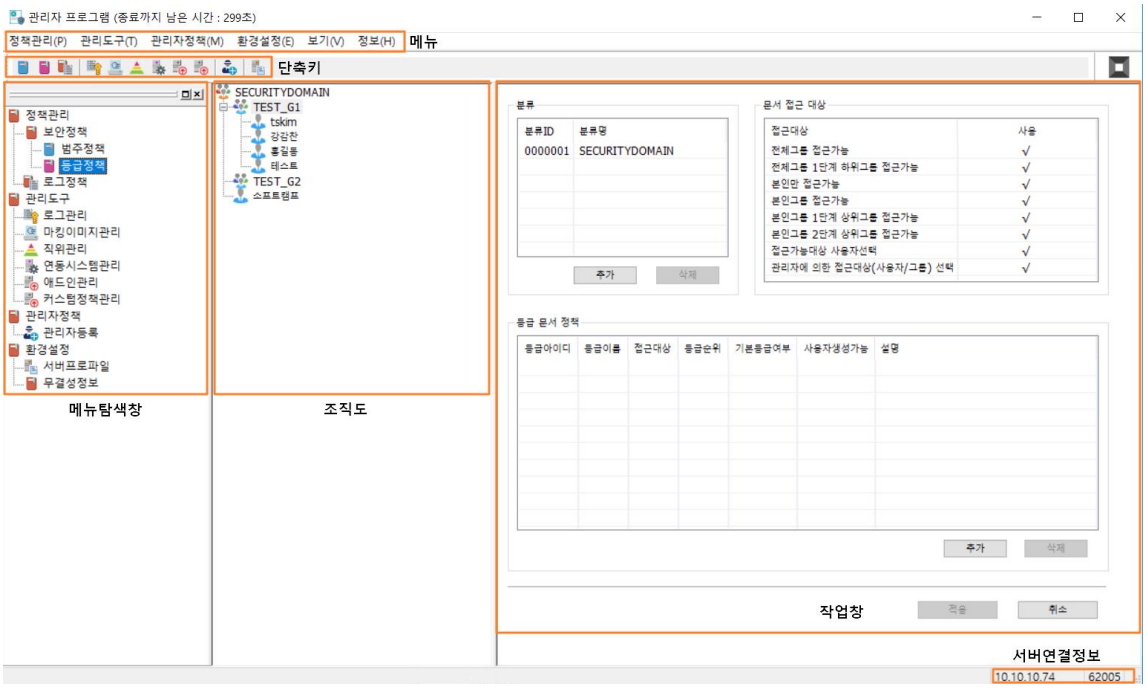
3) 최초 로그인 시 변경한 아이디와 비밀번호를 이용하여 정상적으로 로그인하면, 아래와 같이 Console 이 실행됩니다.



5.2. 메뉴 구성

본 장에서는 Console 의 구성에 대해 설명합니다.

Console 은 아래와 같이 구성되어 있습니다.



표기 규칙	표기 규칙 내용
메뉴	Console 의 기능을 수행할 수 있는 메뉴입니다. 각각의 메뉴를 선택하면 하위 메뉴가 표시됩니다.
단축키 (아이콘 메뉴)	관리자는 Console 의 기능을 메뉴를 통해 선택할 필요없이 아이콘을 클릭하면 아이콘에 해당하는 기능을 수행할 수 있습니다.
메뉴탐색창	Console 의 메뉴를 트리 형태로 표시합니다. 메뉴에서 **보기>메뉴탐색창**을 선택하거나, 메뉴탐색창의 우측 상단의 **[x]**를 클릭하면 메뉴탐색창이 닫힙니다
조직도	사용자 및 그룹을 트리 형태로 표시합니다.
작업창	Console 의 기능 수행 작업을 위한 창입니다.
서버연결정보 (IP/PORT)	현재 접속되어 있는 Document Security Server 의 IP 와 Port 의 정보를 나타냅니다.

아래는 메뉴, 아이콘 메뉴, 메뉴탐색창에서 제공하는 항목입니다.

메뉴대분류	메뉴소분류	메뉴	메뉴탐색창	아이콘 메뉴
정책관리	보안정책>범주정책	정책관리>보안정책>범주정책	범주정책	
	보안정책>등급정책	정책관리>보안정책>등급정책	등급정책	
	로그정책	정책관리>로그정책	로그정책	
관리도구	로그관리	관리도구>로그관리	로그관리	
	마킹이미지관리	관리도구>마킹이미지관리	마킹이미지관리	
	직위관리	관리도구>직위관리	직위 관리	
	연동시스템관리	관리도구>연동시스템관리	연동시스템관리	
	애드인관리	관리도구>애드인관리	애드인관리	
	커스텀정책관리	관리도구>커스텀정책관리	커스텀정책관리	
관리자정책	관리자등록	관리자정책>관리자등록	관리자등록	
환경설정	서버프로파일	환경설정>서버프로파일	서버프로파일	
보기	메뉴탐색창	보기>메뉴탐색창	X	X
정보	프로그램정보	정보>프로그램정보	X	X

각 메뉴 항목의 역할은 다음과 같습니다.

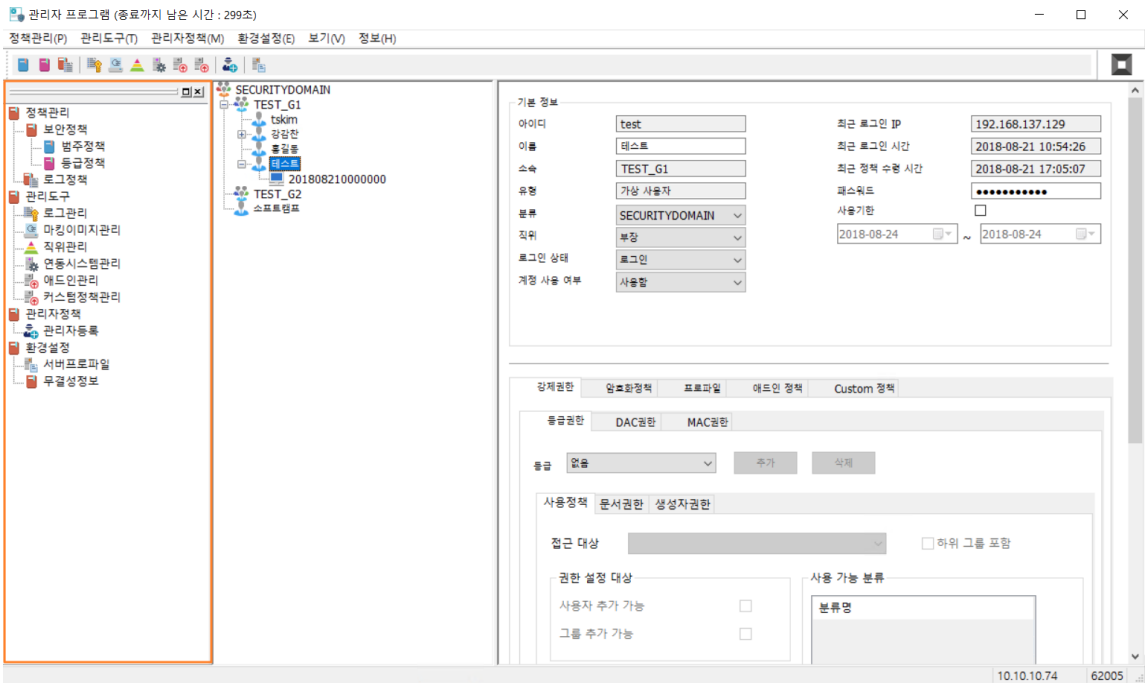
메뉴	메뉴 역할
정책관리>보안정책>범주정책	문서 암호화 정책 중 하나인 범주 정책을 설정할 수 있습니다.
정책관리>보안정책>등급정책	문서 암호화 정책 중 하나인 등급 정책을 설정할 수 있습니다.

정책관리>로그정책	사용자 및 관리자 로그에서 어떠한 종류의 로그를 취합할 것인지를 설정할 수 있습니다.
관리도구>로그관리	'**정책관리>로그정책**'에서 설정한 로그를 조회하고 저장, 삭제할 수 있습니다.
관리도구>마킹이미지관리	마킹이미지파일을 관리할 수 있습니다.
관리도구>직위관리	직위이름을 관리할 수 있습니다.
관리도구>애드인관리	애드인을 관리할 수 있습니다.
관리도구>커스텀정책관리	커스텀정책을 관리할 수 있습니다.
관리자정책 >관리자등록	보안 관리자 정보를 관리하고, 보안 관리자의 관리범위(조직) 및 메뉴 사용 권한을 설정할 수 있습니다.
환경설정>서버프로파일	최고 보안 관리자에 대한 정보 변경, Document Security Client V5.0 (이하 'Client'라고 함)의 인증서버 접속 정책 및 로그서버 정보 설정 등을 수행할 수 있습니다.
보기>메뉴탐색창	닫아진 메뉴탐색창을 다시 표시되게 할 수 있는 것으로, 메뉴탐색창이 닫아진 경우에만 버튼이 활성화됩니다.
정보>프로그램정보	Console 프로그램의 버전 정보 및 시리얼 정보 등을 확인할 수 있습니다.

5.3.메뉴탐색창

본 장에서는 Console 의 **'메뉴탐색창'**에 대해 설명합니다.

1) Console 을 실행하면 다음과 같이 **'메뉴탐색창'**이 활성화 되어 있습니다.



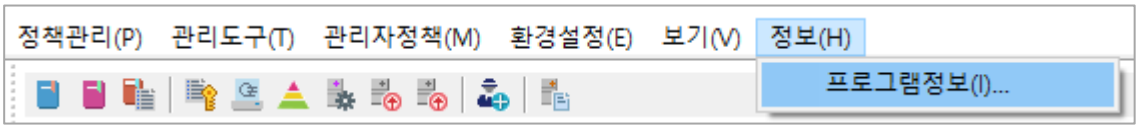
2) '**메뉴탐색창**'의 우측 상단의 **[ㅁ]** 버튼은 다음과 같이 독립된 창을 실행합니다. 독립된 창의 타이틀바를 드래그하여 조직도 상단에서 놓으면 다시 원래의 위치로 돌아옵니다.

3) **'메뉴탐색창'**의 **[x]** 버튼을 클릭하면 **'메뉴탐색창'**이 닫힙니다. Console 상단 메뉴의 **'보기>메뉴탐색창'**을 선택하면 원래의 위치에 **'메뉴탐색창'**이 다시 나타납니다.

5.4.프로그램 정보 확인

관리자는 Console 의 정보(버전 정보, 시리얼 번호 등)를 확인할 수 있습니다.

1) Console 의 상단 매뉴에서 **정보>프로그램정보**를 선택합니다.



2) **<관리자 프로그램 정보>** 창이 나타납니다. Console 의 버전 정보, 시리얼 번호를 확인할 수 있습니다. **[확인]**을 클릭하면 창이 닫힙니다.

5.5.종료

본 장은 Console 을 종료하는 과정을 설명합니다.

Console 을 종료하여면 트레이에서 Console 을 우클릭하여 '**닫기**'를 클릭하거나, Console 실행 화면 우측 상단의  을 클릭하십시오.

6. 정책관리

본 장은 문서 암호화 정책에 대해 설명합니다.

관련링크

a. 분류설정

b. 보안정책

c. 개인/그룹 정책

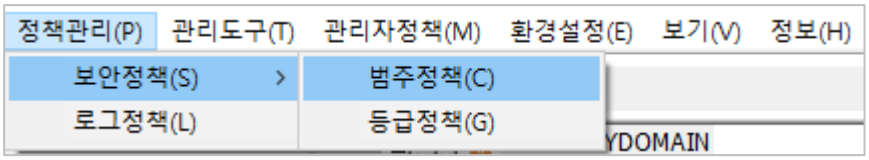
d. 로그정책

6.1. 분류설정

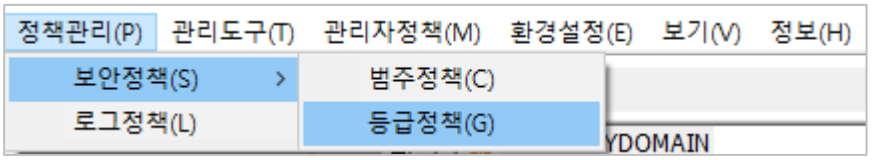
본 장은 분류설정에 대해 설명합니다. 분류는 '범주 정책' 또는 '등급 정책'에서 추가/변경/삭제가 가능합니다.

분류 추가

1) 분류를 설정하기 위해 Console 상단 메뉴의 **'정책관리>보안정책>범주정책'** 또는 **'정책관리>보안정책>등급정책'**을 선택, 또는 ( ) 아이콘을 클릭합니다.

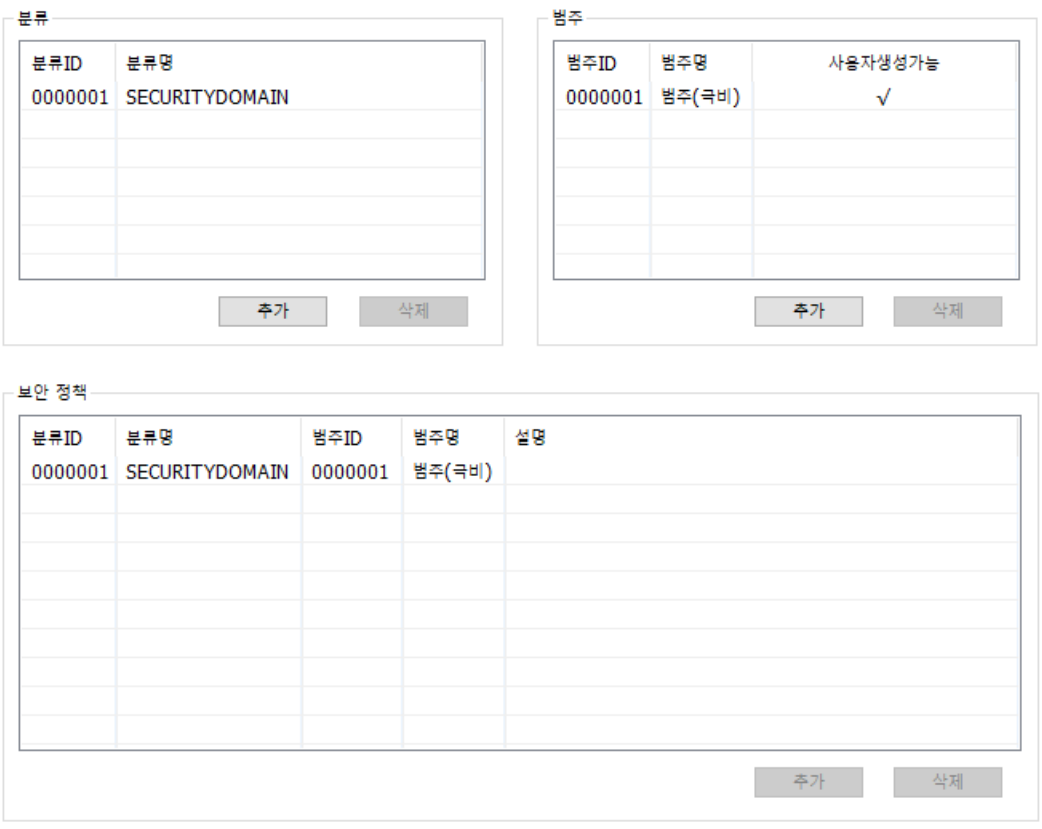


정책관리>보안정책>범주정책

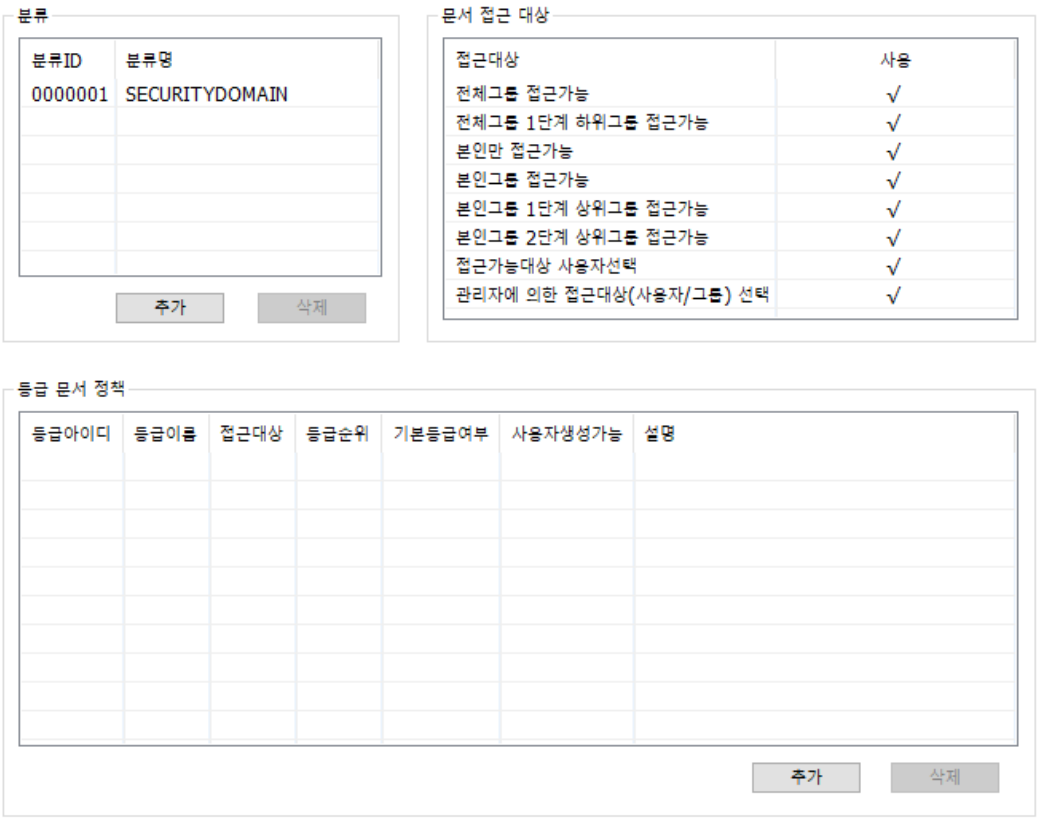


정책관리>보안정책>등급정책

2) 작업 윈도우에 아래와 같은 창이 표시됩니다. **'분류'**에서 **[추가]**를 클릭합니다.

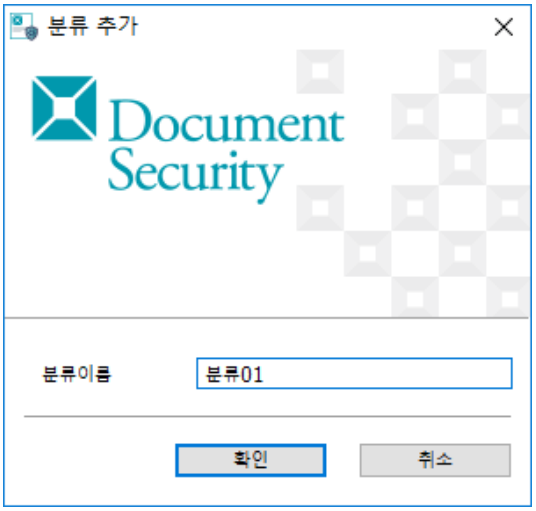


정책관리>보안정책>범주정책을 선택한 경우에 표시되는 작업창

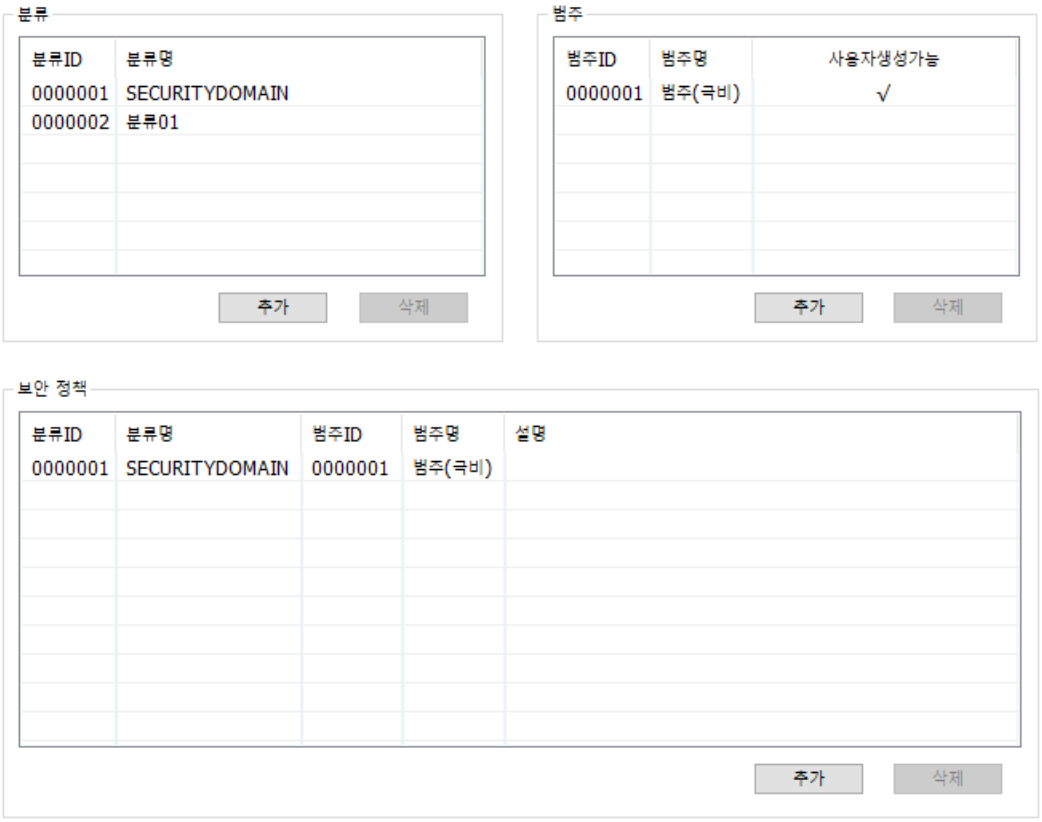


정책관리>보안정책>등급정책을 선택한 경우에 표시되는 작업창

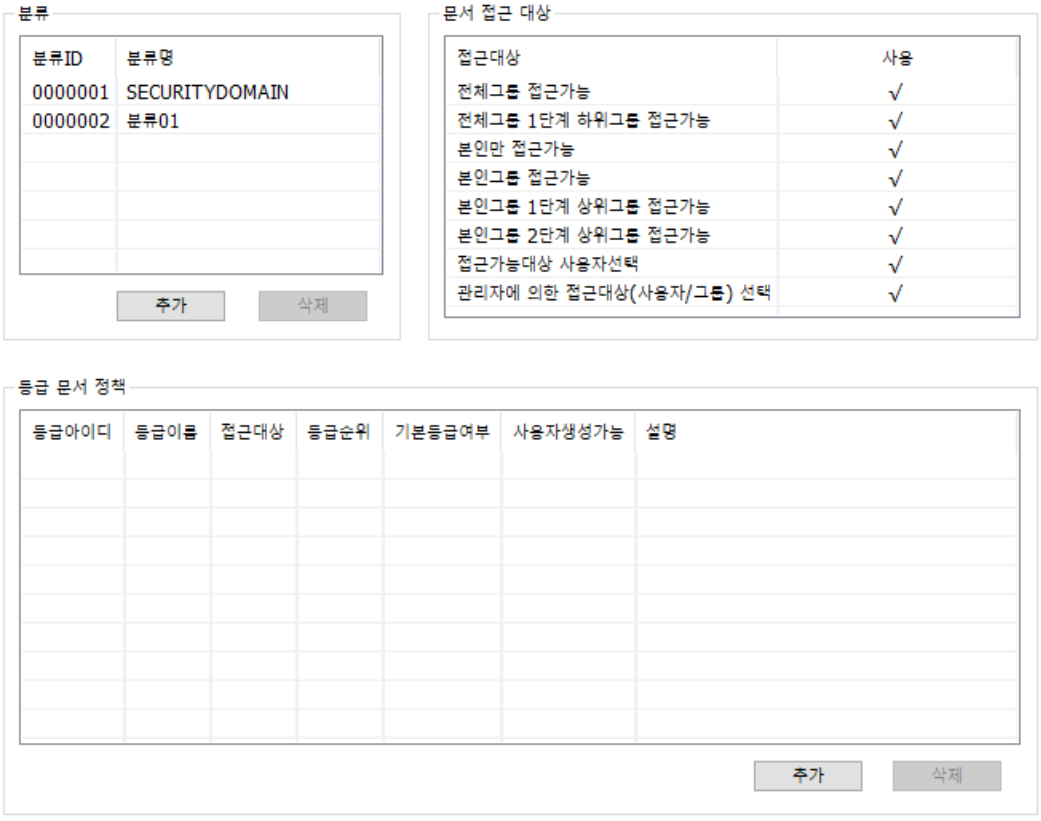
3) 아래와 같이 **<분류 추가>** 창이 출력되면, 분류 이름을 설정하고, **[확인]**을 클릭합니다. **[취소]**를 클릭하면 분류 추가가 취소됩니다. 분류 이름은 반각 255 자까지 입력할 수 있습니다.



4) 아래와 같이 작업 윈도우의 **'분류'** 아래의 테이블에 추가한 분류가 나타납니다.



정책관리>보안정책>범주정책을 선택하여 분류를 추가한 경우



정책관리>보안정책>등급정책을 선택하여 분류를 추가한 경우

참고: 분류 ID 는 추가 시 자동적으로 생성되는 ID 입니다. 새로운 항목을 추가 할 때 마다 증가된 수치로 생성됩니다. 각각의 메뉴에서 추가한 분류는 동기화됩니다.

6.2. 보안정책

본 장은 전사적으로 적용되는 문서 암호화 정책에 대해 설명합니다.

관련링크

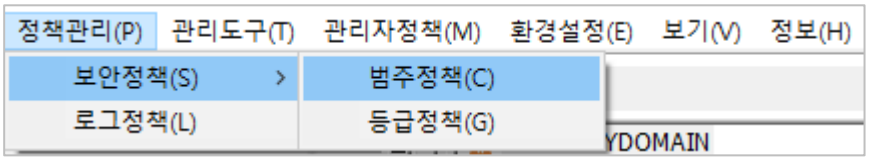
a. 범주

b. 등급

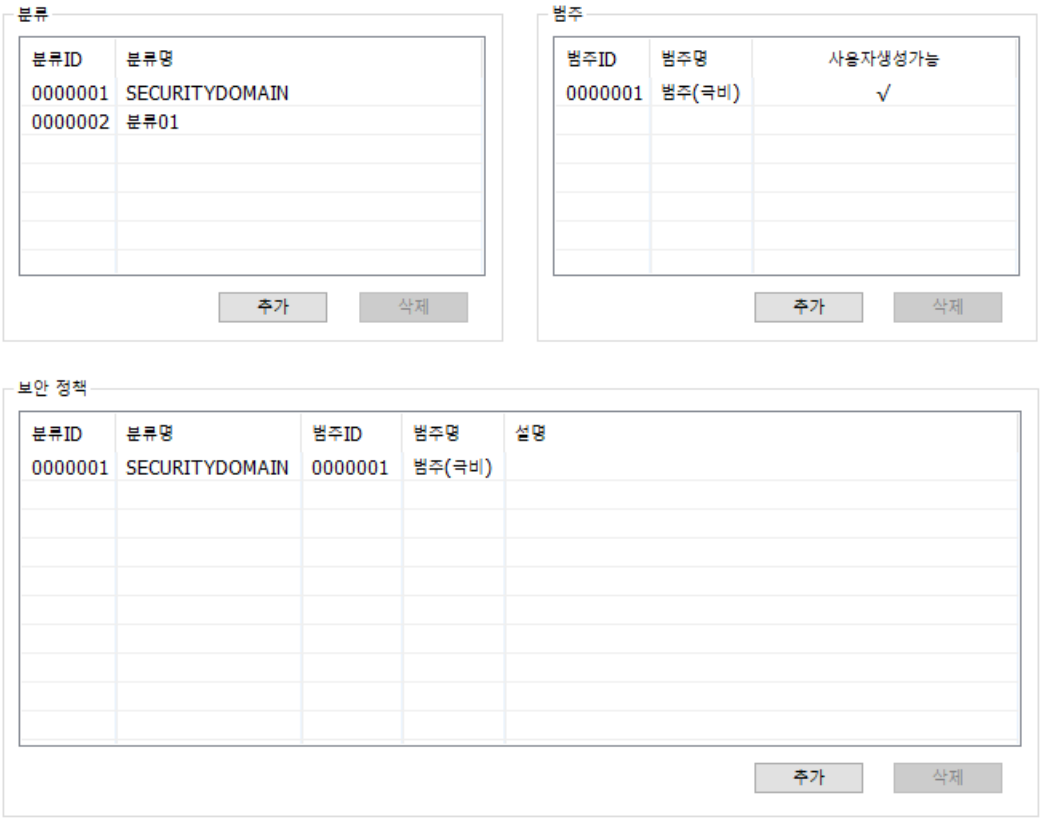
6.2.1. 범주정책

본 장은 범주 정책을 설정하는 방법에 대해 설명합니다. 범주 정책은 모든 사용자에게 적용되는 암호화 정책입니다. 사용자가 속한 분류에 따라 범주 정책으로 암호화된 문서에 대해 정해진 권한을 가집니다. 예를 들어 '**분류 01**'에 속한 사용자는 '**범주 01**' 정책으로 암호화된 문서에 대해 열람/편집 권한을 가진다면, 똑같은 '**범주 01**' 정책으로 암호화된 문서이지만 '**분류 02**'에 속한 사용자는 열람/편집 권한이 없을 수 있습니다. 범주 정책을 생성하기 위해서는 하나 이상의 분류가 추가되어 있어야 합니다.

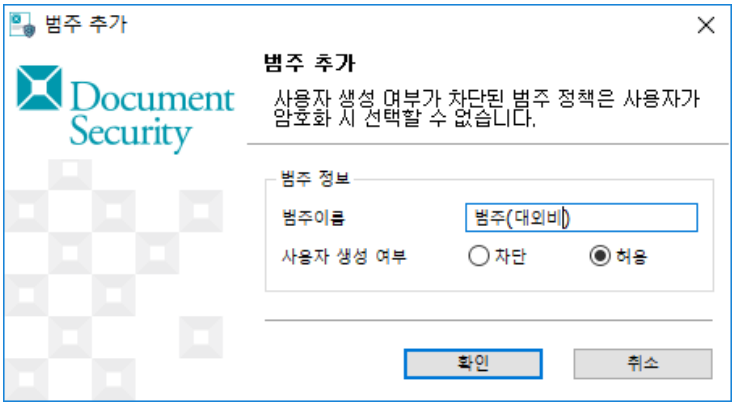
1) '**범주 정책**'을 등록하기 위해 Console 상단 메뉴의 '**보안정책>범주정책**'을 선택, 또는 ( ) 아이콘을 클릭합니다.



2) 다음과 같은 작업창이 표시됩니다.

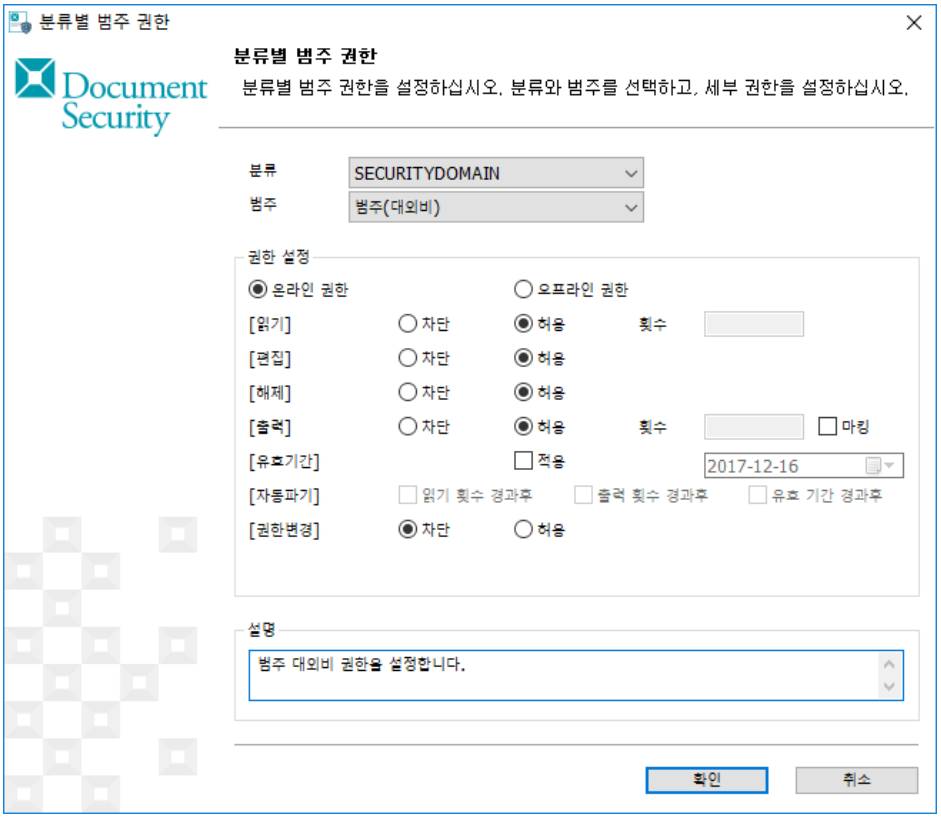


5) 하나 이상의 분류가 추가되어 있다면, **'범주'**라고 되어 있는 부분의 하단의 **[추가]**를 클릭합니다. 아래와 같은 창이 표시되면 범주 정책을 설정합니다. 범주 이름은 반각 255 자까지 입력할 수 있습니다.



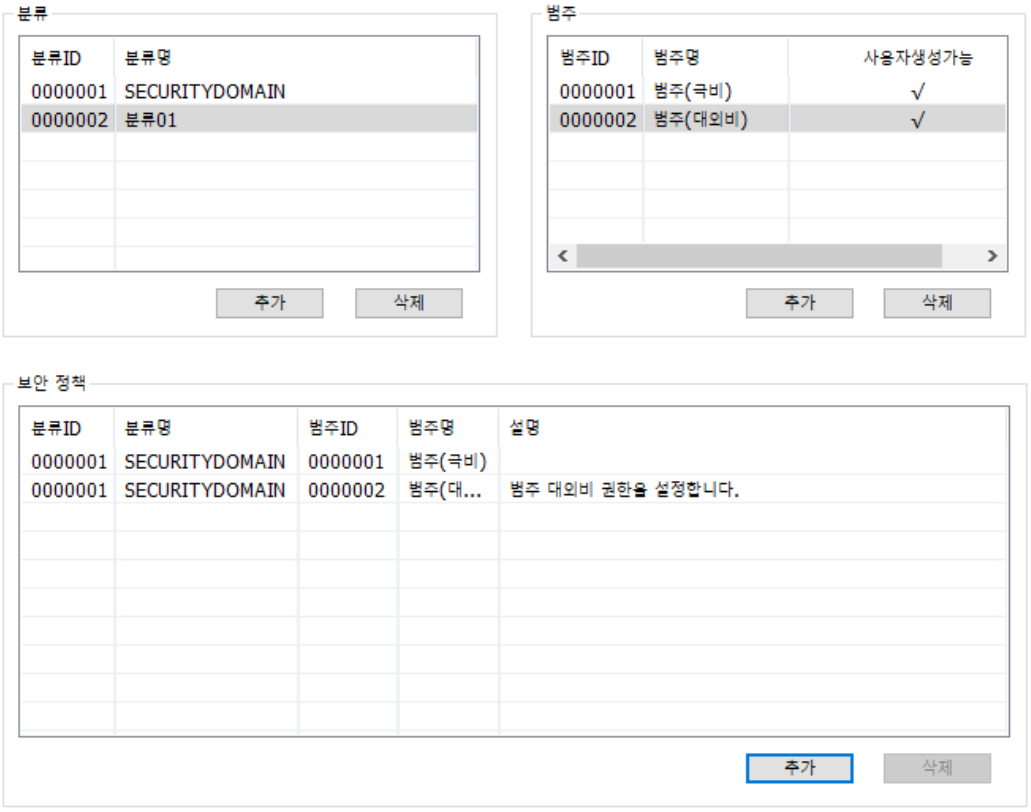
항목		내용
범주정보	**범주이름**	범주 정책의 이름을 입력합니다.
	사용자 생성 여부	차단을 체크하면 사용자가 해당 범주 정책으로 문서를 암호화할 수 없습니다. 허용을 체크하면 사용자가 해당 범주 정책으로 문서를 암호화할 수 있습니다.

3) 추가한 범주에 대해 특정 분류에 속한 사용자가 가지는 권한을 설정하기 위해 보안정책의 **[추가]**를 클릭합니다. 아래와 같은 창이 표시됩니다.



항목	내용
분류	풀다운메뉴에서 추가한 분류 중에 정책을 설정할 분류를 선택합니다.
범주	풀다운메뉴에서 추가한 범주 중에 정책을 설정할 범주를 선택합니다.
온라인 권한 / 오프라인 권한	온라인 로그인 시에 적용되는 권한을 설정하려면 **'온라인 권한'**을, 오프라인 로그인 시에 적용되는 권한을 설정하려면 **'오프라인 권한'**을 설정합니다.
[읽기]	읽기 권한의 **'차단'** 또는 **'허용'**을 선택합니다. **'허용'**할 경우, **'횟수'**를 입력하면 읽기 가능 횟수가 설정됩니다. 0 으로 설정하면 횟수 제한없이 읽기가 가능합니다. 숫자 0~99999 까지 입력가능합니다.
[편집]	편집 권한의 **'차단'** 또는 **'허용'**을 선택합니다.
[해제]	해제 권한의 '**차단'** 또는 '**허용'**을 선택합니다.
[출력]	출력 권한의 '**차단'** 또는 '**허용'**을 선택합니다. '**허용'**할 경우, '**횟수'**를 입력하면 출력 가능 횟수가 설정됩니다. 0 으로 설정하면 횟수 제한없이 출력이 가능합니다. 숫자 0~99999 까지 입력가능합니다.
[유효기간]	**'적용'**을 선택하면 풀다운 메뉴를 이용해 날짜를 설정하여 보안문서의 사용 유효기간을 설정할 수 있습니다.
[자동파기]	읽기 횟수, 출력 횟수, 유효 기간 경과 시 보안문서가 자동파기되도록 설정할 수 있습니다.
[권한변경]	**'허용'**할 경우, 상용자가 암호화된 범주 정책을 다른 범주 정책으로 변경할 수 있습니다. **'차단'**할 경우, 변경이 불가능합니다.
설명	해당 범주 정책의 설명을 입력합니다. 반드시 입력해야 하는 사항은 아닙니다.

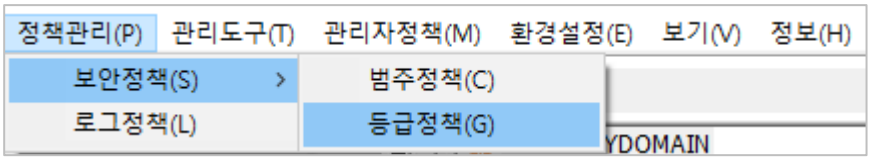
4) 아래와 같이 보안 정책이 추가된 것을 확인합니다.



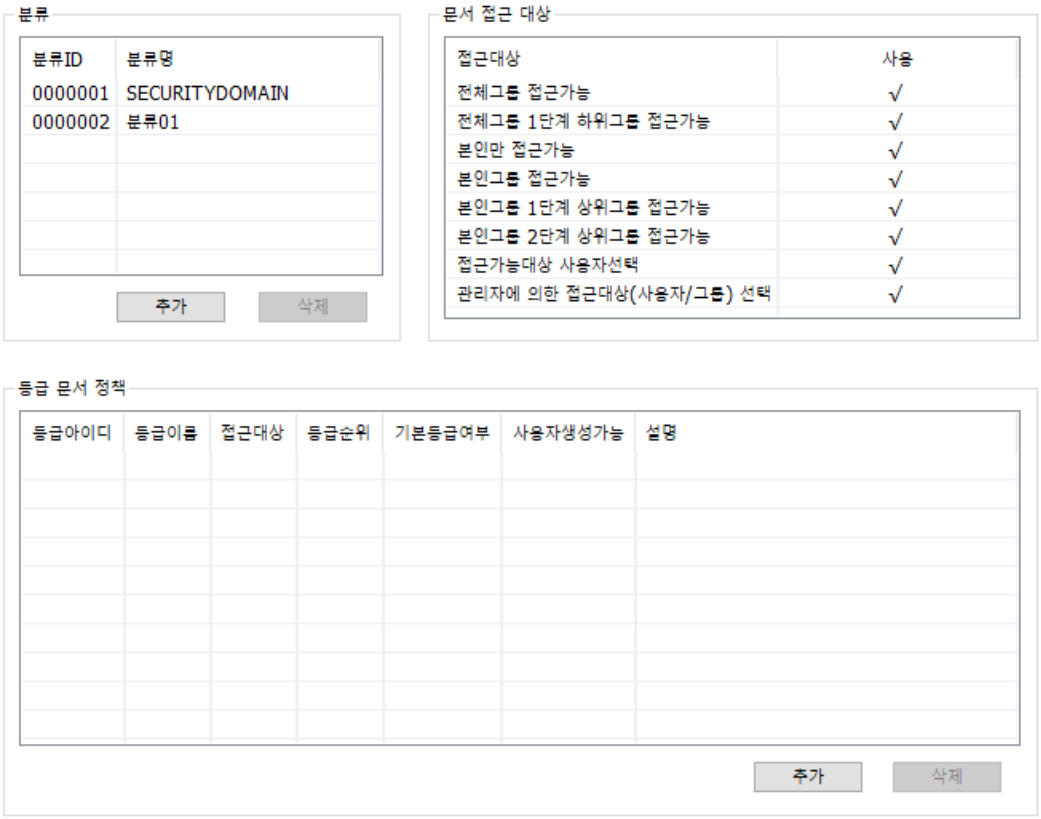
6.2.2. 등급정책

본 장은 등급 정책에 대해 설명합니다. 등급 정책은 범주 정책과 DAC 정책이 혼합된 형태의 암호화 정책으로, 해당 등급 정책으로 암호화된 문서에는 생성자, 오프라인 로그인 상태의 사용자, 온라인 로그인 상태의 사용자가 가지는 권한 및 보안정책이 설정됩니다.

1) **'등급 정책'**을 등록하기 위해 Console 상단 메뉴의 **'보안정책>등급정책'**을 선택, 또는 ( ) 아이콘을 클릭합니다.



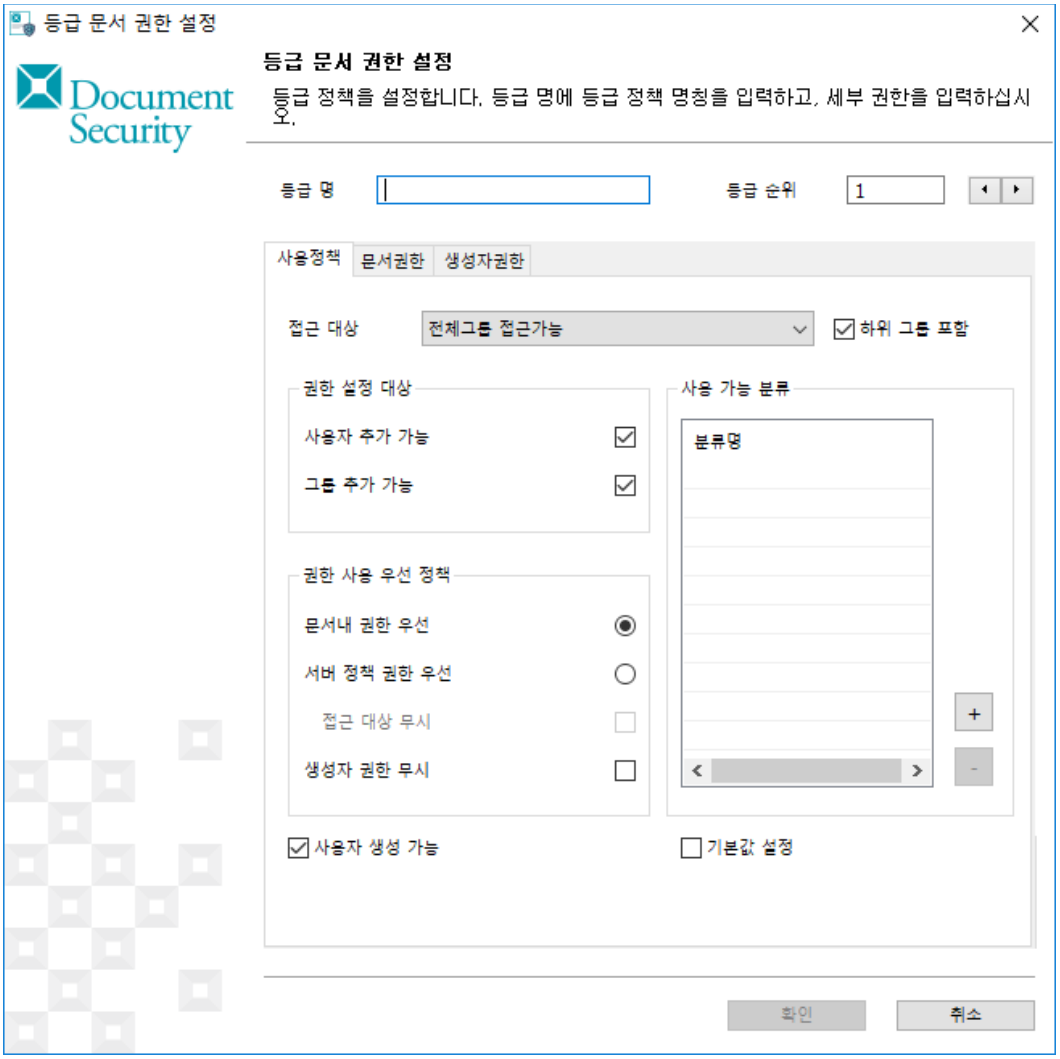
2) 다음과 같은 작업창이 표시됩니다.



3) 등급 문서 정책 오른쪽 아래의 **[추가]**를 클릭하면 아래와 같은 창이 출력됩니다. 본 등급 정책의 이름을 **'등급 명'**에 입력하고, **'등급 순위'**와 **'표시 순서'**를 설정합니다. 등급명은 반각기준 255 자까지 입력가능하며, 등급순위는 숫자 기준 1~99999 까지 입력가능합니다. 사용자가 등급 보안문서의 권한을 변경할 때 높은 등급 순위에서 낮은 등급 순위로 변경이

불가능합니다. **'표시 순서'**는 사용자가 등급 보안문서 생성 시 등급 보안문서 생성 창에서 해당 등급이 표시되는 순서를 의미합니다. 표시 순서가 낮을 수록 먼저 표시됩니다.

'사용정책' 탭에서 다음의 항목을 설정하거나 입력합니다.



항목	내용
접근 대상	접근 가능한 대상을 선택합니다. 접근 가능한 대상에 대한 자세한 설명은 아래의 참조를 확인하십시오. **'하위 그룹 포함'**을 체크한 경우

		선택한 접근 대상의 하위 그룹도 해당 등급 정책으로 암호화한 문서에 접근할 수 있는 권한을 가집니다.
권한 설정 대상	**사용자 추가 기능**	사용자가 해당 등급 정책으로 문서를 암호화할 때 접근 대상에 임의로 사용자 및 그룹을 추가할 수 있습니다. **'사용자 추가 가능'**을 체크하면 사용자는 해당 등급 보안문서의 접근대상에 타사용자를 추가할 수 있습니다.
	그룹 추가 기능	**'그룹 추가 가능'**을 체크하면 사용자는 해당 등급 보안문서의 접근대상에 그룹 및 그룹에 속한 사용자를 추가할 수 있습니다. 사용자는 접근 대상에게 사용 권한을 임의로 부여할 수 있습니다.
권한 사용 우선 정책	**문서내 권한 우선**	사용자가 등급 보안문서를 열람하는 시점에 문서에 포함된 사용 권한을 이용할 지 로그인 시 서버에서 내려 받은 사용 권한을 이용할 지를 선택합니다. **'문서내 권한 우선'**을 선택한 경우 문서에 설정되어 있는 정보를 이용합니다.
	서버 정책 권한 우선	**'서버 정책 권한 우선'**을 선택한 경우 서버에 설정된 접근 권한이 적용됩니다.
	생성자 권한 무시	**'생성자 권한 무시'**를 선택하면 생성자 또한 생성자권한을 따르지 않고 문서권한을 따릅니다.
사용 가능 분류		해당 등급 정책으로 암호화한 문서를 사용할 수 있는 분류를 선택합니다. 등급 보안문서는 사용 가능 분류에 추가된 분류에 속한 사용자와 생성자에 한해 접근이 허용됩니다. 사용 가능 분류에 어떤 분류도 추가하지 않은 경우, 해당 등급으로 암호화해 접근 대상을 변경할 때 모든 사용자를 접근 대상에 포함시킬 수 있습니다.
사용자 생성 가능		**'사용자 생성 가능'**을 체크하지 않으면 사용자는 해당 등급 정책으로 문서를 암호화할 수 없습니다.

기본값 설정	**'기본값 설정'**을 체크하면 사용자가 등급 보안문서를 생성할 경우 등급 선택 시 해당 등급 정책이 디폴트로 선택됩니다. **주의: 강제암호화 정책의 등급문서 암호화 정책이 사용자 지정일 경우와 강제 암호화하지 않을 경우에만 동작합니다.**

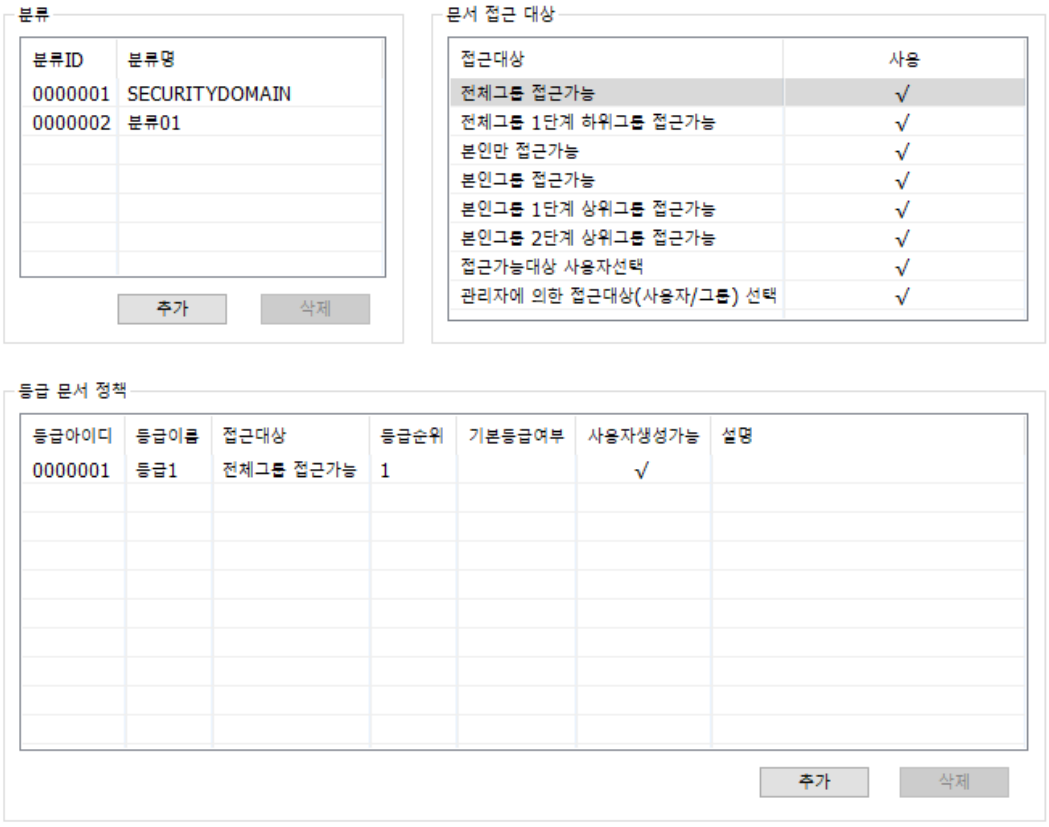
4) **'문서권한'** 탭을 클릭하면 아래와 같은 창이 표시됩니다. 해당 등급에 포함된 사용자의 온라인 권한과 오프라인 권한에 따른 문서의 사용 권한을 설정합니다. 온라인권한은 사용자가 Client 에 정상적으로 로그인하고 서버와 동작이 원활할 때 사용자에게 부여하는 권한입니다. 오프라인권한은 오프라인 로그인 권한을 가진 사용자에 한해서 오프라인일 경우 사용자에게 부여하는 권한입니다.

항목	내용
온라인 권한 / 오프라인 권한	온라인 로그인 시에 적용되는 권한을 설정하려면 **'온라인 권한'**을, 오프라인 로그인 시에 적용되는 권한을 설정하려면 **'오프라인 권한'**을 설정합니다.
[읽기]	읽기 권한의 **'차단'** 또는 **'허용'**을 선택합니다. **'허용'**할 경우, **'횟수'**를 입력하면 읽기 가능 횟수가 설정됩니다. 0 으로 설정하면 횟수 제한없이 읽기가 가능합니다.
[편집]	편집 권한의 **'차단'** 또는 **'허용'**을 선택합니다.
[해제]	해제 권한의 **'차단'** 또는 **'허용'**을 선택합니다.

[반출]	반출 권한의 '**차단**' 또는 '**허용**'을 선택합니다.
[출력]	출력 권한의 '**차단**' 또는 '**허용**'을 선택합니다. '**허용**'할 경우, '**횟수**'를 입력하면 출력 가능 횟수가 설정됩니다. 0 으로 설정하면 횟수 제한없이 출력이 가능합니다.
[유효기간]	'**적용**'을 선택하면 풀다운 메뉴를 이용해 날짜를 설정하여 보안문서의 사용 유효기간을 설정할 수 있습니다.
[자동파기]	읽기 횟수, 출력 횟수, 유효 기간 경과 시 보안문서가 자동파기되도록 설정할 수 있습니다.
[권한변경]	'**허용**'할 경우, 상용자가 암호화된 범주 정책을 다른 범주 정책으로 변경할 수 있습니다. '**차단**'할 경우, 변경이 불가능합니다.

5) '**생성자권한**' 탭을 클릭하면 아래와 같은 창이 표시됩니다. 해당 등급의 보안문서를 생성한 사용자의 온라인 권한과 오프라인 권한을 설정합니다. 설정 방법은 문서권한 설정 방법과 동일하나, [유효기간 연장]은 할 수 없습니다.

6) 등급 정책 설정을 완료했으면 **[확인]**을 클릭하여 설정한 정책을 저장합니다. **[취소]**를 클릭하면 작업이 취소됩니다. 아래와 같이 추가한 등급 정책이 리스트에 표시됩니다.



7) 설정된 등급 문서 정책을 삭제하려면 삭제하고자 하는 정책을 리스트에서 클릭하고 **[삭제]**를 누릅니다. 리스트에서 선택한 등급 문서 정책이 삭제된 것을 확인할 수 있습니다. 이미 설정한 정책을 수정하려면 수정하고자 하는 정책을 더블 클릭합니다. **<등급 문서 권한 설정>** 창이 출력되며 정책을 추가한 것과 동일한 과정으로 수정할 수 있습니다.

6.3. 개인/그룹 정책

본 장은 사용자 및 그룹에 대해 설정하는 문서 암호화 정책에 대해 설명합니다.

관련링크

a. 범주(MAC)

b. 등급

c. DAC

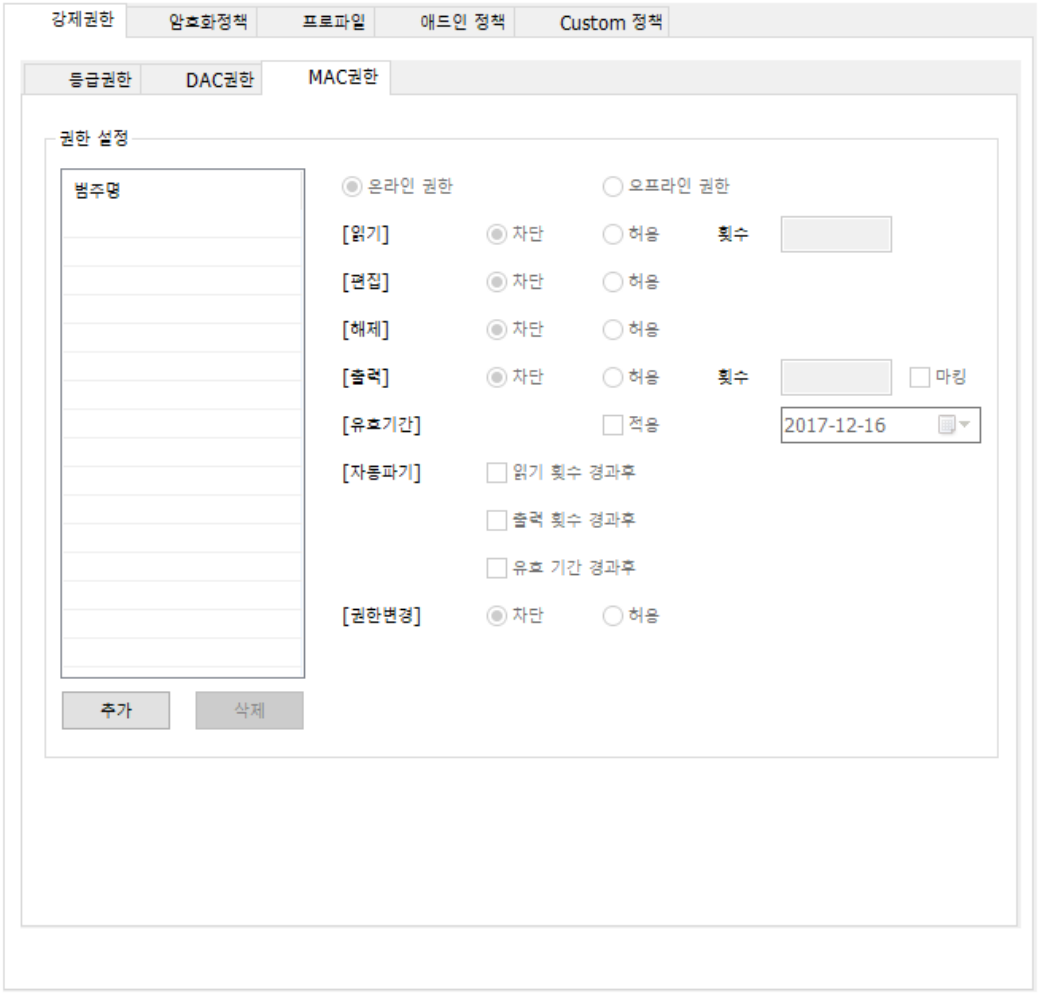
d. 기본 암호화 정책

e. 강제 암호화 정책

6.3.1. 범주(MAC)

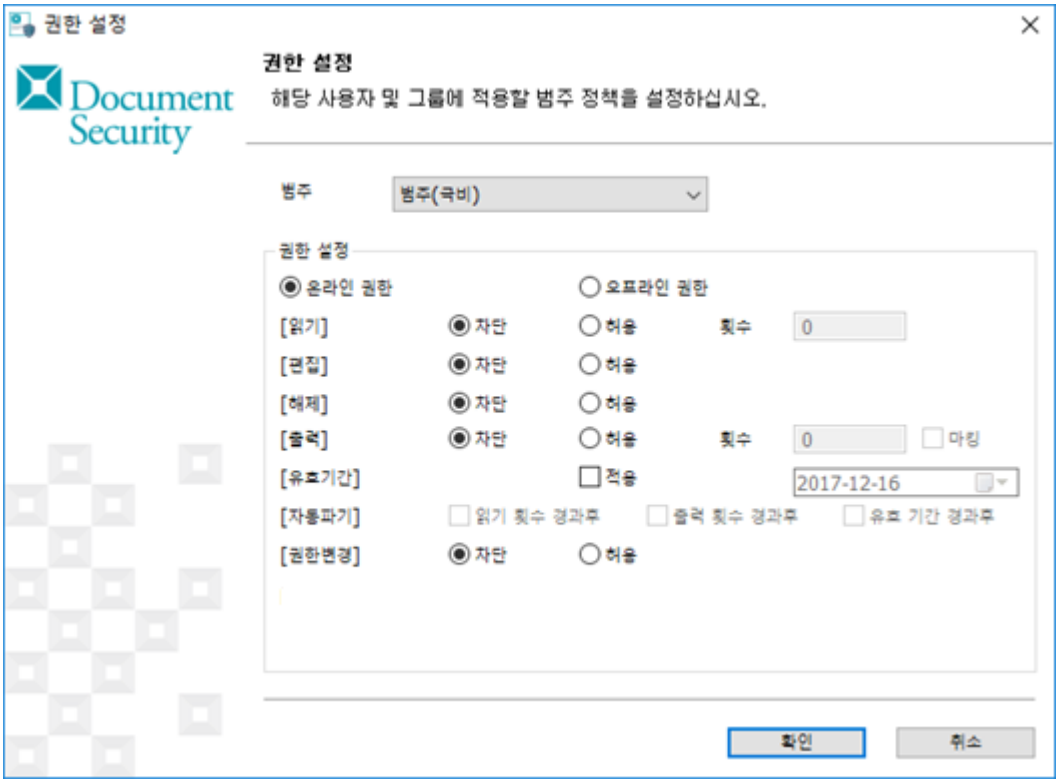
관리자는 전사에 적용하는 범주 정책을 특정 사용자만 다르게 설정할 수 있습니다. 예를 들어 **'분류 01'**에 속한 모든 사용자는 **'범주 01'**로 암호화된 문서에 대해 모두 동일한 권한을 가지지만, 특정 사용자만 다른 권한을 가지게 할 수 있습니다. 이 경우, 사용자가 '**분류 01**'에 속하지만, 다른 '**분류 01**'에 속한 사용자와 다른 권한을 가지게 됩니다.

1) 조직도에서 해당 **'MAC'** 권한을 설정할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'강제권한>MAC 권한'을** 선택합니다. 화면의 구성은 다음과 같습니다.

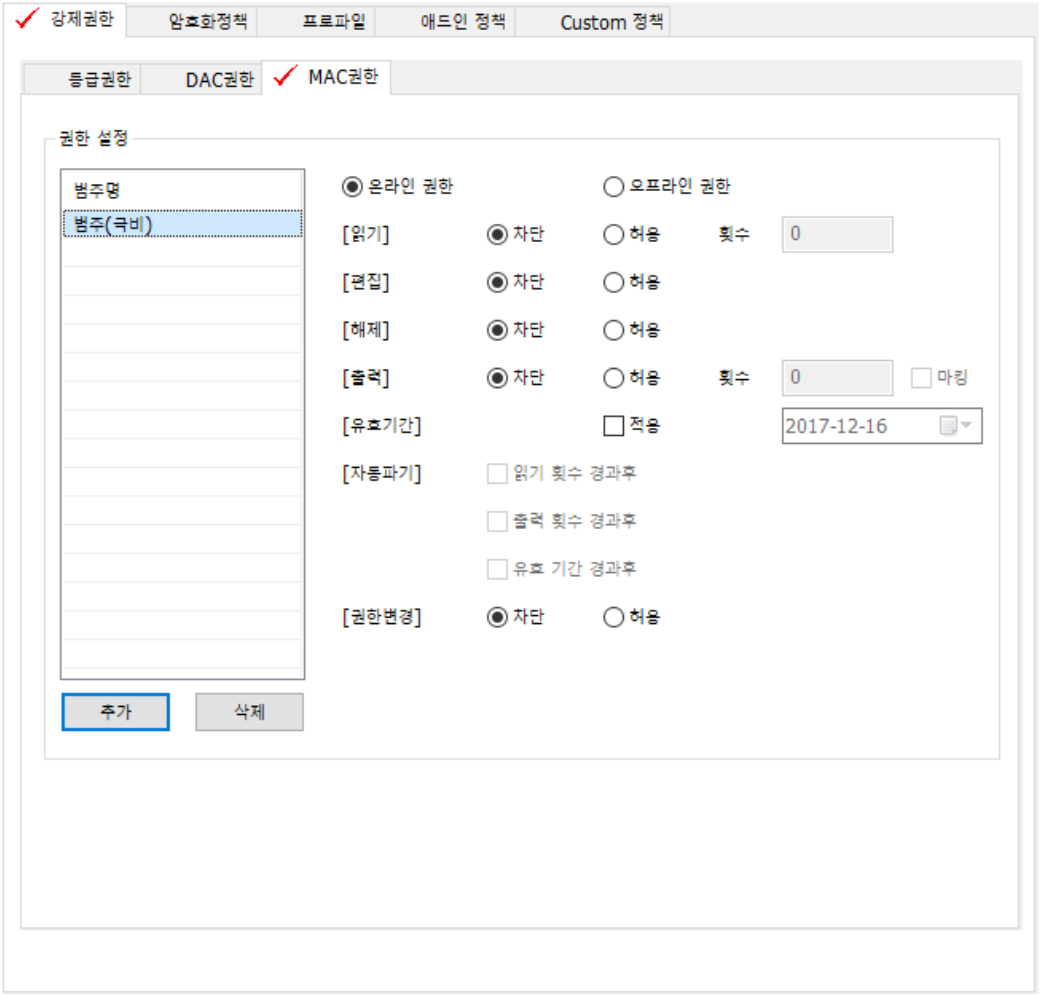


참고 : 아무 범주도 추가되어 있지 않으면, 해당 사용자는 전체의 범주 정책을 따릅니다.

2) **[추가]**를 클릭하면 아래와 전체의 범주에 대해 권한을 설정하는 창이 표시됩니다. 권한을 설정하는 방법은 전체의 범주와 동일합니다.



3) 권한을 설정하고 **[확인]**을 클릭하면 아래와 같이 범주가 추가됩니다. 추가된 범주 정책을 수정하려면 수정하고자 하는 범주를 클릭하고 우측의 활성화된 정책 설정 항목을 변경하면 됩니다. 삭제하려면 삭제하고자 하는 범주를 선택하고 **[삭제]**를 클릭합니다.

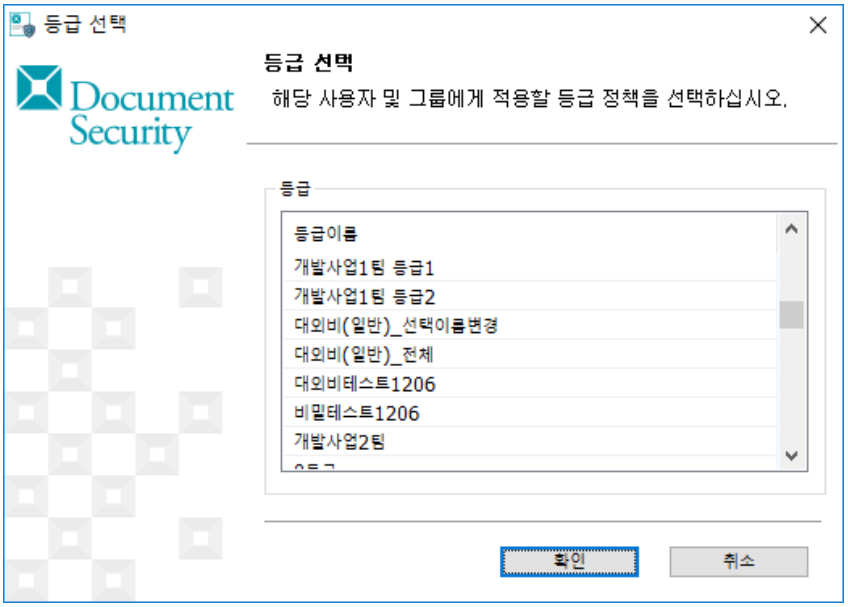


6.3.2. 등급

관리자는 전사에 적용하는 등급 정책을 특정 사용자만 다르게 설정할 수 있습니다.

1) 조직도에서 해당 **'등급'** 권한을 설정할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'강제권한>등급권한'을** 선택합니다. 화면의 구성은 다음과 같습니다.

2) **[추가]**를 클릭하면 아래와 같은 창이 표시됩니다. 사용자에게 다르게 설정할 등급 정책을 선택하고 **[확인]**을 클릭합니다.



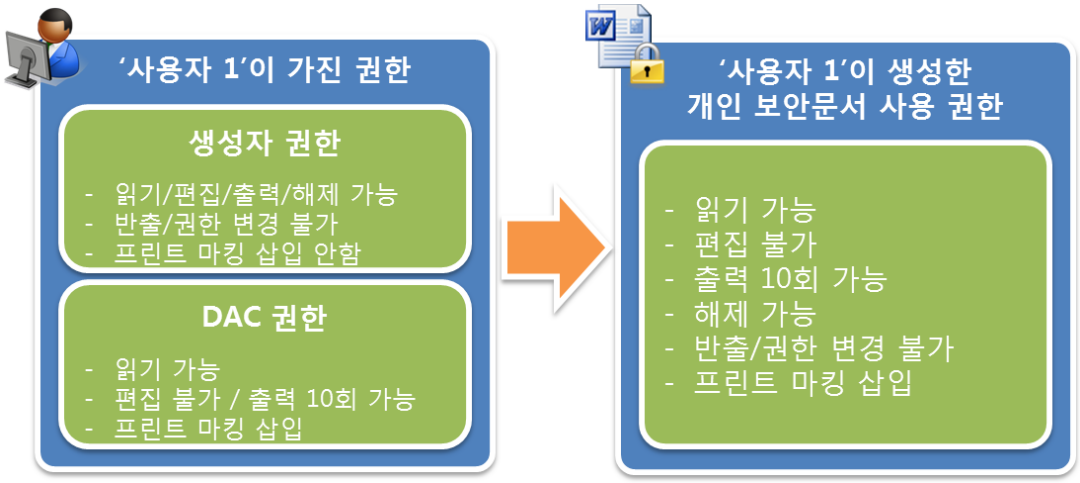
3) 아래와 같이 선택한 등급정책이 표시되고, 설정 항목이 활성화됩니다. 사용자에 대한 증급정책을 설정하는 방법은 전체의 등급정책과 동일합니다. 제한권한만 제외하고 모든 항목을 동일한 방법으로 수정할 수 있습니다.

6.3.3. DAC

본 장은 DAC 권한에 대해 설명합니다.

DAC 이란?

DAC 은 개인 보안문서에 대해 우선적으로 적용하는 권한을 의미합니다. 개인 보안문서를 생성하면, 권한은 생성자 권한을 따르게 되어 있으나, DAC 권한이 적용되어 있는 경우, 생성자 권한보다 DAC 권한이 우선적으로 적용됩니다. DAC 권한이 적용되는 예는 아래와 같습니다.



생성자 권한과 DAC 권한에서 설정한 권한 중에, 동일한 항목인 경우, DAC 권한이 우선 적용됩니다. DAC 권한에서 설정하지 않은 항목의 경우, 생성자 권한이 그대로 적용됩니다.

주의 : 기본 암호화 정책에서 'DAC 문서 오픈시 생성자 권한 적용'을 체크했을 경우, 위와 같이 권한이 적용됩니다. 'DAC 문서 오픈시 생성자 권한 적용'을 체크하지 않으면, 생성자 권한이 적용되지 않아, DAC 권한 내에서만 보안문서 사용이 가능합니다.

DAC 권한 설정 방법

1) 조직도에서 해당 **'DAC'** 권한을 설정할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'강제권한>DAC 권한'을** 선택합니다. 화면의 구성은 다음과 같습니다.

구분	내용
온라인 권한	온라인 로그인 시 적용할 DAC 권한을 설정합니다.
오프라인 권한	오프라인 로그인 시 적용할 DAC 권한을 설정합니다.
[읽기]	읽기 권한을 설정합니다. 읽기 권한을 적용하려면 **'사용'**을 체크하고 **'차단'** 또는 **'허용'** 여부를 설정합니다. 읽기 횟수를 제한하려면 **'횟수'**를 숫자로 입력합니다.
[편집]	편집 권한을 설정합니다. 편집 권한을 적용하려면 **'사용'**을 체크하고 **'차단'** 또는 **'허용'** 여부를 설정합니다.
[해제]	해제 권한을 설정합니다. 해제 권한을 적용하려면 **'사용'**을 체크하고 **'차단'** 또는 **'허용'** 여부를 설정합니다.

[출력]	출력 권한을 설정합니다. 출력 권한을 적용하려면 **'사용'**을 체크하고 **'차단'** 또는 **'허용'** 여부를 설정합니다. 출력 횟수를 제한하려면 **'횟수'**를 숫자로 입력합니다. 프린트 마킹을 삽입하려면 **'마킹'**을 체크합니다.
[유효기간]	유효기간을 설정합니다. 유효기간을 적용하려면 **'사용'**을 체크하고 우측의 날짜를 설정합니다.
[자동파기]	자동파기 여부를 설정합니다. 자동파기를 적용하려면 **'사용'**을 체크하고, 자동파기 시점을 선택합니다. 선택 가능한 시점은 **'읽기 횟수 경과후'**, **'출력 횟수 경과후'**, **'유효 기간 경과후'**입니다.
[권한변경]	권한변경 여부를 설정합니다. 권한변경 권한을 적용하려면 **'사용'**을 체크하고 **'차단'** 또는 **'허용'** 여부를 설정합니다.

6.3.4. 기본 암호화 정책

본 장은 기본 암호화 정책을 설정하는 방법을 설명합니다. 기본 암호화 정책에서는 다음과 같은 정책을 설정할 수 있습니다.

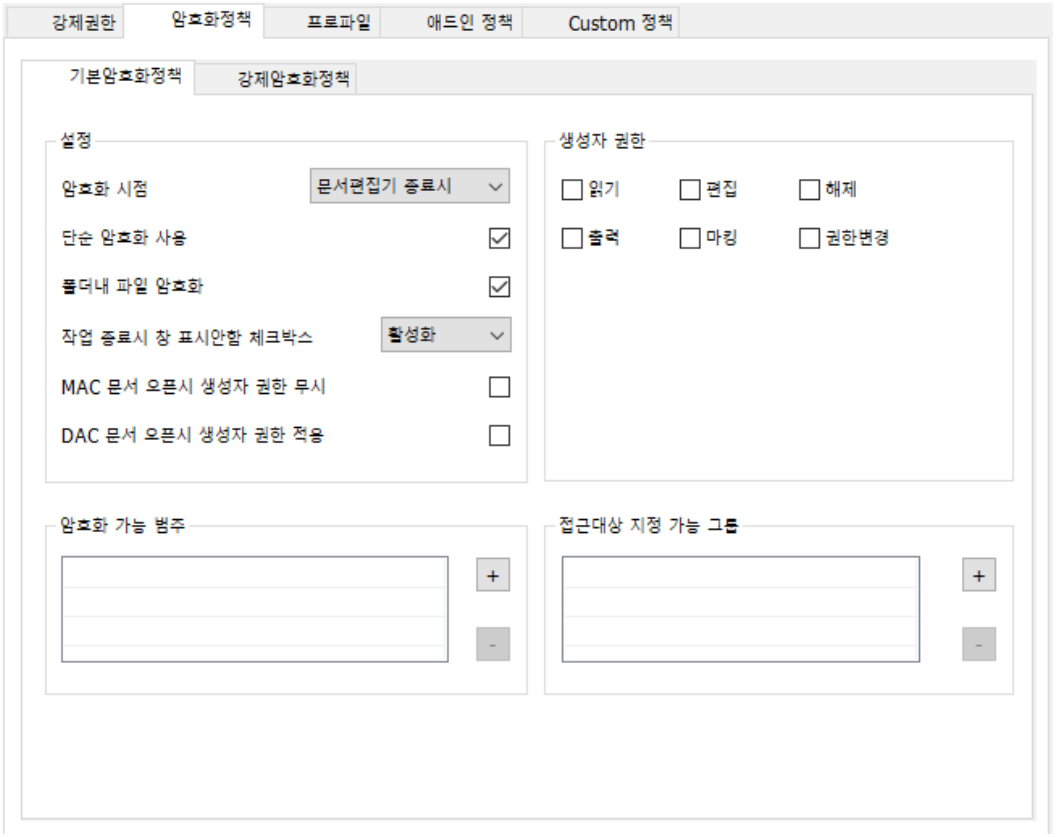
a. **설정 :** 문서 저장 시 및 문서 편집 어플리케이션 종료 시 문서 암호화 여부, 단순 암호화 사용 여부 등

b. **생성자 권한 :** 문서 생성자의 보안문서 사용 권한

c. **암호화 가능 범주 :** 범주 보안 문서 생성 시 사용 가능한 범주 정책

d. **접근대상 지정 그룹 :** 접근 대상자를 지정하여 문서 암호화 시 선택 가능한 그룹

1) 조직도에서 해당 '**기본 암호화 정책**'을 변경할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 '**암호화정책>기본암호화정책**'을 선택합니다. 화면의 구성은 다음과 같습니다.



구분		내용
설정	**암호화 시점**	보안문서 생성시 암호화 시점을 설정 할 수 있습니다. '**문서편집기 종료시**'를 선택하면 문서 편집 프로그램이 종료될 때 사용자에게 종료된 문서 편집 프로그램으로 작업한 모든 문서에 대해 암호화 여부를 묻습니다. '**문서편집기 저장시 (MS 오피스만 지원)**'을 선택하면 편집 중인 문서를 저장할 때와 문서 편집 프로그램이 종료될 때 사용자에게 해당 문서의 암호화 여부를 묻습니다.

		참고: 문서편집기 저장 시 암호화는 MS Office 계열의 어플리케이션 (예: MS Word, MS PowerPoint, MS Excel)만 지원합니다. 여타 어플리케이션은 문서 저장 시에 암호화 여부를 묻는 지 않고, 문서편집기 종료 시에만 암호화 여부를 묻습니다.
	단순 암호화 사용	단순 암호화 기능의 사용 여부를 설정 할 수 있습니다.
	폴더내 파일 암호화	폴더 내의 파일을 일괄적으로 암호화하는 기능의 사용 여부를 설정합니다.
	작업 종료시 창 표시안함 체크박스	작업 종료시 암호화를 진행할 지를 묻는 창의 하단의 **'다음부터 이 창을 표시하지 않음'** 문구 체크 및 활성화 여부를 선택합니다. 드롭 다운 메뉴에서 선택할 수 있는 항목은 아래와 같습니다. • **비활성화 :** 체크 박스가 비활성화됩니다. • **활성화 :** 체크 박스가 활성화되어 사용자가 체크할 수 있습니다. • **감춤 :** 문구 및 체크 박스가 사용자에게 보이지 않습니다. • **비활성화(체크) :** 체크 박스가 체크된 채로 비활성화되어 작업 종료 시 암호화를 진행할 지 묻는 창이 표시되지 않습니다. • **비활성화(언체크) :** 체크 박스가 체크되지 않은 상태로 비활성화됩니다. • **감춤(체크) :** 문구 및 체크박스가 체크된 채로 사용자에게 보이지 않아, 작업 종료 시 암호화를 진행할 지 묻는 창이 표시되지 않습니다.

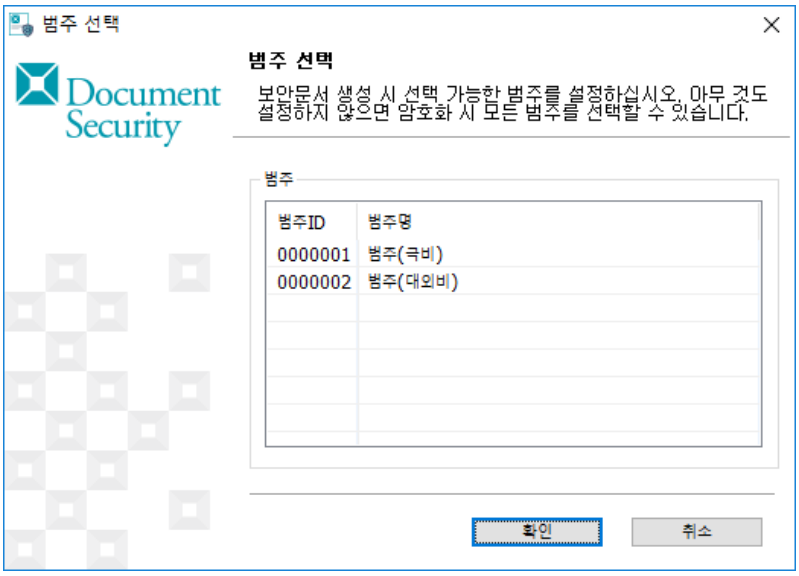
		• **감춤(언체크) :** 문구 및 체크 박스가 사용자에게 보이지 않습니다.
	MAC 문서 오픈시 생성자 무시	체크하면 MAC 문서(범주 보안문서) 오픈 시 생성자 권한을 무시하고, 범주 정책의 권한을 따릅니다.
	DAC 문서 오픈시 생성자 권한 적용	체크하면 DAC 문서 오픈 시 생성자 권한을 적용합니다.
	자동 암호화 폴더	특정 폴더에 저장되는 문서를 자동으로 암호화합니다. **주의: 해당 기능이 동작하려면 Client 패키지에 자동 암호화 폴더가 등록되어 있어야 합니다.**
암호화 가능 범주		사용자의 범주 보안문서 생성 시 선택 가능한 범주 목록을 지정 할 수 있습니다. **참고: 암호화 가능 범주 리스트에 아무것도 설정되어 있지 않은 경우 사용자가 문서 암호화 시 접근 가능 범주에 모든 범주가 표시됩니다.**
생성자 권한		문서 생성자의 보안문서 사용 권한을 설정합니다. 읽기, 편집, 해제, 반출, 출력, 마킹, 권한변경 등의 권한을 설정할 수 있습니다. **참고: 일반 문서의 경우, 반출 권한과 상관없이 외부 전송용 보안 파일을 생성할 수 있습니다.**
접근대상 지정 가능 그룹		사용자가 보안문서 생성시 접근권한을 지정할 수 있도록 조직의 범위를 설정할 수 있습니다.

	참고: 접근대상 지정가능 리스트에 아무것도 설정되어 있지 않은 경우 사용자의 접근대상 변경창의 조직도의 상위 그룹 아래 모든 그룹이 표시됩니다.

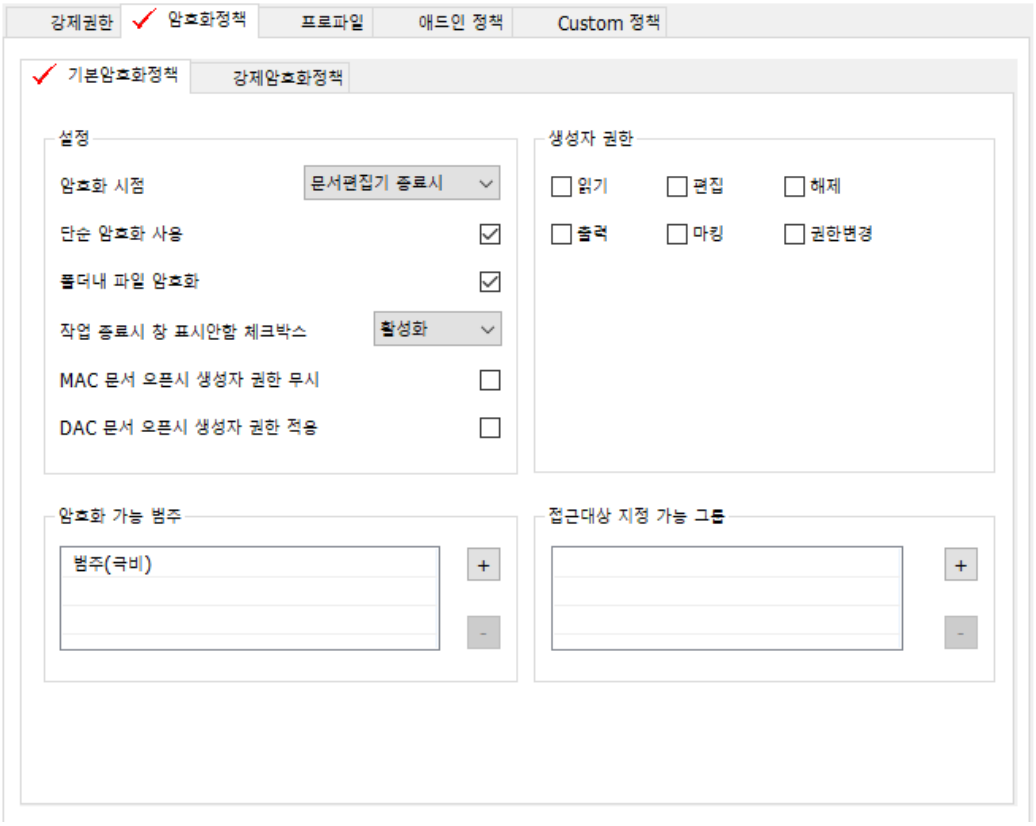
암호화 가능 범주

사용자의 범주 보안문서 생성 시 선택 가능한 범주 목록을 지정 할 수 있습니다.

1) **[+]**를 클릭하면 아래와 같은 창이 출력됩니다. 범주 정책을 선택하고 **[확인]**을 클릭합니다.



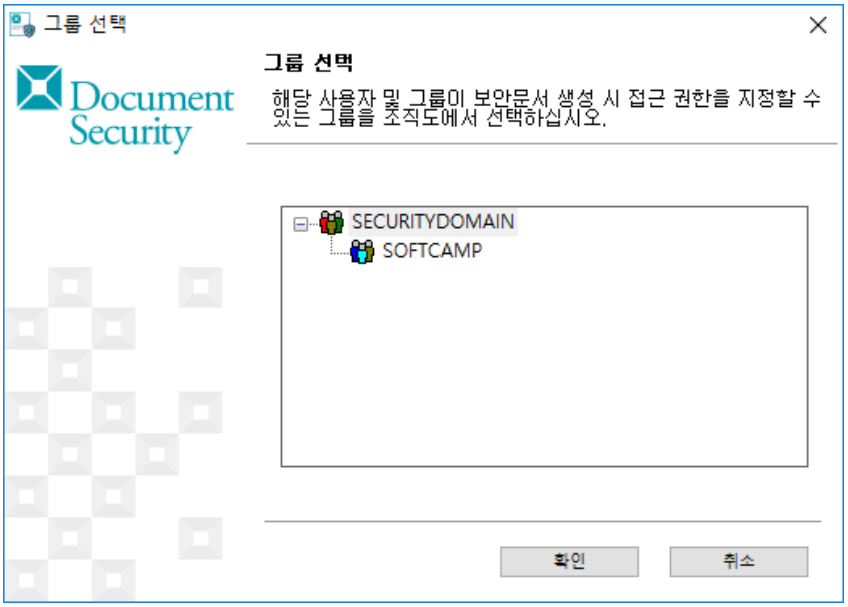
2) 아래와 같이 암호화 가능 범주에 추가됩니다. 이미 추가한 범주를 삭제하려면 삭제하고자 하는 범주를 선택하고 **[-]**를 클릭합니다.



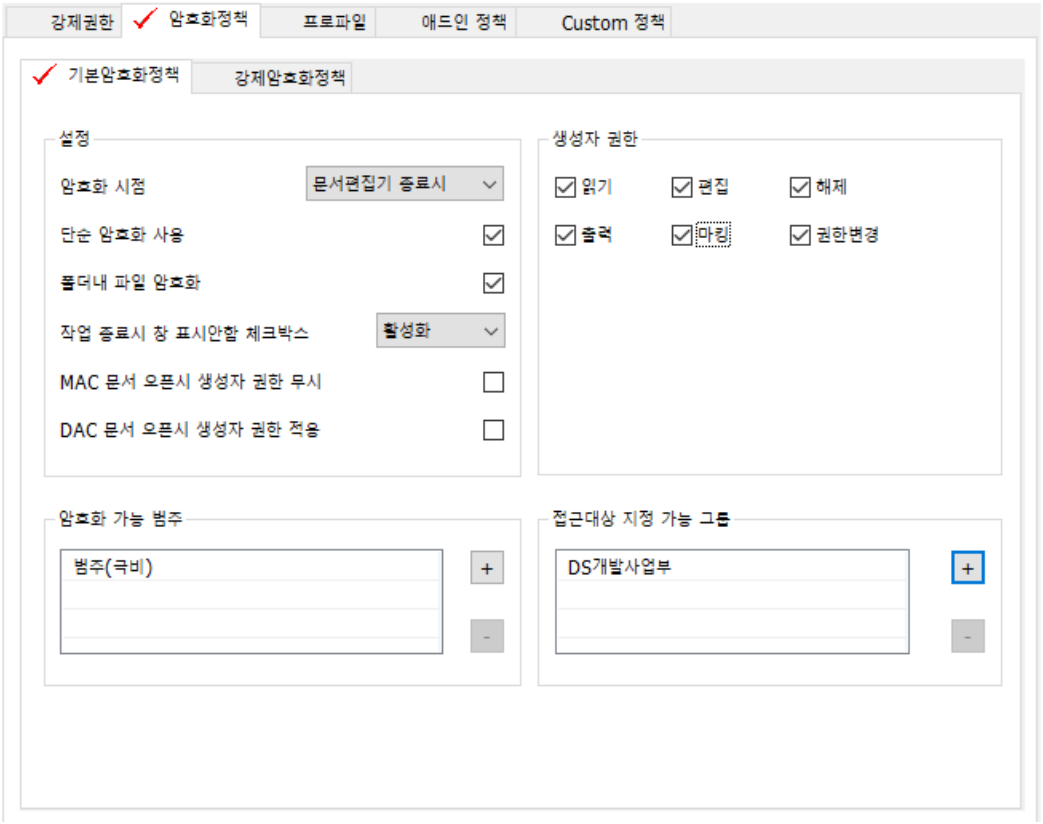
접근대상 지정 가능 그룹

사용자가 보안문서 생성시 접근권한을 지정할 수 있도록 조직의 범위를 설정할 수 있습니다.

1) **[+]**를 클릭하면 아래와 같이 조직도가 출력됩니다. 조직도에서 접근 대상 지정 가능 그룹을 선택하고 **[확인]**을 클릭합니다.



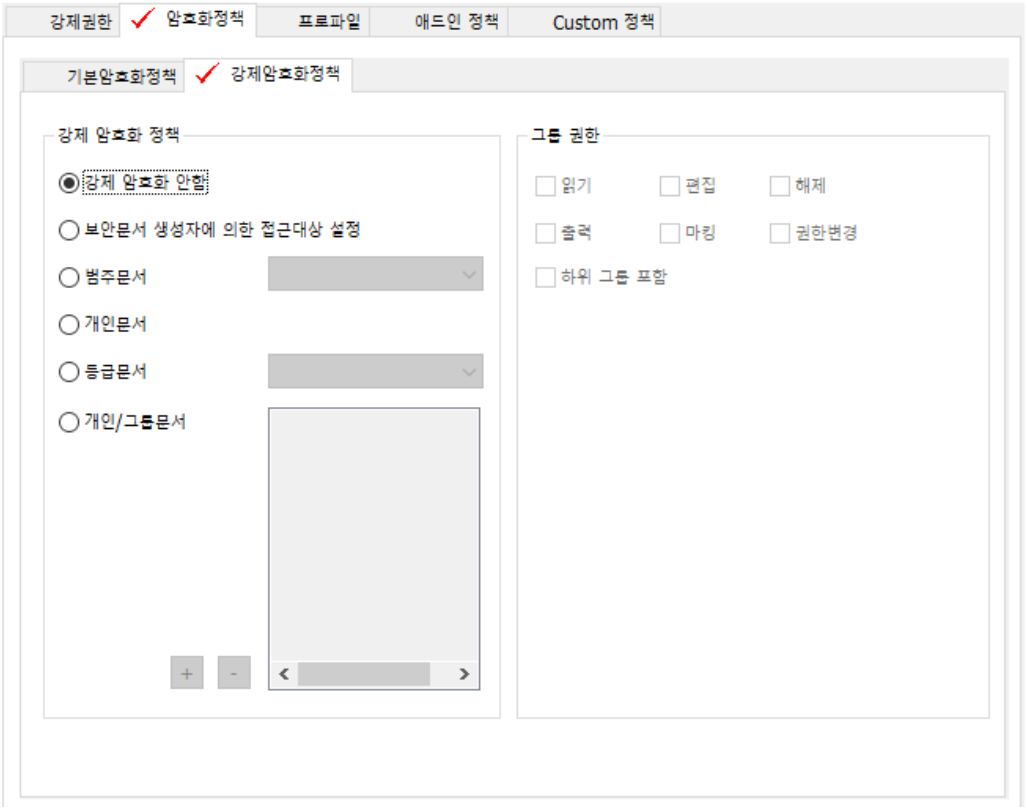
2) 아래와 같이 접근 대상을 지정할 수 있는 그룹이 추가됩니다. 접근 대상 지정 가능 그룹을 삭제하려면 삭제하고자 하는 그룹을 선택하고 **[-]**를 클릭합니다.



6.3.5. 강제 암호화 정책

본 장은 강제 암호화 정책에 대해 설명합니다. '**강제 암호화**'은 사용자가 문서를 생성 시에 사용자에게 암호화 여부를 묻지 않고, 문서 저장이나 종료 시 강제로 암호화하는 것을 의미합니다. 강제 암호화 정책에서는 강제 암호화 시 어떤 정책으로 암호화할 지 설정하고, 강제 암호화 예외 프로세스를 설정합니다.

1) 조직도에서 '**강제 암호화 정책**'을 설정할 사용자 또는 그룹을 선택하고 우측의 작업창의 탭 메뉴에서 '**암호화정책>강제암호화정책**'을 선택합니다. 화면 구성은 아래와 같습니다.

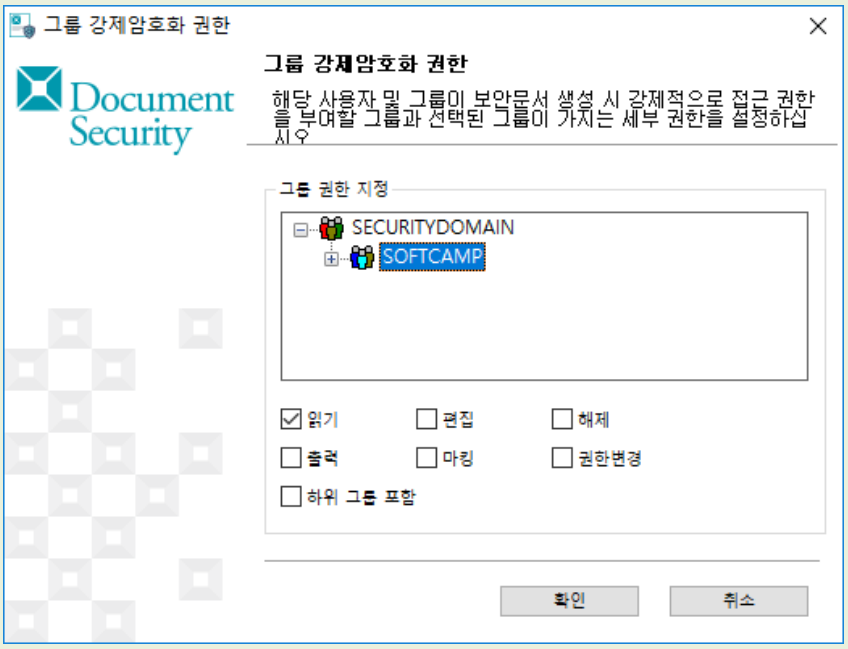


구분		내용
강제 암호화 정책	**강제 암호화 안함**	사용자가 생성한 문서에 대해 강제로 암호화하지 않습니다. 문서 생성 시 암호화 여부를 묻게되며, 사용자가 암호화 방식을 선택하거나, 암호화하지 않을 수 있습니다.
	보안문서 생성자에 의한 접근 대상 설정	사용자가 문서 생성 시 생성자가 접근대상을 설정하여 암호화하도록 강제됩니다.
	범주문서	사용자가 문서 생성 시 관리자가 선택한 범주가 접근할 수 있는 범주 보안문서로 암호화됩니다. 범주 보안문서로 강제 암호화하도록 하려면 '**범주문서**'를 선택하고, 풀다운 메뉴에서 범주를 선택합니다.

	개인문서	사용자가 문서 생성 시 다른 사용자가 접근할 수 없는 개인 보안문서로 암호화되고. 생성자는 **'기본암호화정책'**에서 설정된 생성자 권한에 따라 자신이 생성한 문서를 사용할 수 있습니다.
	등급문서	문서 생성 시 관리자가 선택한 등급이 접근할 수 있는 등급 보안문서로 암호화됩니다. 풀다운 메뉴에서 **'사용자 지정'**을 선택하면 사용자가 등급 보안문서 생성 시 접근 가능 등급을 선택할 수 있습니다.
	개인/그룹문서	문서 생성 시 관리자가 설정한 접근 가능한 대상과 접근 권한을 가지는 보안문서로 암호화됩니다.
그룹 권한		강제 암호화 정책에서 개인/그룹문서를 선택했을 경우에 활성화됩니다. 사용 방법은 아래의 **'참고: 개인/그룹문서 설정법'**을 참고하시기 바랍니다.

참고: 개인/그룹문서 설정법

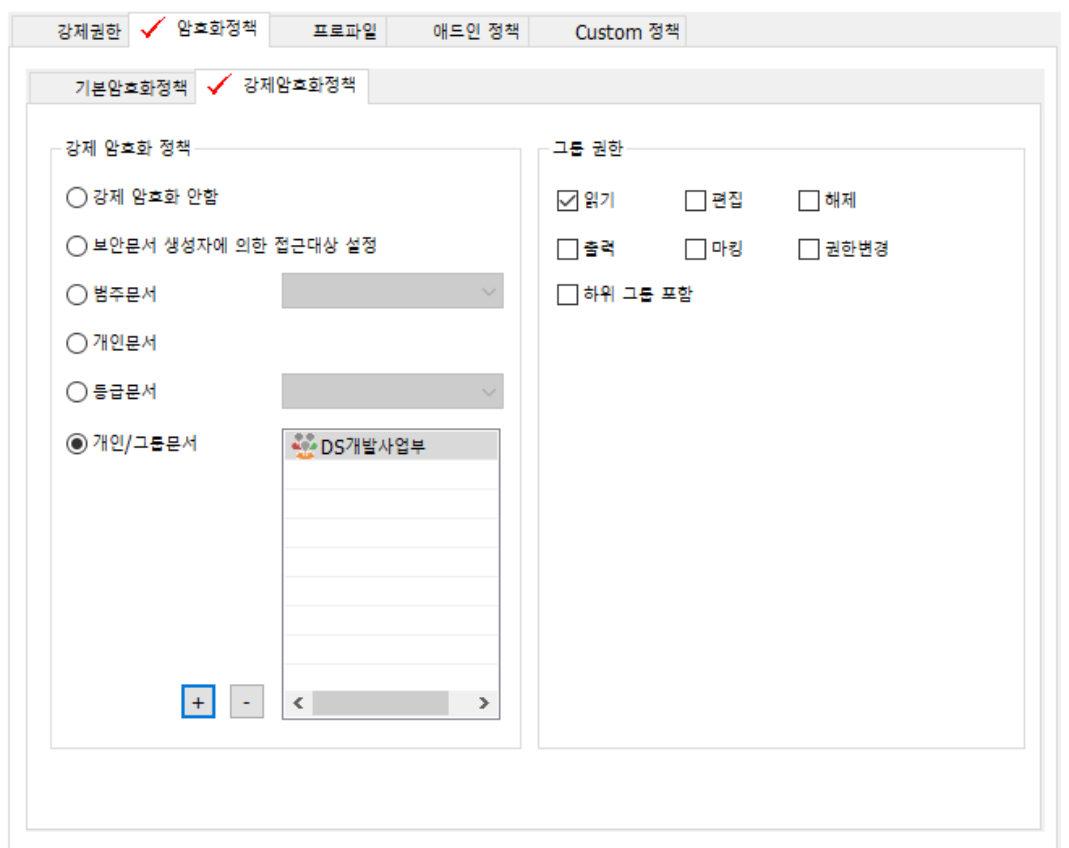
1) 개인/그룹문서를 선택하고 아래의 [+]를 클릭하면 아래와 같은 창이 표시됩니다.



2) 조직도에서 접근 대상이 될 사용자 또는 그룹을 선택하고 읽기, 편집, 해제, 반출, 출력, 마킹, 권한변경 등의 세부 권한을 설정합니다. 하위 그룹 포함을 체크하면 선택한 그룹의 하위에 속한 사용자 및 그룹 또한 동일한 권한을 가집니다.

3) [확인]을 클릭하며 권한 설정을 마칩니다.

4) 아래와 같이 리스트표에 선택한 대상이 추가된 것을 확인할 수 있습니다.



5) 설정한 권한을 수정하려면 대상을 리스트표에서 선택하고 우측의 그룹 권한을 추가한 것과 동일한 방법으로 권한을 재설정합니다. 접근 대상을 삭제하려면 삭제하려는 대상을 선택하고 [-]를 클릭합니다.

참고: 암호키 생성 알고리즘과 암호키 등에 대한 설정

문서 암호화를 위한 DEK 는 검증필 암호 모듈인 XecureCrypto 2.0.1.1 의 난수발생기를 이용하여 암호키를 생성하며, 별도로 인가된 관리자가 암호키 생성 및 암호화 알고리즘과 관련하여 설정하는 UI 및 환경설정 파일은 제공하지 않습니다.

본 TOE 는 안전한 암호알고리즘 사용에 대한 규칙을 준수하고 있습니다.

참고: 암호키 분배

TOE 의 암호키는 안전하게 암호화된 통신 구간을 통해 Server 에서 TOE 의 각 구성요송인 Client, Console 로 전달됩니다. TOE 는 RSAES-OAEP 를 이용하여 암호키를 분배합니다.

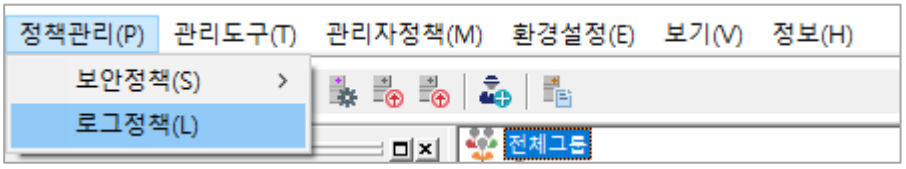
참고: 암호키 파기

TOE 는 인가된 관리자에 의한 정책 삭제, 사용자 및 그룹 삭제, 암호화 문서의 복호화 시 이루어집니다. 삭제된 암호키는 다시 복원할 수 없으며 재활용 할 수 없습니다.

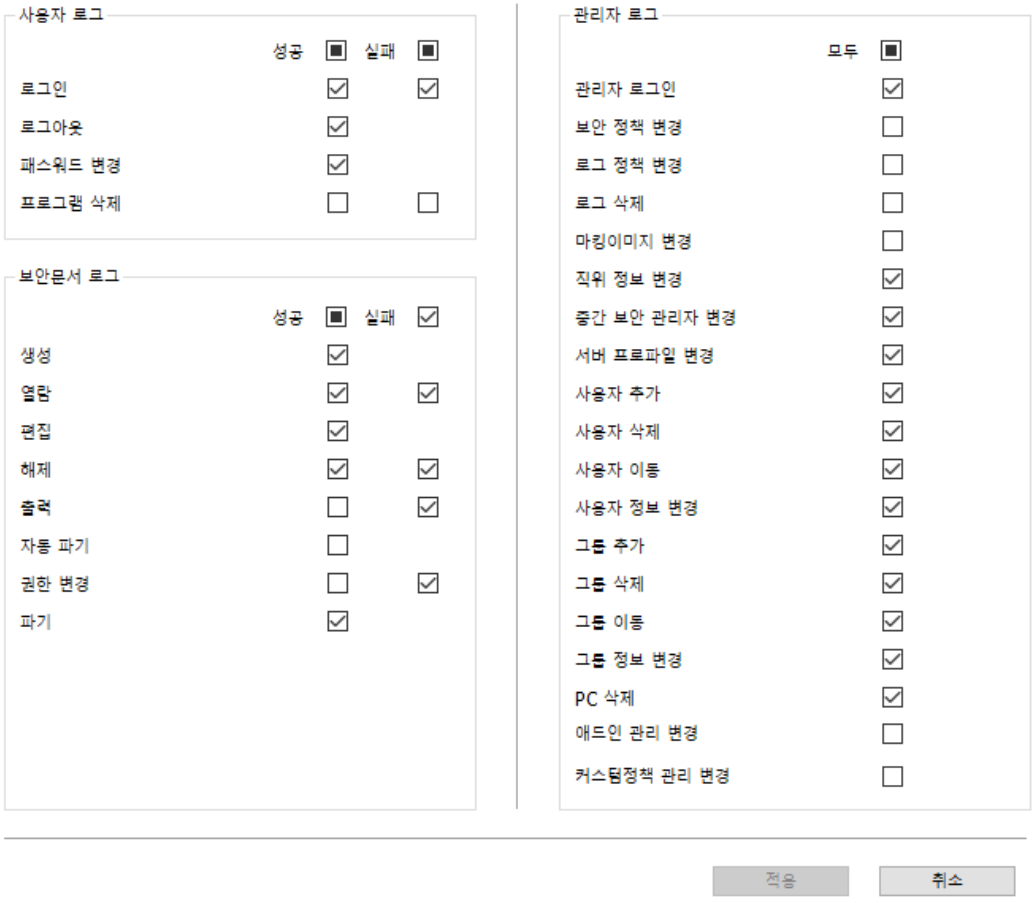
6.4. 로그정책

로그 정책 설정에서는 관리자가 확인하고 싶은 로그의 항목을 설정할 수 있습니다. 관리자는 사용자 및 관리자가 실시하는 동작에 대한 다음의 로그 항목을 설정할 수 있습니다.

1) **'로그 정책'**를 설정하기 위해 Console 상단 매뉴의 **'정책관리>로그정책',** 또는 ( ) 아이콘을 누릅니다.



2) 작업창에 다음과 같이 **'사용자 로그'**, **'관리자 로그'**, **'보안문서 로그'**의 설정 화면이 표시됩니다. 관리자는 다음의 작업에 대한 로그를 남길 것인지 아닌지를 설정할 수 있습니다.



주의 : 사용자 로그, 보안문서 로그, 관리자 로그의 각 감사로그들은 모두 기록되는 것이 기본 설정으로 제공됩니다.

주의 : 감사로그 저장소가 포화상태가 되면 가장 오래된 데이터부터 삭제하여 신규 감사로그를 기록합니다. 감사로그 저장소의 용량이 포화되어 중요한 감사로그가 삭제되지 않도록 관리 상의

주의가 필요합니다. 감사 저장소 포화상태에 대한 임계치는 변경할 수 없으며 기본 값으로 제공됩니다.

- 감사 저장소 포화상태 임계치 : 95 %

참고: 사용자 로그에서 [성공]에 체크를 넣었을 경우에는, 관련 항목에 대한 작업을 성공했을 때의 로그를 남깁니다. [실패]에 체크를 넣었을 경우에는, 관련 항목에 대한 작업을 실패했을 때의 로그를 남깁니다.

구분		내용
사용자 로그	로그인	사용자의 로그인 정보를 기록합니다.
	로그아웃	사용자의 로그아웃 정보를 기록합니다
	비밀번호 변경	사용자의 비밀번호 변경 정보를 기록합니다.
	프로그램 삭제	사용자가 Client 를 삭제한 정보를 기록합니다.
관리자 로그	관리자 로그인	최고 보안 관리자 및 보안 관리자가 Console 에 로그인 했을해의 기록을 남깁니다.
	보안 정책 변경	최고 보안 관리자 및 보안 관리자가 각각의 정책을 변경할 시 기록을 남깁니다.
	로그 정책 변경	
	로그 삭제	
	마킹이미지 변경	
	직위 정보 변경	
	중간 보안 관리자 변경	
	서버 프로파일 변경	
	사용자 추가	
	사용자 삭제	

	사용자 이동	
	사용자 정보 변경	
	그룹 추가	
	그룹 삭제	
	그룹 이동	
	그룹 정보 변경	
	PC 삭제	
	애드린 관리 변경	
	커스텀정책 관리 변경	
보안문서 로그	**생성**	사용자가 보안문서에 대한 각각의 행위 시 기록을 남깁니다.
	열람	
	편집	
	해제	
	출력	
	자동 파기	보안문서가 자동으로 파기된 기록을 남깁니다.
	권한 변경	사용자의 보안문서의 권한을 변경했을 때 기록을 남깁니다.
	파기	보안문서의 파기됐을 때 기록을 남깁니다.

7. 관리도구

본 장에서는 관리도구에서 제공하는 메뉴에 대해서 설명합니다.

관련링크

a. 로그관리

b. 마킹 이미지 관리

c. 직위 관리

d. 연동 시스템 관리

e. 애드인 관리

7.1. 로그 관리

로그 란

'로그'란 사용자 및 관리자에 대한 TOE **사용 기록**을 말합니다. 로그는 **'사용자 로그', '관리자 로그', '보안문서 로그'**의 3 가지로 구성됩니다. 로그는 **'로그정책'**을 통해 선택적인 기록의 관리가 가능합니다.

'로그관리'에서는 로그의 **'조회'** 가 가능합니다. 관리자는 **'로그정책'**에서 설정된 **'사용자 로그'**와 **'관리자 로그'**, 그리고 **'보안문서 로그'**를 각각의 로그종류 및 검색 기간, 작업자, 소속 등에 따라 조회, 별도 저장 등의 관리가 가능합니다.

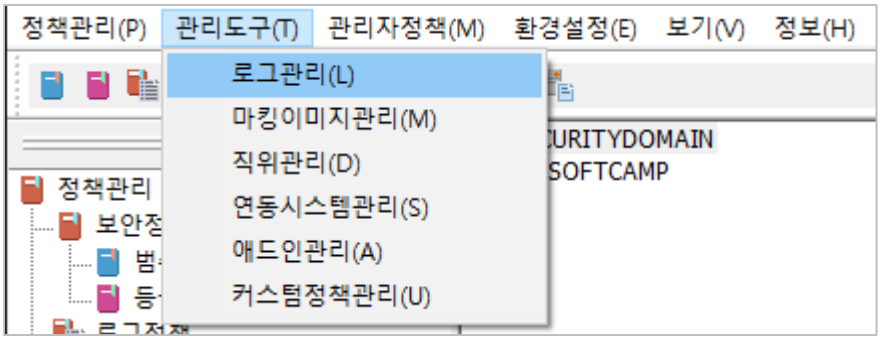
이러한 **'로그정책'** 을 통하여 관리자는 사용자의 Client 사용에 대한 모든 로그에 대한 기록을 조회할 수 있습니다.

관리자는 TOE 를 사용하는 것에 대한 각종 로그 ('**정책관리>로그정책**'로 설정한 내용에 관한 로그)를 조회할 수 있습니다. 조직도에서 선택된 각각의 사용자 또는 그룹에 대한 변경사항을 사용자, 관리자, 보안문서로 각각 구분하여 조회가 가능합니다. 본 TOE 에서 기록하는 감사대상 사건은 보안목표명세된 감사대상 사건과 동일하며, 다음 표와 같습니다.

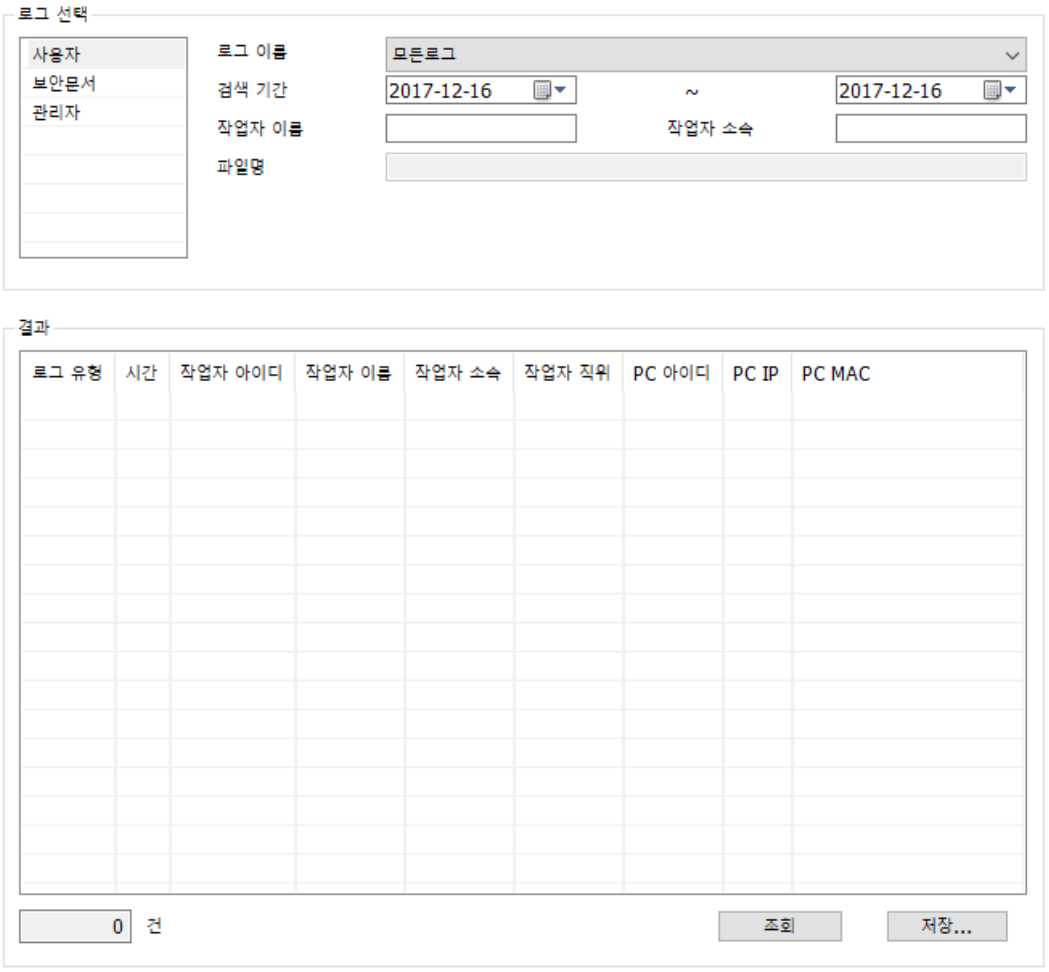
보안기능 컴포넌트	감사대상 사건	추가적인 감사기록 내용
FAU_ARP.1	잠재적인 보안 위반으로 인하여 취해지는 대응행동	
FAU_SAA.1	분석 메커니즘의 동작개시와 동작정지, 도구에 의한 자동대응	
FAU_STG.3	임계치를 초과했을 경우의 대응행동	
FAU_STG.4	감사 저장이 실패했을 경우의 대응행동	
FCS_CKM.1(2)	행동의 성공과 실패	
FCS_CKM.2	행동의 성공과 실패 (문서 암·복호화와 관련된 키 분배에만 적용)	
FCS_CKM.4	행동의 성공과 실패 (문서 암·복호화와 관련된 키 파기에만 적용)	
FCS_COP.1	암호 연산의 성공과 실패, 암호 연산의 유형	
FDP_ACF.1	SFP에 의해서 다루어지는 객체에 대한 오퍼레이션 수행 의 성공적인 요청	객체의 식별 정보
FIA_AFL.1	실패한 인증 시도의 한계치 도달과 취해진 대응행동, 적절하다면 이어서 일어나는 정상 상태로의 회복	
FIA_IMA.1(확장)	상호인증의 성공/실패	
FIA_UAU.1	인증 메커니즘의 모든 사용	
FIA_UAU.4	인증데이터의 재사용 시도	
FIA_UID.1	제공된 사용자 신원을 포함하여 사용자 식별 메커니즘의 모든 사용	
FMT_MOF.1	TSF 기능에 대한 모든 변경	
FMT_MSA.1	보안속성 값 대한 모든 변경	
FMT_MSA.3	허가 규칙이나 제한 규칙의 기본 설정에 대한 변경, 보안속성의 초기값에 대한 모든 변경	
FMT_MTD.1	TSF 데이터 값에 대한 모든 변경	변경된 TSF 데이터 값
FMT_PWD.1(확	비밀번호에 대한 모든 변경	

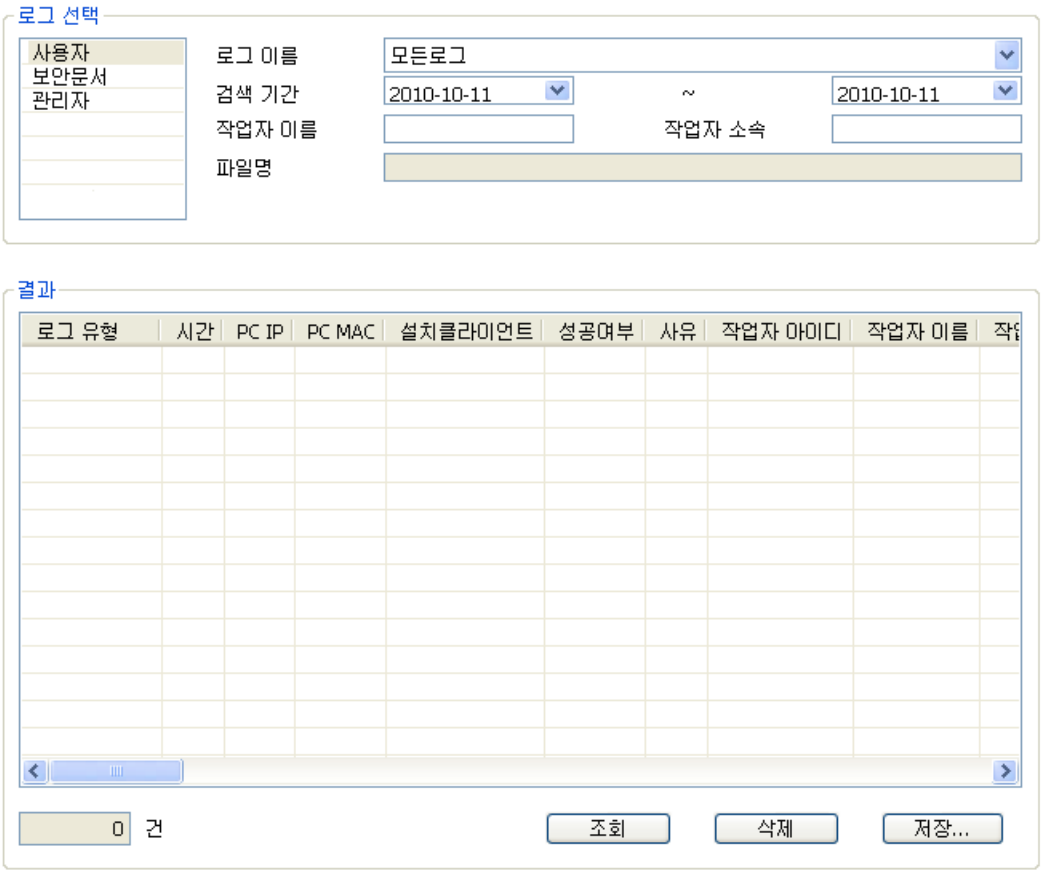
장)		
FMT_SMF.1	관리기능 사용	
FMT_SMR.1	역할을 분담하는 사용자 그룹에 대한 변경	
FPT_TST.1	TSF 자체 시험의 실행과 시험 결과	무결성 위반 시 변경된 TSF 데이터 혹은 실행코드
FTA_MCS.2	동시 세션 수의 제한에 기반한 새로운 세션 거부	
FTA_SSL.5(확장)	상호작용 세션의 잠금 또는 종료	
FTA_TSE.1	세션 설정 메커니즘으로 인한 세션 설정 거부, 사용자 세션을 설정하려는 모든 시도	

1) 조직도에서 **'로그 조회'**를 하기 위해 해당 사용자 또는 그룹을 선택한 뒤 Console 상단 매뉴의 **'관리도구>로그관리'**를 선택, 또는 ( ) 아이콘을 클릭합니다.



2) 다음과 같이 작업창에 **<로그조회>** 창이 나타납니다.


로그 선택
사용자
보안문서
관리자
로그 이름
모든로그
검색 기간
2017-12-16
~
2017-12-16
작업자 이름
작업자 소속
파일명
결과
로그 유형
시간
작업자 아이디
작업자 이름
작업자 소속
작업자 직위
PC 아이디
PC IP
PC MAC
0
건
조회
저장...



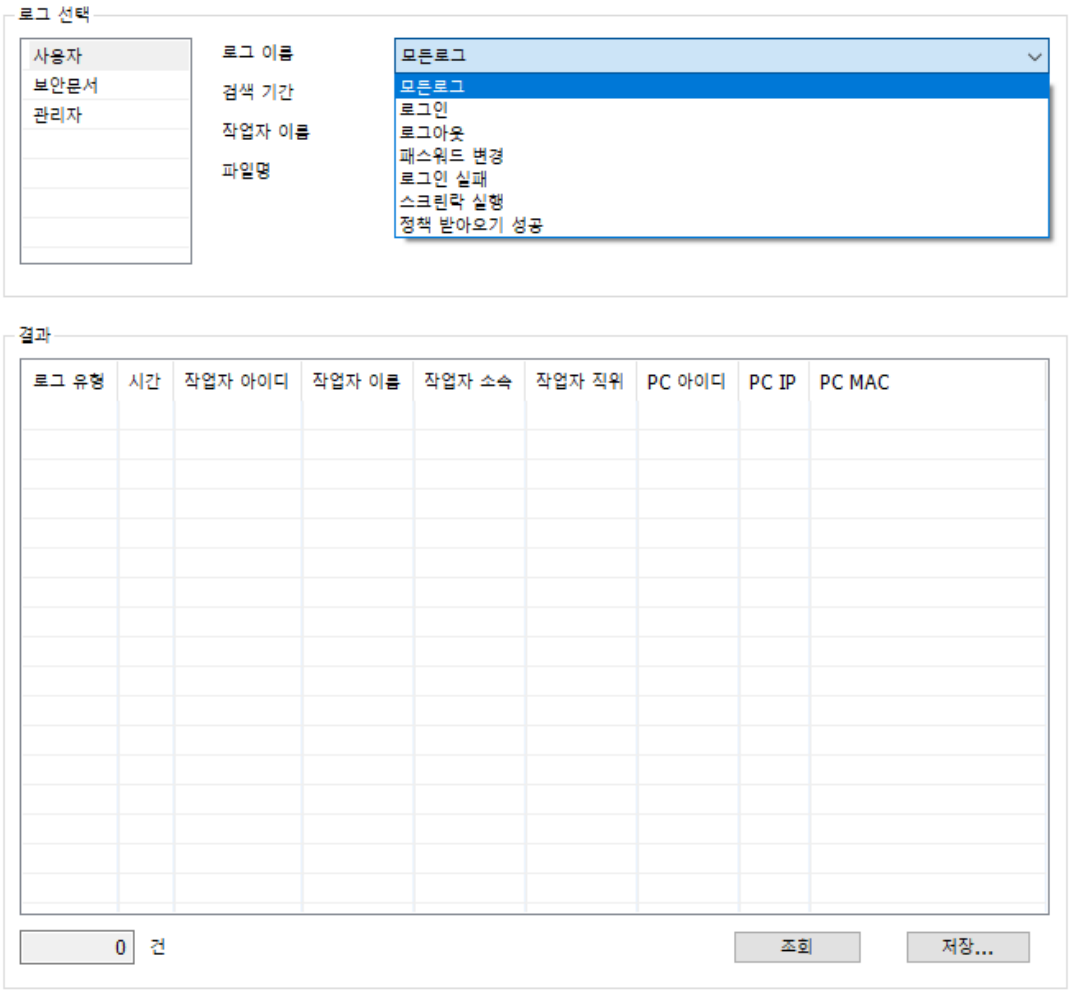
3) 작업 창의 **'로그선택 '**매뉴에서 검색할 항목을 선택합니다. 선택되는 로그 검색 항목에 따라 그에 해당되는 **'로그 이름'**의 항목이 나타나게 됩니다.

a. **사용자** : 사용자 관련 로그의 조회를 실시할 때에 선택합니다.

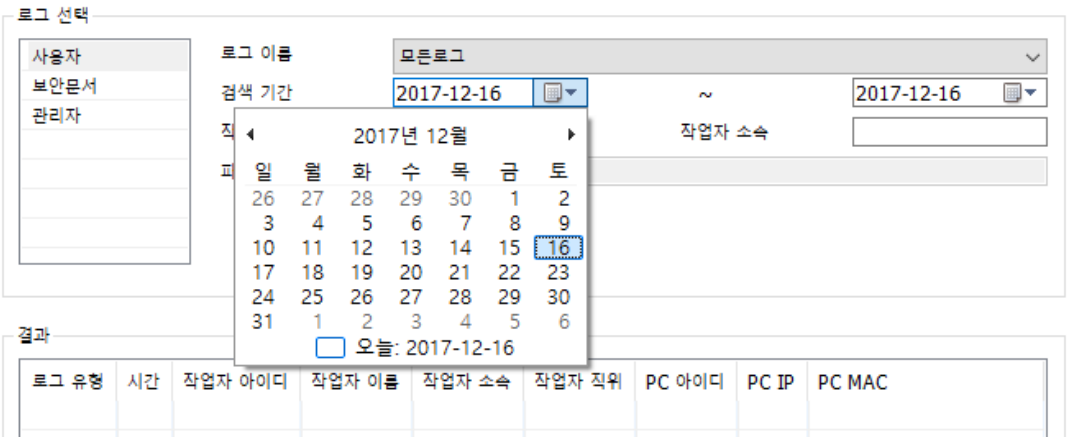
b. **관리자** : 관리자 관련 로그의 조회를 실시할 때에 선택합니다.

c. **보안문서** : 보안문서 관련 로그의 조회를 실시할 때에 선택합니다.

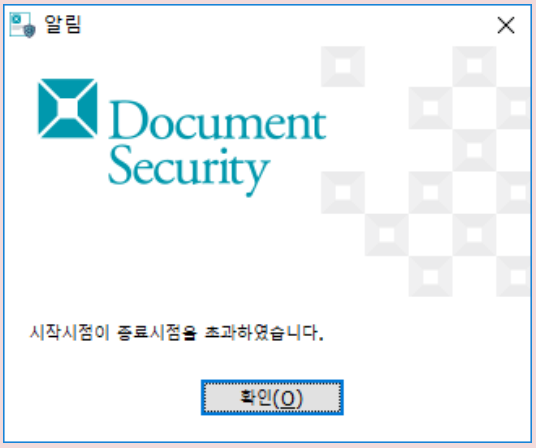
4) **'로그 이름'**의 드롭 다운 매뉴로부터 조회 대상 로그를 선택합니다. 모든 로그를 선택하면 조회 대상에 관한 모든 로그를 조회할 수 있습니다.



5) 로그명을 선택한 후 **'검색 기간'**을 설정합니다.

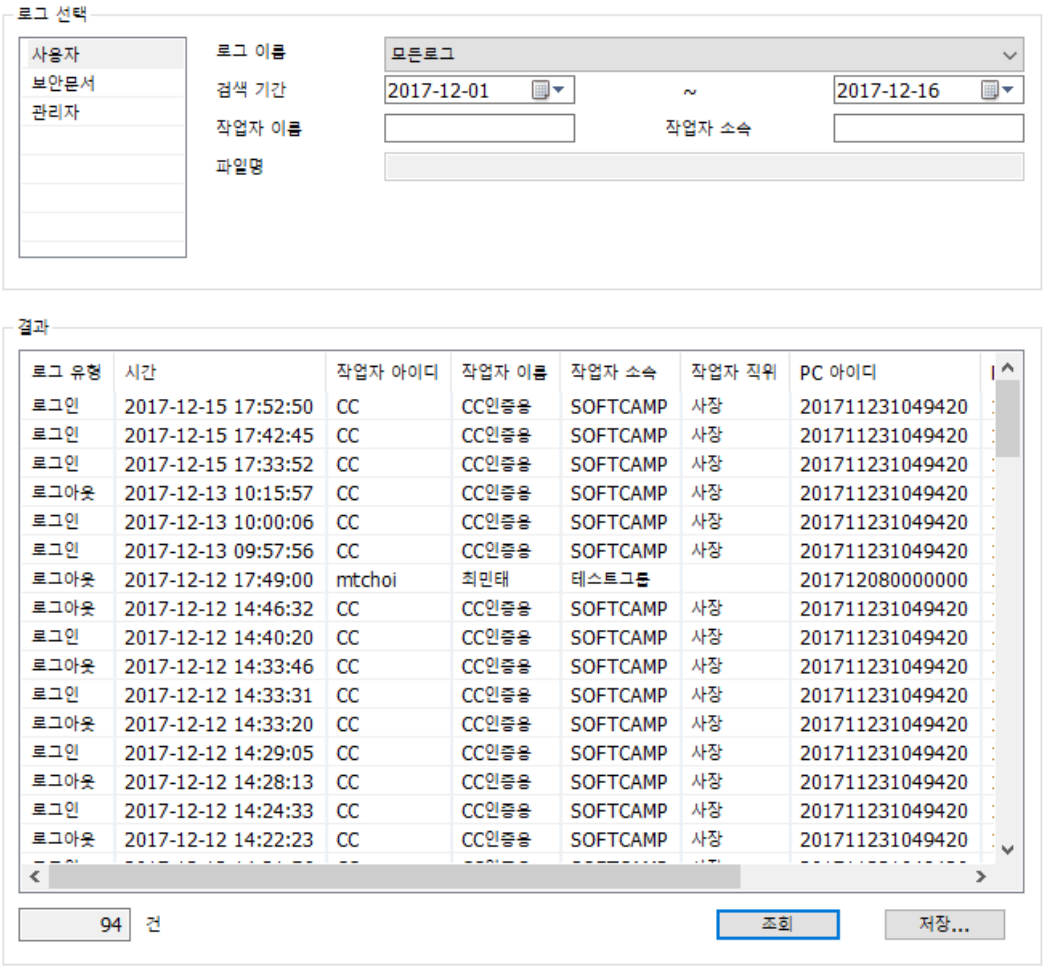


주의: 검색 기간을 선택할 때에, 검색 종료일이 검색 개시일부터 전날 첨부로 설정하고 로그 조회를 할 경우에는, 다음과 같은 메세지가 표시됩니다. 이러한 경우, 검색 기간을 다시 올바르게 입력해 주세요.



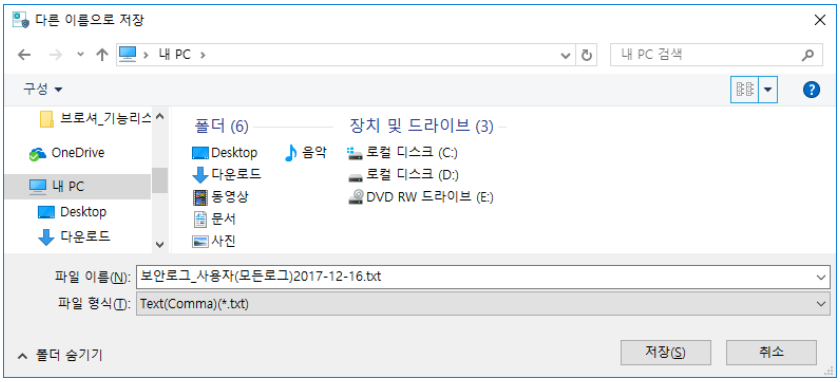
6) **'작업자 이름', '작업자 소속'** 등 상세 검색 조건을 입력합니다. **'파일명'**은 로그 조회의조건이 **'보안문서'**로 설정되었을 시 활성화 됩니다. 이 모든 조건은 필수 입력 조건이 아닙니다. 작업자 이름은 반각 50 자까지, 작업자 소속은 반각 50 자까지 입력가능합니다.

7) 해당 조건의 설정이 모두 완료되면 **[조회]**를 클릭합니다. 다음과 같이 결과 목록을 확인할 수 있습니다.



주의 : '관리자 로그' 검색 시 관리자의 PC 가 내부 네트워크에서 '자동 아이피 할당'이 설정 되었을 경우 'PC MAC' 정보가 정상적으로 나타나지 않을 수 있습니다.

8) 해당 로그는 **[저장]** 버튼을 클릭하여 원하는 위치에 *.TXT 파일의 형태로 저장이 가능합니다.



참고: 로그명의 드롭 다운 매뉴에 표시되는 로그의 타입에 관한 설명입니다.

구분		내용
사용자 로그	로그인	사용자의 로그인 정보를 기록합니다.
	로그아웃	사용자의 로그아웃 정보를 기록합니다
	비밀번호 변경	사용자의 비밀번호 변경 정보를 기록합니다.
	프로그램 삭제	사용자가 Client 를 삭제한 정보를 기록합니다.
	업그레이드	사용자의 업그레이드 정보를 기록합니다.
관리자 로그	관리자 로그인	최고 보안 관리자 및 보안 관리자가 Console 에 로그인 했을해의 기록을 남깁니다.
	로그 정책 변경	최고 보안 관리자 및 보안 관리자가 각각의 정책을 변경할 시 기록을 남깁니다.
	감사 정책 변경	
	로그 삭제	
	업그레이드 관리	
	마킹이미지 변경	
	직위 정보 변경	

	서버 프로파일 변경	
	사용자 추가	
	사용자 삭제	
	사용자 이동	
	사용자 정보 변경	
	그룹 추가	
	그룹 삭제	
	그룹 이동	
	그룹 정보 변경	
	PC 삭제	
	PC 정보변경	
보안문서 로그	**생성**	사용자가 보안문서에 대한 각각의 행위 시 기록을 남깁니다.
	열람	
	편집	
	해제	
	출력	
	반출 (보안문서)	사용자가 보안문서의 외부 전송 파일을 생성했을 때 기록을 남깁니다.
	반출 (일반문서)	사용자가 일반문서의 외부 전송 파일을 생성했을 때 기록을 남깁니다.
	자동 파기	보안문서가 자동으로 파기된 기록을 남깁니다.
	권한 변경	사용자의 보안문서의 권한을 변경했을 때 기록을 남깁니다.
	삭제	보안문서가 삭제됐을 때 기록을 남깁니다.

	파기	보안문서의 파기됐을 때 기록을 남깁니다.
	암호화 취소	문서 편집 어플리케이션 종료 시 사용자가 문서를 암호화하지 않았을 때 기록을 남깁니다.

7.2. 마킹 이미지 관리

관리자는 보안문서 또는 일반문서를 출력할 때에 삽입되는 마킹이미지를 추가, 편집 및 삭제할 수 있습니다. 프린트 마킹 시 삽입될 수 있는 이미지들을 전체적으로 관리하는 것으로, 실질적인 사용은 개인/그룹별 마킹 설정에서 사용자 및 그룹별로 적용할 수 있습니다.

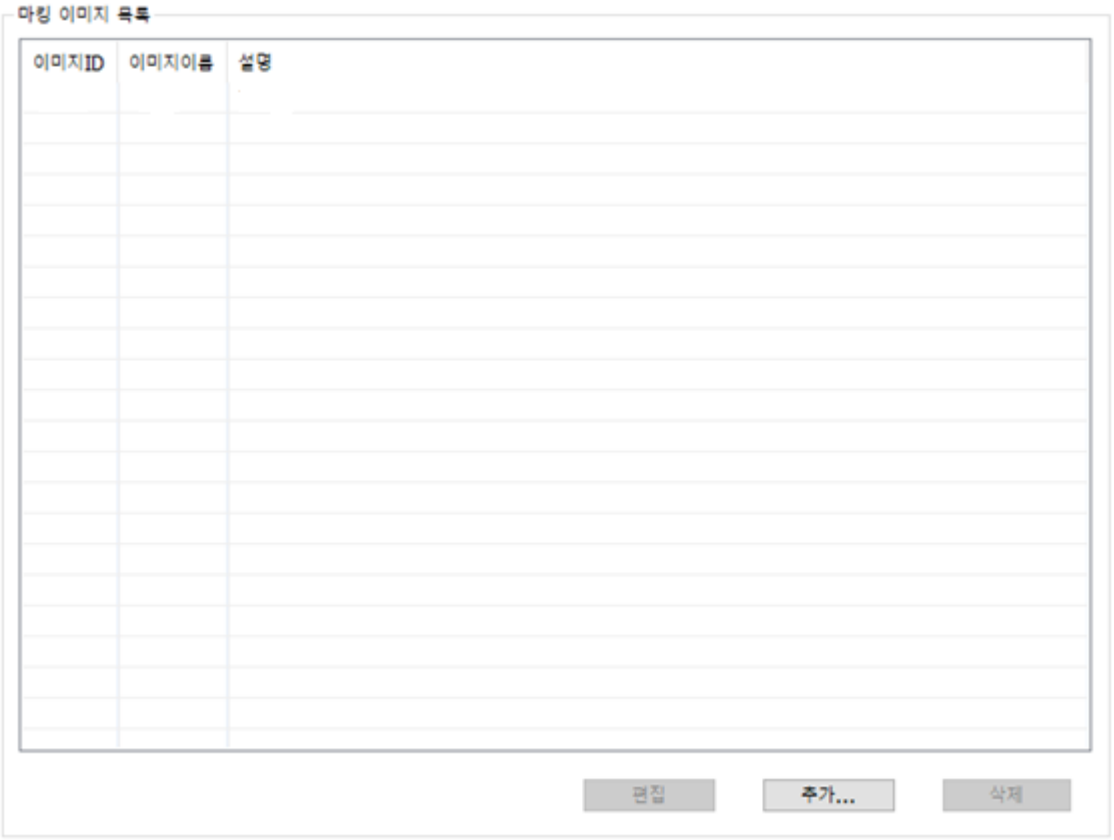
마킹 이미지 관리 시 주의사항

1) 마킹 이미지가 등록되어 있지 않으면, 개인/그룹별 마킹 설정에서 사용자 및 그룹의 출력물에 삽입할 이미지를 설정할 수 없습니다.
2) 마킹 이미지는 반드시 bmp 확장자 파일이어야 하며, 흑백이어야 합니다.
3) 마킹 이미지의 사이즈는 반드시 정사각형이어야 하며, 800 X 800(100KB)미만이어야 합니다.

마킹 이미지 관리 방법

1) 마킹 이미지를 관리하기 위해 Console 상단 매뉴의 **'관리도구>마킹이미지관리',** 또는 () 아이콘을 클릭합니다.

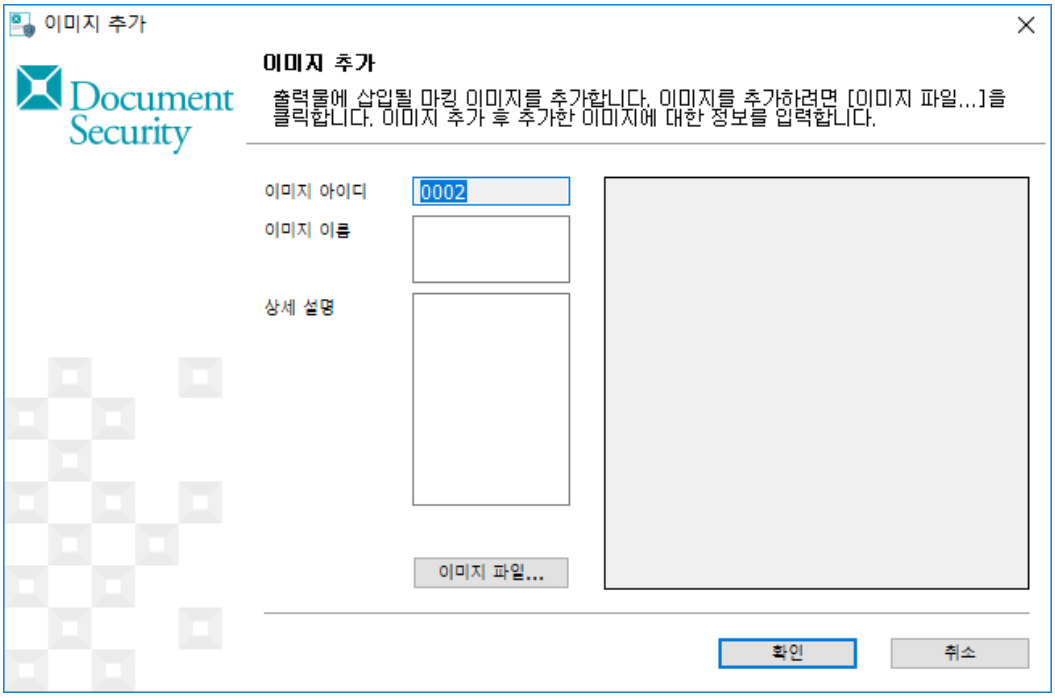
2) 작업 윈도우에 **'마킹 이미지 목록'**이 표시됩니다. 구성은 다음과 같습니다.



구분	내용
마킹 이미지 목록	등록되어 있는 마킹 이미지의 정보(이미지 ID, 이미지이름, 설명)이 나타납니다. 해당 리스트를 더블클릭하여 세부내용을 수정할 수 있습니다.
편집	마킹 이미지 목록에서 선택된 마킹 이미지의 내용을 수정할 수 있습니다.
추가	새로운 마킹 이미지를 등록할 수 있습니다.
삭제	마킹 이미지 목록에서 선택된 마킹 이미지를 삭제합니다. 단, 사용중인 마킹 이미지는 삭제할 수 없습니다.

마킹 이미지 추가

1) 마킹 이미지를 추가하기 위해 작업 윈도우에서 **[추가...]**를 클릭하면 다음과 같이 **<이미지 추가>**창이 나타납니다.



a. **이미지 아이디 :** 추가되는 마킹이미지의 순서에 따라 자동으로 설정되는 순번입니다.

b. **이미지 이름 :** 관리자가 사용할 마킹 이미지 이름을 입력합니다. 이름은 반각 50 자까지 입력가능합니다.

c. **이미지 파일 :** 마킹이미지로 등록될 이미지의 경로를 입력합니다.

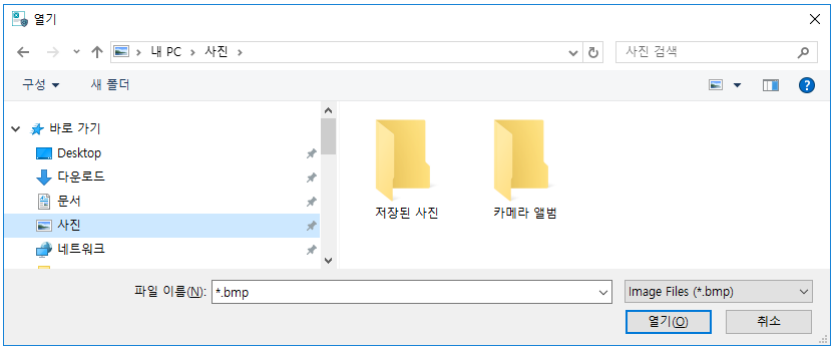
d. **상세 설명 :** 리스트에서 열람할 상세설명을 입력합니다. 설명은 반각 255 자까지 입력가능합니다.

주의 : 마킹 이미지는 반드시 다음의 조건에 부합되어야 합니다.

1. 흑백 비트맵 이미지 파일(흑백의 '*.bmp' 확장자 파일)

2. 최대 사이즈는 800 X 800(100KB) 픽셀의 정사각형

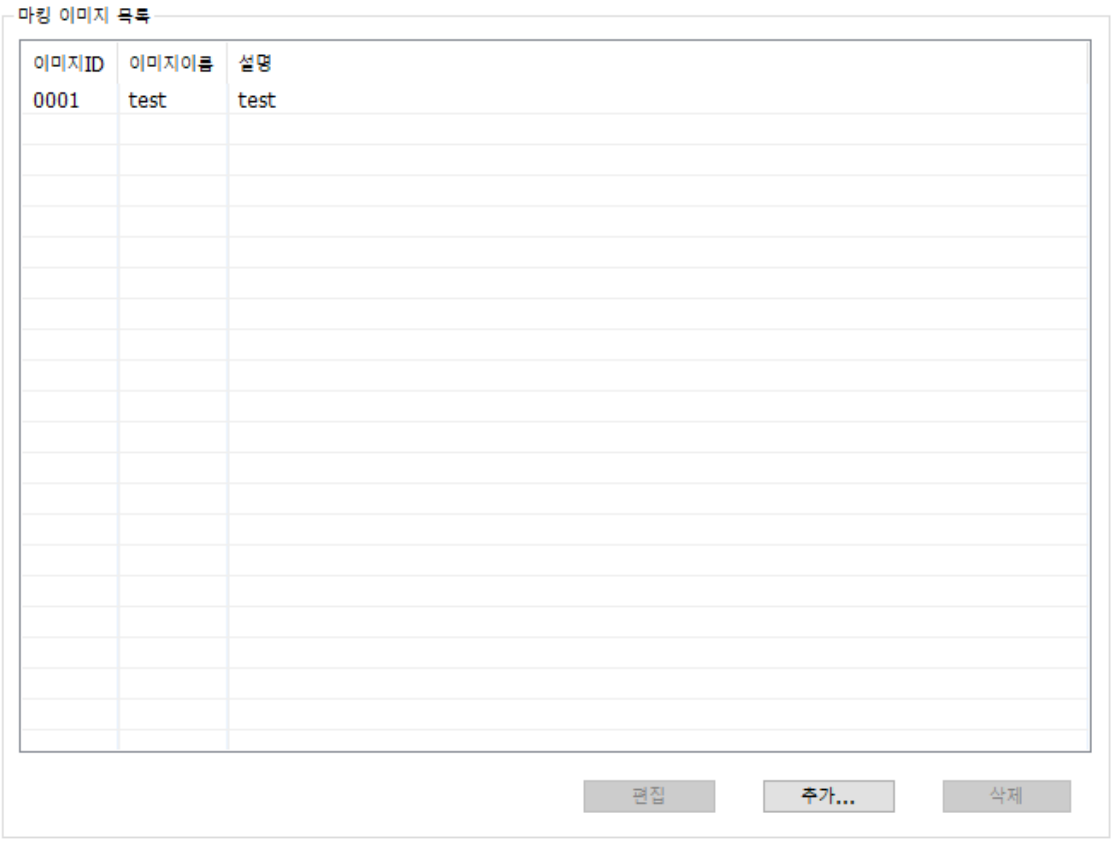
1) **'이미지 이름'**을 입력한 후 이미지 파일을 추가하기 위해 **[이미지 파일...]**를 클릭하면 다음과 같은 창이 나타납니다. 준비한 마킹 이미지를 검색하여 **[열기]**를 클릭합니다.



2) **'이미지 이름'**과 **'상세 설명'**에 설명을 입력 후 등록을 완료하기 위해 **[확인]**을 클릭합니다.

주의 : '이미지 이름'과 '상세설명'은 필수 입력사항입니다.

3) 다음과 같이 리스트에 이미지가 추가되어 있는것을 확인할 수 있습니다.



마킹 이미지 편집 및 삭제

1) '**마킹 이미지 목록**'에서 수정하고자 하는 마킹 이미지를 더블클릭 또는 선택 후 하단의 **[편집]** 버튼을 클릭하면 세부 내용의 수정이 가능합니다.

1) 마킹 이미지를 삭제하고 싶은 경우는 '**마킹 이미지 목록**'에서 삭제하고자 하는 이미지를 선택 후 **[삭제]**를 클릭합니다.

주의 : 해당 이미지가 사용 중인 경우, 아래와 같은 메시지가 출력됩니다. 삭제하려면 [예]를 클릭하고, 취소하려면 [아니오]를 클릭합니다.

7.3. 직위 관리

본 장은 직위 관리에 대해 설명합니다. 관리자는 사용자 추가 시 설정할 직위를 추가, 수정 및 삭제할 수 있습니다.

직위 관리 시 주의 사항

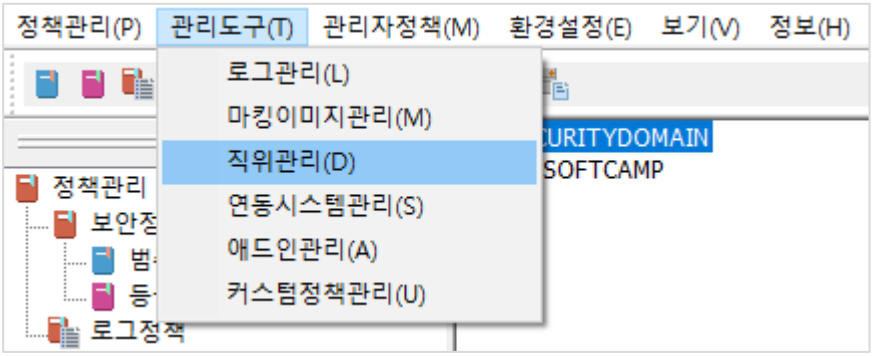
1) 기본적으로 제공하는 직위는 제거할 수 없습니다.

2) 직위를 등록할 때, 생성되는 직위의 ID 번호는 변경할 수 없습니다.

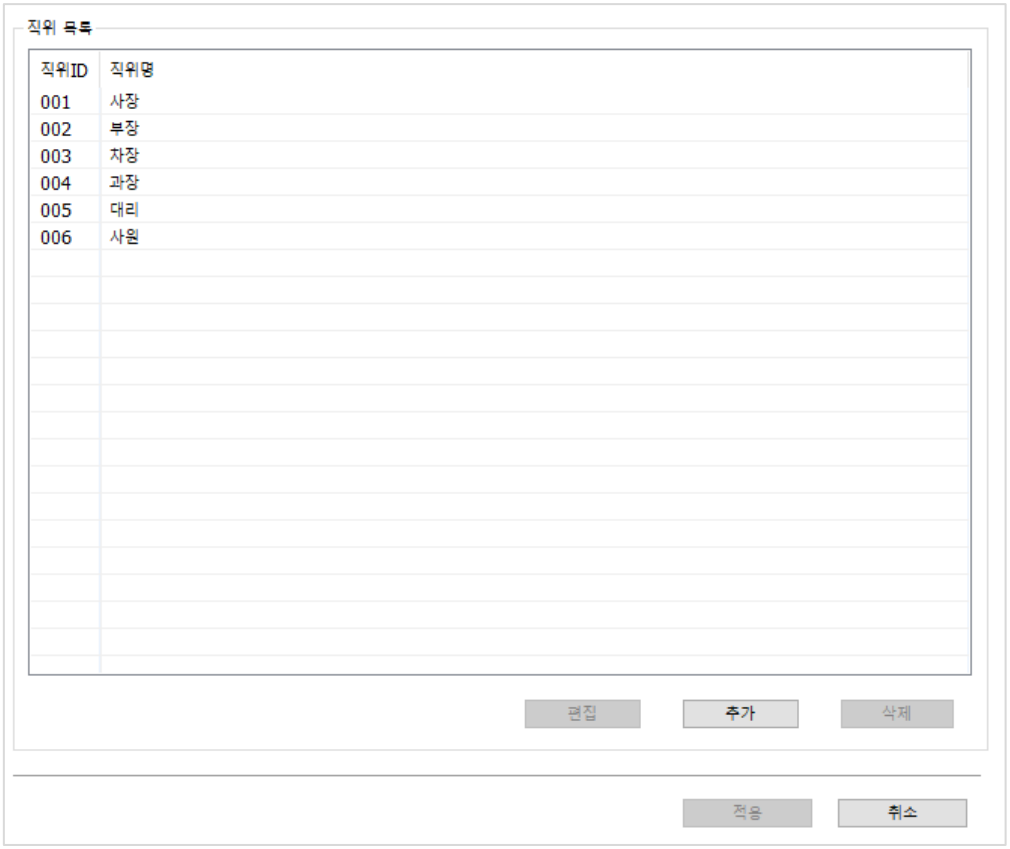
3) 사용자의 직위와 보안정책 및 권한은 연관 관계가 없습니다.

직위 관리 방법

1) 다음과 같이 Console 상단 매뉴에서 **'관리도구>직위 관리'**, 또는 () 아이콘을 클릭합니다.

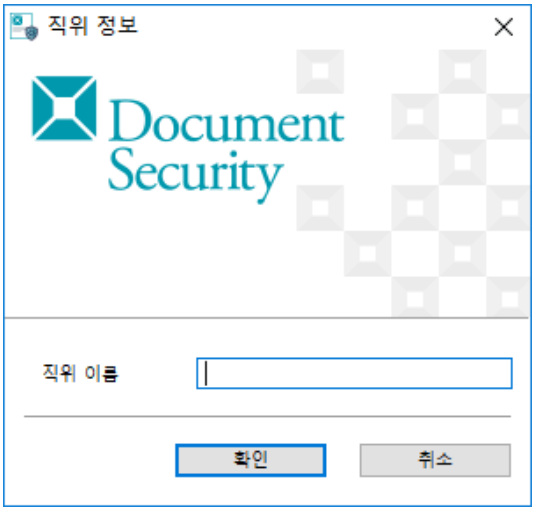


2) 작업 윈도우에 **'직위 목록'** 리스트가 표시됩니다.



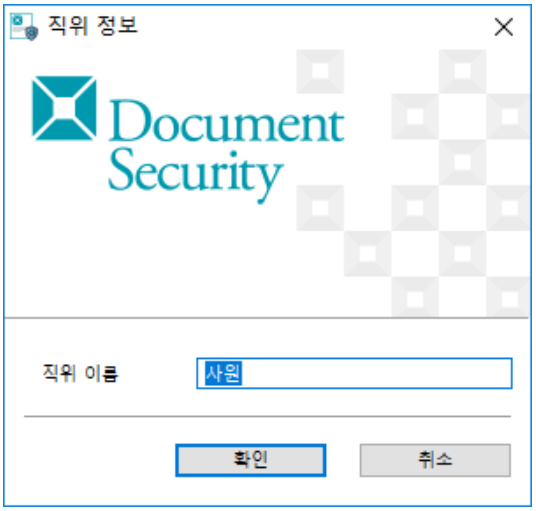
직위 이름 등록

1) 작업 윈도우에서 **[추가]**를 클릭하면 다음과 같은 **<DS 직위 정보>**창이 표시됩니다. **'직위 이름'**에 직위를 입력하고 **[확인]**를 클릭합니다. 직위명은 반각 50 문자까지 입력할 수 있습니다.



직위 목록 편집

1) 직위를 편집하는 경우는 '**직위 목록**' 리스트에서 편집 대상을 선택한 후 작업 윈도우 화면 아래에 있는 **[편집]**을 클릭합니다. 다음과 같이 **<직위 정보>**창이 나타나면 해당 직위 이름을 변경 후 **[확인]**을 클릭하여 수정을 완료합니다.



직위 목록 삭제

1) 직위를 삭제하는 경우는 **'직위 목록'** 리스트에서 삭제 대상을 선택하고 작업 윈도우 화면 아래에 있는 **[삭제]**를 클릭합니다.

7.4. 연동 시스템 관리

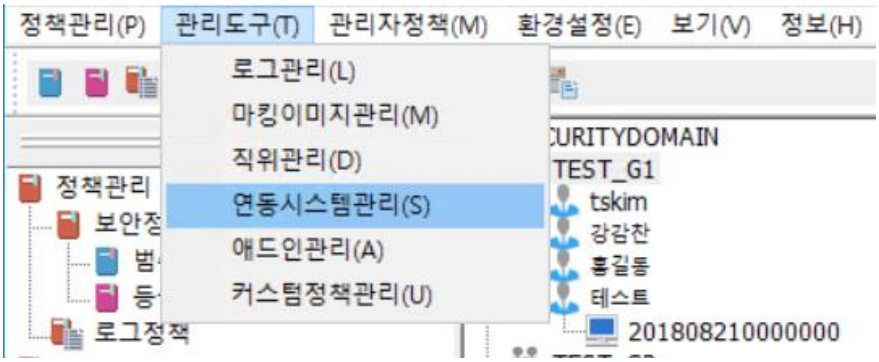
본 장은 연동 시스템의 관리에 대해 설명합니다. 연동 시스템은 주로 기간계 시스템(Legacy System ; KMS, EDMS, PMS 등)으로 기관의 문서를 보관하고 공유하는 시스템 중 Client 와 연동되어, 문서의 공유나 보관에 보안이 적용되는 시스템을 의미합니다. DS 는 연동 모듈을 통해서 연동 시스템에서 다운로드하는 문서를 암호화하거나, 업로드하는 문서를 복호화하는 기능을 제공합니다. 해당 기능은 다음의 2 가지 API 에 의해서 제공됩니다.

7.5. 애드인 관리

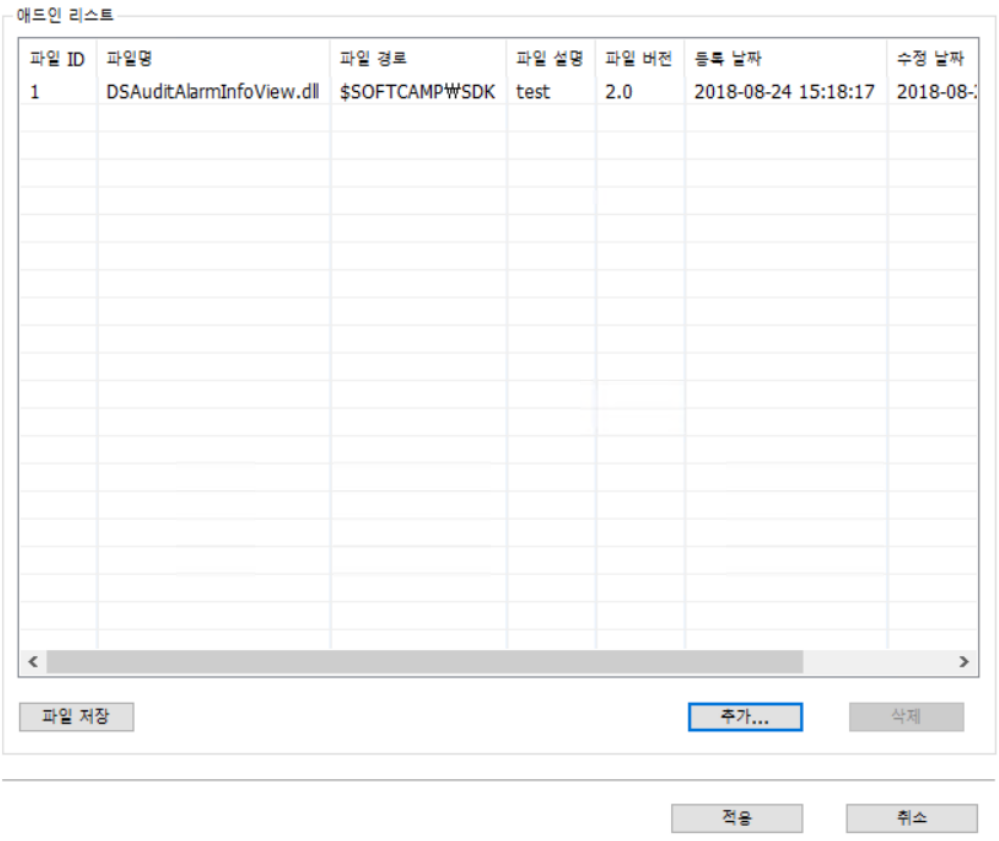
본 장은 애드인 관리에 대해 설명합니다.

애드인 관리 방법

1) 다음과 같이 Console 상단 매뉴에서 **'관리도구>애드인관리'**, 또는 () 아이콘을 클릭합니다.

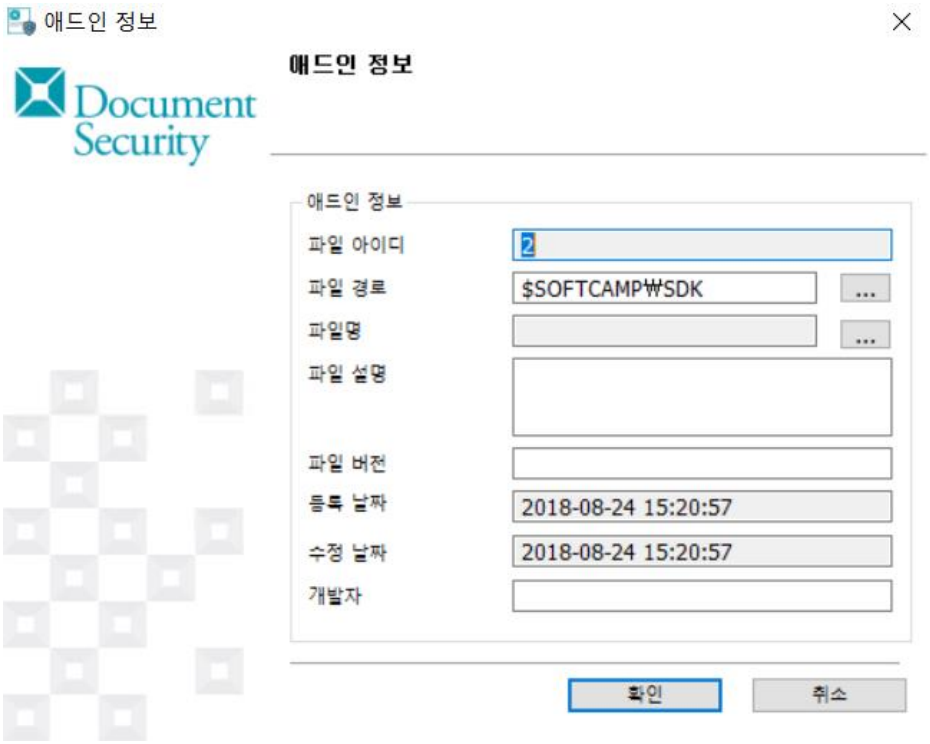


2) 작업 윈도우에 **'애드인 리스트'** 가 표시됩니다.



애드인 추가 등록

2) 작업 윈도우에서 **[추가]**를 클릭하면 다음과 같은 **<애드인 정보>**창이 표시됩니다. **'파일 경로'**에서 파일의 경로를 설정하고, **'파일명'**에서 파일을 선택합니다. **'파일 설명'**과 **'파일버전'**, **'개발자'**를 입력하고 **[확인]**를 클릭합니다. 파일 설명은 반각 255 문자까지 입력할 수 있으며, 파일 버전은 반각 50 자, 개발자 명은 반각 50 자 까지 입력할 수 있습니다.



애드인 삭제

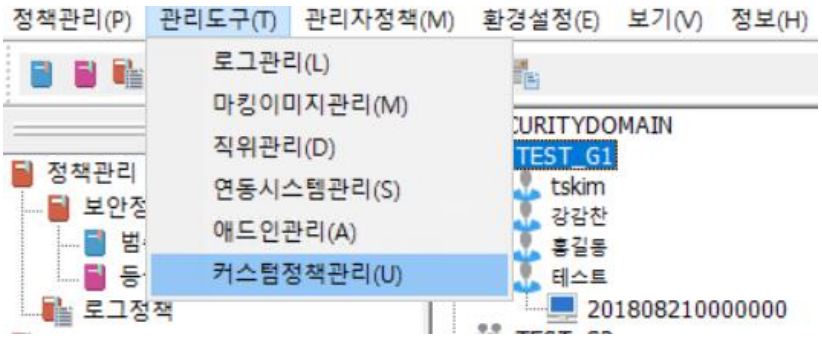
애드인을 삭제하는 경우는 **'애드인 리스트'** 에서 삭제 대상을 선택하고 작업 윈도우 화면 아래에 있는 **[삭제]**를 클릭합니다.

7.6. 커스텀 정책 관리

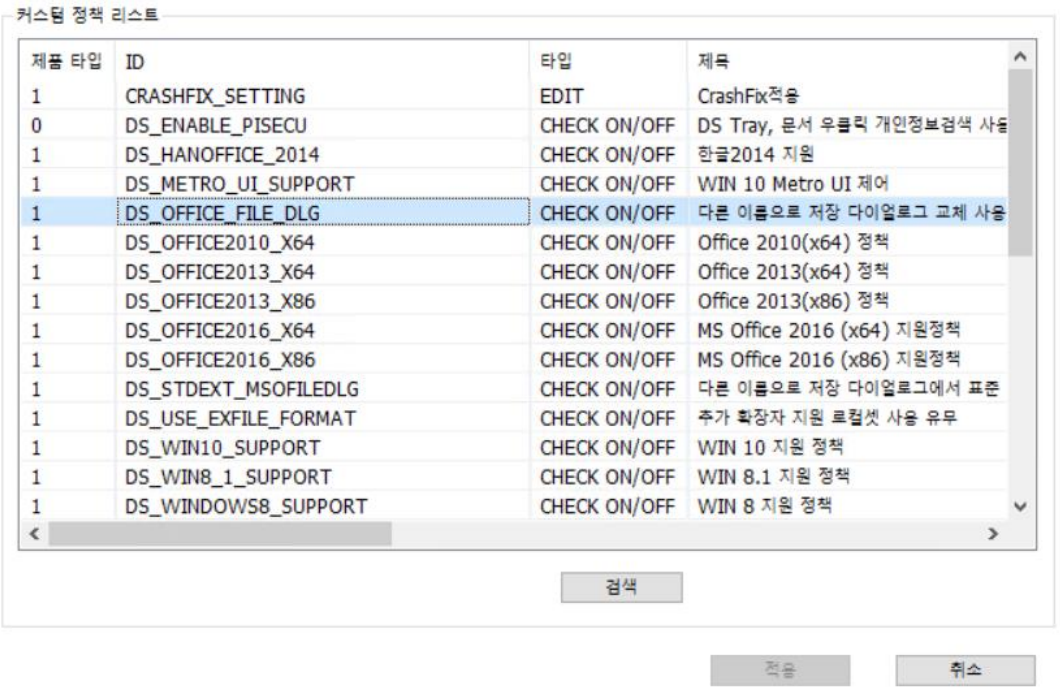
본 장은 커스텀 정책 관리에 대해 설명합니다.

커스텀 정책 관리 방법

1) 다음과 같이 Console 상단 매뉴에서 **'관리도구>애드인관리'**, 또는 ( ) 아이콘을 클릭합니다.

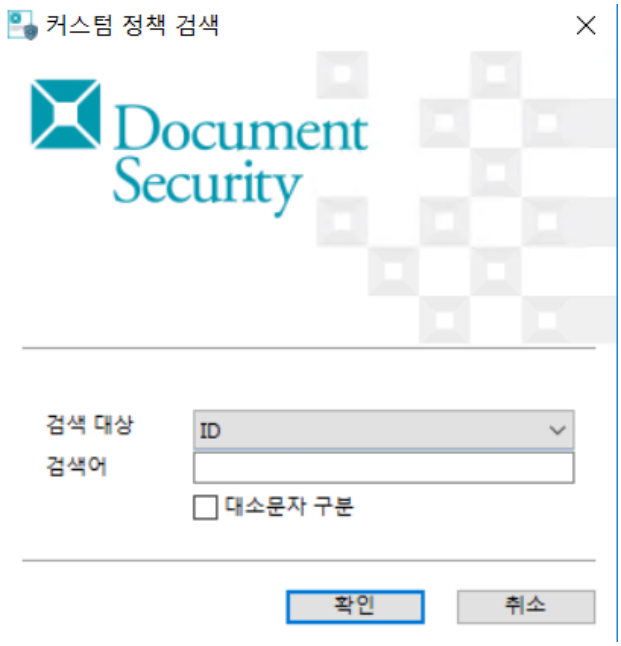


2) 작업 윈도우에 **'커스텀 정책 리스트'** 가 표시됩니다.

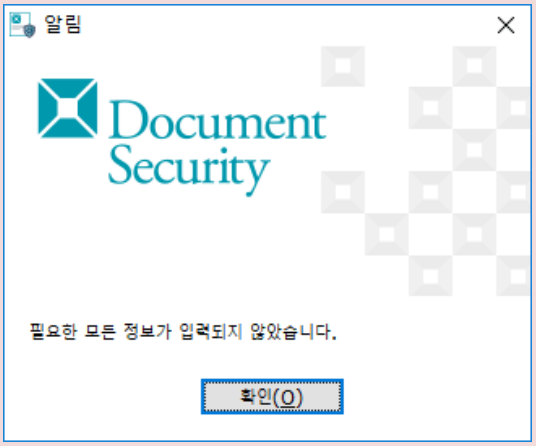


커스텀 정책 검색

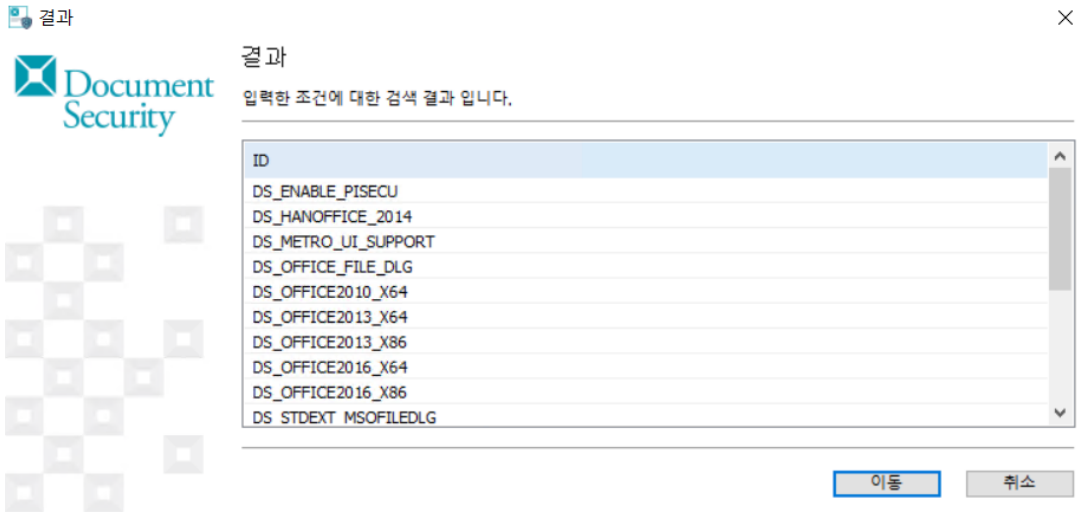
1) 작업 윈도우에서 **[검색]**을 클릭하면 다음과 같은 **<커스텀 정책 검색>**창이 표시됩니다. **'검색 대상'**에서 검색하고자하는 ID, 상세설명, 제목 중에서 선택하고, **'검색어'**에 검색 키워드를 입력한 후 **[확인]**를 클릭하면 커스텀 정책을 검색할 수 있습니다. **'대소문자 구분'**에 체크하면 검색 시 대소문자를 구분하여 검색을 수행합니다. 검색어는 반각 255 자 까지 입력할 수 있습니다.



주의 : 아무런 정보를 입력하지 않고 [확인]을 클릭하면 다음과 같은 경고 메시지가 나타납니다.



2) 검색이 완료되면 다음과 같이 결과 리스트가 표시됩니다.



8. 관리자 정책

본 장은 보안 관리자를 관리하는 방법에 대해 설명합니다.

보안 관리자는 아래와 같이 2 가지로 구분됩니다.

a. **최고보안 관리자** : 설치 시에 디폴트로 생성되는 관리자 계정으로 Console 에서 제공하는 모든 보안 기능을 사용할 수 있습니다.

b. **중간 관리자** : 최고보안 관리자나 다른 중간 관리자에 의해 생성된 관리자로써, 해당 계정을 생성하는 관리자가 허용한 범위 내에서, Console 이 제공하는 기능을 사용하고, 그룹을 관리합니다.

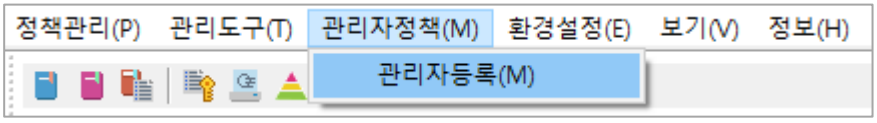
관련링크

a. 관리자 등록

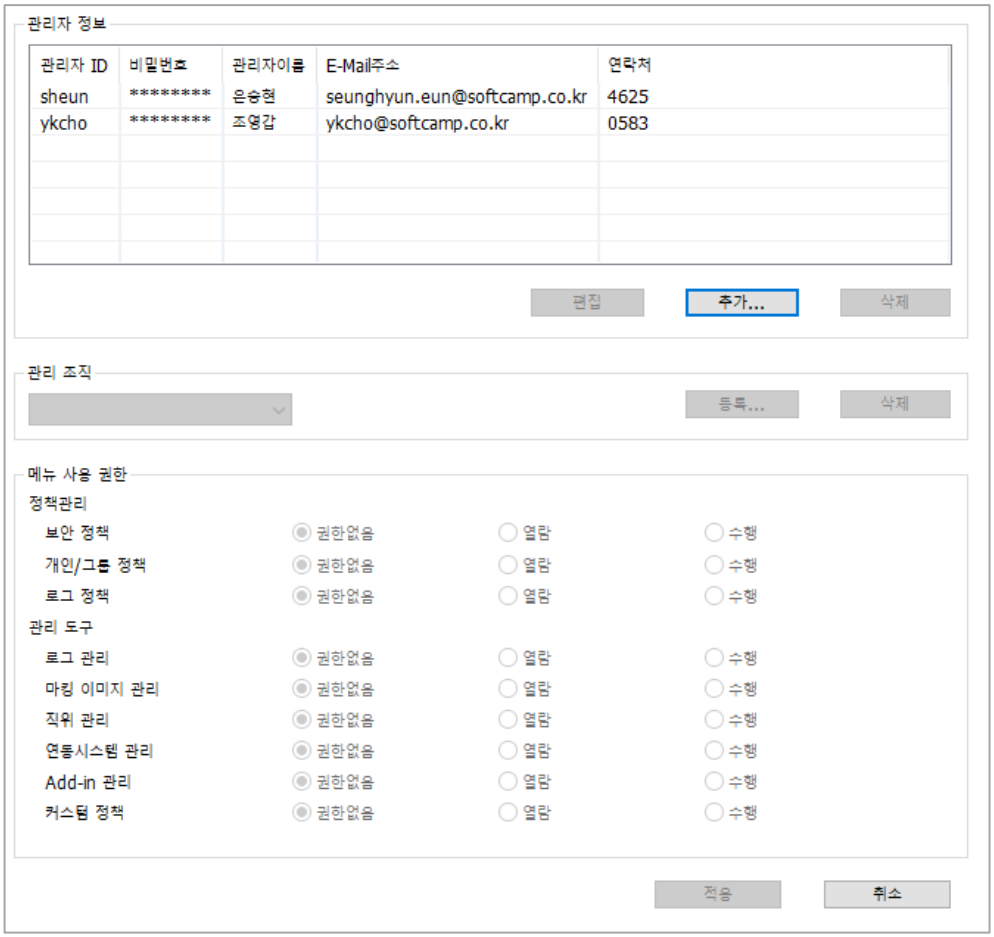
8.1. 관리자 등록

최고 보안 관리자는 관리자등록 기능을 통해 추가로 **'중간 관리자'**를 별도로 등록 지정하여 관리 업무의 실무적인 역할을 대행하도록 설정할 수 있습니다. 중간 관리자는 Console 을 이용한 보안정책 설정, 로그/감사 조회 등의 관리 업무를 수행할 수 있습니다. 중간 관리자가 실행할 수 있는 기능은 최고 보안 관리자의 설정에 의해서 제한되며, 중간 관리자가 관리하는 조직 또는 사용자에 대한 관리 권한만 부여합니다.

1) **'중간 관리자'**를 등록하기 위해 Console 상단 메뉴의 **'관리자정책>관리자등록'**을 선택, 또는 () 아이콘을 클릭합니다.

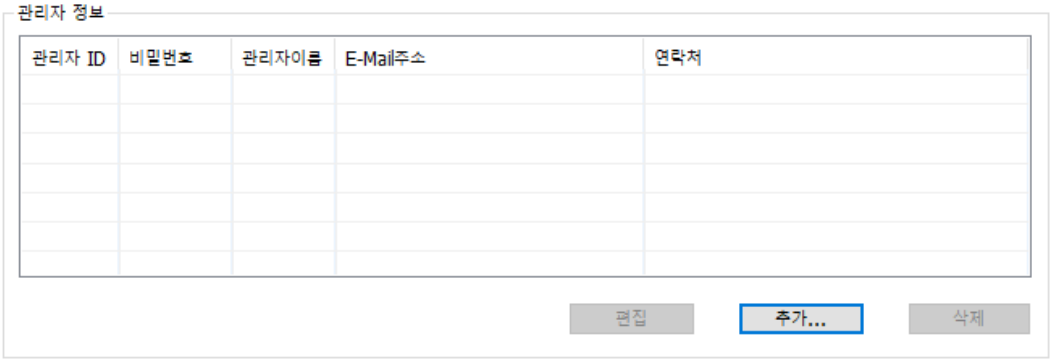


2) Console 의 작업 윈도우에 관리자등록 메뉴가 나타납니다. **'관리자 정보'**에서는 현재 등록되어 있는 관리자의 리스트를 확인할 수 있으며 관리자를 추가 및 삭제하는 것이 가능합니다.

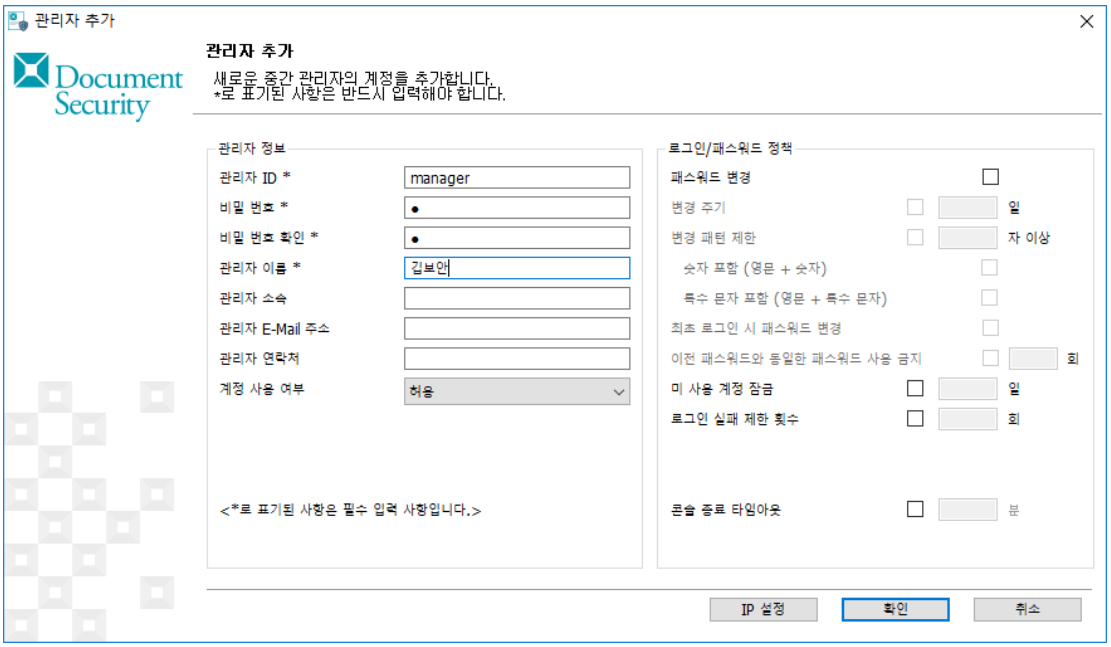


보안 관리자의 추가 및 삭제

1) 작업 윈도우의 보안 관리자 리스트에서 **[추가]**를 누릅니다.



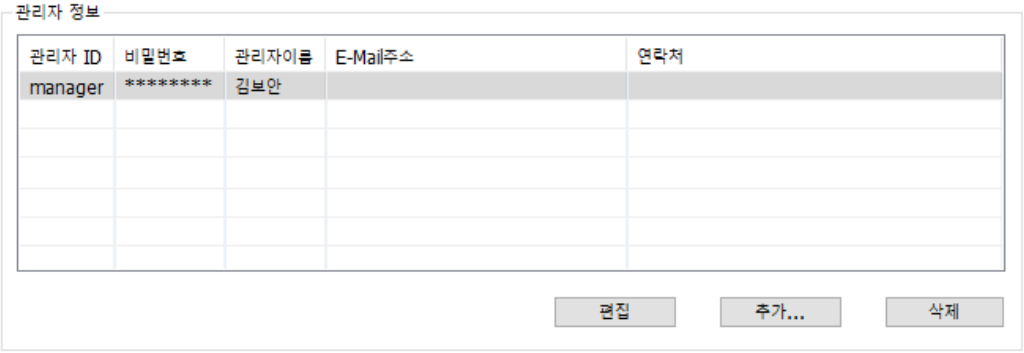
2) **<관리자 추가>**창이 나타나면 각 항목에 대한 신규 관리자 정보를 입력합니다. '*'로 표기된 사항은 필수 입력 항목 입니다.



구분	내용
관리자 ID	신규 관리자의 ID 를 입력합니다. 사용자가 사용중인 ID 와는 다른 아이디를 입력하셔야 합니다. 아이디는 영문,숫자, 특수문자로 1~20 자까지 입력 가능합니다.
비밀 번호	신규 관리자의 비밀번호를 입력합니다. 비밀번호는 반드시 9 문자 이상, 15 문자 이하의 영문과 숫자, 특수문자의 조합을 사용해야 합니다.
비밀 번호 확인	신규 관리자 비밀번호를 다시 한번 입력하여 확인합니다.
관리자 이름	신규 관리자의 이름을 입력합니다. 이름은 반각 1~50 자까지 입력가능합니다.

관리자 소속	신규 관리자의 소속을 입력합니다. 소속은 반각 0~50 자까지 입력가능합니다.
관리자 E-Mail 주소	신규 관리자의 E-mail 주소를 입력합니다. E-mail 주소는 반각 1~50 자까지 입력가능합니다.
관리자 연락처	신규 관리자의 연락처 정보를 입력합니다. 숫자로 1~50 자까지 입력가능합니다.
비밀 번호 변경	비밀 번호 변경에 대한 정책 적용 여부를 활성화 하거나 비활성화 합니다.
변경 주기	비밀 번호의 변경주기를 활성화하고, 기간을 설정합니다. 변경주기는 숫자 1~99999 까지 입력가능합니다.
변경 패턴 제한	변경 패턴 제한을 활성화 합니다. 최소 글자 수를 제한합니다. 기본 값은 9 자 이상입니다.
숫자 포함(영문 + 숫자)	비밀 번호에 숫자를 필수로 포함할 지 여부를 설정합니다. 기본 값은 포함입니다.
특수 문자 포함(영문 + 특수문자)	비밀 번호에 특수 문자를 필수로 포함할 지 여부를 설정합니다. 기본 값은 포함입니다.
최초 로그인 시 패스워드 변경	최초 로그인 시 패스워드 변경을 유도할지 여부를 설정합니다. 기본 값은 변경 필수 입니다.
이전 패스워드와 동일한 패스워드 사용금지	패스워드 변경 시 이전 패스워드와 동일한 패스워드를 사용할 수 없게 할지 여부를 설정합니다.
미 사용 계정 잠금	미 사용 계정에 대한 잠금 설정을 할 수 있습니다.
로그인 실패 제한 횟수	로그인 실패 제한 횟수를 설정합니다. 기본 값은 5 회 입니다.
콘솔 종료 타임아웃	유휴시간에 따른 콘솔 종료 타임아웃 시간을 설정합니다. 기본 값은 5 분(300 초) 입니다.

3) **'관리자'**의 정보 입력이 끝난 후 **[확인]**을 클릭하면 다음과 같이 관리자 리스트에 신규 관리자가 등록됩니다.

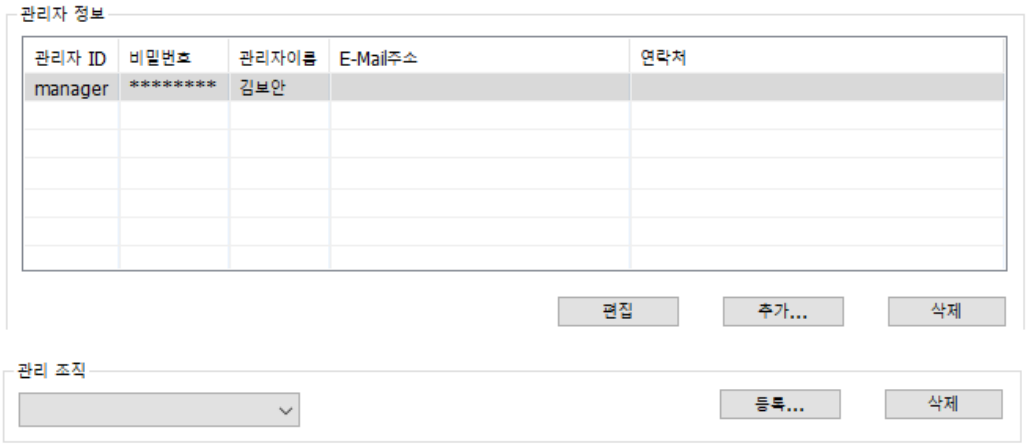


4) 추가되어 있는 관리자를 삭제하고 싶은 경우는 관리자 리스트에서 삭제하고 싶은 관리자를 선택한 뒤 **[삭제]**를 클릭합니다.

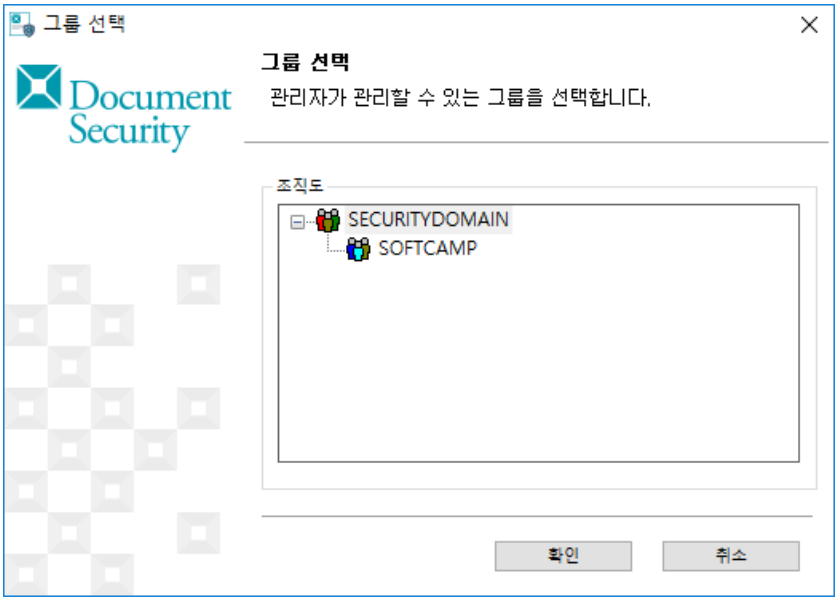
관리 그룹 및 권한 설정

'관리 조직'에서는 관리자가 관리할 수 있는 **'그룹'**을 설정하며, **'메뉴 사용 권한'**에서는 관리자가 Console 에서 사용할 수 있는 권한(사용할 수 있는 메뉴의 범위)을 설정합니다. 관리 조직 및 메뉴 권한 설정을 적용받은 관리자가 Console 에 로그인하면, 설정되어 있는 그룹 정보만 표시되며 최고 보안 관리자에 의해서 허가된 권한만을 사용할 수 있습니다.

1) 작업 윈도우 상단의 **'관리자 정보'**에서 설정하려는 관리자를 선택하고 **'관리 조직'**에서 **[등록...]**을 클릭합니다.



2) <**그룹 선택**>창이 나타나면 해상 관리자의 관리 그룹을 선택하고 **[확인]**을 클릭합니다.



3) **'매뉴 사용 권한'**으로 해당 관리자가 Console 에서 사용 가능한 권한을 설정합니다.

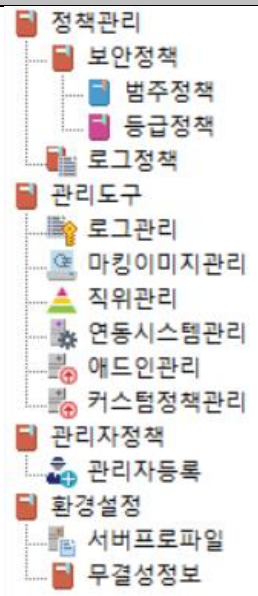
a. **메뉴 설정 범위 :** Console 에서 제공하는 전체 메뉴에 중 중간 관리자에게 할당할 수 있는 메뉴는 그룹의 정책과 사용자를 관리할 수 있는 권한에 국한됩니다. Console 에서 제공하는 메뉴에 대한 자세한 내용은 메뉴 구성을 참조하시기 바랍니다.

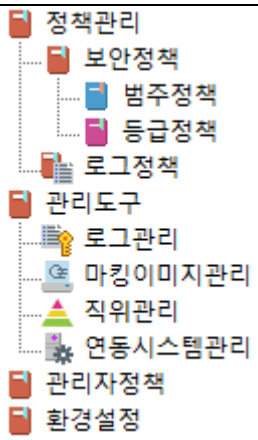
메뉴		메뉴 역할
정책관리	보안 정책	**'정책관리>보안정책'** 메뉴 사용 권한 설정
	개인/그룹 정책	조직도에서 그룹 및 사용자 선택 시 나타나는 작업 윈도우에서의 메뉴 사용 권한 설정
	로그 정책	**'정책관리>로그정책'** 메뉴 사용 권한 설정
관리 도구	로그 관리	'**관리도구>로그관리**' 메뉴에 대한 권한 설정
	마킹 이미지 관리	'**관리도구>마킹이미지관리**' 메뉴에 대한 권한 설정
	직위 관리	'**관리도구>직위관리**' 메뉴에 대한 권한 설정
	연동시스템 관리	'**관리도구>연동시스템관리**' 메뉴에 대한 권한 설정
	Add-in 관리	'**관리도구>애드인관리**' 메뉴에 대한 권한 설정
	커스텀 정책	'**관리도구>커스텀정책관리**' 메뉴에 대한 권한 설정

b. **권한 분류 :** 각 메뉴에 대한 사용 권한을 **'권한없음'**, **'열람'**, **'수행'** 이라는 세가지 중 하나로 설정할 수 있습니다. 기본값은 **'권한없음'** 입니다.

구분	내용
권한없음	관리자가 Console 로 로그인한 경우, 화면에서 해당 메뉴가 표시되지 않습니다.
열람	관리자가 Console 로 로그인한 경우, 메뉴는 표시되나 설정값을 변경할 수는 없습니다.
수행	관리자가 Console 로 로그인한 경우, 메뉴가 표시되며 설정값을 변경할 수 있습니다.

4) 보안관리자는 메뉴 사용이 제한되며 실행할 수 있는 기능만 표시됩니다. 보안관리자는 다음의 표와 같이 사용 권한이 있는 메뉴만이 표시됩니다.

구분	내용
최고 보안 관리자 메뉴	

보안관리자 메뉴의 예	

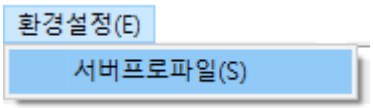
9. 환경설정

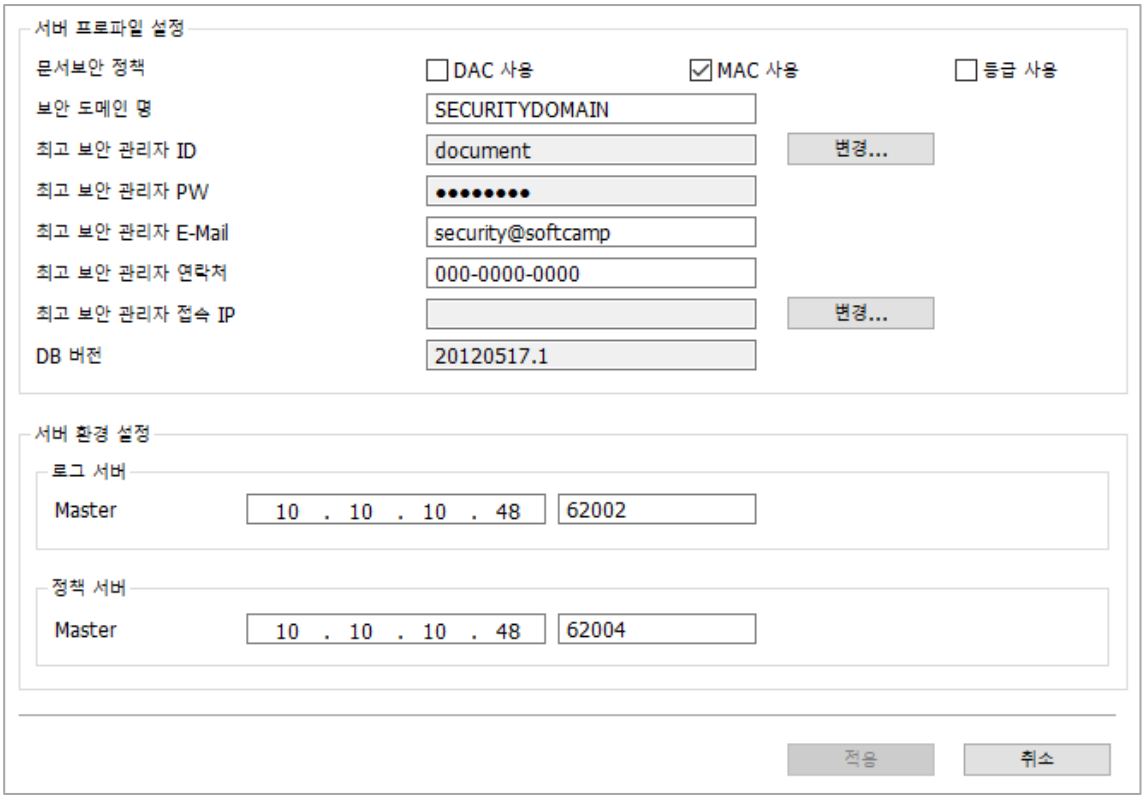
본 장은 SoftCamp Document Security 의 환경 설정에 대해 설명합니다. 환경 설정은 **'서버프로파일'**의 메뉴가 있습니다.

서버프로파일

관리자는 '서버프로파일' 메뉴에서 보안 도메인 명을 변경하거나 최고보안 관리자의 계정(ID, PW, E-mail, 연락처)를 변경할 수 있습니다. 또한, 사용할 암호화 정책 선택, 서버 환경 설정을 할 수 있습니다. 최고 보안 관리자의 계정 정보(ID, PW)를 설치 후 최초 로그인 시 변경하도록 유도합니다. 만약 최초 로그인 시 ID 와 PW 를 변경하지 않으면 Console 을 사용할 수 없습니다. 또한, '서버프로파일' 메뉴에서는 LMS 의 IP 와 접속포트에 대하여 설정할 수 있으며, Client 의 인증 서버 접속 정책을 설정할 수 있습니다. LMS 의 IP 와 접속포트가 정상적으로 설정되지 않으면 Client 가 정상적으로 로그인될 수 없습니다.

Console 상단 메뉴의 '**환경설정>서버프로파일**' 또는 바로가기 메뉴의 ( )를 클릭하여 표시되는 작업창에서 가능합니다. 다음과 같이 창이 구성되어 있습니다.





관련링크

a. 서버프로파일 설정

9.1. 서버프로파일 설정

본 장은 **'서버프로파일'** 메뉴에 대하여 설명합니다. '서버프로파일' 메뉴에서는 크게 **'서버 프로파일 설정'**란, **'서버 환경 설정'**란으로 나누어 있습니다. 아래는 각각에 대하여 설명합니다.

서버 프로파일 설정

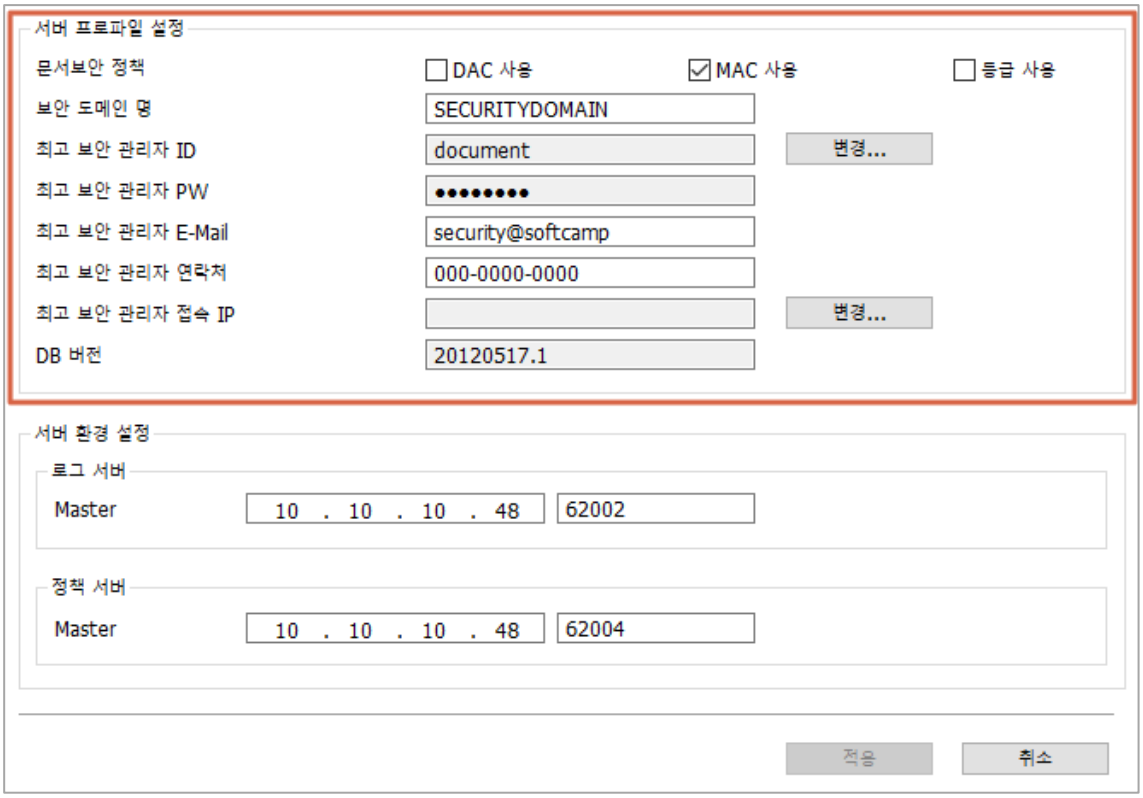
서버 프로파일 설정에서는 크게 아래와 같은 기능을 제공합니다.

a. **문서보안 정책 선택** : 사용할 문서 암호화 정책을 선택합니다.

b. **최고 보안 관리자 계정 변경** : 최고보안 관리자의 계정을 변경합니다.

c. **서버 정보 확인** : 사용 중인 Server 의 정보를 확인합니다.

'서버프로파일 설정'을 하기 위해 Console 상단 메뉴의 '**환경설정>서버프로파일'** 또는 바로가기 메뉴의 ()를 클릭하면 다음과 같은 창이 나타납니다.



a. 문서보안 정책 선택

문서보안 정책에서 사용할 암호화 정책을 설정합니다. 체크되지 않은 항목은 Client 에서 문서 암호화 시 해당 정책을 선택하여 암호화할 수 없습니다.

설정	영향
DAC 사용 체크	사용자는 접근 대상을 설정한 공용 보안문서를 생성할 수 있습니다.
DAC 사용 언체크	사용자는 접근 대상을 설정한 공용 보안문서를 생성할 수 없습니다.
MAC 사용 체크	사용자는 범주 보안문서를 생성할 수 있습니다.
MAC 사용 언체크	사용자는 범주 보안문서를 생성할 수 없습니다.
등급 사용 체크	사용자는 등급 보안문서를 생성할 수 있습니다.
등급 사용 언체크	사용자는 등급 보안문서를 생성할 수 없습니다.

a. 최고 보안 관리자 계정 변경

최고 보안 관리자는 **'보안 도메인'**에 등록되어 있는 모든 **'그룹'**과 **'사용자'**의 보안 책임을 담당하는 관리자를 말합니다. 최고 보안 관리자는 정책관리, 보안감사, 각 그룹 및 사용자에 대한 권한, 업그레이드 관리 등 모든 정책에 대한 관리 권한을 가지고 있습니다.

주의 : 최고 보안 관리자의 아이디와 비밀번호는 최고 보안 등급으로 관리되어야 하며, 분실 시에는 시스템 전체에 큰 문제를 일으킬 수 있으므로 주의를 요합니다.

1) **'최고 보안 관리자'**의 계정 설정은 **'서버 프로파일 설정'**에서 이루어집니다. 구성은 다음과 같습니다.

a. **보안 도메인 명 :** 보안 도메인 명을 설정할 수 있습니다. 반각 1~50 자까지 입력가능합니다.

b. **최고 보안 관리자 ID :** 최고 보안 관리자의 아이디(ID) 정보로, 우측의 **[변경...]** 을 선택하여 최고 보안 관리자의 계정 정보(아이디 및 비밀번호 정보)를 변경할 수 있습니다. 다만 현재 등록되어 있는 보안 관리자 ID 와 동일한 ID 로는 변경할 수 없습니다.

c. **최고 보안 관리자 PW :** 최고 보안 관리자의 비밀번호 정보로, 우측의 **[변경...]** 을 선택하여 최고 보안 관리자의 계정 정보(아이디 및 비밀번호 정보)를 변경할 수 있습니다.

d. **최고 보안 관리자 E-Mail :** 최고 보안 관리자의 메일 주소 정보로, 변경이 가능합니다. E-mail 주소는 반각 1~50 자까지 입력가능합니다.

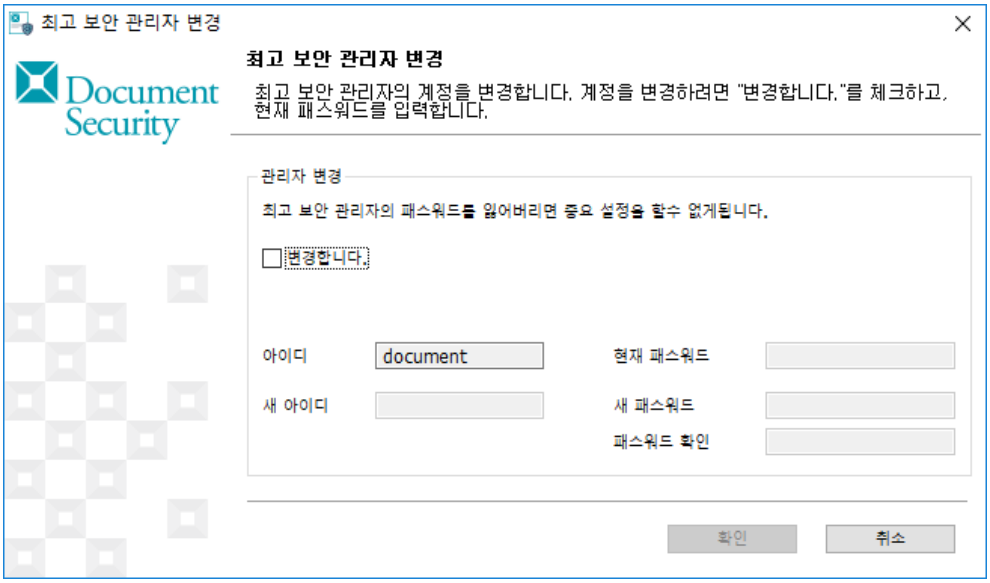
e. **최고 보안 관리자 연락처 :** 최고 보안 관리자의 연락처 정보로, 변경이 가능합니다. 숫자로 1~50 자까지 입력가능합니다.

f. **최고 보안 관리자 접속 IP :** 최고 보안 관리자의 접속 IP 정보로, 변경이 가능합니다.

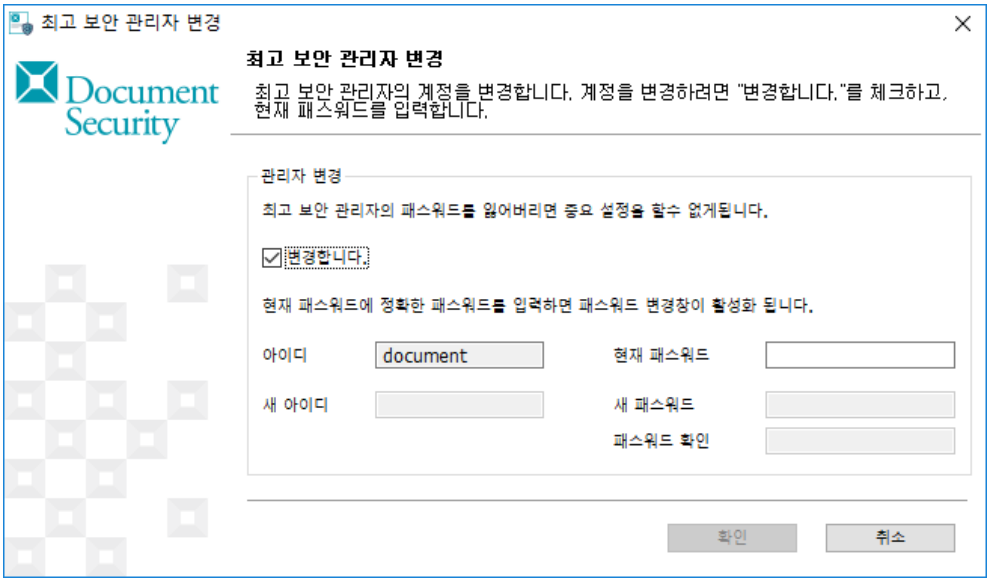
2) **'최고 보안 관리자 ID'**와 **'최고 보안 관리자 PW'**를 변경하기 위해 **'작업 윈도우'**의 **'서버 프로파일 설정'**의 **'최고 보안 관리자 ID'**의 옆에 있는 **[변경...]** 을 누릅니다.

참고 : 보안 도메인 명, 최고 보안 관리자 E-Mail, 최고 보안 관리자 연락처 등은 입력창에서 수정 후 하단의 [적용] 버튼을 클릭하면 바로 수정됩니다. 하지만 최고 보안 관리자 ID 와 최고 보안 관리자 PW 를 수정하기 위해서는 [변경...] 버튼을 클릭해야 하며, 현재 사용중인 아이디와 비밀번호 인증 후 새로운 아이디와 비밀번호로의 변경이 가능합니다.

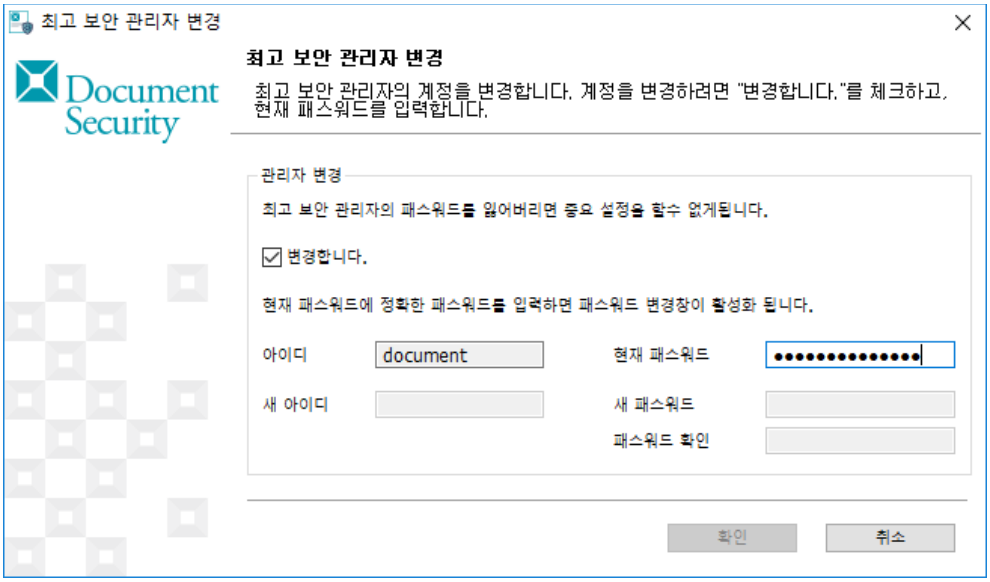
1) 다음과 같이 **<최고 보안 관리자 변경>**창이 나타나면 **[변경합니다]** 체크박스를 선택합니다.



1) **[변경합니다.]** 체크 박스를 선택하면 **'현재 비밀번호에 정확한 비밀번호를 입력하면 비밀번호 변경창이 활성화 됩니다.'** 라는 메시지가 표시되는 것과 동시에 **'현재 비밀번호'** 입력란이 활성화됩니다.



1) 현재 사용하고 있는 비밀번호를 입력합니다. 올바른 비밀번호를 입력했을 경우 **'새 아이디'**와 **'새 비밀번호'**,**'비밀번호 확인'** 입력란 및 **[확인]**버튼이 활성화됩니다. **'새 아이디'**와 **'새 비밀번호', '비밀번호 확인'**란에 변경할 새로운 아이디와 비밀번호를 입력한 후 **[확인]**을 클릭합니다.

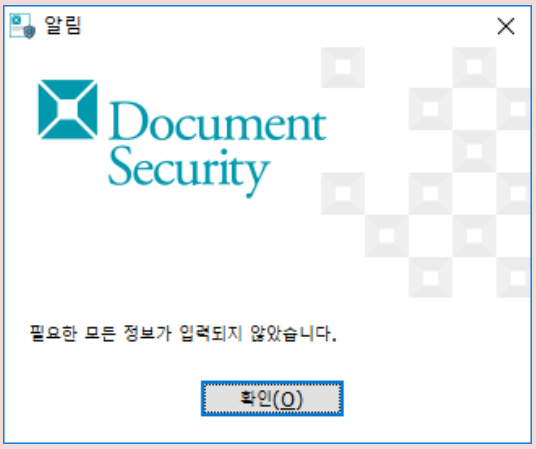


a. **새 아이디** : 최고 보안 관리자의 새로운 아이디를 입력합니다. 아이디는 반각 1~20 자까지 입력 가능합니다.

b. **새로운 비밀번호**: 최고 보안 관리자의 새로운 비밀번호를 입력합니다. 영문, 숫자, 특수문자를 모두 포함하여 9 자 이상부터 15 자리수까지 입력 가능합니다.

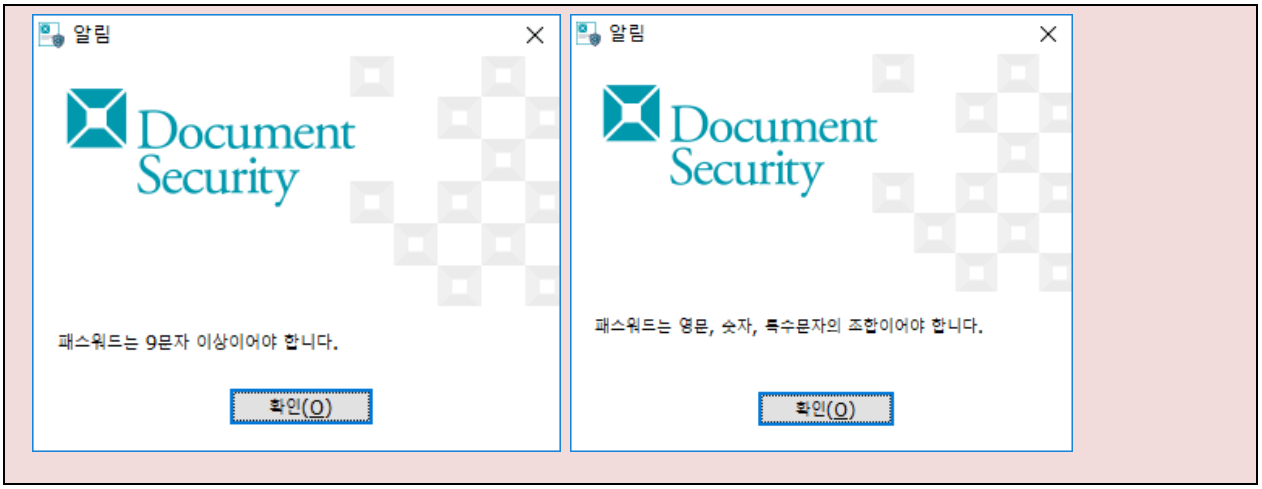
c. **비밀번호 확인**: 새 비밀번호를 확인하는 란입니다. 상위 '**새 비밀번호**'와 동일한 값을 입력합니다.

주의 : 필요한 정보가 모두 입력되어 있지 않은 상태로 [확인]을 클릭하면 다음과 같은 메시지가 표시됩니다. 빠진 내용을 다시 입력 후 [확인]을 클릭하세요.



비밀번호 조합규칙이 적용된 경우, 아래와 같은 메시지가 나타납니다. 비밀번호 조합규칙은 변경할 수 없으며, 제품에 따라 적용되어있지 않을 수 있습니다. 비밀번호 조합규칙은 다음과 같습니다.

- 최소 9 자 이상의 영문대문자, 영문소문자, 숫자, 특수문자 중 3 가지 조합



a. 서버 정보 확인

서버 정보는 Server 의 정보를 나타냅니다. 관리자가 확인할 수 있는 정보는 아래와 같습니다.

-. DS DB 버전 : 서버 DB 의 버전을 표시합니다.

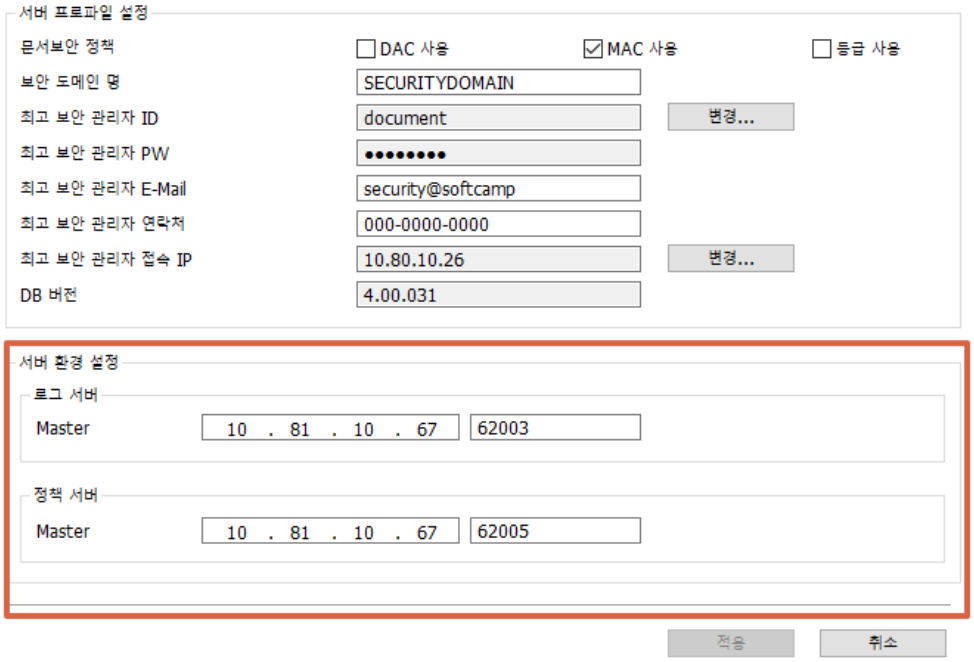
서버 환경 설정

서버 환경 설정에서는 크게 아래와 같은 기능을 제공합니다.

a. 로그 서버 접속 설정

b. 정책 서버 접속 설정

여기에서는 Client 의 사용자가 Server 의 데몬 중 **'로그 서버(LMS)'**와 **'인증 서버(AKS)'** 에 접속할 때 사용되는 정보를 설정합니다. 서버 환경 설정을 하기 위해 Console 상단 메뉴의 **'환경설정>서버프로파일'** 또는 바로가기 메뉴의 ( )를 클릭하면 다음과 같은 창이 나타납니다. 서버 환경 설정은 다음과 같은 창에서 표시된 부분을 통해 할 수 있습니다.



a. 로그 서버 접속 설정

사용자가 Client 사용 시 발생한 로그를 저장하는 **'로그 서버'**의 정보(DS 서버의 IP 주소, Port 번호)를 지정합니다.

구 분	내 용
Master	Master 로 사용되는 로그 서버의 접속 정보입니다. IP 주소 입력창의 각각의 필드는 0 ~ 255 까지의 숫자만 입력할 수 있습니다. 통신포트 입력창에는 0 ~ 65535 까지 숫자만 입력할 수 있습니다.

a. 정책 서버 접속 설정

관리자가 정책을 설정하기 위해 사용할 **'정책 서버'**의 정보(DS 서버의 IP 주소, Port 번호)를 지정합니다.

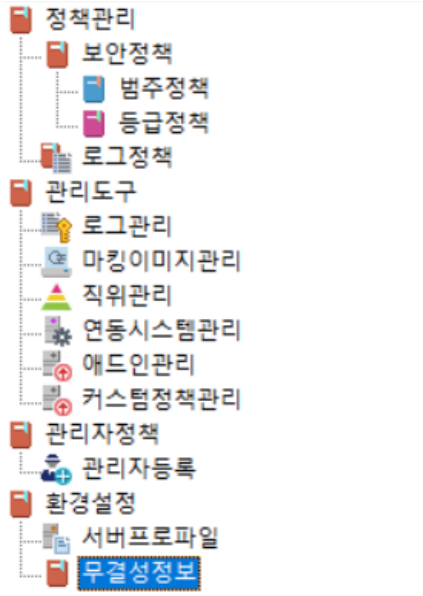
구 분	내 용
Master	Master 로 사용되는 정책 서버의 접속 정보입니다. IP 주소 입력창의 각각의 필드는 0 ~ 255 까지의 숫자만 입력할 수 있습니다. 통신포트 입력창에는 0 ~ 65535 까지 숫자만 입력할 수 있습니다.

9.2. 무결성정보

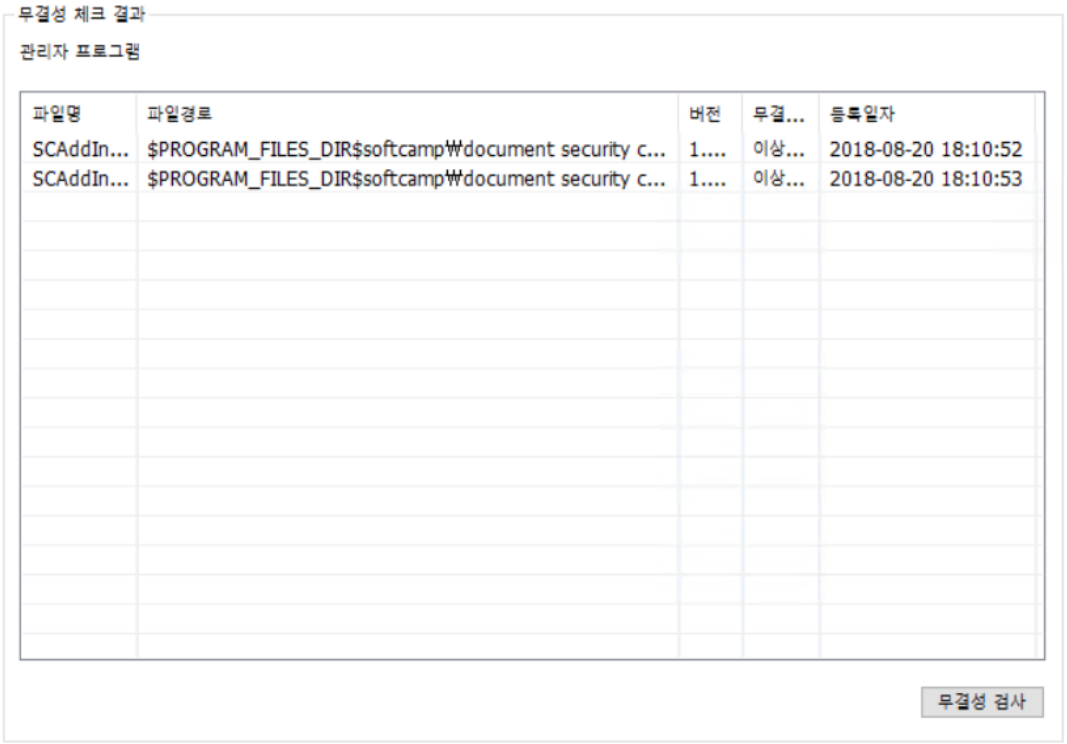
본 장은 **'무결성정보'** 메뉴에 대하여 설명합니다. '무결성정보' 메뉴는 인가된 관리자가 TOE 구성요소들에 대한 무결성 검사를 할 수 있는 기능을 제공합니다.

무결성 검사 방법

1) 다음과 같이 매뉴 탐색창에서 **'환경설정>무결성정보'**를 클릭합니다.



2) 작업 윈도우에 **'무결성 체크 결과'** 가 표시됩니다.



3) 즉시 무결성 검사를 수행하고자 할경우 **'무결성 검사'** 버튼을 클릭하면 무결성 검사 결과 창이 표시됩니다.

참고: 무결성 검사 대상 및 주기

TOE 에 포함되거나 SFR 을 제공하는 모든 파일은 무결성 검사 대상이며, 시동 시 및 정규 운영동안 주기적으로 무결성 검사를 수행합니다. 인가된 관리자가 원하는 경우 Console 을 이용하여 즉시 무결성 검사를 수행할 수도 있습니다.

10. 조직 관리

본 장은 Console 의 조직 관리에 대해 설명합니다.

관리자는 Console 에 있는 조직도를 이용해 사용자/그룹의 추가, 정보의 수정 및 관리를 할 수 있습니다. 조직도에서 그룹 및 사용자를 선택하게 되면 우측 작업창의 상단에 해당 그룹 및 사용자의 기본 정보가 표시됩니다. 화면구성은 다음과 같습니다.

관련링크

a. 기본 정보 관리

b. 조직도 정렬

c. 그룹 관리

d. 사용자 관리

e. 새로고침

f. 검색

10.1. 기본 정보 관리

그룹과 사용자의 **'기본정보'**는 **'조직도'**와 **'작업창'**을 이용하여 관리가 가능합니다.

조직도에 표시되는 내용은 다음과 같습니다.

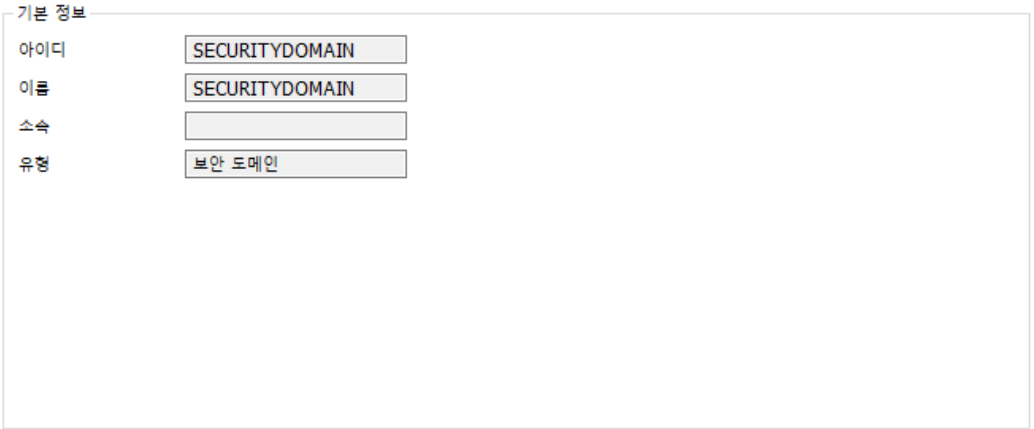
구분	아이콘	내용	비고
도메인 그룹		DS 도메인에 등록되어 있는 전체 그룹을 나타냅니다.	인사 DB 에 등록 되어 관리되는 그룹
실 그룹		사내 사용자의 그룹을 나타냅니다. 그룹은 하위에 복수의 그룹을 포함할 수 있습니다.	
실 사용자		DS 사용 권한이 있는 사내 사용자를 나타냅니다.	

가상 그룹		Console 에서 보안 관리자가 등록한 그룹을 나타냅니다. 실제 인사 DB 에는 등록되어있지 않으나 관리자의 필요에 따라 등록/수정/삭제가 가능합니다.	Console 에서 보안 관리자가 등록한 가상 그룹
가상 사용자		Console 에서 보안 관리자가 등록한 사용자를 나타냅니다. 실제 인사 DB 에는 등록이 되어있지 않으나, 관리자의 필요에 따라 특정 사용자에게 DS 사용 권한을 줄 수 있습니다. 수정/삭제가 가능합니다.	
PC		각각의 사용자가 접속한 PC 를 나타내며, 사용자의 하위에 나타납니다. 다중로그인 권한이 있는 사용자의 경우 복수의 PC 가 나타날 수 있습니다.	사용자 PC

조직도에 표시되는 **'보안 도메인', '그룹', '사용자'**의 **'기본 정보'** 관리는 다음과 같습니다.

보안 도메인

'보안 도메인'을 선택하였을 시 작업창에 다음과 같은 기본정보가 나타납니다.



구분	내용	변경여부
아이디	보안 도메인의 아이디를 나타냅니다.	X
이름	보안 도메인의 이름을 나타냅니다.	X
소속	보안 도메인의 소속을 나타냅니다.	X
유형	보안 도메인의 유형을 나타냅니다.	X

실 그룹

'실 그룹'을 선택하였을 시 작업창에 다음과 같은 기본정보가 나타납니다.

구분	내용	변경여부
아이디	인사 DB 에 등록되어 있는 그룹의 아이디를 나타냅니다.	X
이름	인사 DB 에 등록되어 있는 그룹의 이름을 나타냅니다.	X
소속	인사 DB 에 등록되어 있는 그룹의 소속을 나타냅니다.	X
유형	인사 DB 에 등록되어 있는 그룹의 유형을 나타냅니다.	X

실 사용자

'실 사용자'를 선택하였을 시 작업창에 다음과 같은 기본정보가 나타납니다.

구분	내용	변경여부
아이디	인사 DB 에 등록되어 있는 사용자의 **아이디**를 나타냅니다.	X
이름	인사 DB 에 등록되어 있는 사용자의 **이름**을 나타냅니다.	X
소속	인사 DB 에 등록되어 있는 사용자의 **소속**을 나타냅니다.	X
유형	인사 DB 에 등록되어 있는 사용자의 **유형**을 나타냅니다.	X
분류	인사 DB 에 등록되어 있는 사용자의 분뷰를 나타냅니다.	O
직위	인사 DB 에 등록되어 있는 사용자의 **직위**를 나타냅니다.	X
로그인 상태	현재 사용자의 **로그인 상태**를 나타냅니다. **참조: 로그인 상태는 Server 에 현재 기록되어 있는 사용자의 로그인 상태입니다. 로그인 상태를 변경하더라도 실제 사용자 PC 에서 로그인 상태가 변경되지 않습니다.**	O
계정 사용 여부	DS 에서 사용되는 사용자의 **계정 사용 여부**를 나타냅니다. • **사용안함** : 계정 사용을 중지하며, 사용자는 로그인할 수 없습니다.	O

	• **사용함** : 정상적인 사용이 가능합니다. • **로그인실패제한** : 사용자가 일정 횟수의 로그인이 실패하였을 시 설정되며, 사용자는 로그인할 수 없습니다. (참조 : 로그인 - **로그인 실패 제한 횟수**)	
최근 로그인 IP	사용자의 **최근 로그인 IP** 를 나타냅니다.	X
최근 로그인 시간	사용자의 **최근 로그인 시간**을 나타냅니다.	X
최근 정책 수령 시간	Server 에서 사용자의 **최근 정책 수령 시간**을 나타냅니다.	X
비밀번호	Client 로그인 시 사용되고 있는 사용자의 비밀번호를 나타냅니다. 사용자가 비밀번호를 분실하였을 시, 관리자는 비밀번호를 변경하여 (변경 후 하단의 **[적용]** 버튼을 클릭) 적용할 수 있습니다. 비밀번호 변경 시 비밀번호 조합규칙을 따릅니다.	O
사용기한	사용자의 사용기한을 지정합니다. 디폴트 표시일은 서버의 날짜입니다.	O

가상 그룹

'가상 그룹'을 선택하였을 시 작업창에 다음과 같은 기본정보가 나타납니다.

구분	내용	변경여부
아이디	Server 에 등록되어 있는 그룹의 아이디를 나타냅니다.	X
이름	Server 에 등록되어 있는 그룹의 이름을 말합니다. 이름은 반각 0~50 자까지 입력가능합니다.	O
소속	Server 에 등록되어 있는 그룹의 소속을 나타냅니다.	X
유형	Server 에 등록되어 있는 그룹의 유형을 나타냅니다.	X

가상 사용자

'가상 사용자'을 선택하였을 시 작업창에 다음과 같은 기본정보가 나타납니다.

구분	내용	변경여부
아이디	Server 에 등록되어 있는 사용자의 **아이디**를 나타냅니다.	X
이름	Server 에 등록되어 있는 사용자의 **이름**을 말합니다.	O
소속	Server 에 등록되어 있는 사용자의 **소속**을 나타냅니다.	X

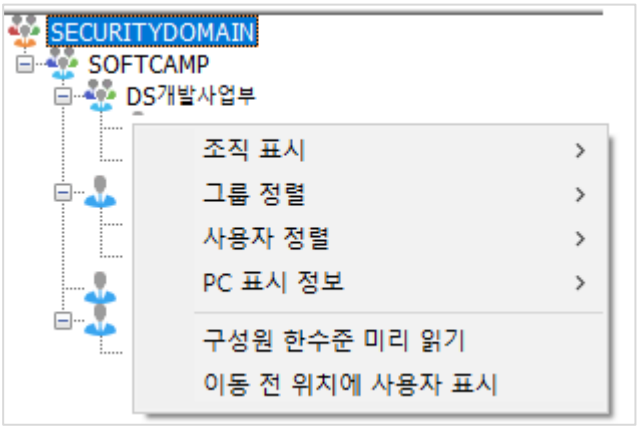
유형	Server 에 등록되어 있는 사용자의 **유형**을 나타냅니다.	X
분류	Server 에 등록되어 있는 사용자의 **분류**을 나타냅니다.	O
직위	Server 에 등록되어 있는 사용자의 **직위**를 나타냅니다.	O
로그인 상태	현재 사용자의 로그인 상태를 나타냅니다. **참조: 로그인 상태는 Server 에 현재 기록되어 있는 사용자의 로그인 상태입니다. 로그인 상태를 변경하더라도 실제 사용자 PC 에서 로그인 상태가 변경되지 않습니다.**	O
계정 사용 여부	DS 에서 사용되는 사용자의 계정 사용 여부를 나타냅니다. **사용안함** : 계정 사용을 중지하며, 사용자는 로그인할 수 없습니다. **사용함** : 정상적인 사용이 가능합니다. **로그인실패제한** : 일정 횟수의 로그인이 실패하였을 시 계정 사용의 제한을 둡니다. (참조 : 로그인 - **로그인 실패 제한 횟수**)	O
최근 로그인 IP	사용자의 **최근 로그인 IP** 를 나타냅니다.	X
최근 로그인 시간	사용자의 **최근 로그인 시간**을 나타냅니다.	X
최근 정책 수령 시간	Server 에서 사용자의 **최근 정책 수령 시간**을 나타냅니다.	X
비밀번호	DS 로그인 시 사용되고 있는 사용자의 비밀번호를 나타냅니다. 사용자가 비밀번호를 분실하였을 시, 관리자는 비밀번호를 변경하여 (변경 후 하단의 **[적용]** 버튼을 클릭) 적용할 수 있습니다. 비밀번호 변경 시 비밀번호 조합규칙을 따릅니다.	O
사용기한	사용자의 사용기한을 지정합니다. 디폴트 표시일은 서버의 날짜입니다.	O

10.2. 조직도 정렬

본 장은 조직도 정렬에 대해 설명합니다.

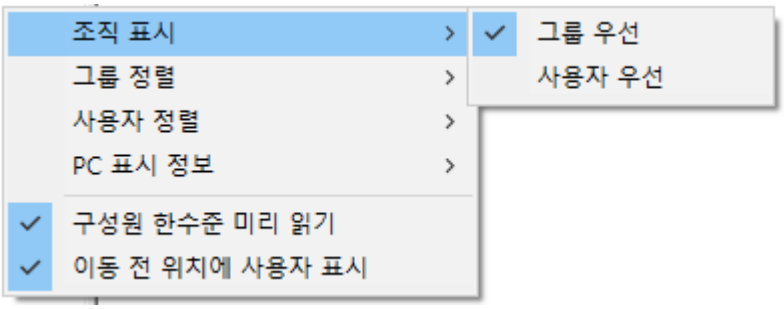
조직도 우클릭 기능

'조직도'의 빈 공간을 우클릭하면 아래와 같은 메뉴가 출력됩니다. 관리자는 각각의 메뉴로 조직도 표시 및 정렬 등을 커스터마이징(개인화)할 수 있습니다. 각 항목에 대한 설명은 다음과 같습니다. 기본적으로 실사용자는 가상사용자에 대해 우선순위로 정렬됩니다.

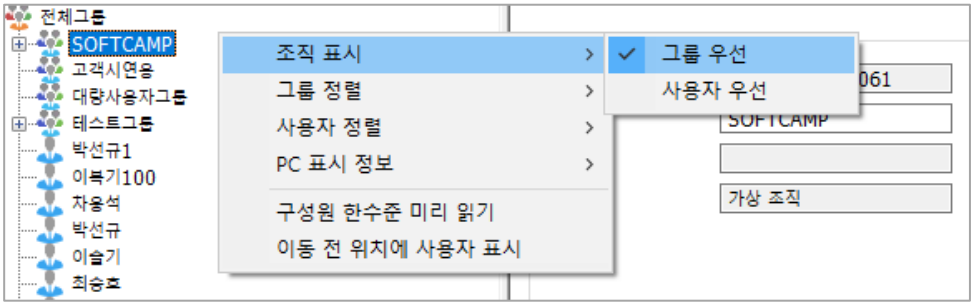


그룹표시

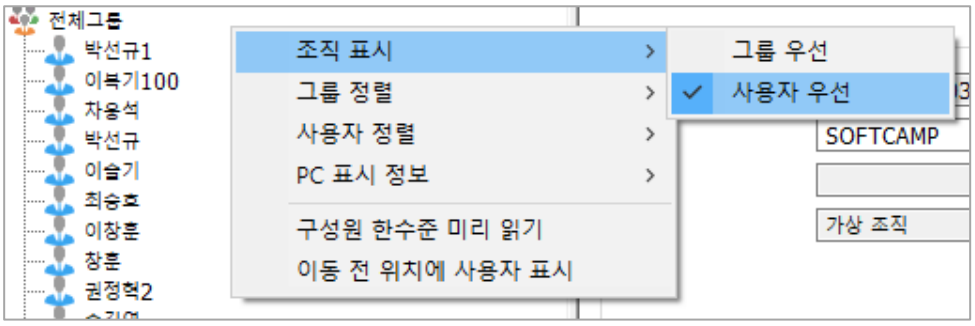
조직도 정렬의 우선순위를 그룹 우선 순이나 사용자 우선 순으로 선택할 수 있습니다.



1) **그룹 우선** : 그룹을 우선으로 정렬합니다.



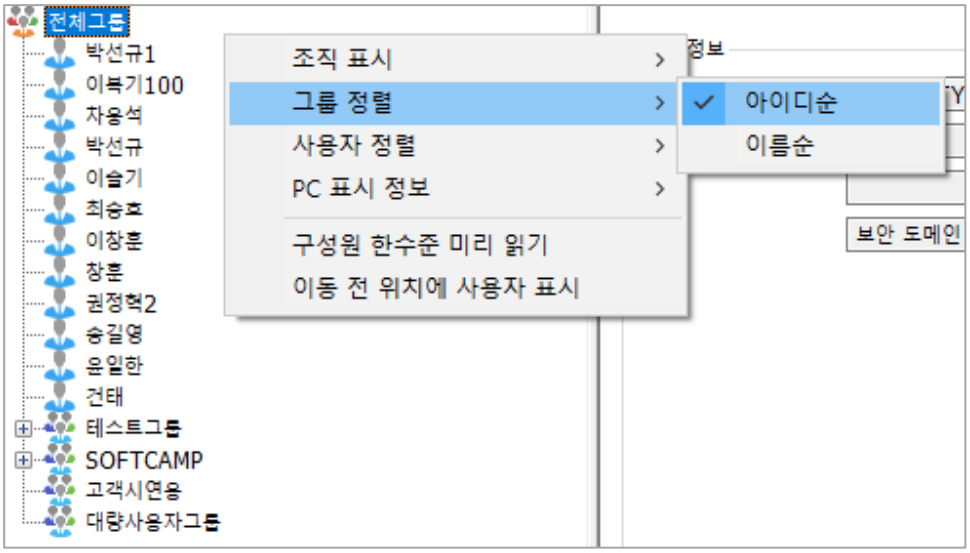
2) **사용자 우선** : 사용자를 우선으로 정렬합니다.



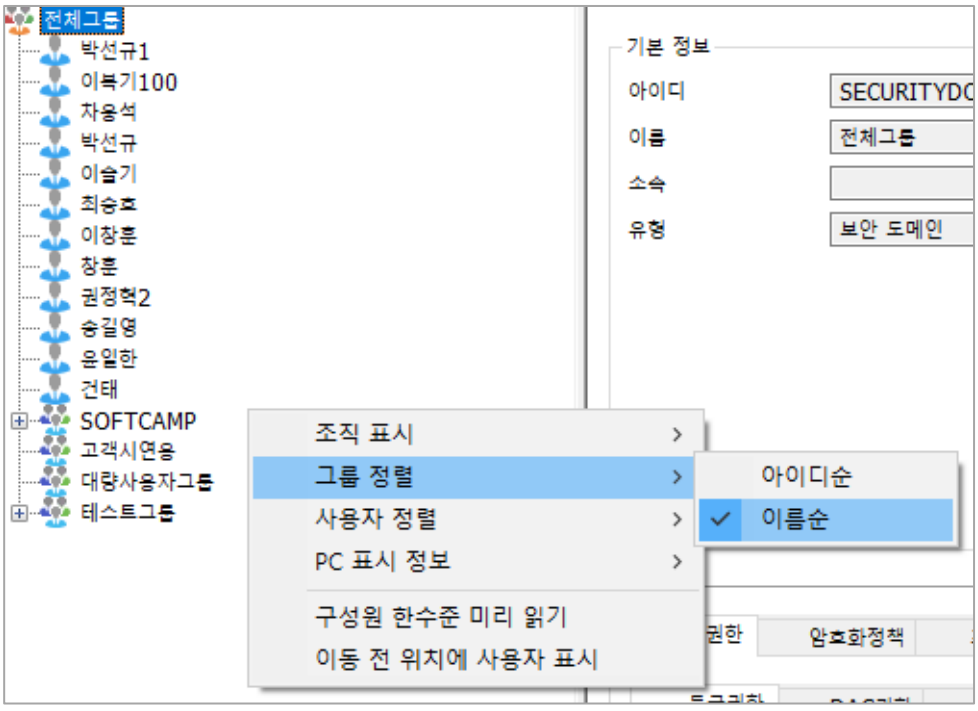
그룹정렬

그룹 정렬의 우선순위를 아이디 순이나 이름 순으로 선택할 수 있습니다. 정렬값은 인사 DB 등록 시 등록된 값을 의미합니다.

1) **아이디순** : 그룹을 아이디순으로 정렬합니다.



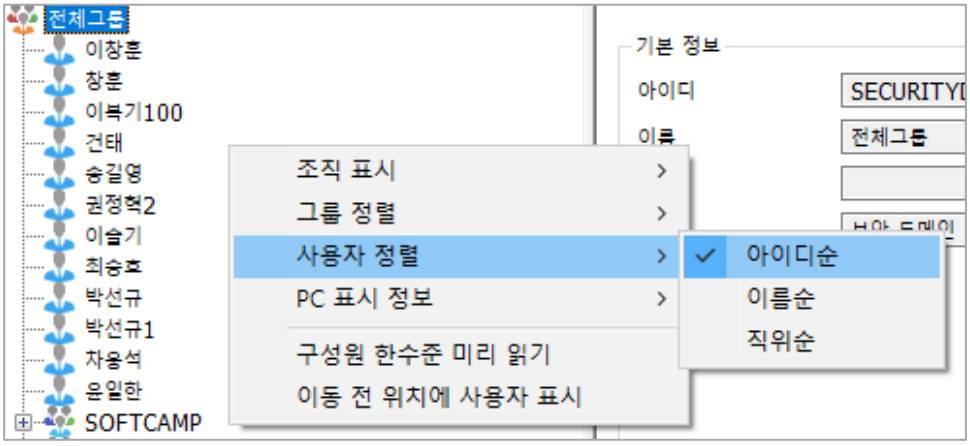
2) **이름순** : 그룹을 이름 순으로 정렬합니다.



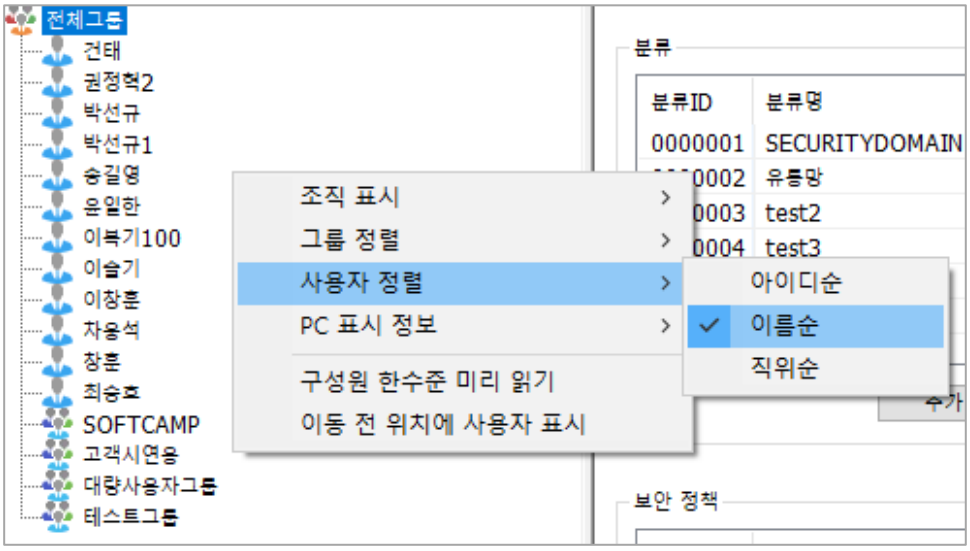
사용자정렬

사용자 정렬의 우선순위를 아이디 순이나 이름 순, 직위 순으로 선택할 수 있습니다.

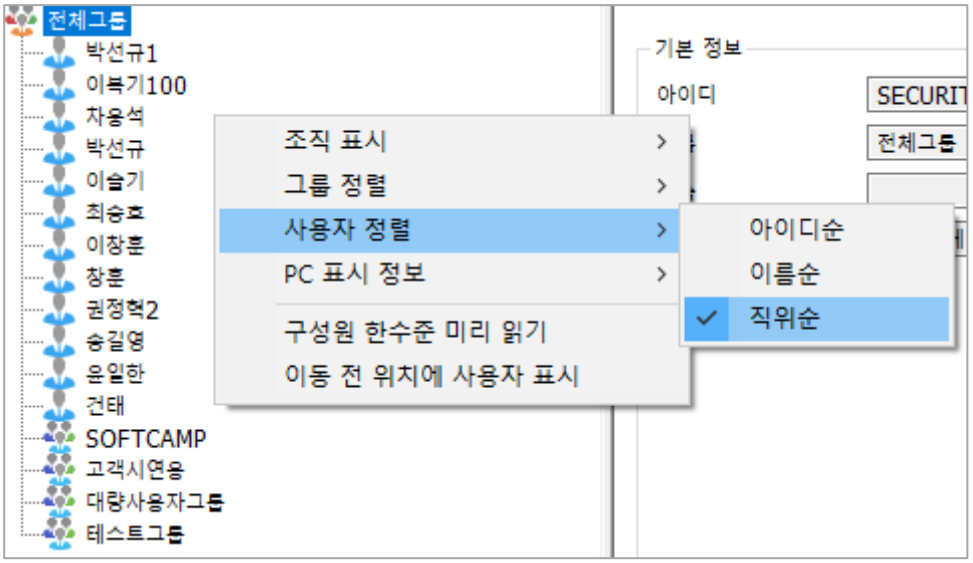
1) **아이디순** : 아이디 순으로 정렬합니다.



2) **이름순** : 이름 순으로 정렬합니다.

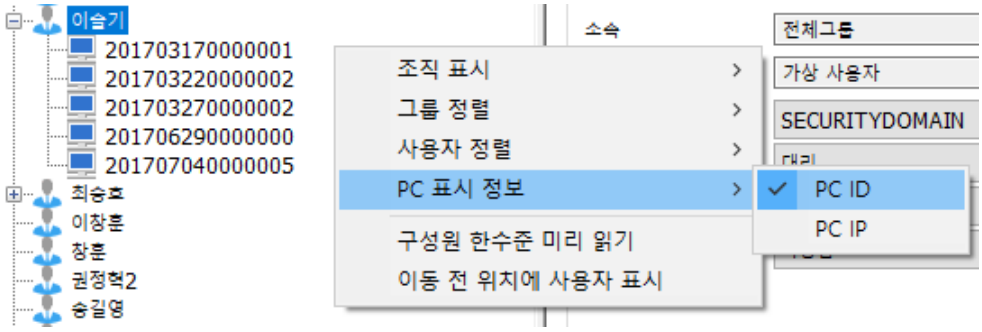


3) **직위순** : 직위 순으로 정렬합니다.



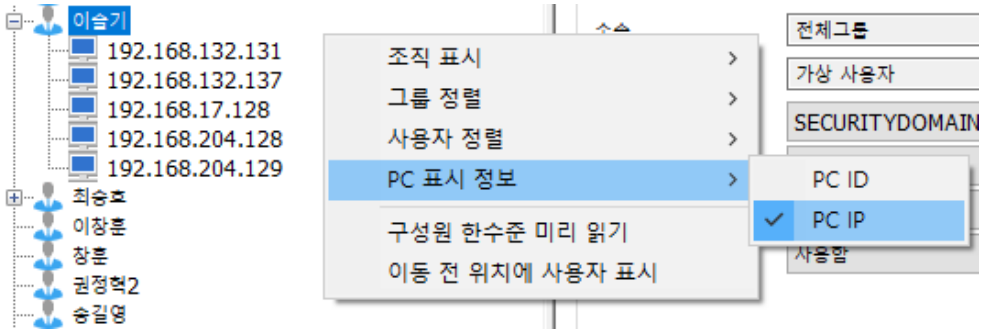
PC 표시 정보

1) **PC ID :** PC ID 를 표시합니다.



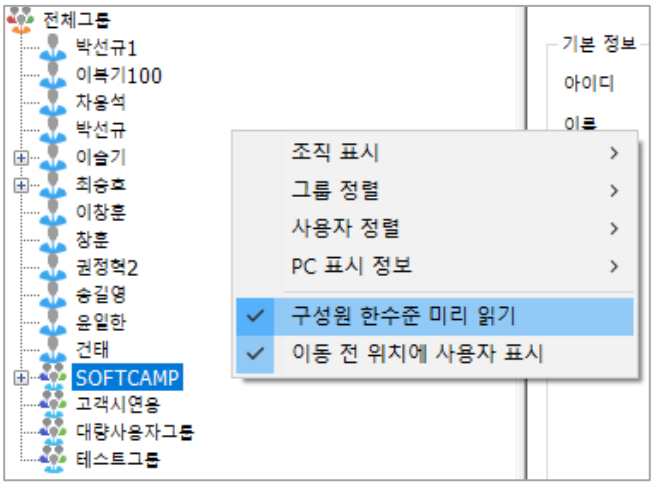
참고 : PC ID 는 자동적으로 생성되는 값입니다. PC ID 는 사용자가 Client 로 최초 로그인하는 시간값(14 자리) 그리고 동일한 시간으로 최초 로그인한 경우 PC 들을 구분하기 위한 값(1 자리)로 구성됩니다. 예로 PCID 가 201006101800220 인 경우, 이 PC 는 2010 년 6 월 10 일 18 시 00 분 22 초에 해당 사용자로 최초 로그인한 것이며, 해당 시간내에서 처음으로 등록된 PC 입니다.

2) **PC IP :** PC IP 를 표시합니다.



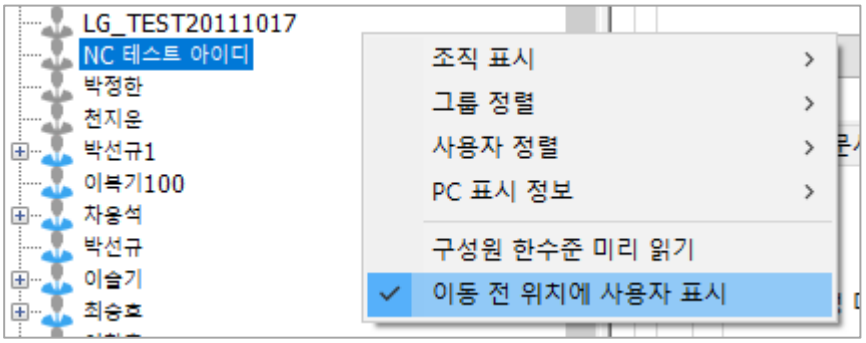
구성원 한수준 미리 읽기

조직도에서 현재 표시되는 그룹의 한 수준 아래의 구성원을 미리 읽어 그룹에 구성원이 있는 경우, 그룹 아이콘의 좌측에 '+'표시를 보여줍니다. 이 항목이 선택되지 않은 경우, 관리자가 조직도에서 그룹 선택 시 선택한 그룹의 한 수준 아래 구성원(그룹이나 사용자)은 표시되지만, 이 하위 그룹 아래 또 다른 구성원이 존재하는지에 대해서는 '+' 표시를 미리 보여주지 않습니다. 그룹의 구성원을 한 수준을 미리 읽어오는 것은 해당 그룹을 검색할 시 바로 리스트가 표시되는 장점이 있지만, 많은 그룹을 한꺼번에 표시할 때는 불필요한 리스트까지 읽어오는 현상으로 오히려 시스템이 느려질 수 있습니다.



이동 전 위치에 사용자 표시

이는 Console 상에서만 사용자 위치를 이동시킨 경우, 인사 DB 상의 사용자 위치 정보와 Console 상의 사용자 위치 정보가 서로 다름을 관리자에게 확인시켜주기 위한 기능입니다. 사내 그룹, 사내 사용자, 사외 그룹, 사외 사용자의 위치를 Console 에서 이동하였을 시, 이동 전 위치(인사 DB 상의 위치)에 사용자를 표시합니다. 이동 전 사용자의 아이콘은 회색으로 표시되며, 이동된 사용자의 아이콘은 정상적으로 표시됩니다.



10.3. 그룹 관리

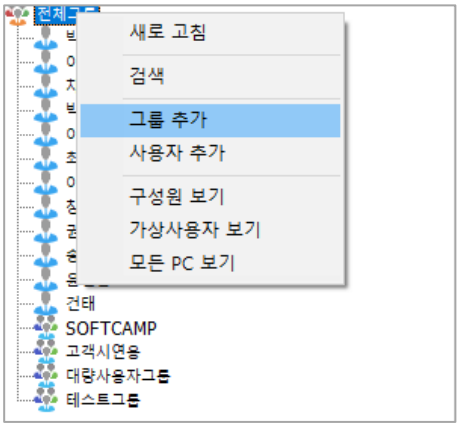
인사 DB 연동 시 관리자는 Console 조직도에서 인사 DB 에 등록된 사내/외 그룹 및 사용자를 확인할 수 있습니다.

관리자는 '**그룹 추가**', '**그룹 삭제**' 메뉴를 통하여 또 다른 그룹을 추가하거나 삭제할 수 있습니다. 이 그룹은 '가상 그룹'으로써 Server DB 에만 존재할 뿐 인사 DB 에는 등록되지 않습니다. 그리고 이 그룹은 상위 그룹의 속성을 그대로 따릅니다.

그룹 추가

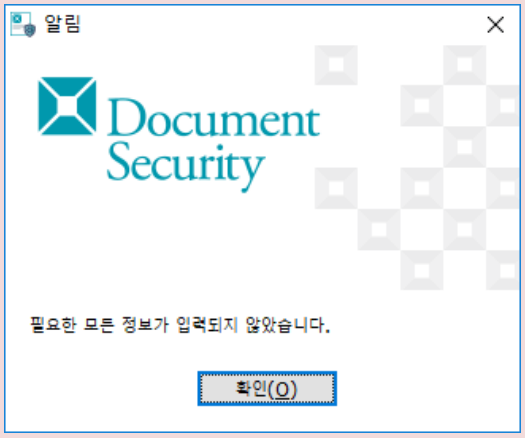
관리자는 **'그룹 추가'** 메뉴를 통하여 **'가상 그룹'**을 추가할 수 있습니다. 사용 방법은 다음과 같습니다.

1) 조직도 상에서 추가하고 싶은 그룹의 상위 그룹을 선택한 후 마우스 오른쪽 클릭으로 표시되는 메뉴에서 **'그룹 추가'**를 선택합니다.

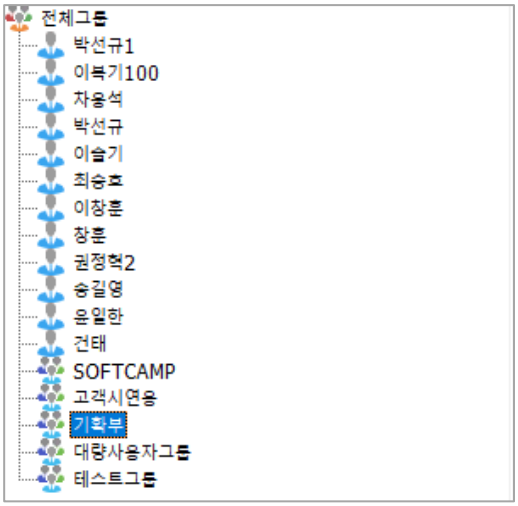


2) **<그룹 추가>** 창에서 **'그룹 정보'**의 **'이름'** 란에 그룹명을 입력 후 **[확인]**을 클릭합니다. 이때 그룹명은 반각 50 문자까지 입력할 수 있습니다.

주의 : 아무것도 입력하지 않고 [OK]를 누르면, 다음과 같은 메세지가 표시되고, 그룹 추가를 할 수 없습니다.



3) 다음과 같이 새로운 그룹이 추가됩니다.



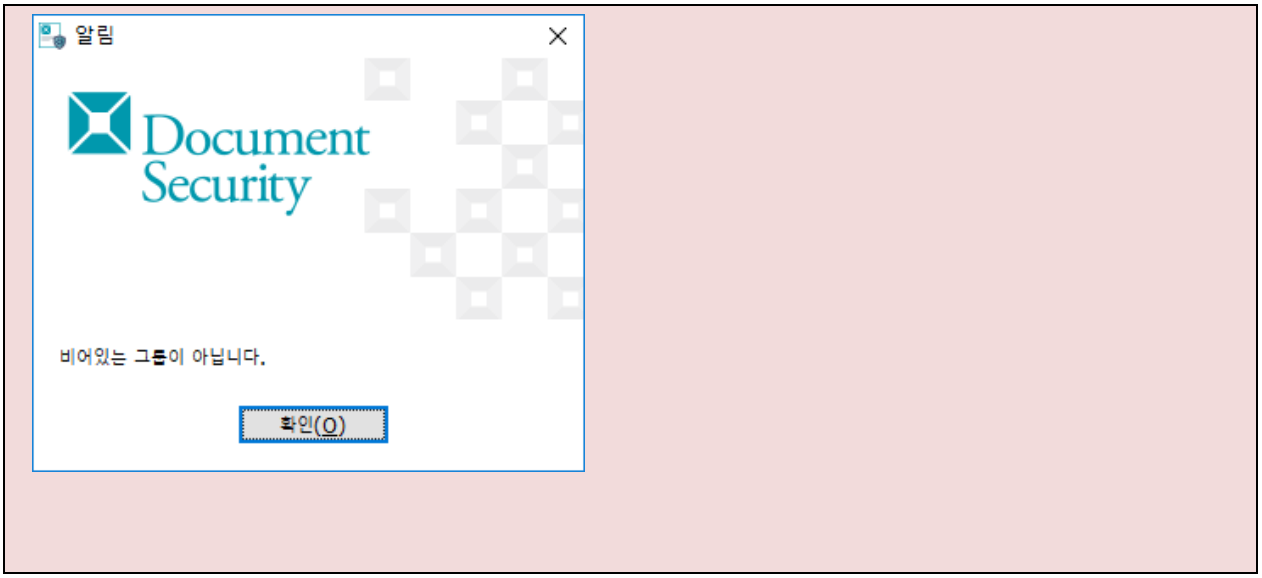
참고 : 그룹 추가 시 최초 권한은 추가 직전 선택되어진 상위 그룹 또는 사용자의 권한을 동일하게 반영합니다.

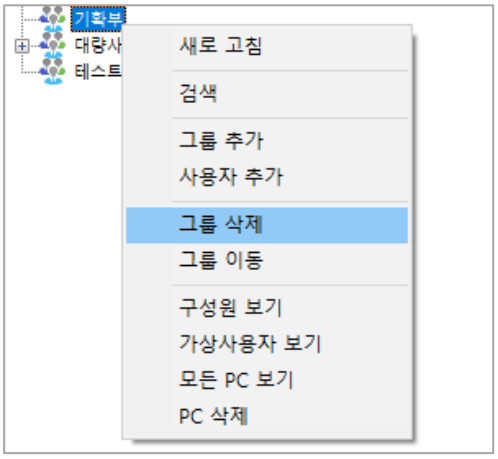
그룹 삭제

'그룹 삭제'는 조직도 관리를 위해 그룹을 삭제하는 매뉴입니다. 사용 방법은 다음고 같습니다.

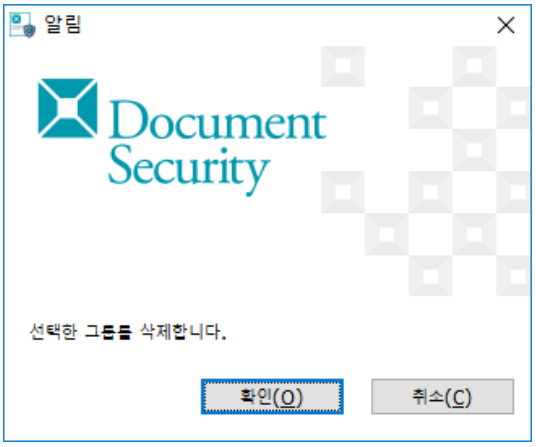
1) 조직도 상에서 삭제하고 싶은 그룹을 선택한 후 마우스 오른쪽 클릭으로 표시되는 매뉴에서 **'그룹 삭제'**를 선택합니다.

주의 : 삭제하는 그룹의 하위에 유저가 있으면 그룹은 다음과 같은 애러 메시자가 표시되며 삭제되지 않습니다. 그룹 삭제를 실행하기 전에 유저를 삭제, 또는 이동을 먼저 실행해야 합니다.





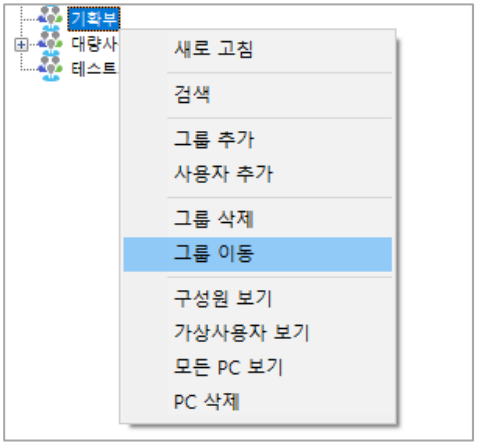
2) **[확인]을** 클릭하여 그룹 삭제를 완료합니다.



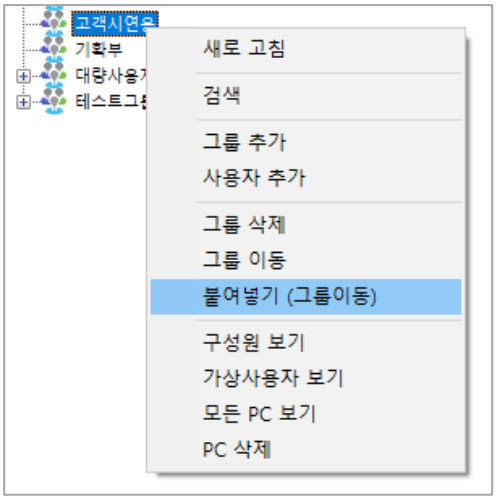
그룹 이동

'그룹 이동'은 조직도 관리를 위해 그룹을 이동하는 매뉴입니다. 사용 방법은 다음고 같습니다.

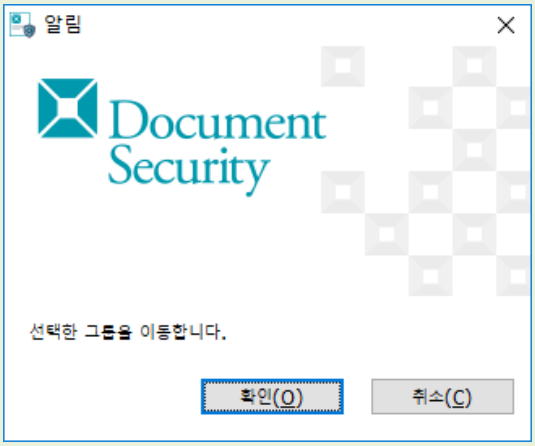
1) 조직도 상에서 이동시키고 싶은 그룹(대상 그룹)을 선택 후 마우스 오른쪽 클릭으로 표시되는 메뉴에서 **'그룹 이동'**을 선택합니다.



2) 이동할 그룹(대상 그룹을 위치시키고자 하는 상위 그룹)을 선택한 후 마우스 오른쪽 클릭으로 **'붙여넣기 (그룹이동)'**을 선택하여 이동을 완료합니다.



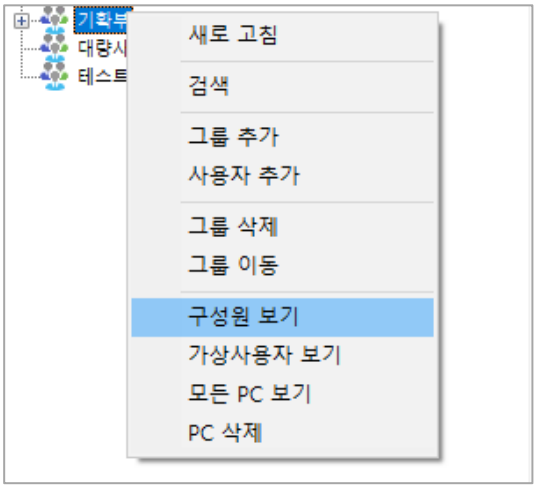
참고 : 그룹을 드래그&드롭하여 이동시킬 수도 있습니다. 그룹을 클릭한 채로 위치시키고자 하는 그룹에 드롭하면, 아래와 같은 알림창이 나타납니다. [확인]을 클릭하면 그룹 이동이 완료됩니다.



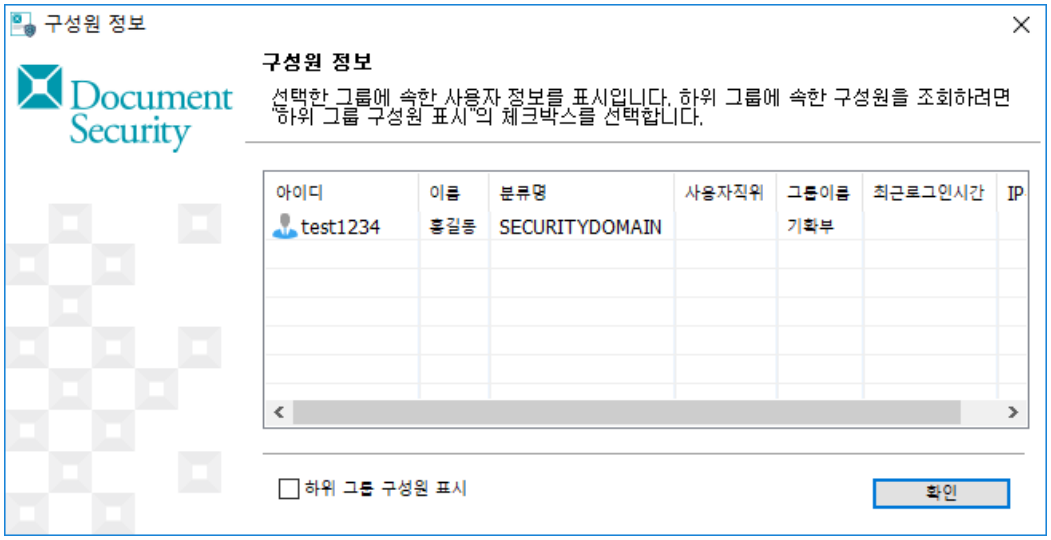
구성원 표시

'구성원 표시'는 조직도의 그룹에 속해있는 구성원을 리스트 형태로 보기 위한 매뉴입니다. 사용 방법은 다음고 같습니다.

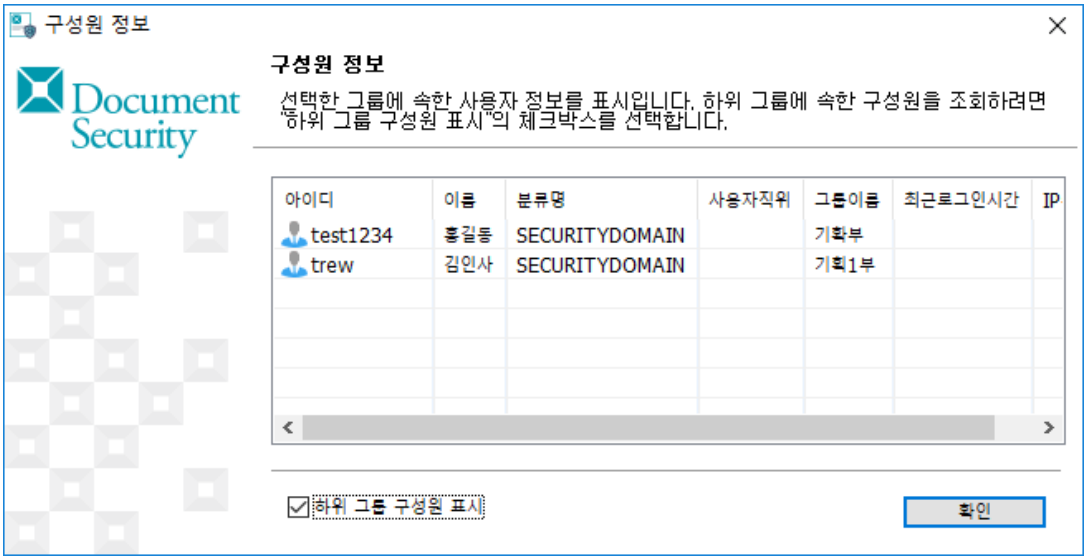
1) 조직도 상에서 구성원을 검색할 그룹을 선택한 후 마우스 오른쪽 클릭으로 표시되는 매뉴에서 **'구성원 보기'**를 선택합니다.



2) **<구성원 정보>**화면에서 선택한 그룹에 속한 사용자 정보를 볼 수 있습니다.



3) **'하위 그룹 구성원 표시'**를 선택한 경우, 해당 그룹의 하위 그룹에 속하고 있는 사용자까지 모두 표시됩니다.

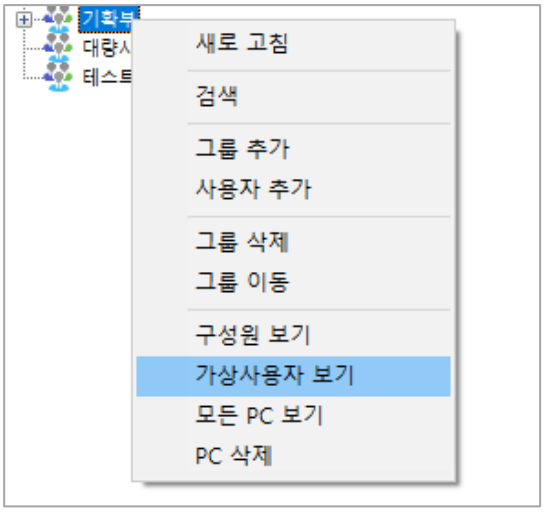


가상 사용자 표시

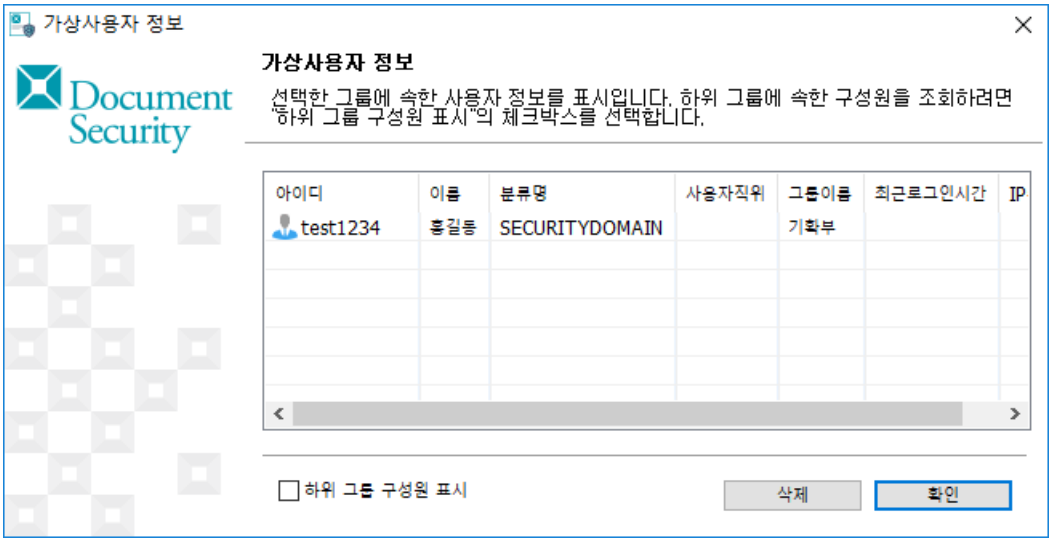
'가상사용자 표시'는 그룹에 속해있는 구성원 중 **'가상사용자'**만을 리스트 형태로 보기 위한 메뉴입니다. 사용 방법은 다음과 같습니다.

참고 : 가상 사용자는 관리자가 조직도에서 직접 '사용자 추가' 메뉴를 사용하여 생성한 사용자를 말합니다. 가상 사용자는 DS 를 도입한 기업이나 기관의 인사 DB 에 포함되지 않는 사용자를 의미합니다.

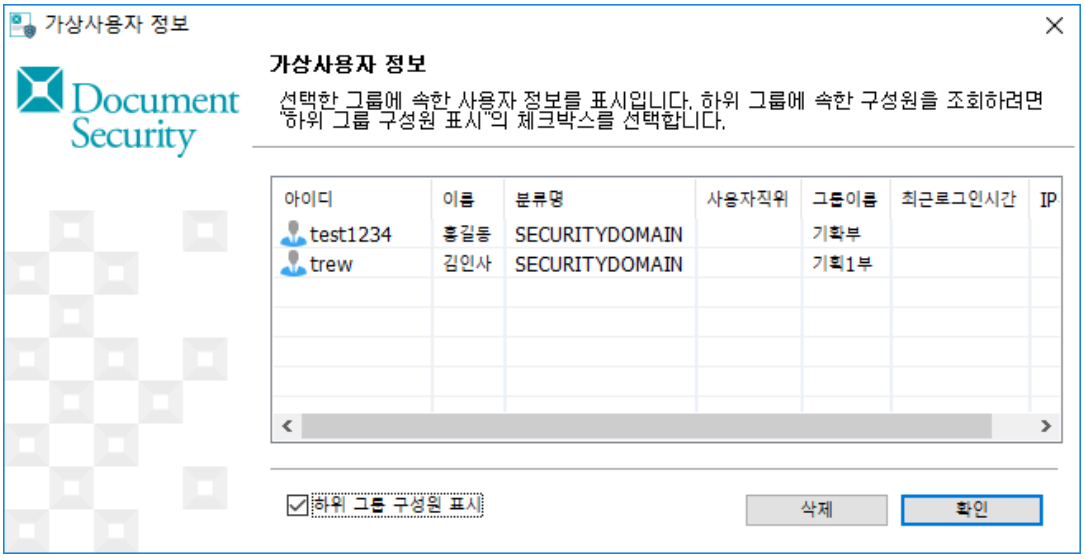
1) **'가상사용자'**를 보기 위한 그룹을 선택한 후 마우스 오른쪽 클릭으로 표시되는 메뉴에서 **'가상사용자 보기'**를 선택합니다.



2) <**가상사용자 정보**>창에서 선택한 그룹에 속한 가상사용자 정보를 볼 수 있습니다.



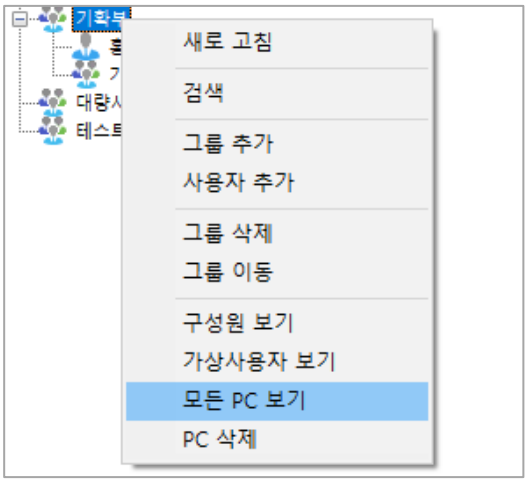
3) '**하위 그룹 구성원 표시**'를 선택한 경우, 해당 그룹의 하위 그룹에 속한 가상사용자까지 모두 표시됩니다.



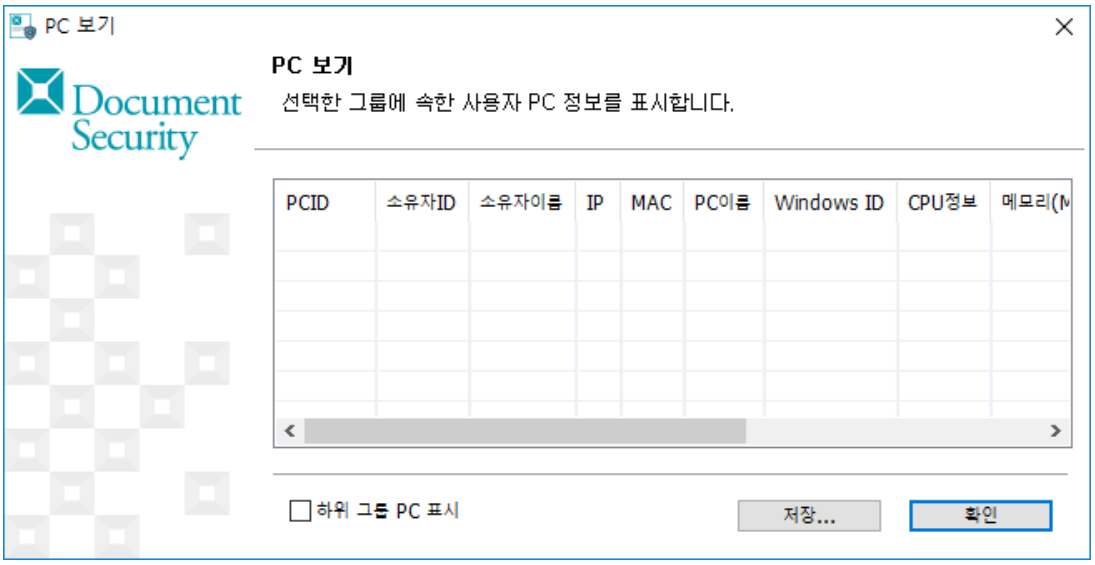
모든 PC 보기

'모든 PC 보기'는 조직도의 그룹에 속해있는 PC 를 리스트 형태로 보기 위한 메뉴입니다. 사용 방법은 다음과 같습니다.

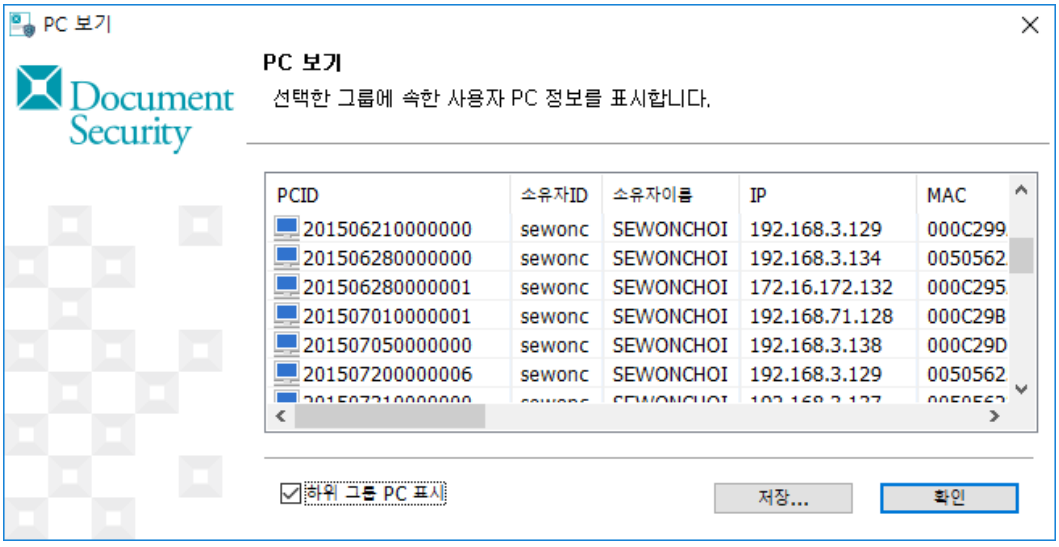
1) PC 리스트를 보기 위한 그룹을 선택한 후 마우스 오른쪽 클릭으로 표시되는 메뉴에서 **'모든 PC 보기'**를 선택합니다.



2) **<PC 보기>**창에서 선택한 그룹에 속한 사용자의 PC 정보를 볼 수 있습니다.



3) '**하위 그룹의 PC 표시**'를 선택한 경우, 해당 그룹의 하위 그룹에 속한 사용자의 PC 정보까지 모두 표시됩니다.



10.4. 사용자 관리

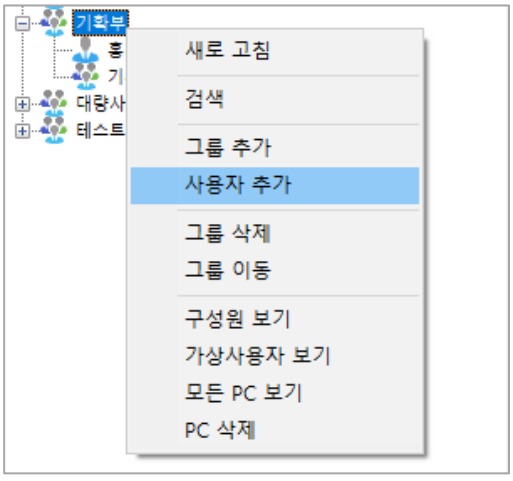
본 장은 사용자 추가/삭제/변경 등 사용자 관리 기능에 대해 설명합니다.

사용자 추가

관리자는 **'사용자 추가'** 매뉴를 이용하여 **'가상 사용자'**를 추가 및 관리할 수 있습니다. **'가상 사용자'**는 인사 DB 에 등록되기 이전의 사용자, 또는 임시로 특정 사용자에게 DS 사용 권한이 필요할 시 사용합니다.

참고 : 사용자를 추가한 후 동일한 프로파일을 사용자를 인사 DB 에 추가하였을 시 '가상 사용자'는 '일반 사용자'로 자동 전환됩니다.

1) 추가하려는 사용자의 소속 그룹을 선택한 선택한 후 마우스 오른쪽 클릭하여 표시되는 매뉴에서 **'사용자 추가'**를 선택합니다.



2) 추가하는 사용자의 아이디, 이름, 직위 및 비밀번호를 입력하고 **[확인]**을 클릭하여 사용자의 추가를 완료합니다.

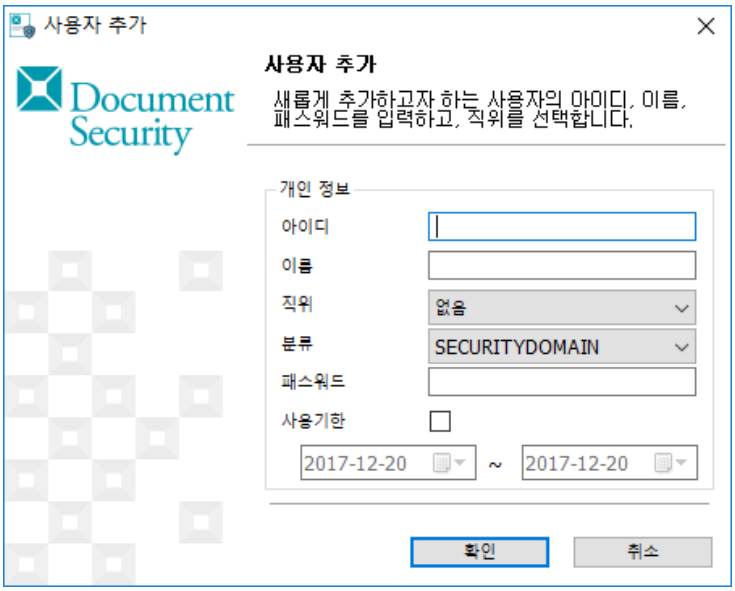
a. **아이디** : 추가하는 사용자가 사용하는 로그인 아이디를 지정합니다. ID 는 반각 20 문자까지 입력을 할 수 있습니다.

b. **이름** : 추가하는 사용자의 이름을 입력합니다. 이름은 반각 50 문자까지 입력을 할 수 있습니다.

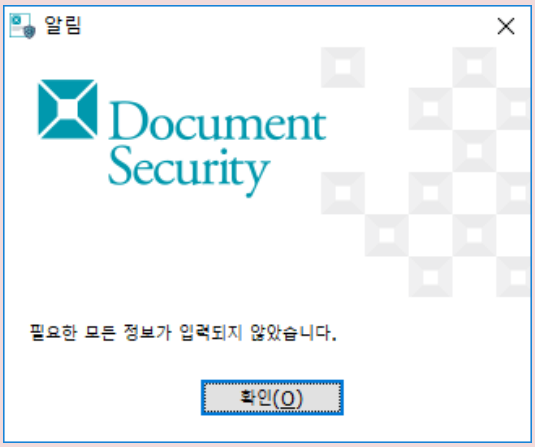
c. **직위** : 추가하는 사용자의 직위를 선택합니다. 직위는 '직위 관리'로 추가/생성/변경할 수 있습니다.

d. **비밀번호** : 추가하는 사용자가 사용할 비밀번호를 입력합니다. 비밀번호는 반각 15 문자까지 입력을 할 수 있습니다. (이때 비밀번호 생성규칙을 반드시 따릅니다.)

e. **사용기한** : 사용기한을 입력합니다.



주의 : 필요한 정보를 입력하지 않고[확인]을 클릭하면 다음과 같은 메세지가 표시며 사용자의 추가를 할 수 없습니다.



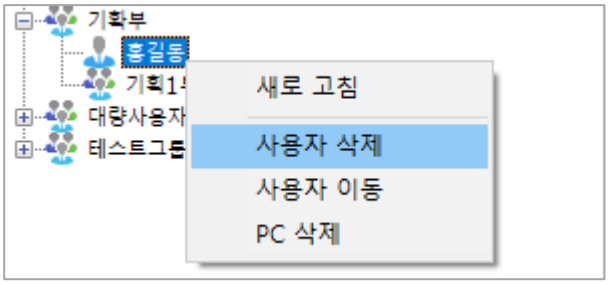
참고 : 사용자를 추가한 후 아이디와 비밀번호를 유저 본인에게 전할 때는 다른 사용자나 사외 사람에게 유출되지 않도록 주의합니다.

참고 : 사용자는 발급받은 아이디와 비밀번호로 Client 최초 접속 시 아이디와 비밀번호를 변경해야 합니다.

참고 : 사용자 추가 시 최초 권한은 추가 직전 선택되어진 상위 그룹 또는 사용자의 권한을 동일하게 반영합니다.

사용자의 삭제

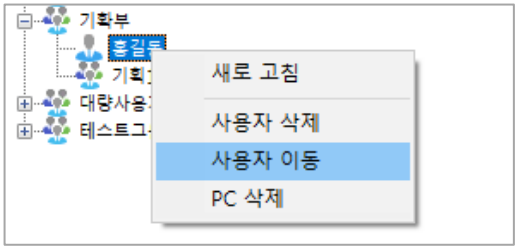
1) 삭제하려는 사용자를 선택한 선택한 후 마우스 오른쪽 클릭으로 표시되는 매뉴에서 **'사용자 삭제**를 선택합니다.



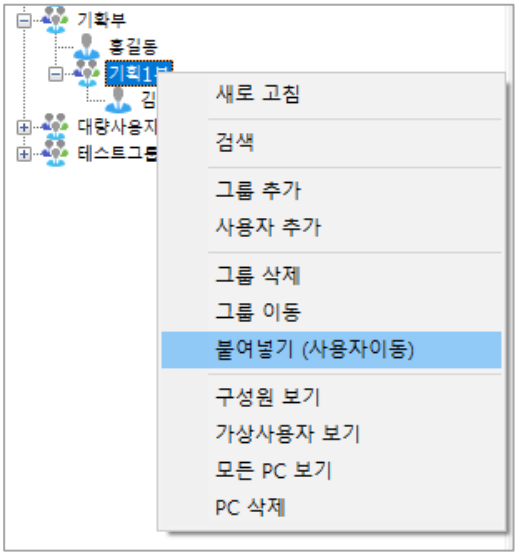
2) **[확인]**을 클릭하여 사용자 삭제를 완료합니다.

사용자 이동

1) 이동하려는 사용자를 선택한 선택한 후 마우스 오른쪽 클릭으로 표시되는 매뉴에서 **'사용자 이동'**을 선택합니다.



2) 사용자가 이동될 그룹을 선택한 후 마우스 오른쪽 클릭으로 **'붙여넣기 (사용자이동)'**를 선택하여 사용자 이동을 완료합니다.

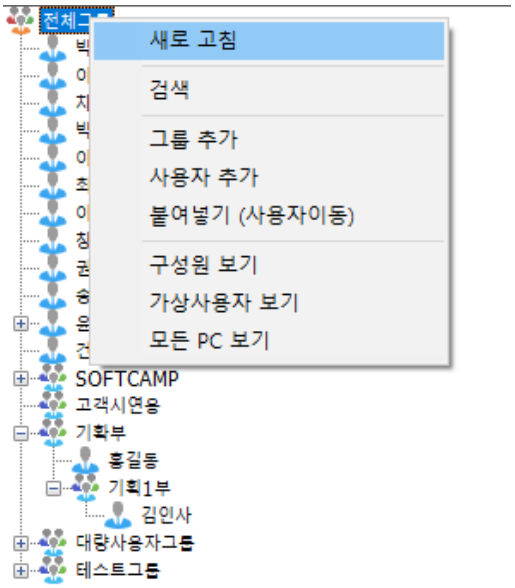


참고 : 이동하고 싶은 사용자를 드래그하여 이동할 수도 있습니다. 이동하고 싶은 유저를 선택한 채로, 이동처의 그룹에 드롭 합니다.

10.5. 새로고침

본 장은 조직도의 새로그침에 대해 설명합니다. 새로고침을 하면 조직도의 최신 정보를 불러옵니다. 사용자 추가, 삭제 등 조직도를 변경하는 작업을 하기 전에 새로 고침을 수행하기를 권장합니다.

1) 조직도의 그룹이나 사용자를 오른쪽 클릭으로 표시되는 매뉴에서 **'새로고침'**을 선택합니다.



2) 조직도가 최신 상태로 갱신됩니다.

10.6. 검색

본 장은 Console 의 검색 기능에 대해 설명합니다.

관련링크

a. 기본 검색

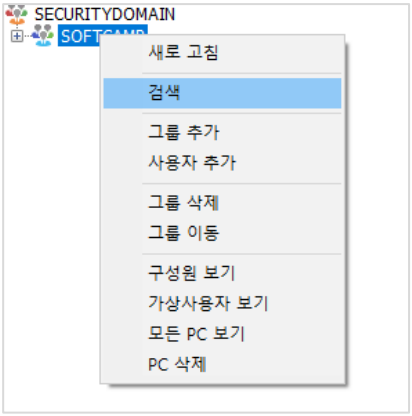
10.6.1. 기본 검색

사용자는 조직도의 **'검색'** 기능으로 그룹 또는 개인의 이름이나 아이디를 이용하여 검색을 실행할 수 있습니다. 또한 사용자의 PC 정보를 검색할 수 있습니다.

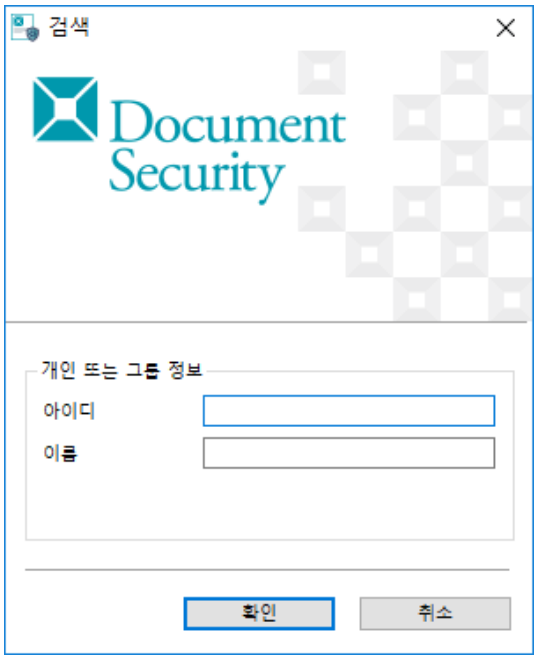
사용자 / 그룹 검색

1) 찾으려는 검색 대상 그룹을 선택한 후 오른쪽 클릭으로 표시되는 매뉴에서 **'검색'**을 선택합니다.

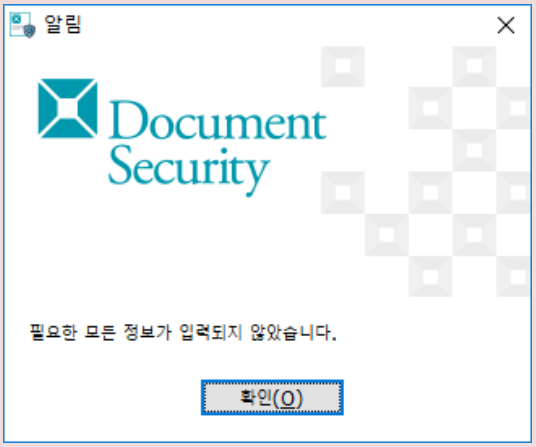
주의 : 해당 그룹에 속한 유저만 검색할 수 있습니다. 모든 유저를 대상으로 검색하고 싶은 경우는 '최상위그룹'을 선택해 검색합니다.



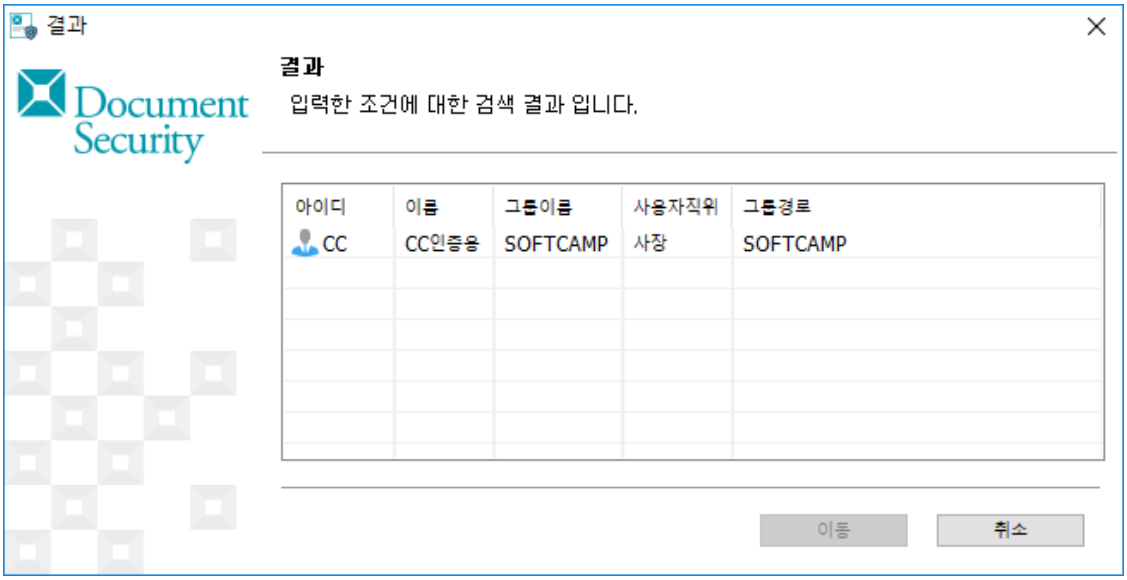
2) **'아이디'** 또는 **'이름'**을 입력한 후 **[확인]**를 눌러 사용자 또는 그룹을 검색합니다. 사용자를 검색하는 경우 사용자의 아이디 또는 이름을 입력하며, 그룹을 검색하는 경우는 그룹의 아이디 또는 그룹명을 입력합니다. 아이디는 반각 20 문자까지 이름은 반각 50 문자까지 입력할 수 있습니다.



주의 : 아무런 정보를 입력하지 않고 [확인]을 클릭하면 다음과 같은 경고 메시지가 나타납니다.



3) 검색이 완료되면 다음과 같이 결과 리스트가 표시됩니다.



4) 리스트에서 해당 사용자를 선택 후 **[이동]**을 클릭하면 Console 메인 화면의 그룹에서 해당 유저/그룹으로 이동합니다.

11. 보안 정책

본 장은 보안 정책에 대해 설명합니다.

관련링크

a. 프로파일

b. 프린트 마킹

c. 복사/붙여넣기

d. APP 제어

11.1. 프로파일

본 장에서는 사용자 및 그룹별 프로파일 설정 방법에 대해 설명합니다. 관리자가 설정할 수 있는 프로파일의 항목은 다음과 같습니다.

➢ **로그인** : 로그인 관련 정책을 설정합니다.

➢ **비밀번호** : 비밀번호의 변경 및 조합 관련의 정책을 설정합니다.

➢ **기본설정** : 프로그램 삭제 허용, 사용자 알림 메시지 사용 등을 설정합니다.

관련링크

a. 로그인 : 로그인 관련 정책을 설정합니다.

b. 비밀번호 : 비밀번호의 변경 및 조합 관련의 정책을 설정합니다.

c. 기본 설정 : 프로그램 삭제 허용, 사용자 알림 메시지 사용 등을 설정합니다.

11.1.1. 로그인

관리자는 로그인에 관련한 보안 정책을 사용자별 또는 그룹별로 지정할 수 있습니다.

1) 조직도에서 해당 **'로그인'** 정책을 변경할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>로그인'**을 선택합니다. 화면의 구성은 다음과 같습니다.

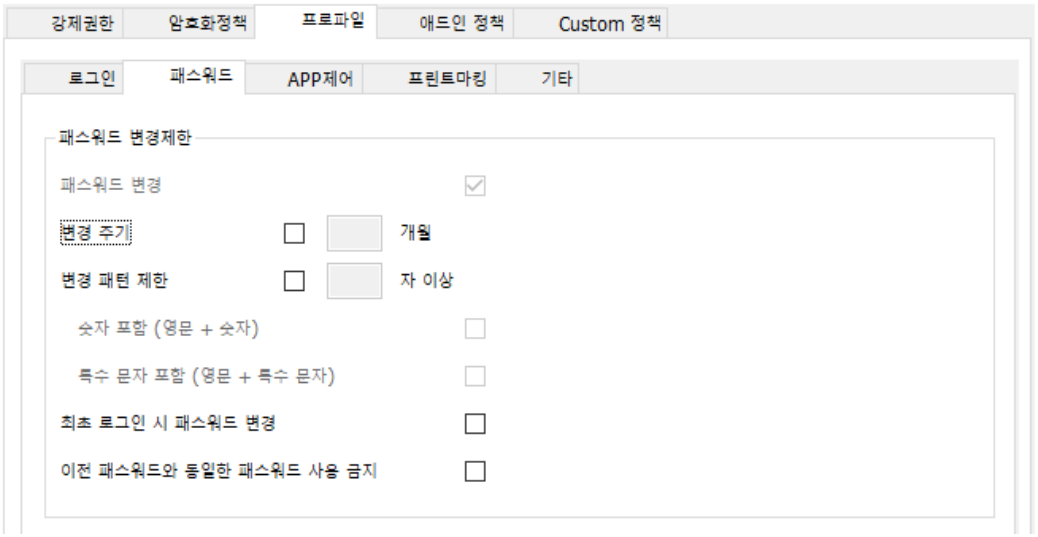
구분	내용
윈도우 시작후 문서보안 로그인 실행	윈도우가 부팅된 후 로그인창이 자동으로 나타납니다.

다중 로그인 허용	하나의 사용자 계정으로 여러개의 PC 에서 Client 를 로그인할 수 있습니다.
로그전송 실패시 강제 로그아웃	Client 에서 Server 로의 로그전송이 실패하였을 시 강제로 로그아웃을 하여 보안영역을 보호하는 기능입니다. 단, 사용자에게 오프라인로그인 권한이 있을시에는 사용자가 오프라인 로그인 후 사용이 가능합니다.
ID / PW 인증실패시 동작	- **로그아웃 :** 로그아웃 처리가 됩니다. - **재 로그인창 표시 :** 재 로그인창이 표시됩니다.

11.1.2. 비밀번호

관리자는 사용자의 비밀번호에 관한 보안정책을 사용자별 또는 그룹별로 지정할 수 있습니다.

1) 조직도에서 해당 **'비밀번호'** 정책을 변경할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>비밀번호'**를 선택합니다. 화면의 구성은 다음과 같습니다.



구분	내용
비밀번호 변경	사용자가 임의로 비밀번호를 변경할 수 있는 권한을 줍니다.
변경 주기	체크박스를 선택한 후 주기를 '**개월**' 단위로 입력하면, 주기적으로 비밀번호를 강제 변경하도록 설정할 수 있습니다.
변경 패턴 제한	로그인 비밀번호의 변경 시 조합의 규칙을 결정할 수 있습니다. • **체크박스** : 패스우드의 변경 패턴에 대한 강화된 제약을 설정할 수 있습니다. 구체적으로 ✓아이디와 같은 비밀번호 입력 차단합니다. ✓3 글자 이상 연속된 숫자/영문자 입력을 차단합니다(오름/내림차순) ✓3 글자 이상 반복된 값의 입력을 차단합니다. • ~ 자 이상 : 비밀번호의 최소 글자수를 설정합니다. • 숫자 포함(영문 + 숫자) : 영문과 숫자를 포함하는 값 만을 허용합니다. • 특수 문자 포함(영문 + 특수문자) : 특수문자를 포함하는 값 만을 허용합니다.
최초 로그인 시 비밀번호 변경	사용자가 최초 로그인 시 비밀번호를 변경하도록 설정합니다.

이전 비밀번호와 동일한 비밀번호 사용 금지	사용자가 비밀번호 변경 시 이전의 비밀번호와 같은 비밀번호로의 변경을 차단합니다.

주의 : 숫자 포함, 특수 문자 포함, 최초 로그인 시 비밀번호 변경은 최초 설치 시 디폴트(Default)로 활성화되어 있습니다.

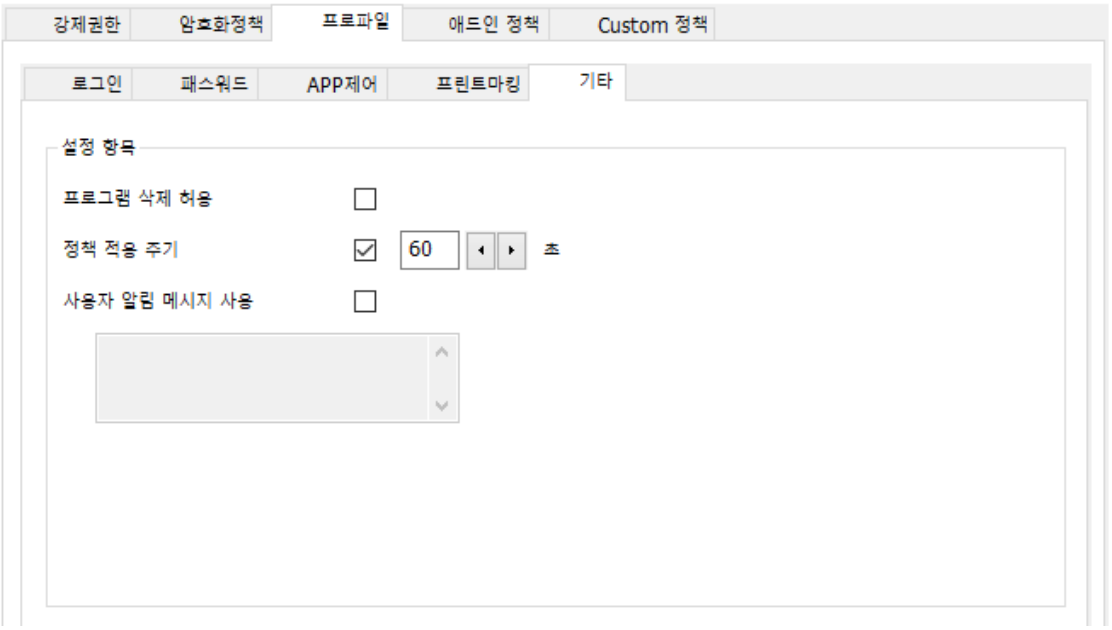
참고 : '변경 패턴 제한' 항목을 체크한 경우, 사용자가 비밀번호 변경 시 3 글자 이상의 오름/내림차순 문자열 및 반복문자열의 입력할 수 없도록 제어합니다. 따라서 이 항목을 체크한 경우, softcamp321, 111test, testdef1 등의 비밀번호로 변경할 수 없습니다.

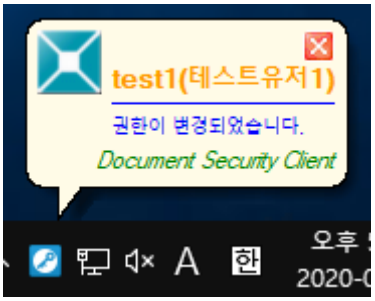
참고: 변경 패턴 제한에서 숫자 포함 (영문 + 숫자)와 특수 문자 포함 (영문 + 특수문자)를 모두 선택하면 사용자는 영문, 숫자, 특수문자를 모두 포함하는 비밀번호를 설정해야 합니다.

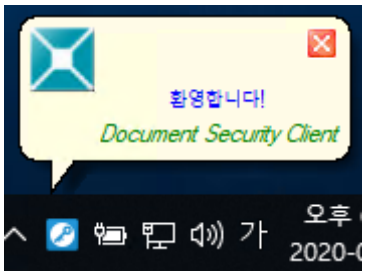
11.1.3. 기본설정

관리자는 사용자별 또는 그룹별로 DS 의 삭제 권한과 사용자가 로그인 시 사용자 알림 메시지등을 설정할 수 있습니다.

1) 조직도에서 해당 **'기본설정'** 정책을 변경할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>기타'**를 선택합니다. 화면의 구성은 다음과 같습니다.

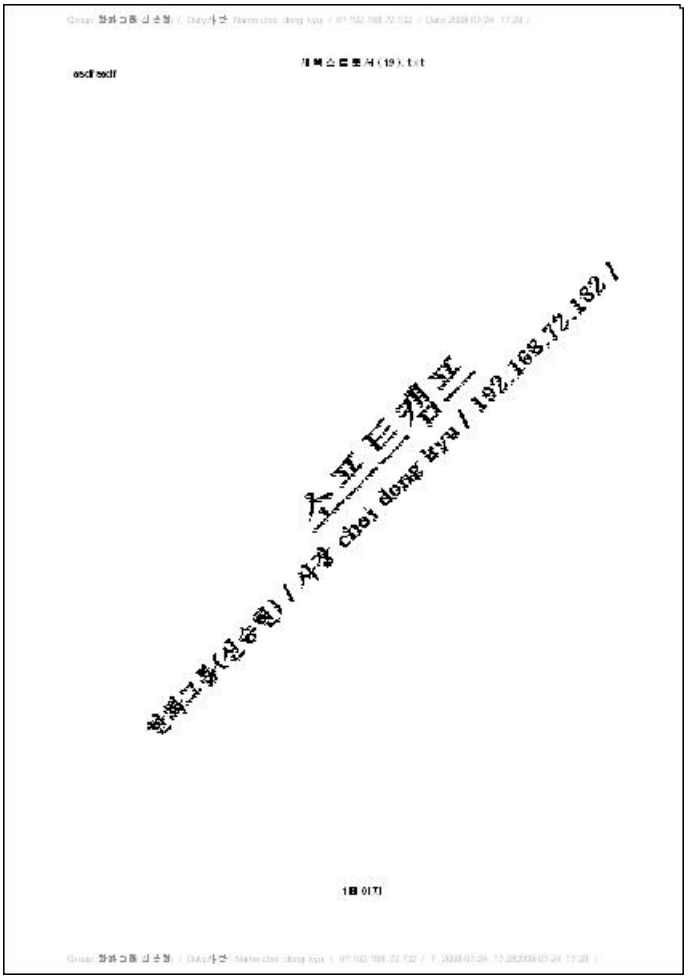


구분	내용
프로그램 삭제 허용	사용자가 Client 를 삭제할 수 있는 권한을 줍니다.
정책 적용 주기	Client 가 Server 로부터 정책을 적용받는 주기를 설정할 수 있습니다. 정책이 변경된 경우, 사용자가 정책을 적용받을 때 사용자의 Client 트레이 아이콘 상단에 아래와 같은 메시지가 표시됩니다. 

사용자 알림 메시지 사용	사용자가 Client 로그인 시 트레이 아이콘에 메세지를 표시할 수 있습니다. 메세지는 총 256 자까지 가능합니다. (예를 들어 관리자가 '환영합니다.'라는 메시지를 입력한 경우, 사용자 로그인 시 아래와 같은 메시지가 표시됩니다.) 

11.2. 프린트 마킹

본 장은 프린트 마킹에 대해 설명합니다. 프린트 마킹은 사용자가 보안문서나 일반문서 출력 시에 인쇄물에 삽입되는 이미지나 문자열을 의미합니다. 프린트 마킹을 통해 인쇄한 사람의 신원, 회사 등의 정보를 알 수 있습니다. 프린트 마킹은 아래와 같이 나타납니다.



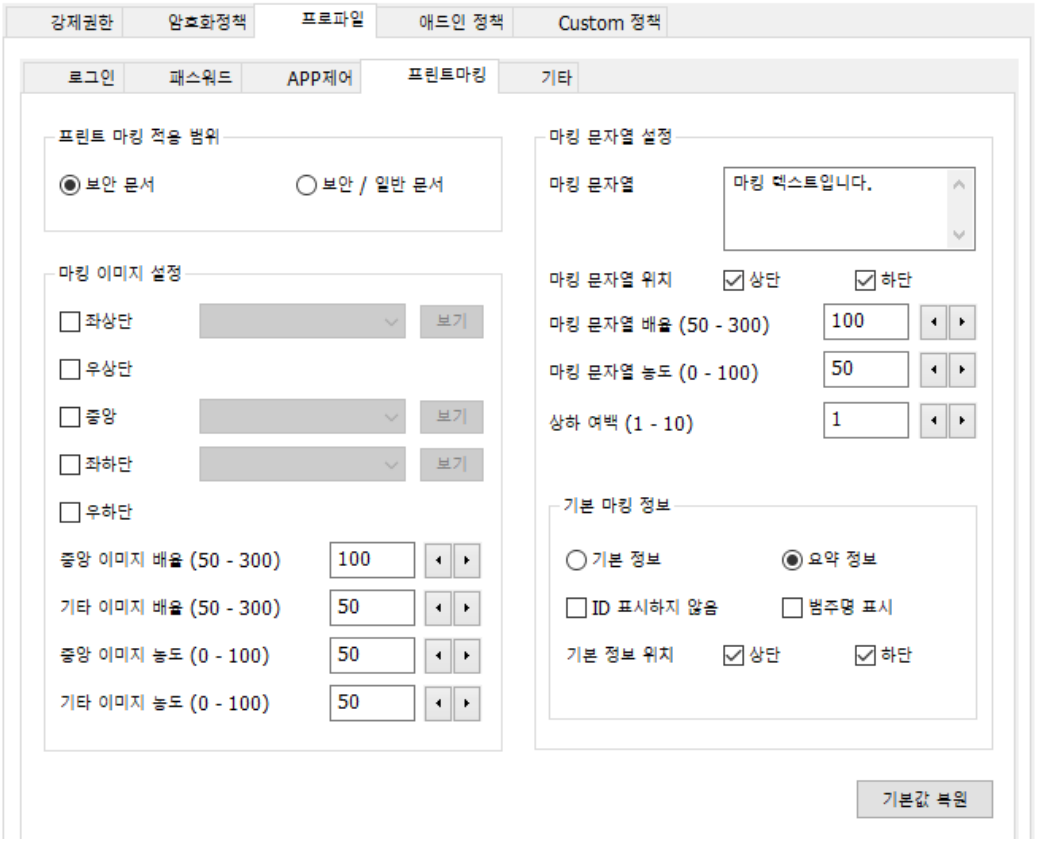
관련링크

a. 개인/그룹별 마킹 설정

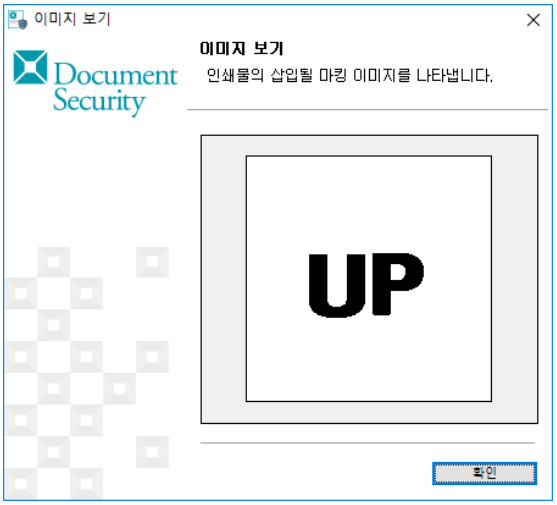
11.2.1. 개인/그룹별 마킹 설정

관리자는 보안문서 또는 일반문서에 삽입할 프린트 마킹의 위치, 내용, 농도 등을 설정할 수 있습니다.

1) 조직도에서 해당 **'프린트 마킹'** 정책을 변경할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>프린트마킹'**을 선택합니다. 화면의 구성은 다음과 같습니다.



구분		내용
프린트 마킹 적용 범위	**보안 문서**	보안문서에만 프린트 마킹을 삽입합니다.
	보안 / 일반 문서	보안문서와 일반문서 모두 프린트 마킹을 삽입합니다.
마킹 이미지 설정	**좌상단**	인쇄용지를 기준으로 각각의 위치를 설정합니다.
	우상단	채크박스를 선택 후 각각의 이미지는
	중앙	**'마킹이미지관리'**에서 등록된 이미지를 대상으로 풀다운
	좌하단	매뉴에서 선택 및 **'보기'** 버튼을 통해 확인할 수

	우하단	있습니다. '**보기**'를 클릭하면 아래와 같은 창이 표시됩니다. 
	중앙 이미지 배율 (50 - 300) **기타 이미지 배율 (50 - 300)** **중앙 이미지 농도 (0 - 100)** **기타 이미지 농도 (0 - 100)**	각각의 이미지에 대한 배율과 농도를 설정합니다. 배율은 '50: 축소 -> 300: 확대' 를 타나내며, 농도는 '0:연함->100:진함'을 나타냅니다. 각각의 설정값은 프린터의 종류 및 각각의 드라이버에 따라 그 기준이 달라질 수 있습니다.
마킹 문자열 설정	**마킹 문자열**	마킹 이미지에 사용될 문자를 입력합니다. **주의: 마킹 문자열을 표시하고 싶은 경우는, 마킹 문자열 위치(상단, 하단)을 설정할 필요가 있습니다.**
	마킹 문자열 위치	입력된 문자열에 대한 마킹 이미지의 위치를 설정합니다.
	마킹 문자열 배율 (50 - 300) **마킹 문자열 농도 (0 - 100)** **상하 여백 (1 - 10)**	입력된 마킹 문자열에 대한 배율, 농도, 여백을 설정합니다.
	기본 정보 / 요약 정보	출력 정보의 표시에 대한 설정입니다.

기본 마킹 정보		**기본 정보 :** • 이름: 김이박/사원 번호: 12345678/부서: 영업본부 **요약 정보 :** • 김이박/12345678/영업본부)
	ID 표시하지 않음	ID 표시 여부를 설정합니다.
	범주명 표시	범주 보안문서일 경우, 범주명을 표시합니다.
	기본 정보 위치	상단과 하단을 선택할 수 있습니다. **주의: 기본 마킹 정보를 표시했을 경우는, 기본 마킹 위치(상단, 하단)의 설정을 실시할 필요가 있습니다.**

참고: 보안문서 프린트 마킹 설정 시 [기본값 복원]을 클릭하면 아래와 같이 설정됩니다.

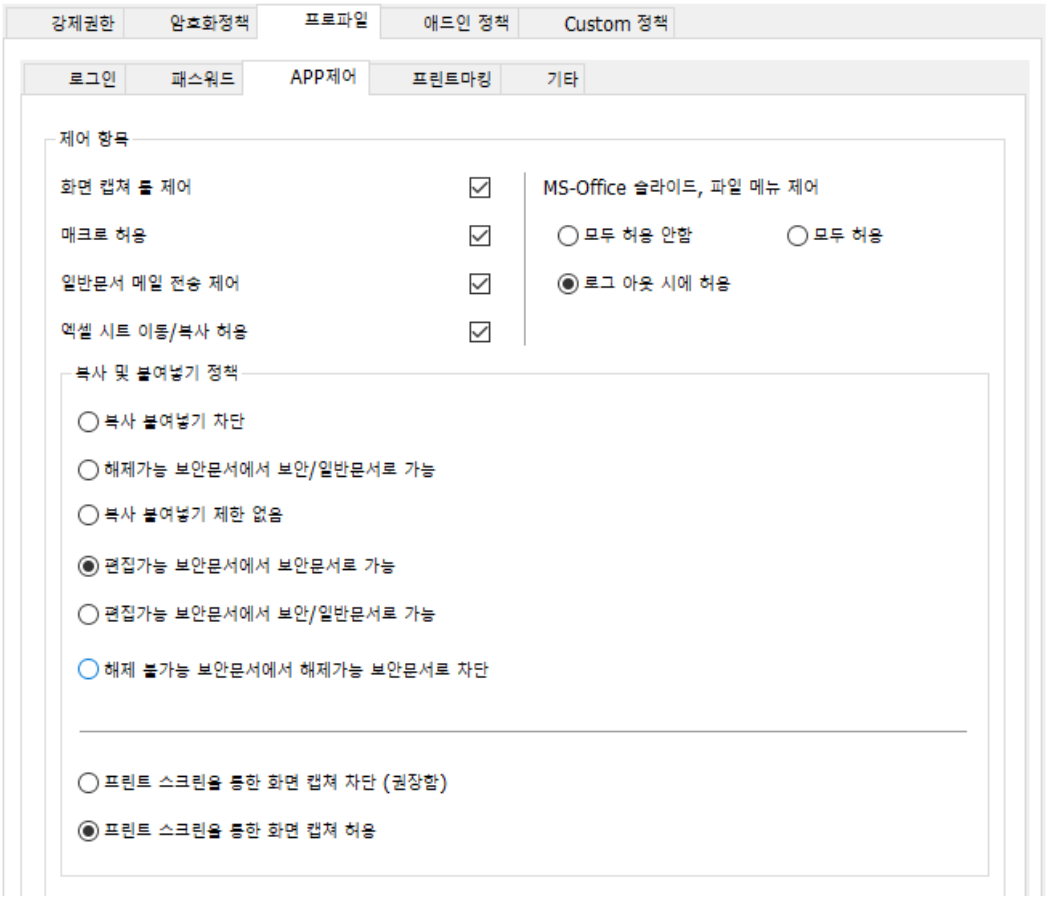
구분		기본값
프린트 마킹 적용 범위	**보안 문서** **보안 / 일반 문서**	보안 문서
마킹이미지 설정	**좌상단**	체크안함
	우상단	체크안함
	중앙	체크안함
	좌하단	체크안함
	우하단	체크안함
	중앙 이미지 배율	100
	기타 이미지 배율	50
	중앙 이미지 농도	50
	기타 이미지 농도	50

마킹 문자열 설정	**마킹 문자열**	
	마킹 문자열 위치	상단, 하단 모두 체크안함
	마킹 문자열 배율	100
	마킹 문자열 농도	50
	상하 여백	1
기본 마킹 정보	**기본 정보 요약 정보**	요약정보
	ID 표시하지 않음	체크안함
	범주명 표시	체크안함
	기본 정보 위치	상단, 하단 모두 체크안함

11.3. 복사/붙여넣기

본 장은 복사 붙여넣기 정책 설정에 대해 설명합니다. 관리자는 보안문서 내의 내용에 대한 복사 붙여넣기 (Copy & Paste) 정책을 설정할 수 있습니다.

1) 조직도에서 **'복사 붙여넣기'** 정책을 설정할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>APP 제어'**을 선택합니다. 화면의 구성은 다음과 같습니다.



2) 다음의 항목 중에 하나를 선택합니다.

a. **복사 붙여넣기 차단** : 보안문서 내의 내용에 대한 복사 / 붙여넣기가 전부 차단됩니다.

b. **해제가능 보안문서에서 보안/일반문서로 가능** : 암호화 해제 가능한 보안문서 내의 내용에 대한 복사 / 붙여넣기가 자유롭게 허용됩니다.

c. **편집가능 보안문서에서 보안문서로 가능 (외부 전송 파일 저장기능삭제, 파일 및 폴더에 대한 복호화 메뉴 삭제됨)** : 편집/해제 가능한 보안문서 내의 내용에 대한 복사 / 붙여넣기가 보안문서에 한해 허용됩니다. 일반문서로는 붙여넣기할 수 없습니다. 단, 외부 전송 파일을 저장할 수 없고, 보안문서를 복호화할 수 없습니다.

d. **복사 붙여넣기 제한 없음** : 보안문서 내의 내용에 대한 복사 / 붙여넣기가 자유롭게 허용됩니다.

e. **편집 가능한 보안문서에서 보안문서로 가능 :** 편집/해제 가능한 보안문서 내의 내용에 대한 복사 / 붙여넣기가 보안문서에 한해 허용됩니다. 일반문서로는 붙여넣기할 수 없습니다.

f. **편집 가능한 보안문서에서 보안/일반문서로 가능 :** 편집/해제 가능한 보안문서 내의 내용의 복사 / 붙여넣기가 자유롭게 허용됩니다.

11.4. APP 제어

본 장은 Client 와 연동된 문서 편집 어플리케이션에서 제공하는 일부 기능의 사용을 제어하는 기능에 대해 설명합니다.

관련링크

a. MS Office 기능 제어

b. 프로그램 실행 제어

11.4.1. MS OFFICE 기능 제어

본 장은 MS Office 기능 제어과 관련된 정책을 설정하는 방법에 대해 설명합니다.

관리자가 사용자에 대해 설정 가능한 MS Office 기능 제어 정책은 아래와 같습니다.

a. **Microsoft Office 슬라이드 및 파일 메뉴 제어 :** MS Office Word 및 PowerPoint 에서 제공하는 일부 슬라이브 및 파일 메뉴의 사용을 차단합니다.

b. **메크로 제어 :** MS Office 에서 메크로 사용을 제어합니다.

c. **Microsoft Excel 시트 이동 / 복사 제어 :** 보안문서(엑셀 파일)에 대해 시트의 이동 및 복사를 제어합니다.

d. **보내기, 게시 기능 제어 :** Microsoft Office 에서 제공하는 '**보내기**'와 **'게시'** 기능을 제어할 수 있습니다.

MS Office 기능 제어 정책 설정 방법

1) 조직도에서 해당 **'MS Office 기능 제어'** 정책을 설정할 사용자 또는 그룹을 선택한 뒤 작업창의 탭 매뉴에서 **'프로파일>APP 제어'**을 선택합니다. 화면의 구성은 다음과 같습니다.

2) 다음의 항목을 설정합니다.

a. **매크로 허용 :** 체크하면 매크로의 사용을 차단합니다. 상세 내용은 아래의 **'매크로 제어'**를 참고하시기 바랍니다.

b. **일반문서 메일 전송 제어 :** 체크하면 Microsoft Office 에서 제공하는 '**보내기**'와 **'게시'** 기능을 제어합니다. 상세 내용은 아래의 **'보내기, 게시 기능 제어'**를 참고하시기 바랍니다.

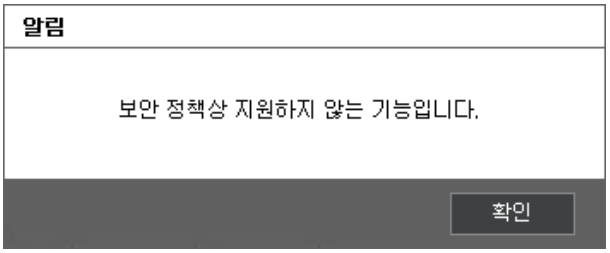
c. **엑셀 시트 이동/복사 허용 :** 체크하면 보안문서(엑셀 파일)에 대해 시트의 이동 및 복사를 제어합니다. 상세 내용은 아래의 **'Microsoft Office Excel 시트 이동 / 복사 제어'**를 참고하시기 바랍니다.

d. **MS-Office 슬라이드, 파일 메뉴 제어 : 모두 허용 안함**을 선택하면 MS Office 슬라이드 및 파일 메뉴을 제어합니다. **모두 허용**을 선택하면 MS Office 슬라이드 및 파일 메뉴을 제어하지 않습니다. **로그 아웃 시에 허용**을 선택하면 로그인 시에는 MS Office 슬라이드 및 파일 메뉴을 제어하고, 로그아웃한 상태에서는 제어하지 않습니다. 상세 내용은 아래의 **'MS Office 슬라이드 및 파일 메뉴 제어'**를 참고하시기 바랍니다.

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 있음으로 보안문서의 내용과 일반문서의 내용을 병합하여 새로운 일반문서 생성이 가능하여, 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.



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

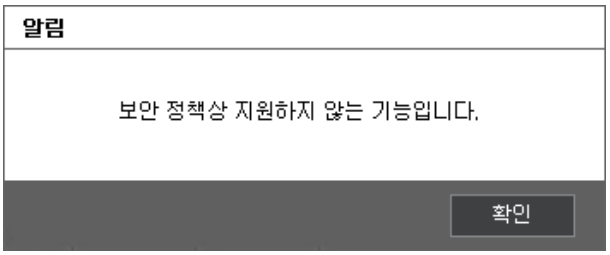
1) 게시>CD 용 패키지

2) 게시>슬라이드 게시

3) 게시>Microsoft Office Word 에서 유인물 만들기

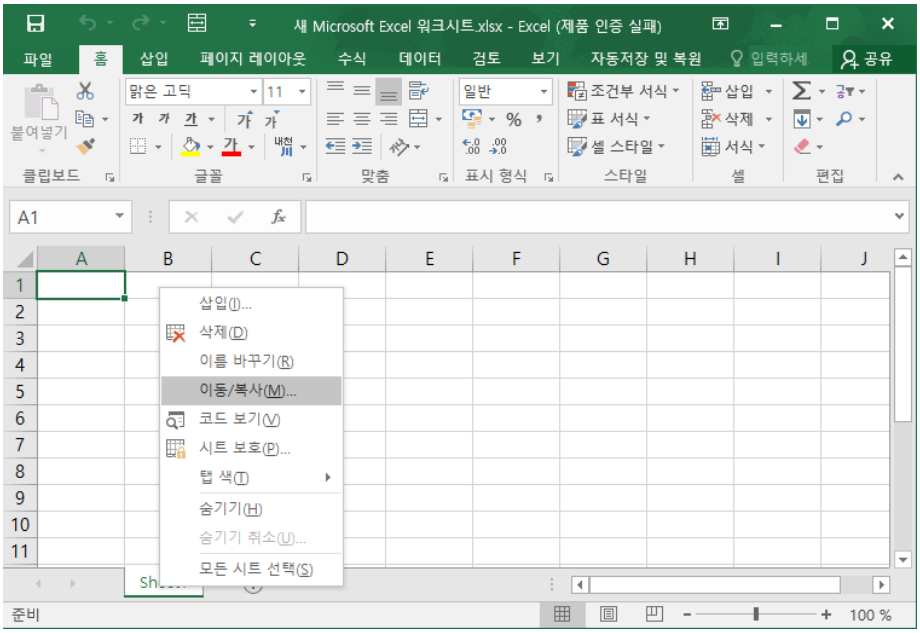
참고 : 보안문서의 경우, 위의 기능은 관리자의 설정과 관계없이 차단됩니다.

위의 기능들이 시도될 경우, 아래와 같은 메시지가 출력됩니다.

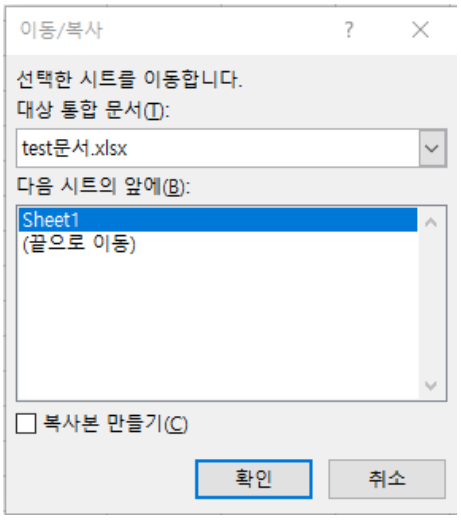


Microsoft Office Excel 시트 이동 / 복사 제어

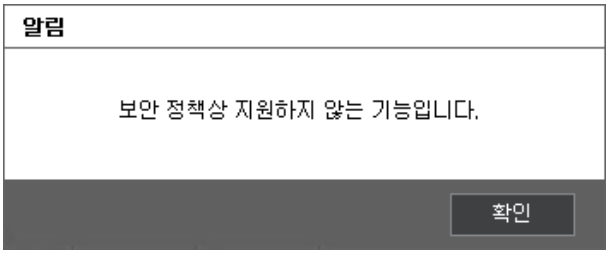
Client 는 MS Office Excel 의 보안문서에 대해 시트의 이동 및 복사를 제어합니다. 관리자의 권한에 따라 암호화된 엑셀 문서의 시트를 다른 엑셀 문서로 이동 및 복사하는 것이 차단됩니다. 아래의 그림과 같이 시트 이동 및 복사를 수행할 경우 드롭다운 메뉴가 비활성화되어, 다른 엑셀문서를 선택할 수 없습니다.



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

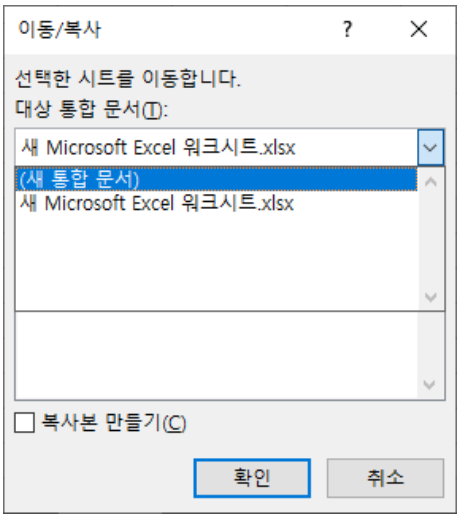


드롭다운 메뉴를 사용할 경우



알림 메세지가 나타나고 드롭다운 메뉴는 사용할수 없습니다.

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



드롭다운 메뉴에서 엑셀문서 선택 가능

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 택스트

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.