독스토리(DocStory)
제품설명서

에스엠테크놀러지(주)

제품 설명서 버전 관리

날짜	대상버전	주요 변경 내용	작성자
2019/09/10	V1.15.0.1	독스토리 관리자 모듈 설치 방법 변경	이희진
2021/01/21	V1.15.1.2	독스토리 관리자 모듈 업그레이드 및 설치방법 변경	이연주
2021/07/16	V1.15.1.3	제품 버전 업데이트, 명칭 및 일부 표현 변경	이연주
2021/09/24	V1.15.1.4	제품 설명서 전체 변경	안순용

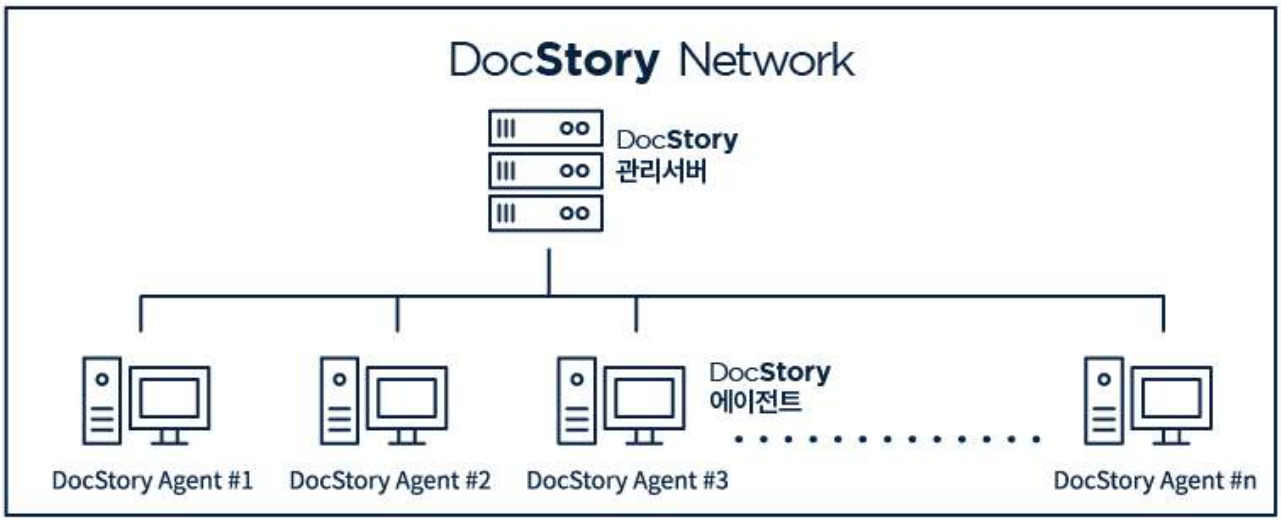
저작권 안내

상표

목차

I 시스템 환경

솔루션 구성도



운영환경

(1) 관리서버 운영 환경 설정

OS	CentOS 7.6.1810 Minimal
Web Server	Apache 2.4.48
Application Server	Tomcat
Database	MariaDB 10.3.14
Network Application	Node 10.19.0
Node Package Manager	NPM 6.13.4

(2) 방화벽 허용 Port

443/TCP	8080/TCP	7000/TCP

(3) 에이전트 운영 환경

CPU	intel/AMD 4코어 이상 및 호환 프로세서
RAM	6GB 이상
HDD	10GB 이상 여유공간
OS	Microsoft Windows 7Home/Pro/Ent/Ult SP1 7601(32bit,64bit) 이상
	Microsoft Windows 8Pro/Ent 9200(32bit, 64bit) 이상
	Microsoft Windows 8.1Pro/Ent 9600(32bit, 64bit) 이상
	Microsoft Windows 10Home/Pro/Ent 1507 10240(32bit, 64bit) 이상
	Microsoft Windows 11Home/Pro/Pro for Workstation/Ent/Edu/Pro Edu 22471(32bit, 64bit) 이상

(4) 독스토리 제품 정보

독스토리 관리자 모듈(관리서버)	
버전	V1.4.1.3
파일명	DsManager.tar
해시값	D17AEE1AC1D860EEBAB484E3D966B0E3978AE47B34D30491F5434174BDC00AE1221623854C06C75F526556E4EAC0BE449E26925EC17EC9ABA94D3B94FFD76BC8

독스토리 에이전트(클라이언트PC)	
버전	V1.15.1.3
파일명	DsInstall.exe
해시값	531027766F65E32F750EAC7759F522B165AAEF41A1C96679BB28F1DE375441FB52D5FA576D69B24BDBAD06086E126674F2C79CA4D3ECA191A36B0076888CAB2F

Ⅱ 독스토리 관리자 모듈 설치 방법

(1) 서버 운영체제(OS) 설치

CentOS 7.6.1810 Minimal을 독스토리 관리 서버에 설치합니다.

(2) 설치 파일 복사

설치 파일 ds_server_install_v1.4.1.3.tar 파일을 복사합니다.

(3) 설치 파일 압축 풀기

[root@localhost ~]# tar –xvf ds_server_install_v1.4.1.3.tar 명령어를 입력합니다.

(4) 관리자 모듈 운영 패키지(환경설정, 관리자 모듈 무결성 검사) 설치

[root@localhost ~]# ./rpm.sh 명령어를 입력합니다.

설치 이후 자동으로 재부팅 합니다.

(5) 관리자 모듈 최초 접속

관리자 운영모드에 접속하기 위해서는 웹 브라우저 주소 표시줄에 설치 시 설정했던 관리 서버의 인터넷주소(예: https://***.***.***.***:8080)로 접속합니다.

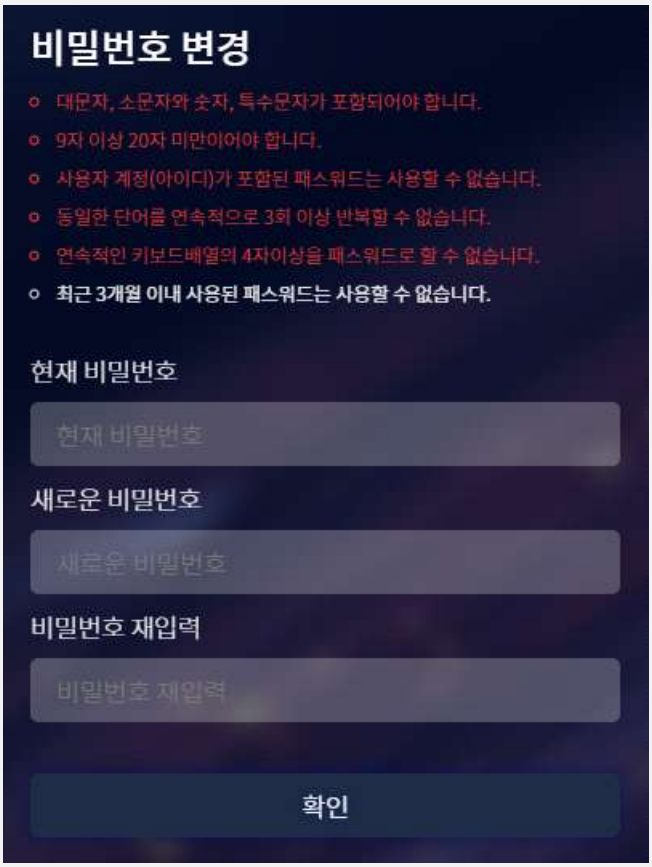
(6) 최초 접속 시 DBMS 계정 생성

관리자 모듈 설치 후 최초 관리자 모듈 접속 시 DBMS계정 생성 창이 보여집니다.

※ 비밀번호 생성 규칙
- 비밀번호 설정 시 9자 이상, 20자 이내의 숫자, 영문(대/소문자), 특수문자 조합으로 설정해야 합니다.
- 사용자 계정(아이디)과 동일한 패스워드는 사용할 수 없습니다.
- 동일한 단어를 연속적으로 3회 이상 반복할 수 없습니다.
- 연속적인 키보드 배열의 4자 이상을 패스워드로 사용할 수 없습니다.
- 최근 3개월 이내 사용한 패스워드는 사용할 수 없습니다.

(7) 관리자 계정 변경

관리자 모듈 설치 후 관리자 모듈 최초 접속 시 Default 계정으로 접속 후 계정 정보를 변경해야 합니다.



※ 비밀번호 생성 규칙
- 비밀번호 설정 시 9자 이상, 20자 이내의 숫자, 영문(대/소문자), 특수문자 조합으로 설정해야 합니다.
- 사용자 계정(아이디)과 동일한 패스워드는 사용할 수 없습니다.
- 동일한 단어를 연속적으로 3회 이상 반복할 수 없습니다.
- 연속적인 키보드 배열의 4자 이상을 패스워드로 사용할 수 없습니다.
- 최근 3개월 이내 사용한 패스워드는 사용할 수 없습니다.

Ⅲ 독스토리 에이전트 설치 방법

배포프로그램(PMS 또는 별도 프로그램) 이용 시

(1) 배포 PC운영체제: Microsoft Windows7~11 (서버제외)

[Ⅰ.시스템환경-운영환경-에이전트운영환경]의 지원OS 참고]

(2) 설치경로

- 32비트 운영체제: C:₩Program Files₩SMT₩DocStory₩
- 64비트 운영체제: C:₩Program Files (x86)₩SMT₩DocStory₩

(3) 설치 유무 판단 파일

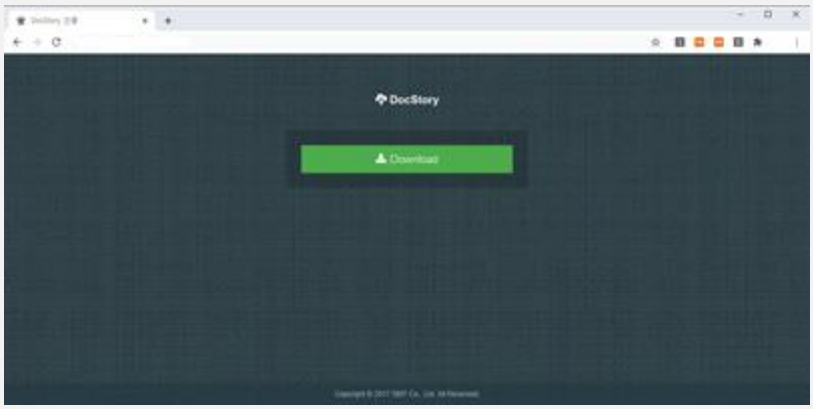
- 32비트 운영체제: C:₩Program Files₩SMT₩DocStory₩lookup₩DsClient.mc
- 64비트 운영체제: C:₩Program Files (x86)₩SMT₩DocStory₩lookup₩DsClient.mc

사용자 직접 설치 시

(1) 설치파일 준비

제공받으신 DocStory설치 CD 또는 관리서버의 다운로드 웹페이지(https://***.***.***.***) 접속하여 다운로드 받거나 설치 파일을 별도 저장매체(USB 등)를 통해 설치할 클라이언트PC에 설치 파일을 준비합니다.

※ DocStory 에이전트 설치 프로그램의 배포 방법은 구매하신 업체나 기관에서 기 보유하고 계신 배포 프로그램으로도 배포가 가능하나 여기서는 설치 파일을 이용하여 직접 설치하는 경우를 설명하여 드립니다.



(2) 다운로드 받은 경로에서 설치 파일을 실행합니다.

(3) 스텔스 설치

사용자 직접 설치 시에도 PMS 설치와 동일한 설치 파일을 제공하기 때문에 설치 진행과정과 관련되어 일반 사용자에게 설치 진행 절차는 제공되지 않습니다.

(4) 설치 완료

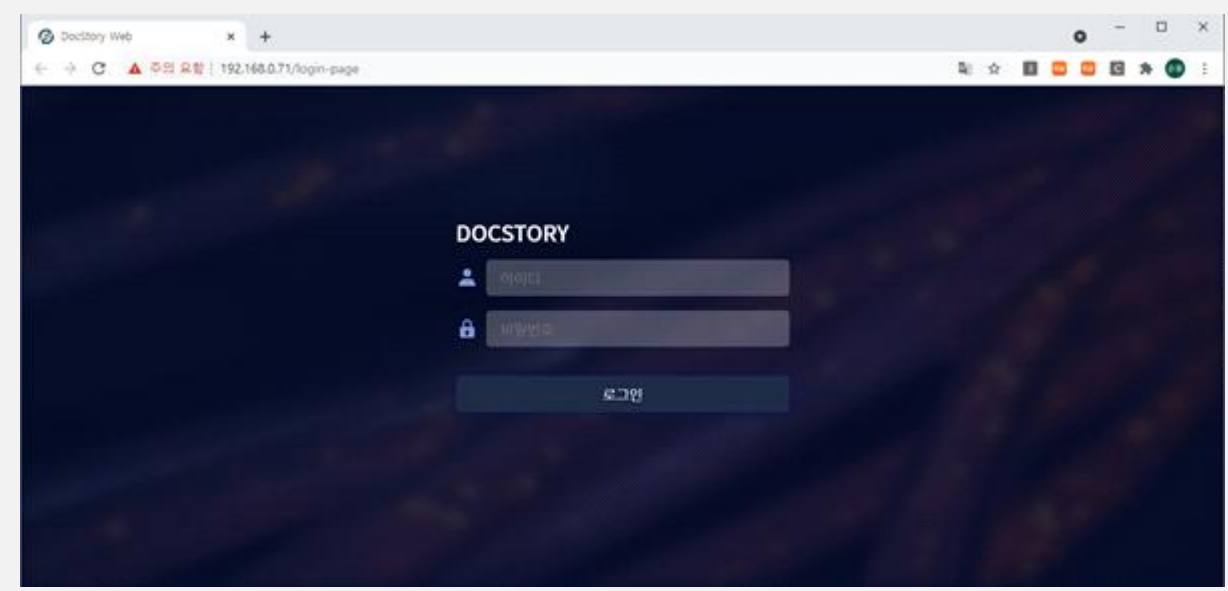
설치가 성공적으로 완료되면 화면 우측 하단에 '독스토리' 아이콘이 표시됩니다.

※ 왼쪽 그림과 같이 트레이 아이콘에 독스토리 아이콘이 표시됩니다.

IV 관리자 페이지 접속 및 로그인

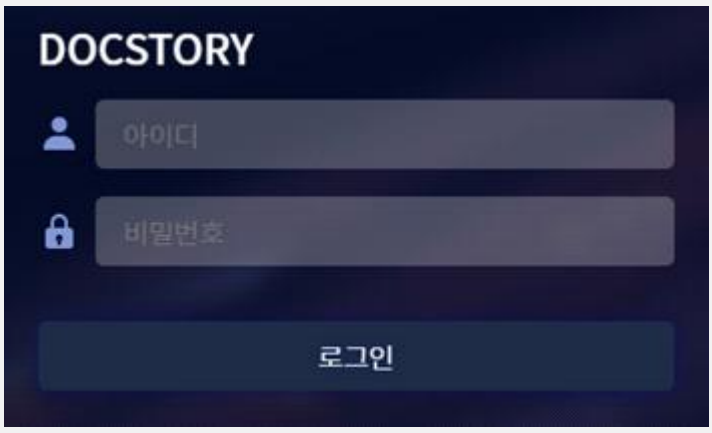
관리자 페이지 접속

관리자 운영모드에 접속하기 위해서는 웹 브라우저 주소 표시줄에 설치 시 설정한 관리 Server의 IP주소 (https://***.***.***.***)를 입력하여 접속하시면 됩니다.



1. 관리자 로그인

로그인 화면에서 독스토리에 등록된 관리자 아이디와 비밀번호를 입력하시고 "로그인" 버튼을 클릭하면 관리자 화면에 접속됩니다.



V 메인화면(Dashboard)

기본 화면

관리자 로그인 후 첫 화면은 "Dashboard" 화면으로 설치된 전체 에이전트 정보와 차단 정보를 실시간으로 확인할 수 있습니다.

1. 라이선스 현황

대시보드 상단에 라이선스, 연결상태, 서버용량 정보를 실시간으로 보여줍니다.

- **총 라이선스** : 구매한 라이선스 수와 클라이언트에 설치된 에이전트의 수를 나타냅니다.
- **등록** : 클라이언트PC에 독스토리 에이전트를 설치한 수량입니다.
- **접속** : 현재 활성화된 에이전트 수량을 나타냅니다.
- **만료** : 일정 기간 이상 접속하지 않은 에이전트 수량을 나타냅니다.

2. 서버용량

- **서버용량** : 사용중인 독스토리 관리서버의 저장공간 이용량과 잔여량을 보여줍니다.

3. TOP5클라이언트PC

클라이언트PC에 이벤트가 많이 발생한 순서로 상위 5개의 클라이언트PC를 보여줍니다. 선택에 따라 10, 25, 50, 100개의 클라이언트PC 리스트를 볼 수 있습니다. 또한, 선택에 따라 일간, 주간, 월간 순위를 볼 수 있습니다.

일간 TOP클라이언트PC는 24시간 전부터 지금 시간까지 클라이언트 에이전트에서 발생한 이벤트 빈도가 가장 큰 것부터 나열합니다. 선택에 따라 상위 5개, 10개, 25개, 50개, 100개의 클라이언트PC가 보여집니다.

주간 TOP클라이언트PC는 7일 전부터 오늘까지 클라이언트 에이전트에서 발생한 이벤트 빈도가 가장 큰 것부터 나열합니다. 선택에 따라 상위 5개, 10개, 25개, 50개, 100개의 클라이언트PC가 보여집니다.

월간 TOP클라이언트PC는 30일 전부터 오늘까지 클라이언트 에이전트에서 발생한 이벤트 빈도가 가장 큰 것부터 나열합니다. 선택에 따라 상위 5개, 10개, 25개, 50개, 100개의 클라이언트PC가 보여집니다.

4. 차단로그 통계 그래프

(1) 오늘 통계

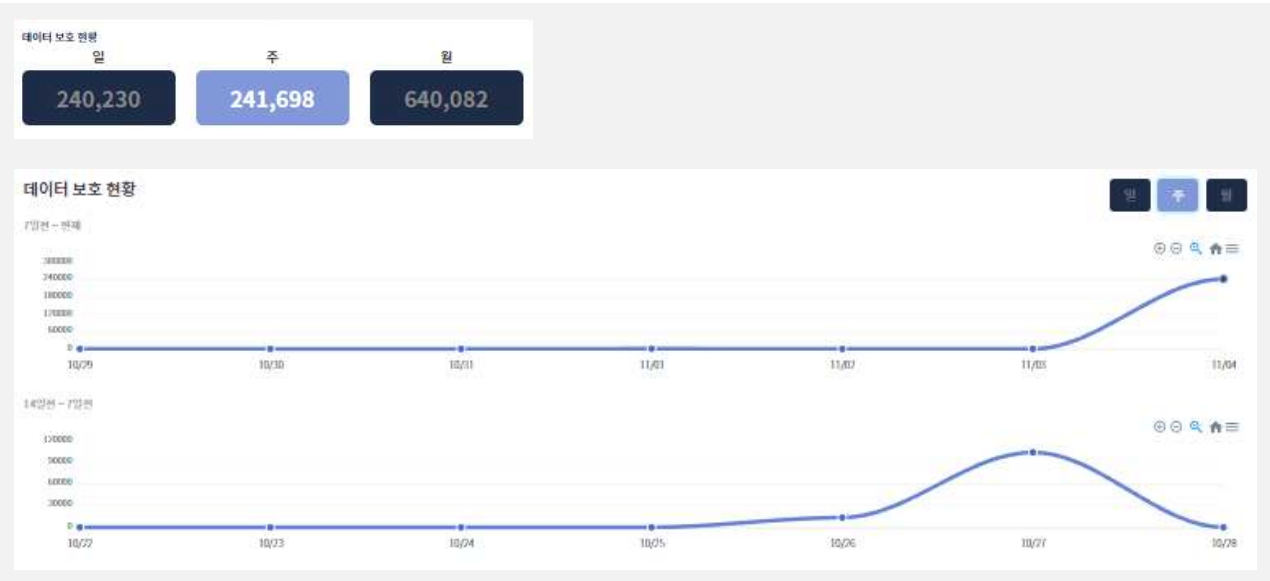
- 차단된 프로세스 현황을 시간별로 보여줍니다.

- 금일 통계(24시간 전부터 현시간까지)는 위쪽 그래프에 시간별로 발생 이벤트 수가 표시되고, 전일 통계(48시간 전부터 24시간 전까지)는 아래 그래프에 발생 이벤트 수가 표시되어 서로 비교할 수 있도록 지원합니다.

(2) 이번주 통계

- 한 주 간 차단된 프로세스 현황을 보여줍니다.

- 금주 통계(7일전부터 현재까지)는 위쪽 그래프에 일별 발생 이벤트의 수가 표시되고, 전주 통계(14일전부터 7일전까지)는 아래쪽 그래프에 일별 발생 이벤트 수가 표시되어 서로 비교할 수 있도록 지원합니다.

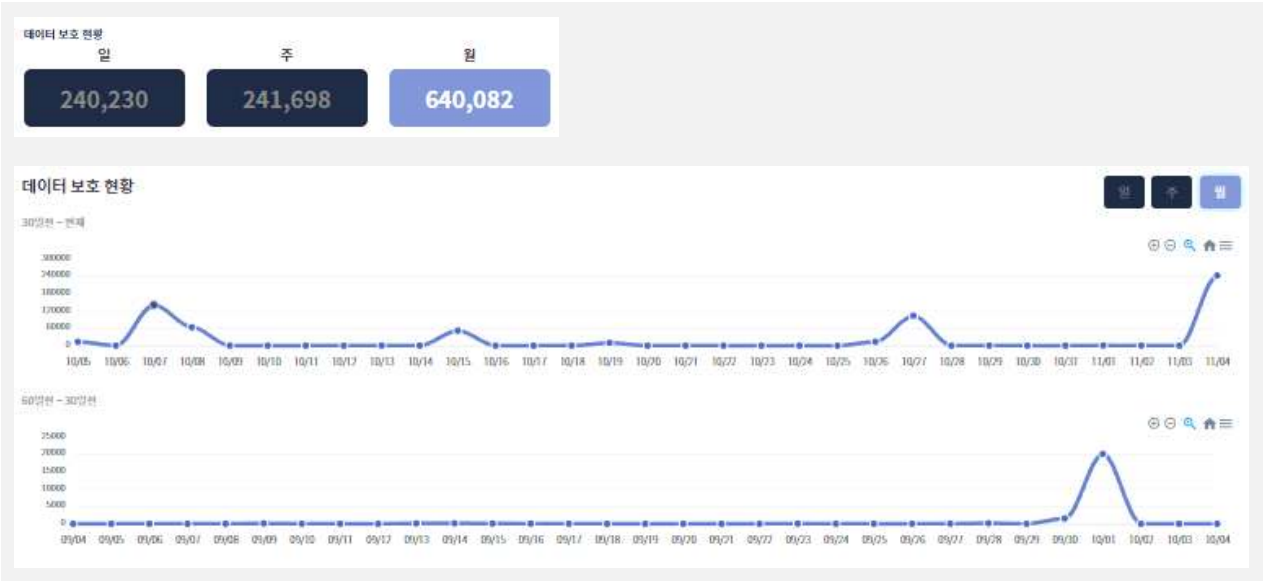


(3) 이번달 통계

- 한 달 간 차단된 프로세스 현황을 보여줍니다.

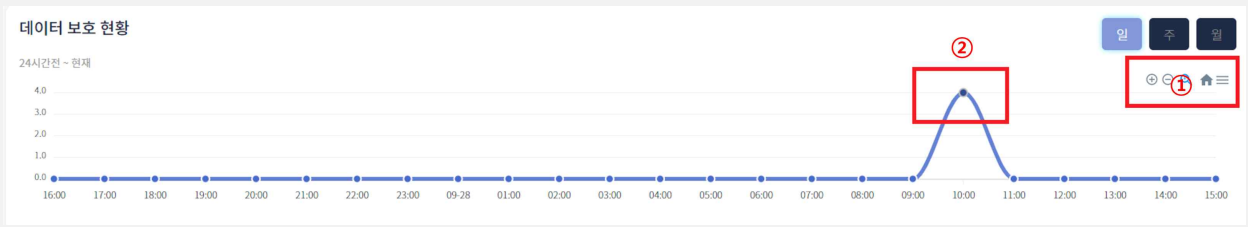
- 이번 달 통계(30일 전부터 현재까지)는 위쪽 그래프에 일별 발생 이벤트

수가 표시되고, 지난 달 통계(60일 전부터 30일 전까지)는 아래쪽 그래프에 발생 이벤트 수가 표시되어 서로 비교할 수 있도록 지원합니다.



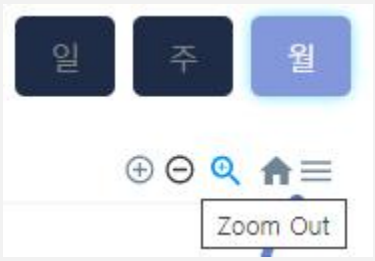
데이터 보호 현황 그래프 상세

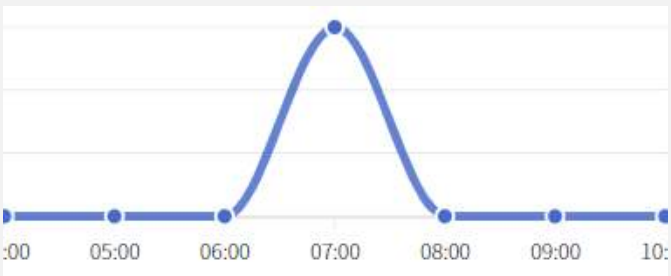
비인가 프로세스에 의한 보호대상 파일 접근 시 차단한 이벤트의 발생빈도를 시간대별로 확대 및 축소하여 모니터링 할 수 있습니다. 또한, 각 그래프의 꼭지점들에 대한 상세 정보를 확인 할 수 있습니다.



1. 그래프 확대 및 축소

데이터보호 현황 화면의 우측 상단에 Zoom in/Zoom out 버튼이 있어서 그래프를 확대 및 축소할 수 있습니다. 또한, Reset Zoom 버튼을 클릭하면 원상태로 되돌려집니다.

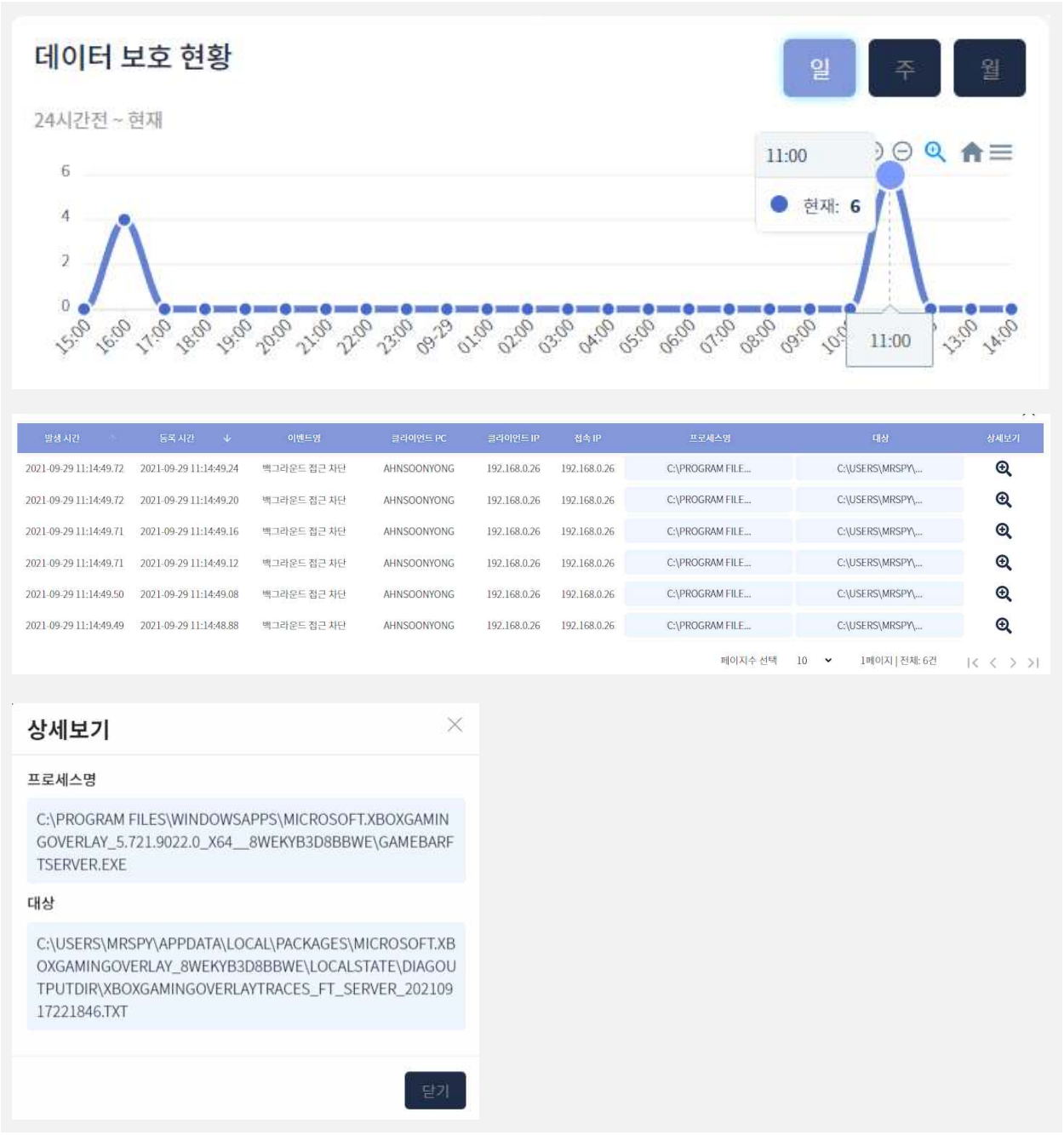




2. 이벤트 선택

그래프의 특정 꼭지점을 선택하시면 해당 시간대에 발생된 이벤트 상세 내역

이 그래프 아래에 리스트로 빠르게 확인하여 즉시 대응할 수 있습니다.



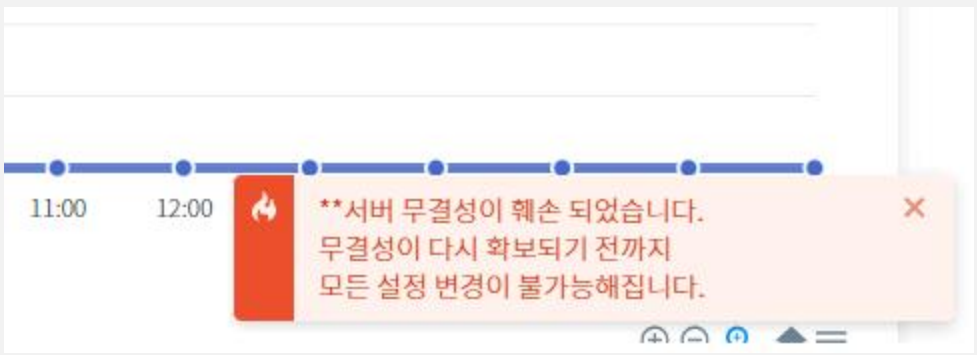
관리자 모듈 무결성 훼손과 대응

관리자 모듈에 대한 무결성 검사는 1일 1회 자동으로 실시(오전1:00)하며, 수동으로 진행하는 검사는 [설정관리-운영환경설정]화면의 우측 상단에 있는 [무결성 검증]버튼을 클릭하면 진행됩니다.

수동으로 진행하는 서버 무결성 검증에 대하여서는
[IX.설정관리-운영환경설정]을 참고하시기 바랍니다.

1. 관리자 모듈 무결성 훼손 시 화면 정보

관리자 모듈 무결성 훼손 시 관리자 모듈의 모든 설정 값을 변경할 수 없습니다. 다만, 기존 설정에 의해 진행되는 작업과 에이전트와의 통신은 유지됩니다.



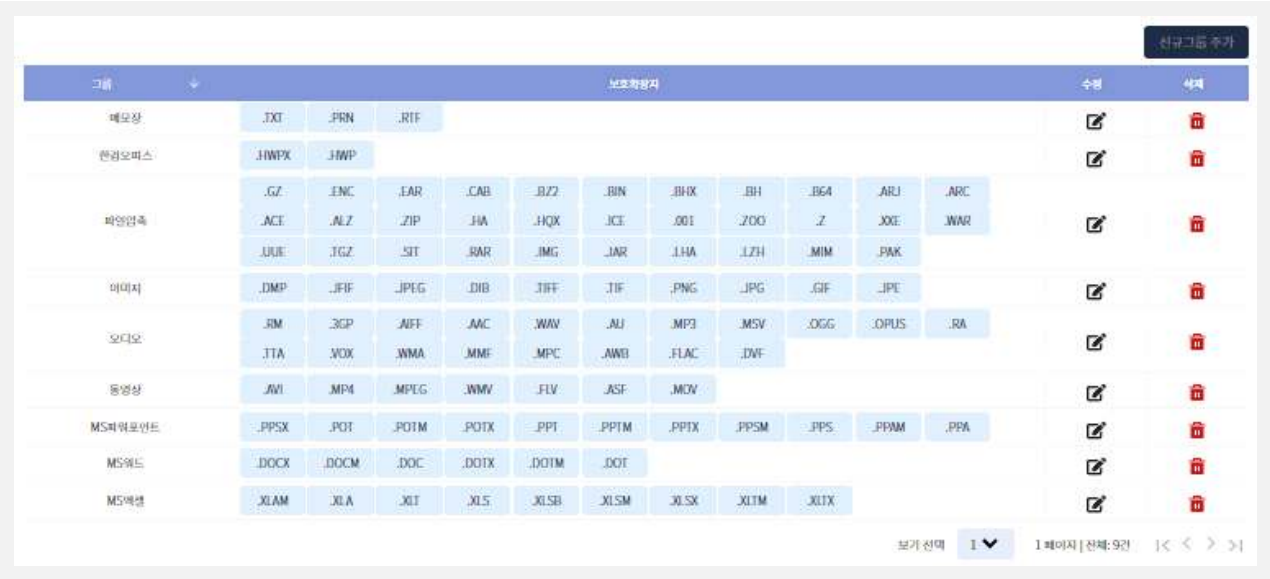
2. 관리자 모듈의 무결성 훼손 시 대응 방법

관리자 모듈의 무결성 훼손을 확인 하는 즉시 구매처나 개발사인 에스엠테크놀러지(주)에 즉시 통보하여 주시고 알려드리는 방법에 따라 대응해주시기 바랍니다.

VI 데이터보호정책

보호확장자

보호확장자는 비인가프로세스의 접근으로부터 보호하기 위한 대상으로 파일 유형을 등록 및 관리할 수 있는 기능을 제공합니다.



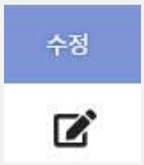
1. 신규그룹추가

관리의 편의성을 위하여 보호대상 파일을 유형별로 묶어 관리할수 있도록 합니다. 신규그룹 추가 시 기본 하나 이상의 해당 유형의 파일 확장자를 등록할 수 있도록 지원합니다.

생성되거나 수정된 확장자의 내역은 즉시 각 에이전트에 전송되어 바로 적용됩니다.

2. 수정

각 그룹에 속한 보호대상 확장자의 내역을 수정(추가,삭제)할 수 있는 기능입니다. 이때 그룹명은 수정할 수 없고, 각 그룹에 속한 확장자에 대하여 추가 및 삭제할 수 있습니다.



선택한 그룹의 [수정]버튼을 클릭하면 해당 그룹의 확장자 내역을 수정할 수 있는 팝업창이 열립니다.

보호 대상 확장자는 추가/삭제 가능합니다.

3. 삭제

선택한 그룹의 삭제 시 해당 그룹에 속한 확장자 내역까지 삭제됩니다.
삭제 시 해당 내용은 즉시 에이전트에 전달되어 바로 적용됩니다.

해당 그룹을 삭제할 때 해당 그룹에 속한 삭제 버튼을 클릭합니다.

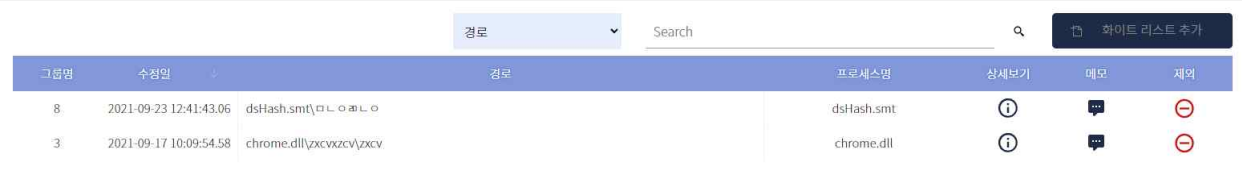
보호 확장자 그룹의 삭제는 신중해야할 중요한 행위이기 때문에 삭제 시 확인하는 단계를 거치게 됩니다.

삭제가 성공적으로 완료되면 성공 메시지로 알려드립니다.

화이트리스트

화이트리스트에 등록된 프로세스는 보호대상 확장자에 접근할 수 있습니다.

관리자 모듈에서 보이는 화이트리스트 정보는 수정일, 경로, 프로세스명으로 실제 동일한 경로의 동일한 프로세스명이라하더라도 Hash가 다르면 다른 프로세스로 처리됩니다. 관리의 편의성을 위하여 관리자 화면에 Hash는 보이지 않습니다.

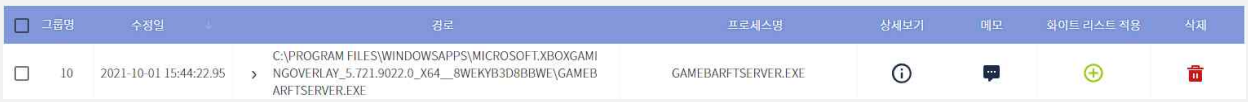


1. 화이트리스트 추가/제외

화이트리스트에 등록할 수 있는 수단은 수동등록과 차단리스트 목록 중 선택하여 등록하는 방법이 있습니다.

화이트리스트 수동 추가

업로드 버튼을 클릭하면 열리는 윈도우 탐색기 창으로 해당 파일을 찾고, 해당 경로를 입력하여 추가합니다.



[데이터보호정책-차단프로세스] 리스트에서 화이트리스트 적용 버튼을 클릭하면 해당 프로세스는 자동으로 화이트리스트로 적용되며 해당 프로세스는 차단프로세스에서 제외됩니다.

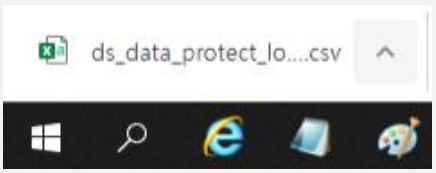
[데이터보호정책-화이트리스트] 리스트에서 제외 버튼을 클릭하면 해당 프로세스는 화이트리스트에서 제외됩니다. 이때 수동으로 화이트리스트에 추가한 항목이 아닌 차단프로세스에서 화이트리스트 등록 진행한 경우는 화이트리스트 제외 즉시 해당 프로세스는 차단프로세스 목록으로 이동됩니다.

2. 상세보기

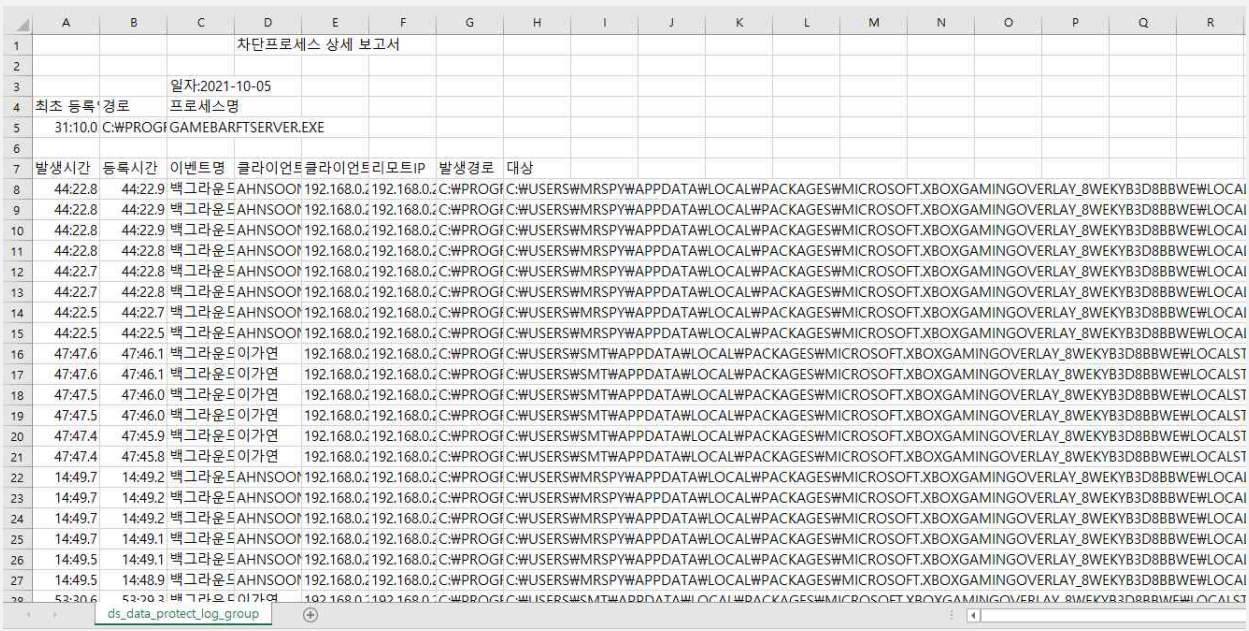
차단프로세스에서 화이트리스트로 등록한 경우 해당 프로세스(동일한Hash기준)의 모든 차단 리스트에 대한 정보를 모아서 볼수 있도록 정보를 제공합니다.

발생시간, 등록시간, 이벤트명, 클라이언트PC, IP정보, 프로세스명과 해당 프로세스가 접근한 대상 프로세스명의 정보가 보여집니다.

상세보기 창 우측 상단의 [Excel]버튼 클릭



상세내역에 대한 레포팅을 엑셀파일로 내려받을 수 있습니다.



	A	B	C	D	E	F	G	H
1				차단프로세스 상세 보고서				
2								
3			일자:2021-10-05					
4	최초 등록	경로	프로세스명					
5	31:10.0	C:₩PROGF	GAMEBARFTSERVER.EXE					
6								
7	발생시간	등록시간	이벤트명	클라이언트	클라이언트	리모트IP	발생경로	대상
8	44:22.8	44:22.9	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
9	44:22.8	44:22.9	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
10	44:22.8	44:22.9	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
11	44:22.8	44:22.8	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
12	44:22.7	44:22.8	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
13	44:22.7	44:22.8	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
14	44:22.5	44:22.7	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
15	44:22.5	44:22.5	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
16	47:47.6	47:46.1	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
17	47:47.6	47:46.1	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
18	47:47.5	47:46.0	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
19	47:47.5	47:46.0	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
20	47:47.4	47:45.9	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
21	47:47.4	47:45.8	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST
22	14:49.7	14:49.2	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
23	14:49.7	14:49.2	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
24	14:49.7	14:49.2	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
25	14:49.7	14:49.1	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
26	14:49.5	14:49.1	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
27	14:49.5	14:48.9	백그라운드	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCAI
28	53:30.6	53:29.3	백그라운드	이가연	192.168.0.2	192.168.0.2	C:₩PROGF	C:₩USERS₩SMT₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WEKYB3D8BBWE₩LOCALST

ds_data_protect_log_group

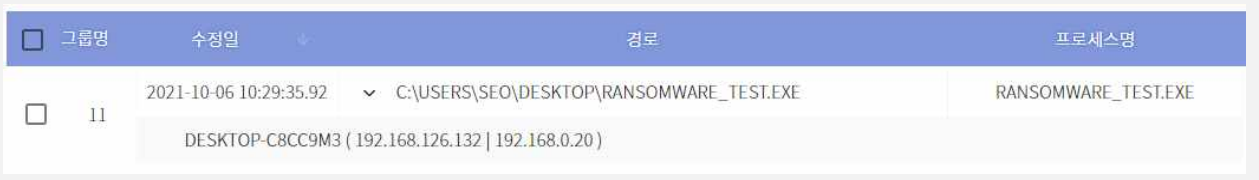
차단프로세스

[데이터보호정책-보호확장자]에서 등록한 보호대상 파일에 접근하는 프로세스들 중에 비인가프로세스의 접근을 차단하고 그에 관한 정보를 제공합니다.

인가프로세스의 정의는 윈도우운영체제 기본 프로세스, 코드사인되어 있는 프로세스, 화이트리스트 등록 프로세스에 포함되는 경우입니다. 이외의 모든 프로세스는 비인가프로세스로 판단하여 보호대상 파일에 접근하는 것을 원천 차단합니다.

1. 차단 항목별 클라이언트PC 정보

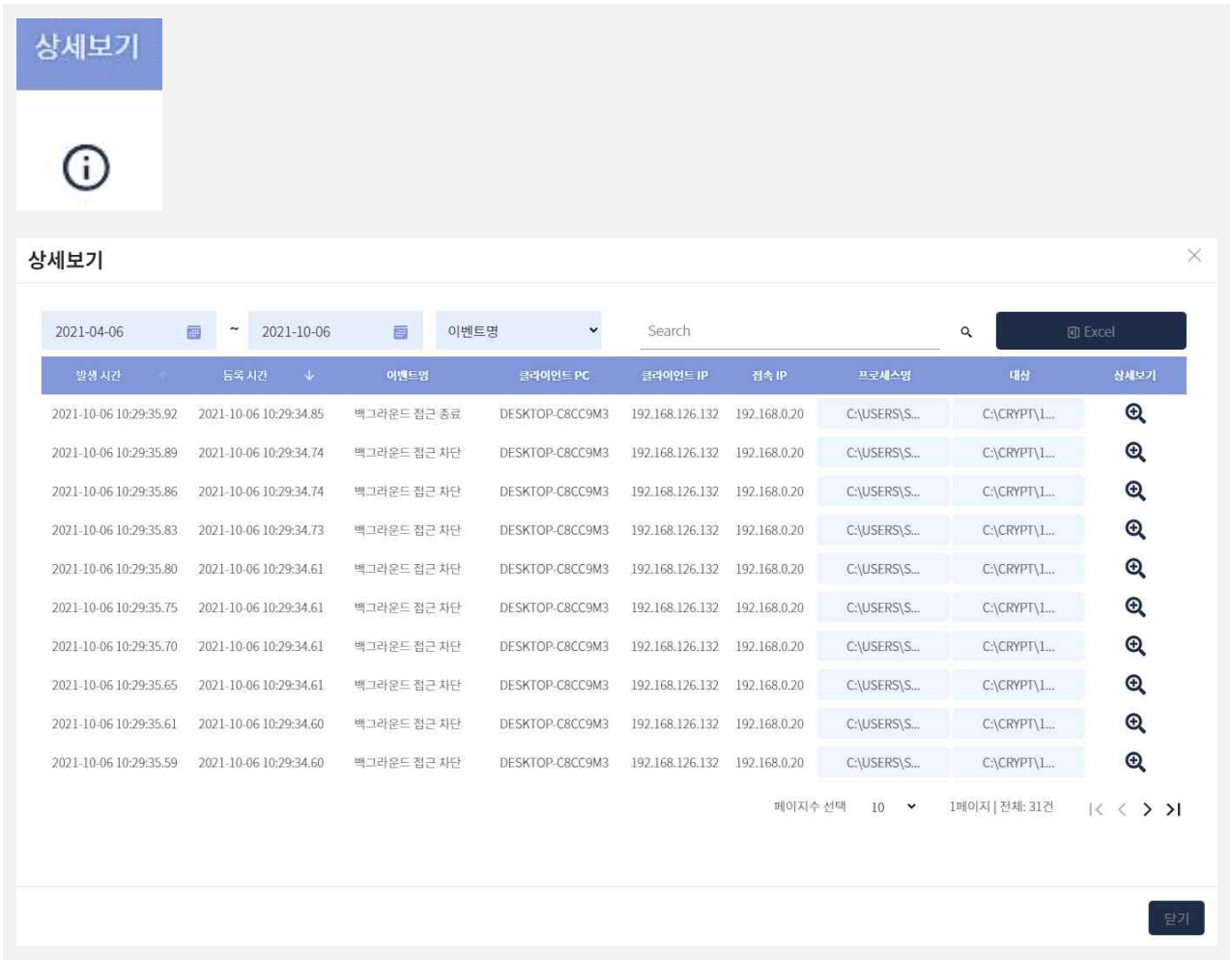
차단 리스트의 항목 내역 중 경로 표시 앞부분의 [>]를 클릭하면 해당 차단 프로세스가 실행되어 차단된 클라이언트PC 리스트를 정보를 제공합니다.



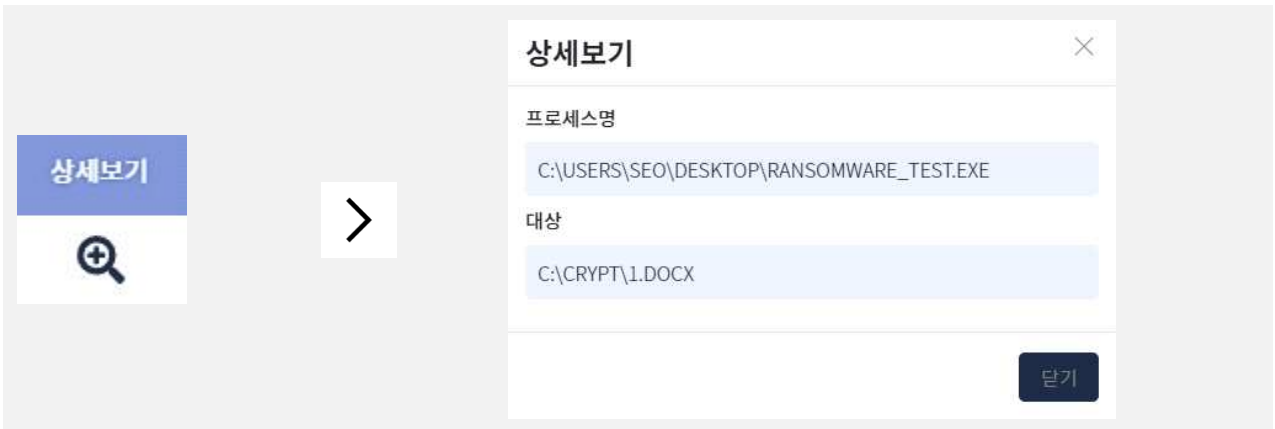
2. 상세보기

차단프로세스 리스트의 상세보기 표시를 클릭하면 팝업창에 선택한 차단 프로세스(동일한Hash기준)의 모든 차단 리스트에 대한 정보를 모아서 볼수 있도록 정보를 제공합니다.

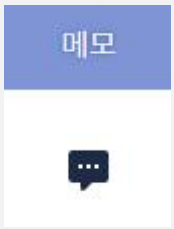
발생시간, 등록시간, 이벤트명, 클라이언트PC, IP정보, 프로세스명과 해당 프로세스가 접근한 대상 프로세스명의 정보가 보여집니다.



상세보기 이이콘을 클릭하면 프로세스명, 대상에 대한 전체 정보를 확인 할 수 있습니다.



3. 메모



차단 프로세스를 지속적으로 모니터링이 필요할 경우 간략한 내용을 적어 후속 조치때 참고할 수 있습니다.

메모는 작성자 계정, 작성일, 작성내용으로 한번 입력하면 수정할 수 없게 하여 작성내용의 유효성을 유지합니다.

4. 화이트리스트 적용

차단프로세스의 리스트 중 확인을 통하여 화이트리스트로 적용할 수 있습니다. 이때 해당 차단프로세스의 모든 정보는 화이트리스트로 이관되고 이는 모든 에이전트로 전송되어 즉시 적용됩니다.

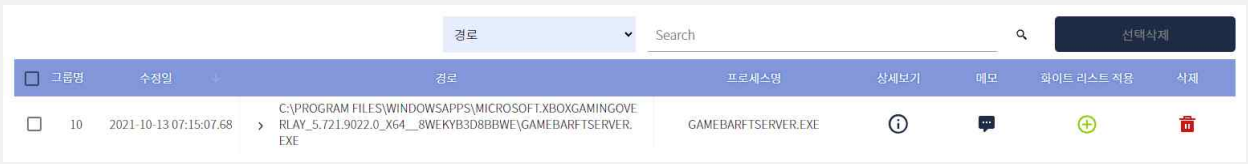
<-- 클릭 시 즉시 적용

5. 차단내역 삭제

[데이터보호정책-차단프로세스]의 리스트는 삭제하여도 해당 내용에 대한 [감사로그-데이터보호이벤트]의 내역은 삭제되지 않습니다.

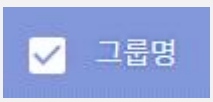
(1) 단일 항목 삭제

리스트의 해당 항목의 우측 삭제 아이콘을 클릭하시면 해당 내역은 삭제 됩니다.



(2) 복수 항목 삭제

복수의 내역을 삭제할 경우 리스트 좌측의 체크박스를 체크한 후 선택한 차단리스트 삭제



화면에 나타난 리스트 한페이지 전체를 선택할 경우 제목 옆 체크박스에 체크하면 화면 출력 리스트 한페이지 전체가 선택됩니다.

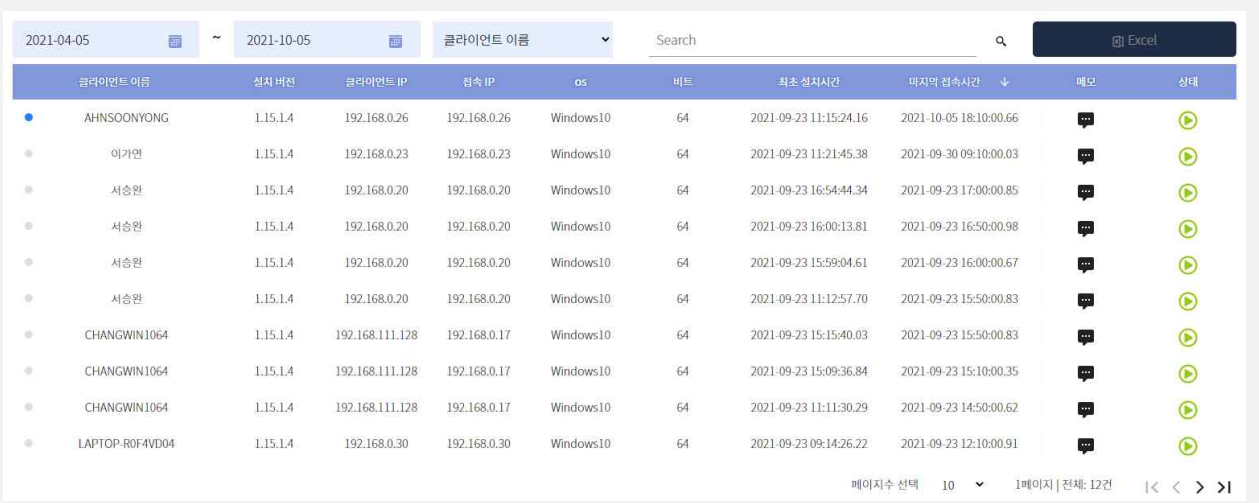
삭제할 복수의 항목을 선택한 후 리스트 우측 상단에 있는 선택삭제 버튼을 클릭하면 선택한 항목 모두가 삭제 됩니다.

Ⅶ 클라이언트 관리

클라이언트 정보

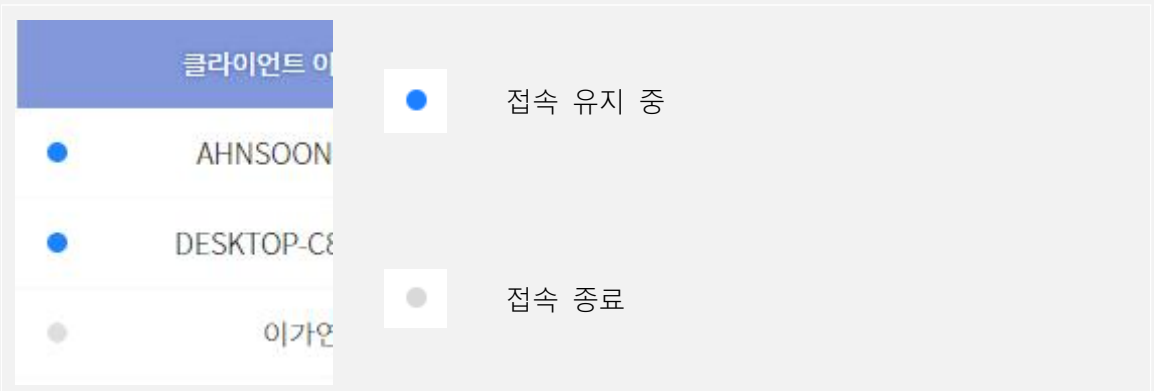
독스토리 에이전트가 설치된 클라이언트PC에 대한 정보입니다.

실시간 클라이언트 접속 상태, 클라이언트PC명, 에이전트 설치버전, IP, 설치되어 있는 OS, 에이전트 설치일, 최종 접속 시간, 클라이언트PC에 대한 간략한 메모 등의 정보를 확인 할 수 있습니다. 또한, 특정 에이전트의 운용을 중지/실행 할 수 있는 상태 변경 기능을 포함합니다.



(1) 클라이언트 상태

클라이언트 이름 앞 푸른색인 경우 현재 해당 에이전트와 연결 상태를 나타내고, 회색인 경우 해당 에이전트와 접속이 끊긴 상태를 나타냅니다.



(2) 클라이언트 이름

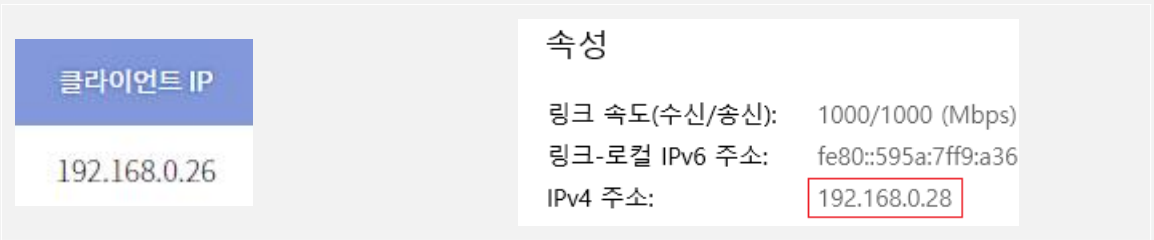
에이전트가 설치된 클라이언트PC에 설정된 장치 이름입니다.

(3) 설치버전

클라이언트PC에 설치되어 있는 독스토리 에이전트 버전을 표시합니다.

(4) 클라이언트IP

클라이언트PC에 설정된 IP주소를 표시합니다.



(5) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다. 이때 클라이언트PC의 IP주소와 다를 수 있습니다. 이는 중간에 공유기나 클라이언트PC에 가상환경 상에 에이전트를 설치하는 경우 다를 수 있습니다.

(6) OS/빌드

클라이언트PC에 설치된 윈도우OS의 버전 정보를 표시합니다.

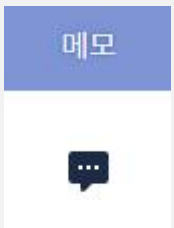
(7) 최초 설치시간

클라이언트PC에 독스토리 에이전트가 설치된 설치시간을 표기합니다.

(8) 마지막 접속시간

에이전트가 마지막 접속했던 시간을 표기합니다.

1. 메모



에이전트에 대한 지속적인 모니터링이 필요할 경우 간략한 내용을 적어 후속 조치때 참고할 수 있습니다.

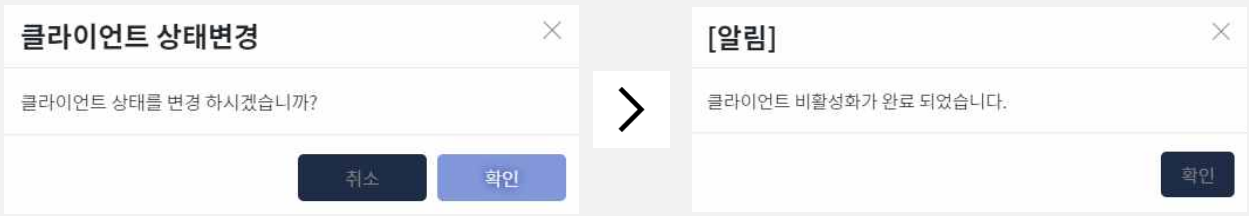
메모는 작성자 계정, 작성일, 작성내용으로 한번 입력하면 수정할 수 없게 하여 작성내용의 유효성을 유지합니다.

2. 에이전트 상태 전환

클라이언트PC에 설치되어 운용 중인 에이전트의 핵심 기능인 비인가프로세스에 의한 차단 기능을 잠시 중지 시킬 필요가 있거나 주요기능 중지 상태를 다시 활성화 시킬 때 사용합니다.

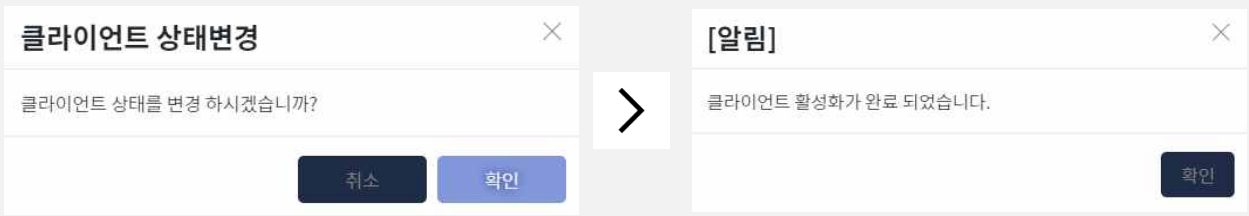
(1) 활성화에서 비활성화로 전환

활성화 상태에서 클릭하면 비활성화 상태로 전환됩니다.
비활성화하면 에이전트의 다른 기능은 정상으로 작동하지만
비인가프로세스에 대한 차단 기능이 중단됩니다.
클라이언트PC에 특이사항 발생 시 테스트 및 초기 설치 시 데이터수집을 위해 이용합니다.



(2) 비활성화에서 활성화로 전환

비 활성화 상태에서 클릭하면 활성화 상태로 전환됩니다.



(3) 클라이언트PC의 독스토리 에이전트 아이콘

활성화 상태의 에이전트 아이콘

비활성화 상태의 에이전트 아이콘

클라이언트 삭제 신청

독스토리 관리자 모듈의 [설정관리-운영환경설정]에서 솔루션 삭제권한 설정이 [삭제제한]으로 되어 있는 경우 클라이언트PC에서 사용자 임의로 삭제할 수 없습니다.

삭제 시도 시 클라이언트 삭제 신청으로 접수되어 관리자의 승인 이후 삭제할 수 있습니다.

(1) 클라이언트PC에서 삭제 신청

(2) 관리자의 삭제 승인 및 거절

관리자는 등록된 삭제 신청에 대하여 승인 및 거절을 진행 할 수 있습니다.

승인 완료 시에만 사용자는 클라이언트PC에 설치된 독스토리 에이전트를 삭제할 수 있습니다.

라이선스 삭제

클라이언트PC를 포맷 후 다시 설치하거나 PC교체가 일어나는 경우에는 독스토리 에이전트의 상태를 확인할 수 없기 때문에 장기 미접속 에이전트 및 설치된 클라이언트PC의 IP가 중복되는 경우 해당 클라이언트PC에 설치된 에이전트의 라이선스를 관리해주어야 합니다.

독스토리는 장기 미접속 IP, 단기 미접속 에이전트라도 IP 중복이 발생하는 경우 에이전트가 삭제 또는 해당 클라이언트PC가 교체되었다고 판단하여 라이선스를 정리할 수 있는 기능을 제공하고 있습니다.

개별 삭제

복수 선택 삭제

Ⅷ 감사로그

감사데이터 검색 및 내려받기

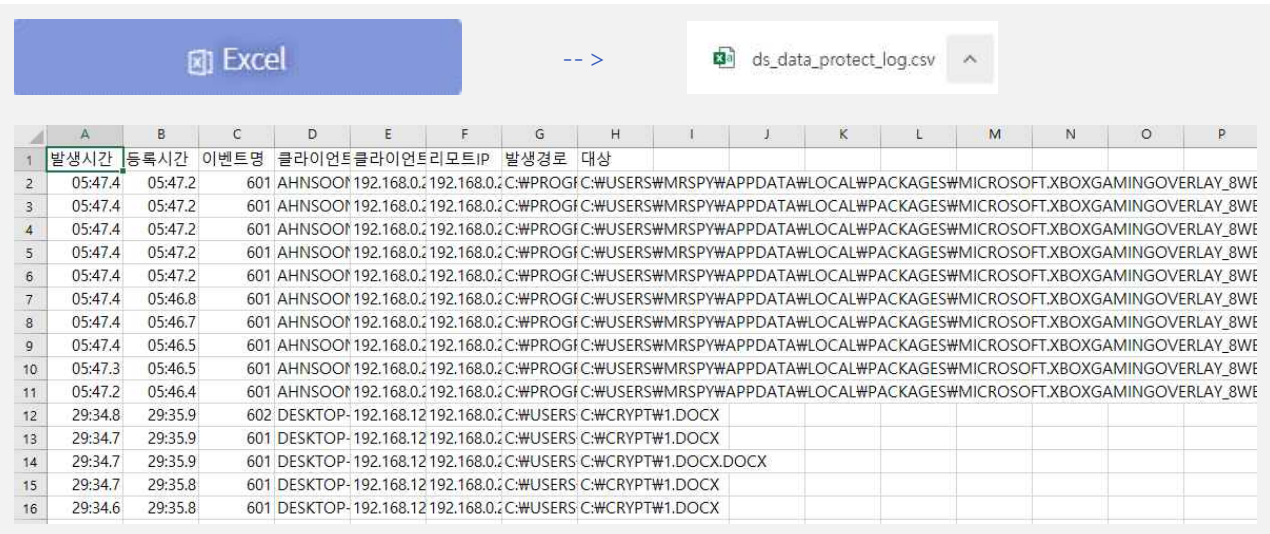
1. 검색 기능

독스토리 관리자 모듈의 모든 리스트에는 강력한 검색 기능이 포함되어 있습니다. 공통적으로 특정 기간에 대한, 선택 항목의 내용에 대한 검색 기능이 제공됩니다.

또한, 시간 항목에는 시간별 올림차순/내림차순 정렬 기능을 제공하여 효과적인 검색을 지원합니다.

2. 감사데이터 내려받기

모든 감사로그는 검색한 리스트에 대하여 CSV형태의 파일로 내려받기 기능을 제공합니다. 이를 이용하여 다양한 분석 및 보고서 작성이 손쉽게 할 수 있도록 지원합니다.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	발생시간	등록시간	이벤트명	클라이언트	클라이언트	리모트IP	발생경로	대상								
2	05:47.4	05:47.2	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
3	05:47.4	05:47.2	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
4	05:47.4	05:47.2	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
5	05:47.4	05:47.2	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
6	05:47.4	05:47.2	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
7	05:47.4	05:46.8	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
8	05:47.4	05:46.7	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
9	05:47.4	05:46.5	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
10	05:47.3	05:46.5	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
11	05:47.2	05:46.4	601	AHNSOON	192.168.0.2	192.168.0.2	C:₩PROGR	C:₩USERS₩MRSPY₩APPDATA₩LOCAL₩PACKAGES₩MICROSOFT.XBOXGAMINGOVERLAY_8WE								
12	29:34.8	29:35.9	602	DESKTOP-	192.168.12	192.168.0.2	C:₩USERS	C:₩CRYPT₩1.DOCX								
13	29:34.7	29:35.9	601	DESKTOP-	192.168.12	192.168.0.2	C:₩USERS	C:₩CRYPT₩1.DOCX								
14	29:34.7	29:35.9	601	DESKTOP-	192.168.12	192.168.0.2	C:₩USERS	C:₩CRYPT₩1.DOCX.DOCX								
15	29:34.7	29:35.8	601	DESKTOP-	192.168.12	192.168.0.2	C:₩USERS	C:₩CRYPT₩1.DOCX								
16	29:34.6	29:35.8	601	DESKTOP-	192.168.12	192.168.0.2	C:₩USERS	C:₩CRYPT₩1.DOCX								

데이터 보호 로그

[데이터보호정책-차단프로세스]에서 발생한 비인가프로세스의 보호대상 파일 접근 차단/종료와 관련한 감사로그입니다.

(1) 발생시간

에이전트에서 발생한 차단/종료 이벤트 발생시간으로 클라이언트PC의 시간 설정에 따릅니다.

(2) 등록시간

에이전트에서 관리서버로 전송한 데이터보호 이벤트 감사로그 서버 입력시간으로 관리서버의 시간 설정에 따릅니다.

(3) 이벤트명

데이터보호 이벤트에 따른 종류는 두가지로 [백그라운드 접근 차단]과 [백그라운드 접근 종료]의 두가지 경우입니다.

① 백그라운드 접근 차단

비인가프로세스가 보호대상 파일에 접근하였을 때 즉시 차단하였다는 로그입니다.

② 백그라운드 접근 종료

[서정관리-운영환경설정]의 솔루션 항목의 [프로세스 중지기능]이 [활성화]상태로 되어 있는 경우, [차단기준점] 설정 횟수 이상의 차단이 발생하는 경우 해당 비인가프로세스는 강제 중지됩니다. 이때 해당 강제 중지에 대한 로그가 백그라운드 접근 종료 이벤트 로그입니다.

(4) 클라이언트PC

데이터보호 이벤트가 발생한 에이전트가 속한 클라이언트PC 명입니다.

(5) 클라이언트IP

클라이언트PC에 설정된 IP주소를 표시합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(6) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

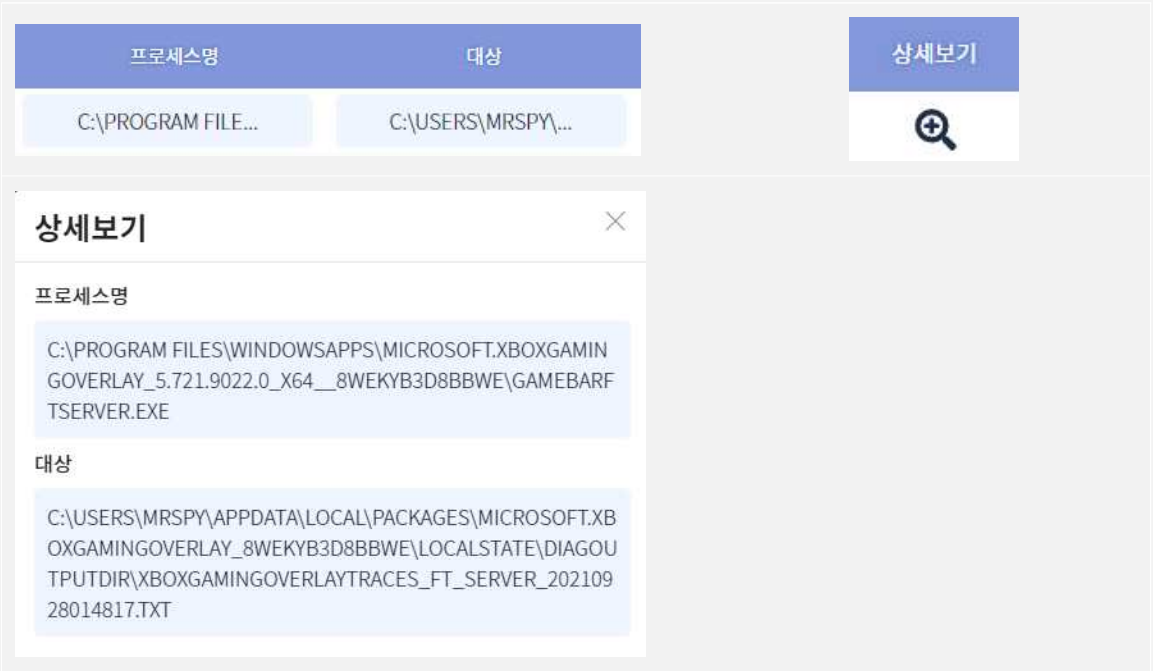
(7) 프로세스명

보호대상 파일에 접근하여 차단/종료된 비인가 프로세스 정보로 프로세스 경로 및 프로세스명을 표시합니다.

(8) 대상

비인가프로세스가 접근한 대상인 보호대상 파일의 정보로 파일경로 및 파일명을 표시합니다.

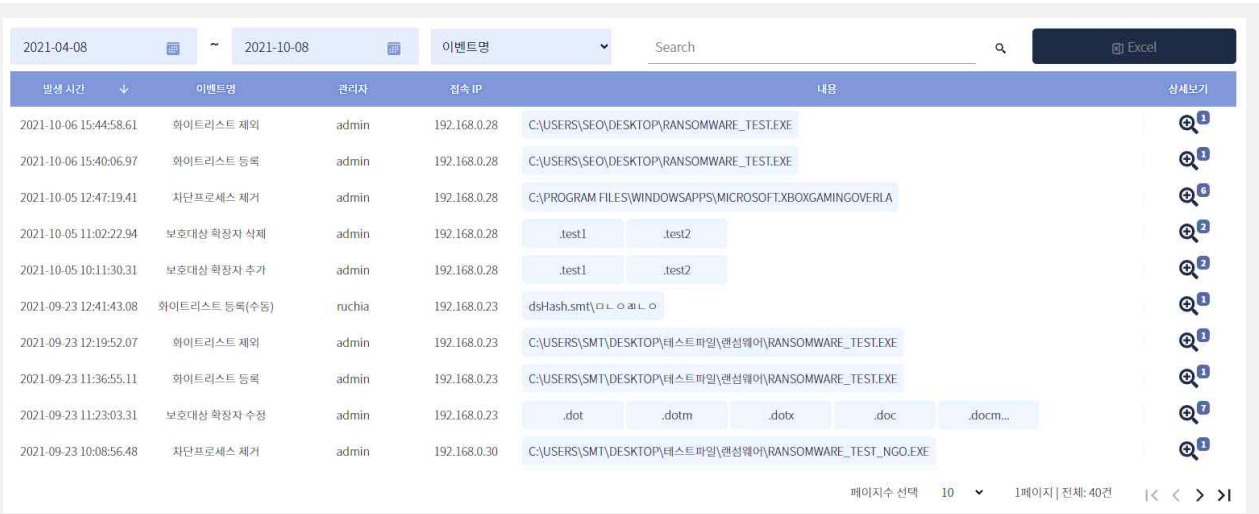
(9) 상세보기



[프로세스명], [대상]의 상세 정보를 표시합니다.

데이터 정책 설정 로그

[데이터보호정책]의 [보호확장자] 추가/삭제/수정 등의 이벤트 발생, [화이트리스트] 등록/제외 이벤트 발생, [차단프로세스] 화이트리스트 등록/차단프로세스 제거 등의 이벤트 발생 관련 감사로그입니다.



(1) 발생시간

해당 이벤트가 발생한 시간을 표기합니다.

(2) 이벤트명

이벤트 내용에 대한 작업유형을 표기합니다.

(3) 관리자

데이터 정책설정 작업을 진행한 관리자 계정 ID를 표기합니다.

(4) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

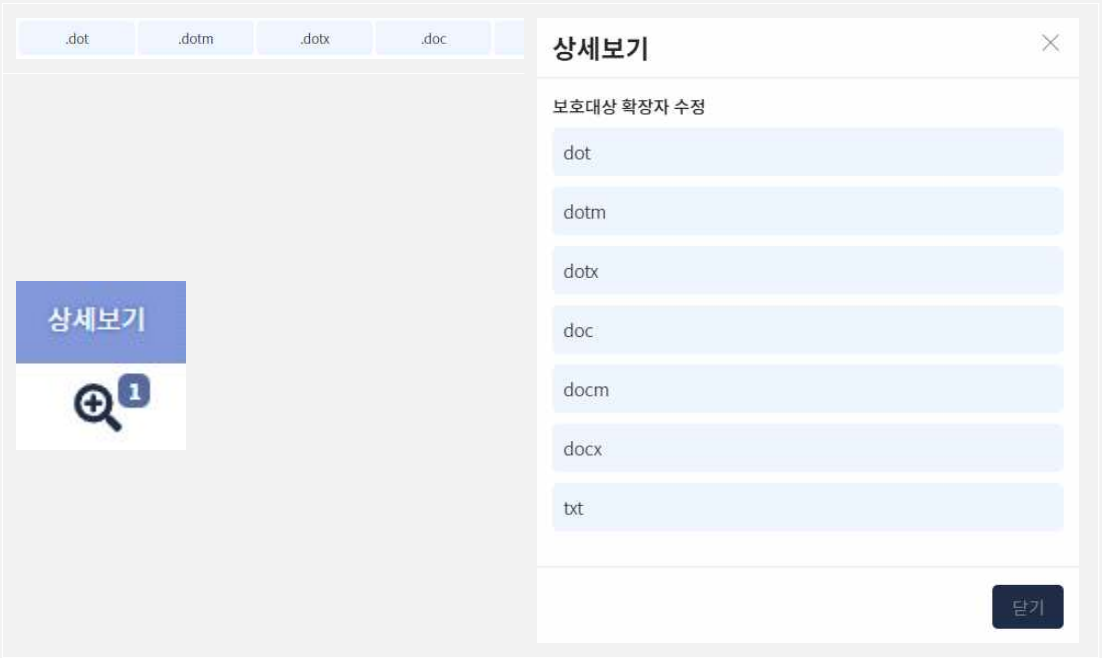
(5) 내용

발생한 이벤트에 대한 간략한 내용을 표기합니다.

(6) 상세보기

① 보호확장자 내용 상세보기

보호 확장자에 대한 변경과 관련한 이벤트를 표기합니다.

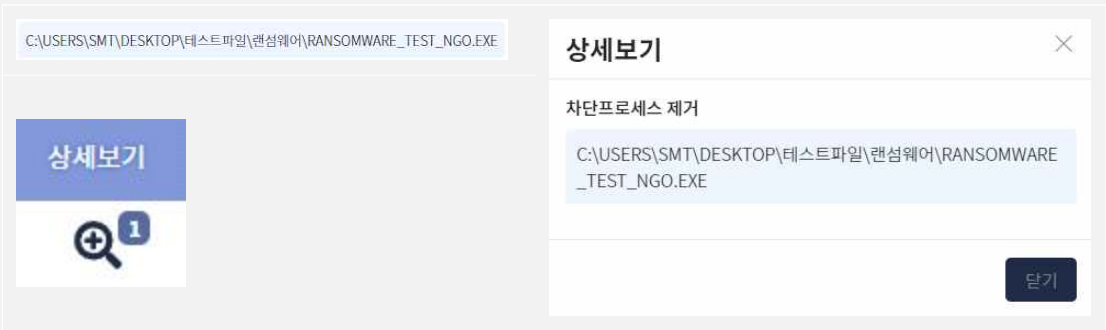


② 화이트리스트 내용 상세보기

화이트리스트 내용에 대한 변경 이벤트를 표기합니다.

③ 차단프로세스 내용 상세보기

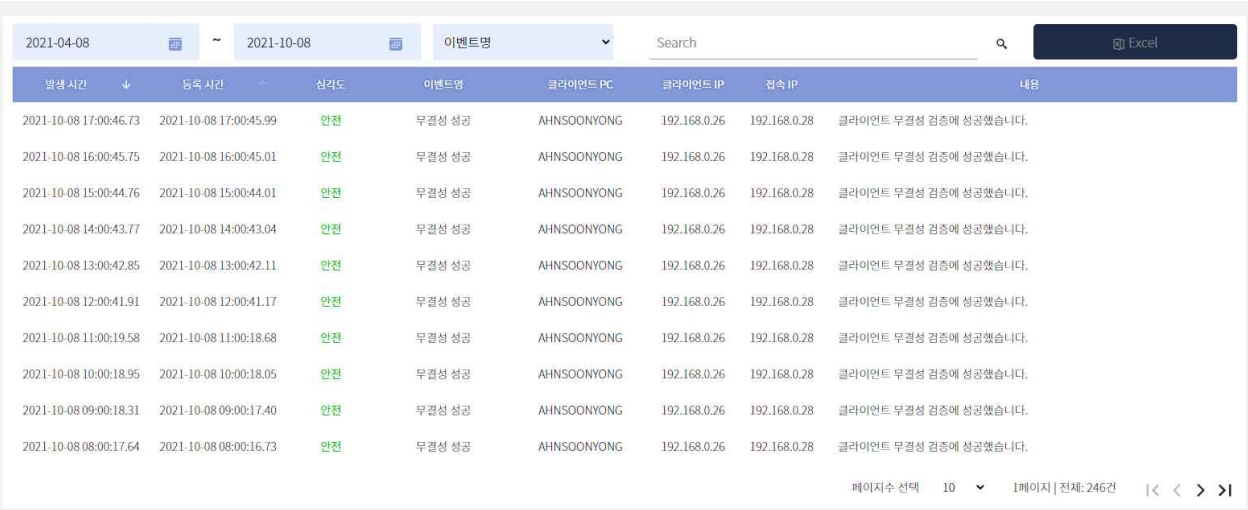
비인가프로세스에 의한 보호대상 파일 접근 시 차단 및 실행 종료에 대한 이벤를
표기합니다.



클라이언트 로그

에이전트가 설치된 클라이언트PC에서 발생하는 감사 내용 중 데이터 보호 이벤트 이외의 내용을 관리서버로 전송 후 관리되는 로그입니다.

주요 내용으로는 에이전트 시작 및 에이전트 무결성 검증에 대한 성공/실패에 대한 이벤트를 저장합니다.



(1) 발생시간

해당 이벤트가 발생한 시간을 표기합니다.

(2) 등록시간

관리서버로 전송되어 등록된 시간을 표기합니다.

(3) 심각도

클라이언트PC에서 발생한 이벤트는 보안에 심각한 이벤트가 포함될 수 있어 관리자가 빠른 대응을 할 수 있도록 발생한 이벤트의 심각도를 표기합니다.

(4) 이벤트명

이벤트 내용에 대한 작업유형을 표기합니다.

(5) 클라이언트PC

이벤트가 발생한 에이전트가 속한 클라이언트PC 명입니다.

(6) 클라이언트IP

클라이언트PC에 설정된 IP주소를 표시합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(7) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(8) 내용

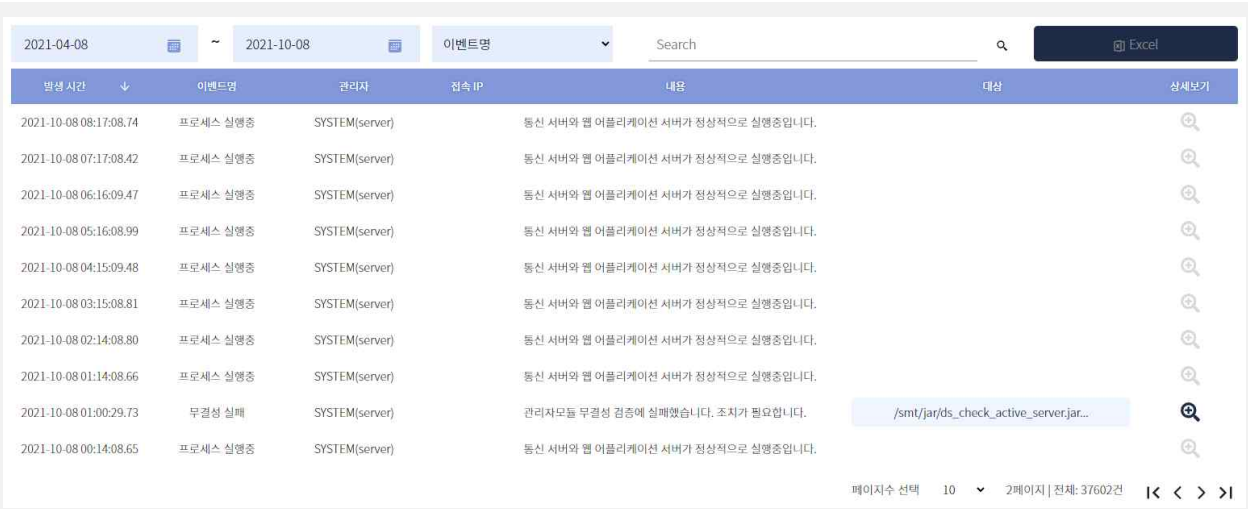
클라이언트PC에서 발생하는 이벤트 내용을 표시합니다.

[설정관리-운영환경설정]에서 팝업표시를 표기로 설정하였을 경우클라이언트PC에 팝업창으로 해당 이벤트 로그가 보여집니다.

시스템 로그

독스토리 관리서버가 설치되어 있는 서버의 상태에 대한 감사 데이터 로그입니다.

주요 내용으로는 에이전트와 통신을 위한 통신서버의 상태, 업데이트 파일의 무결성 상태 및 처리 결과, 관리자 모듈 무결성 검증 결과, 어플리케이션 서버의 상태, 감사기록 시작 및 종료 등에 대한 로그를 저장합니다.



(1) 발생시간

시스템로그 발생 시간을 표시합니다.

(2) 이벤트명

이벤트 종류명을 표기합니다.

(3) 관리자

시스템로그 발생 주체를 표기합니다.

(4) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(5) 내용

시스템에서 발생한 이벤트의 내용을 표기합니다.

(6) 대상

발생한 이벤트의 대상을 표기합니다.

(7) 상세보기

이벤트가 발생한 대상에 대한 정보를 상세히 표기합니다.

운영환경 설정 로그

[설정관리-운영환경설정]에서 발생하는 정책 생성 및 변경에 대한 감사 데이터 로그입니다.

각 설정항목에 대한 자세한 내용은 [IX.설정관리-운영환경설정]을 참고바랍니다.

(1) 발생시간

운영환경설정 이벤트가 발생한 시간을 표기합니다.

(2) 이벤트명

이벤트 종류명을 표기합니다.

(3) 관리자

운영환경설정을 생성 및 변경한 관리자의 ID를 표기합니다.

(4) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

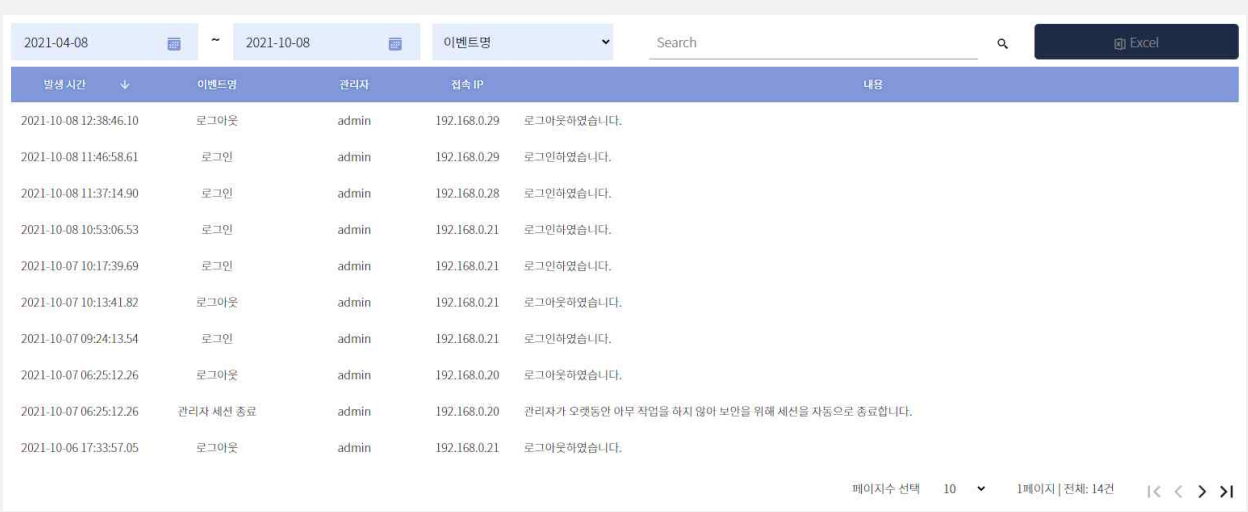
[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(5) 내용

[운영환경 설정]에서 일어난 감사 이벤트에 대한 내용을 상세하게 표기합니다.

계정 설정 로그

관리자의 등록, 수정, 삭제와 각 관리자의 로그인 관련 이벤트 발생의 감사 데이터를 로그로 저장합니다.



(1) 발생시간

계정 설정 로그 이벤트가 발생한 시간을 표기합니다.

(2) 이벤트명

이벤트 종류명을 표기합니다.

(3) 관리자

이벤트 발생 주체를 표기합니다.

(4) 접속IP

독스토리 관리서버에서 에이전트를 바라볼 때 표시되는 IP주소를 표기합니다.

[Ⅶ.클라이언트 관리 - 클라이언트 정보]를 참고하세요

(5) 내용

계정 관련 감사 이벤트에 대한 내용을 상세하게 표기합니다.

IX 설정관리

운영환경 설정

조직의 환경에 따라 다양한 정책을 설정할 수 있도록 지원합니다.
정책 설정 후 화면 하단의 [저장하기]버튼을 클릭하면 변경된 정책은 즉시 반영됩니다.

1. 로그 설정

감사로그의 보존일수를 설정합니다. 정해진 보존일수가 지난 로그는 자동 삭제됩니다.

2. 솔루션 설정

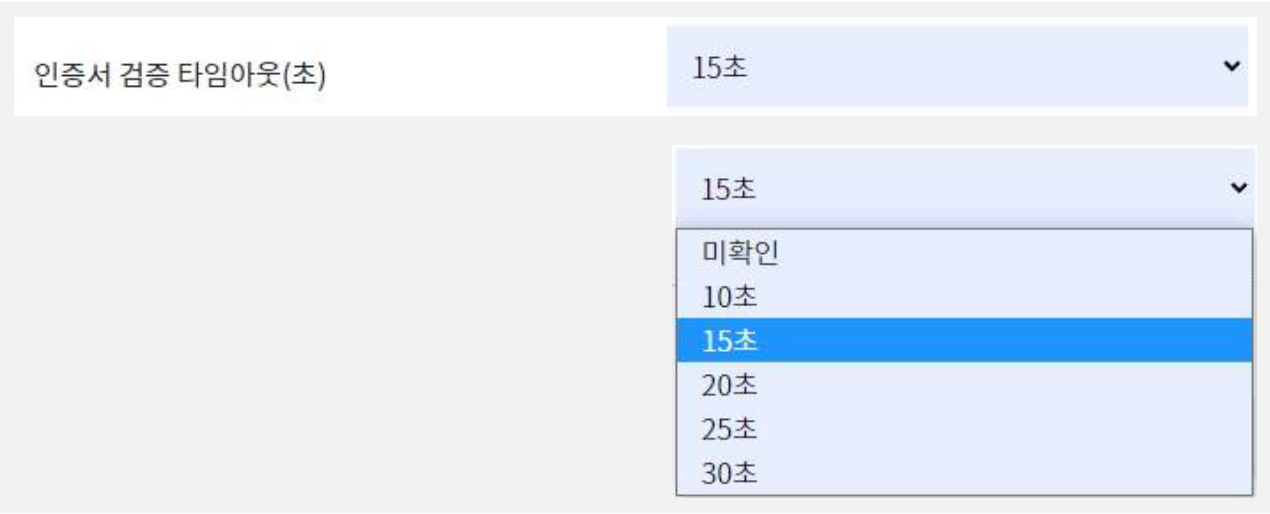
(1) 프로세스 중지기능

비인가프로세스의 보호대상 파일 접근 시 해당 비인가프로세스의 보호대상 파일 접근 횟수가 [차단기준점 설정]횟수를 초과하는 경우
비인가프로세스를 강제로 중지하는 기능을 설정합니다.

(2) DocStory아이콘 노출

클라이언트PC에 독스토리 에이전트가 설치되면 상태표시줄에 독스토리 아이콘이 생성됩니다. 클라이언트PC에 독스토리 아이콘을 노출시키지 않을 경우 해당 기능을 설정할 수 있습니다.

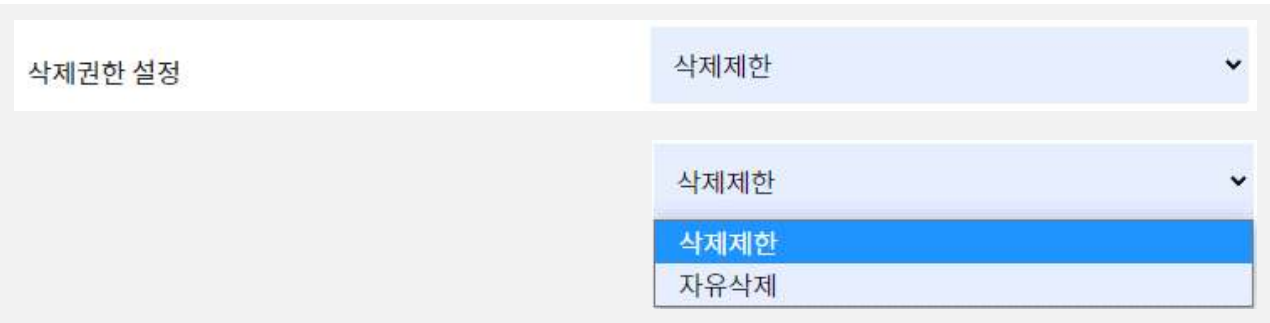
(3) 인증서 검증 타임아웃(초)



(4) 삭제권한 설정

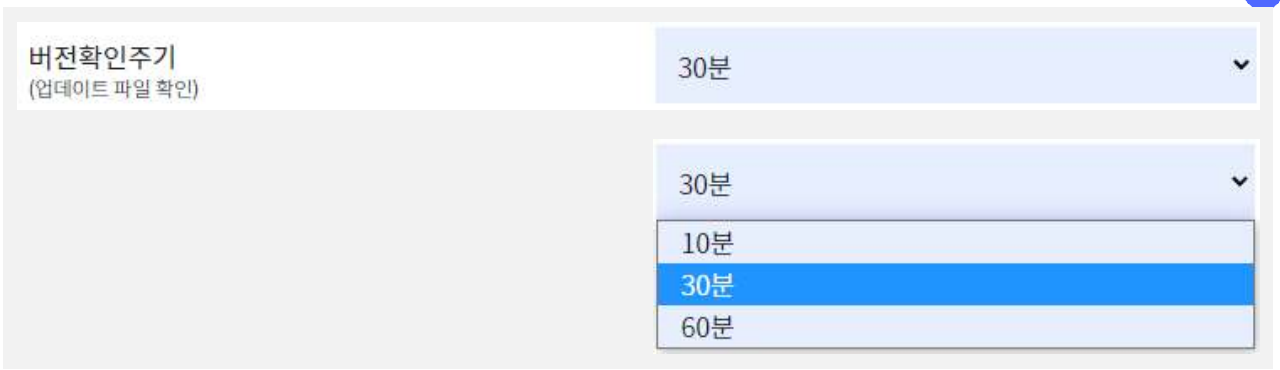
일반 사용자에게 독스토리 에이전트 삭제 권한을 제한하도록 설정할 수 있습니다.

해당 삭제제한 설정 시 에이전트 삭제 방법은 [클라이언트 관리-클라이언트 삭제신청]의 내용을 참고하세요.



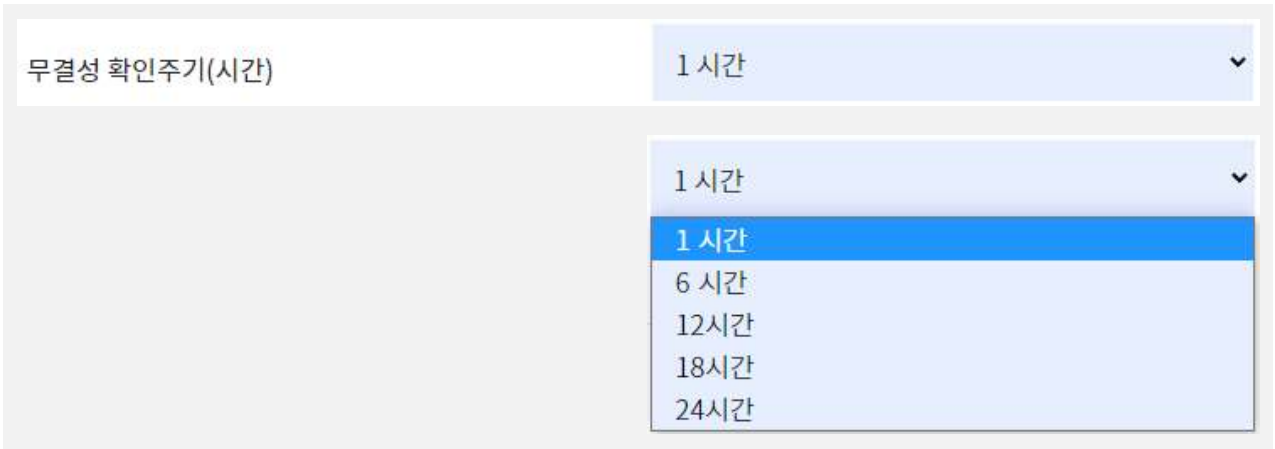
(5) 버전확인 주기(업데이트 파일 확인)

설정된 시간 간격으로 에이전트는 관리서버에 접속하여 에이전트 업데이트 버전을 주기적으로 확인합니다. 운영환경과 네트워크 여건, 그리고 관리 정책에 상황에 맞게 설정합니다.



(6) 무결성 확인 주기(시간)

에이전트는 클라이언트PC가 시작될때마다 무결성 검사를 진행하지만 설정된 시간에 따라 주기적으로 무결성 검사를 진행합니다. 운영환경과 네트워크 여건, 그리고 관리 정책에 상황에 맞게 설정합니다.



3. 팝업표시

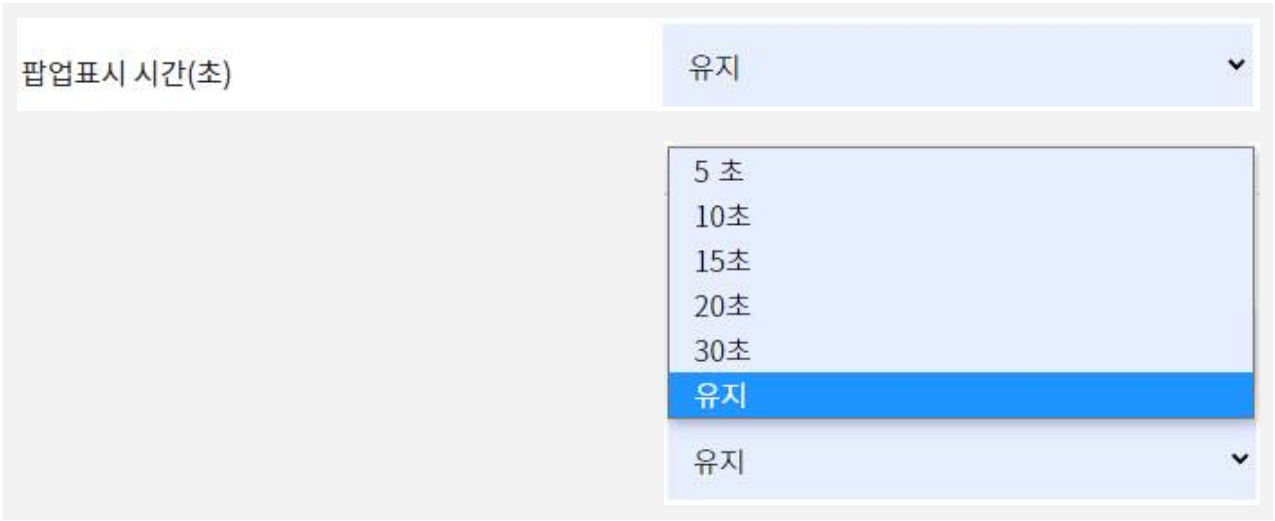
에이전트 화면에 팝업창으로 정보를 표시하는 기능과 관련한 설정입니다.

(1) 팝업표시(팝업표시여부)

클라이언트PC에서 이벤트가 발생하면 해당 PC화면에 이벤트에 대한 알림 팝업이 생성됩니다. 이때 관리자는 에이전트가 설치된 클라이언트PC에 팝업 알림이 생성되지 않기를 원하는 경우 이에 대한 설정을 할 수 있습니다.

(2) 팝업표시 시간(초)

클라이언트PC에 팝업 창이 유지되는 시간을 설정할 수 있습니다. 선택 사항 중 [유지]를 선택하는 경우 사용자가 해당 팝업창을 닫을때까지 창은 유지됩니다.



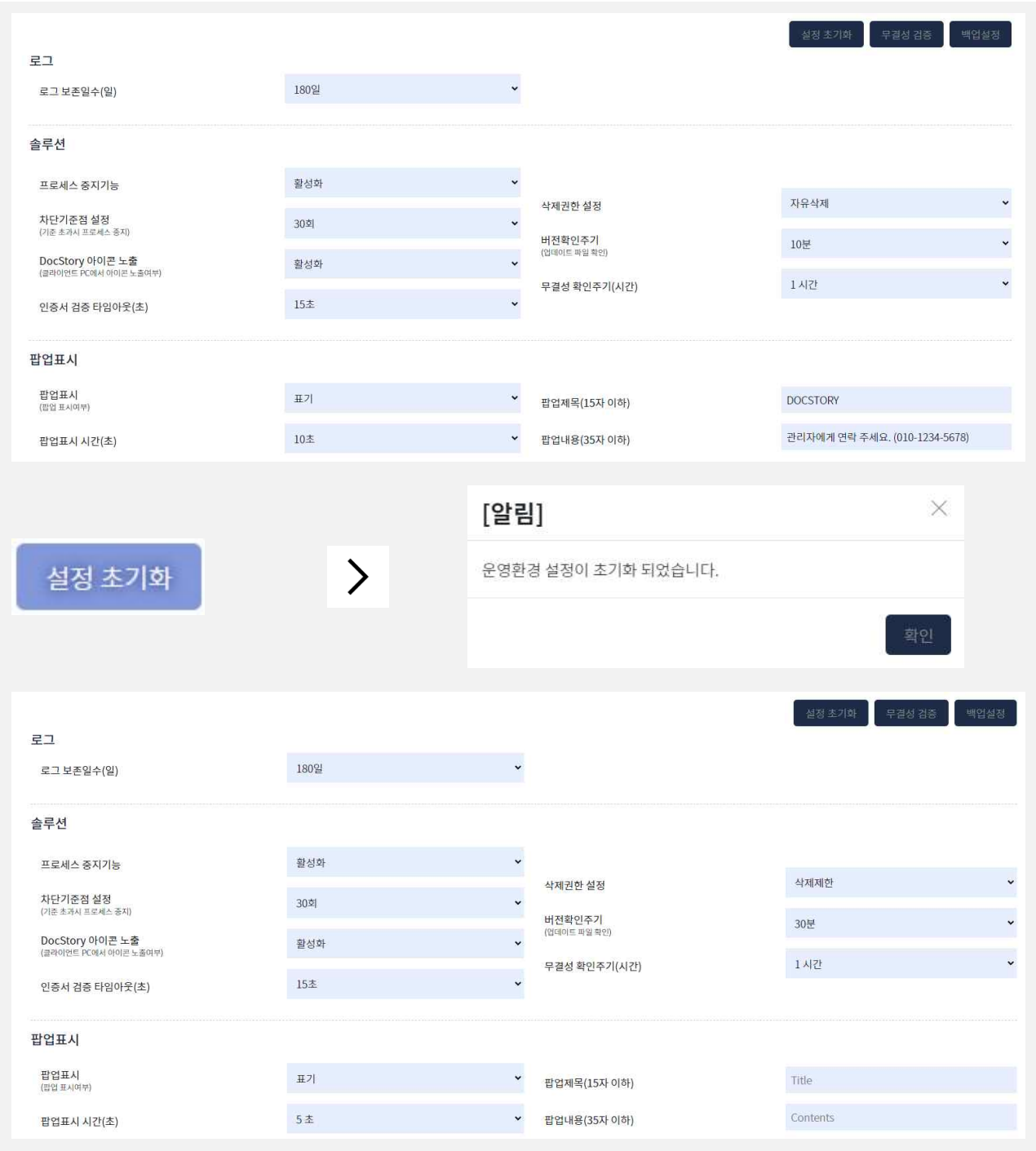
(3) 팝업제목/팝업내용

팝업 창에 제목 및 고정 내용을 표기할 수 있습니다. 이때 제목은 15자 이하, 표기 내용은 35자 이하로 제한됩니다.

4. 설정 초기화

운영환경 설정을 초기화 하기 위해서는 화면 우측 상단의 [설정 초기화]버튼을 클릭하면 초기 설치 시 설정 상태로 초기화 됩니다.

혹여 잘못 초기화 하였을 경우 뒤에 설명할 [백업 설정]에서 백업해두었던 설정을 이용하여 복구하실 수 있습니다.

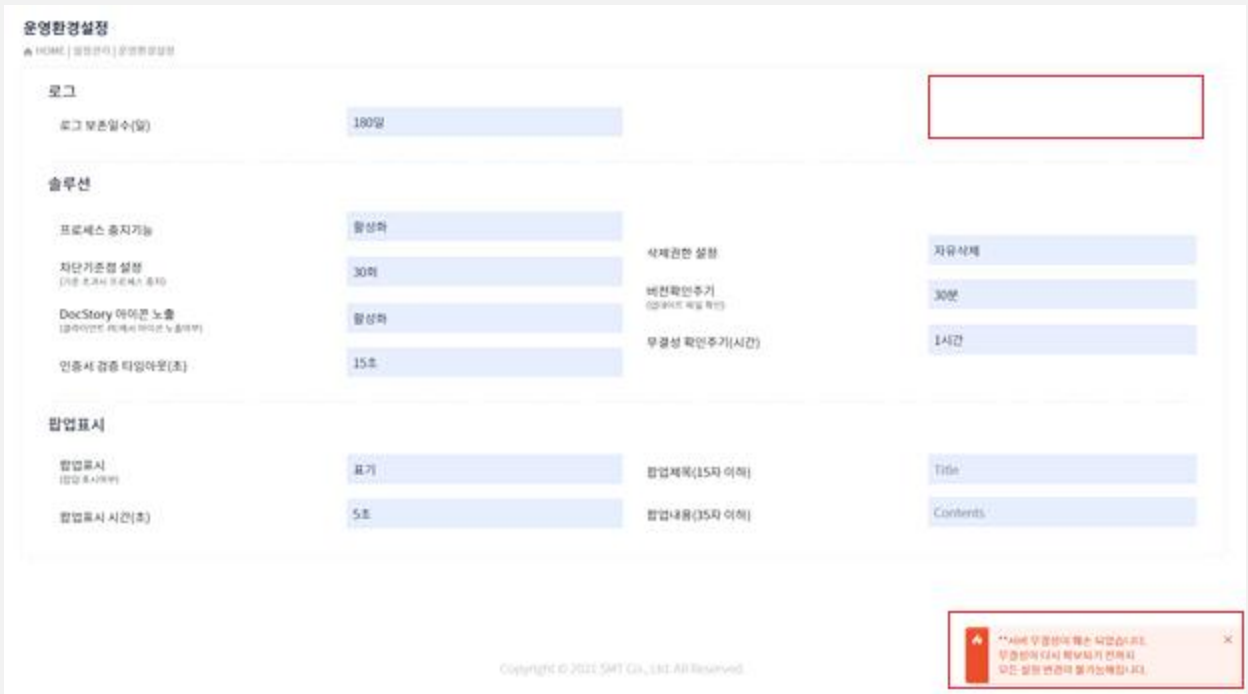


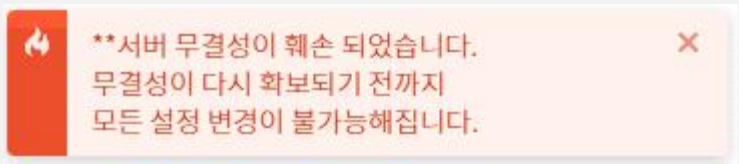
5. 무결성 검증

관리 서버의 무결성 검증을 수동으로 진행하기 위한 기능으로 [설정관리-운영환경설정]의 우측 상단에 있는 [무결성 검증]버튼을 클릭하시면 서버 무결성 검증이 진행됩니다.

서버 무결성 검증 진행 후 무결성 훼손이 발견되는 경우 화면 우측 상단의 [설정 초기화] [무결성 검증] 등의 버튼이 비활성화 되고, 화면 우측 하단에 무결성 훼손에 대한 알림 메시지 팝업이 활성화 됩니다.

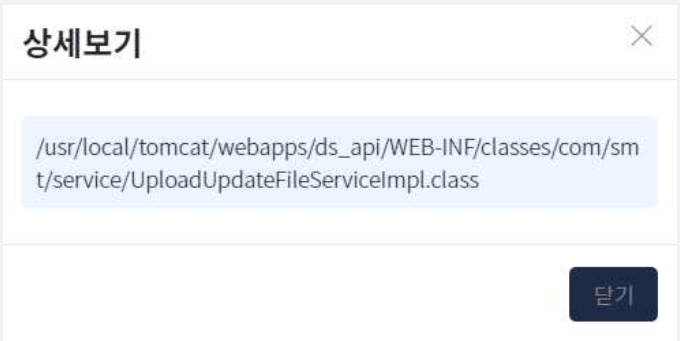
※ 서버 무결성 훼손 시 즉각적으로 구매처나 개발사(에스엠테크놀러지(주))로 연락하여 주시고 알려드리는 방법에 따라 대응해주시기 바랍니다.





서버 무결성 훼손 시 [감사로그-시스템로그]에서 확인 할 수 있는 무결성 실패 로그

발생 시간	이벤트명	관리자	접속 IP	내용	대상	상세보기
2021-10-13 20:22:55.89	무결성 실패	admin	192.168.0.28	관리자모듈 무결성 검증에 실패했습니다. 조치가 필요합니다.	/usr/local/tomcat/webapps/ds_api/WE...	
2021-10-13 20:22:55.66	무결성 실패	admin	192.168.0.28	관리자모듈 무결성 검증에 실패했습니다. 조치가 필요합니다.	/usr/local/tomcat/webapps/ds_api/WE...	



6. 백업설정

운영환경설정에서 적용해온 각종 정책 및 감사로그에 대하여 백업을 할 수 있고, 기존 백업했던 설정 및 로그를 복원할 수 있는 기능입니다.

[설정관리 – 운영환경설정] 화면의 우측 상단에 있는 [백업 설정] 버튼을 클릭하면 백업관련 기능 화면이 생성됩니다.

(1) 백업 옵션 및 백업 대상

백업할 기간을 선택하고, 감사로그 중 백업할 로그를 선택합니다. 이때 정책 중 운영환경 정책과 데이터보호정책은 기본 백업 요소로 선택할 수 없습니다.

① 백업 기간 선택

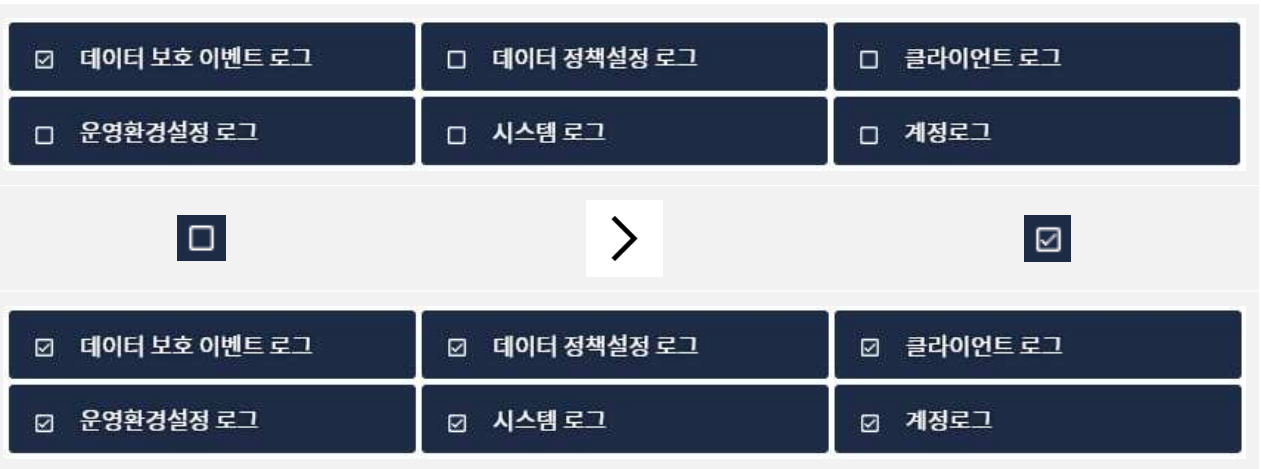
백업할 기간을 선택합니다.

달력에서 원하는 연월일을 선택합니다.
기간 선택 시 시작 날짜는 [설정관리-운영환경 설정]의 로그 보존일수 설정에 따라 현재일 기준 로그 보존일수 이후부터 가능합니다.

② 백업할 감사 로그 선택

감사로그들 중 백업할 로그를 선택합니다. 각 로그 이름 앞의 체크박스에 체크하면 백업 선택이 됩니다.

[운영환경 정책]과 [데이터보호 정책]은 선택사항이 아닙니다.



③ 백업 진행

백업 기간과 백업 항목을 선택한 후 [백업]버튼을 클릭하면 해당 내용이 백업됩니다.

(2) 백업 히스토리

백업된 정책 및 로그를 백업 시간에 따라 리스트로 관리하며, 해당 백업 시점으로 복원 및 백업 데이터를 다운로드 할 수 있습니다.

① 백업 복원

복원할 백업 파일 항목의 [복원] 항목의 아이콘을 클릭하면 해당 백업 파일 내용이 자동 복원됩니다. 이때, 로그의 경우 백업 기간에 해당되지 않는 로그는 삭제되지 않습니다.

② 백업 다운로드

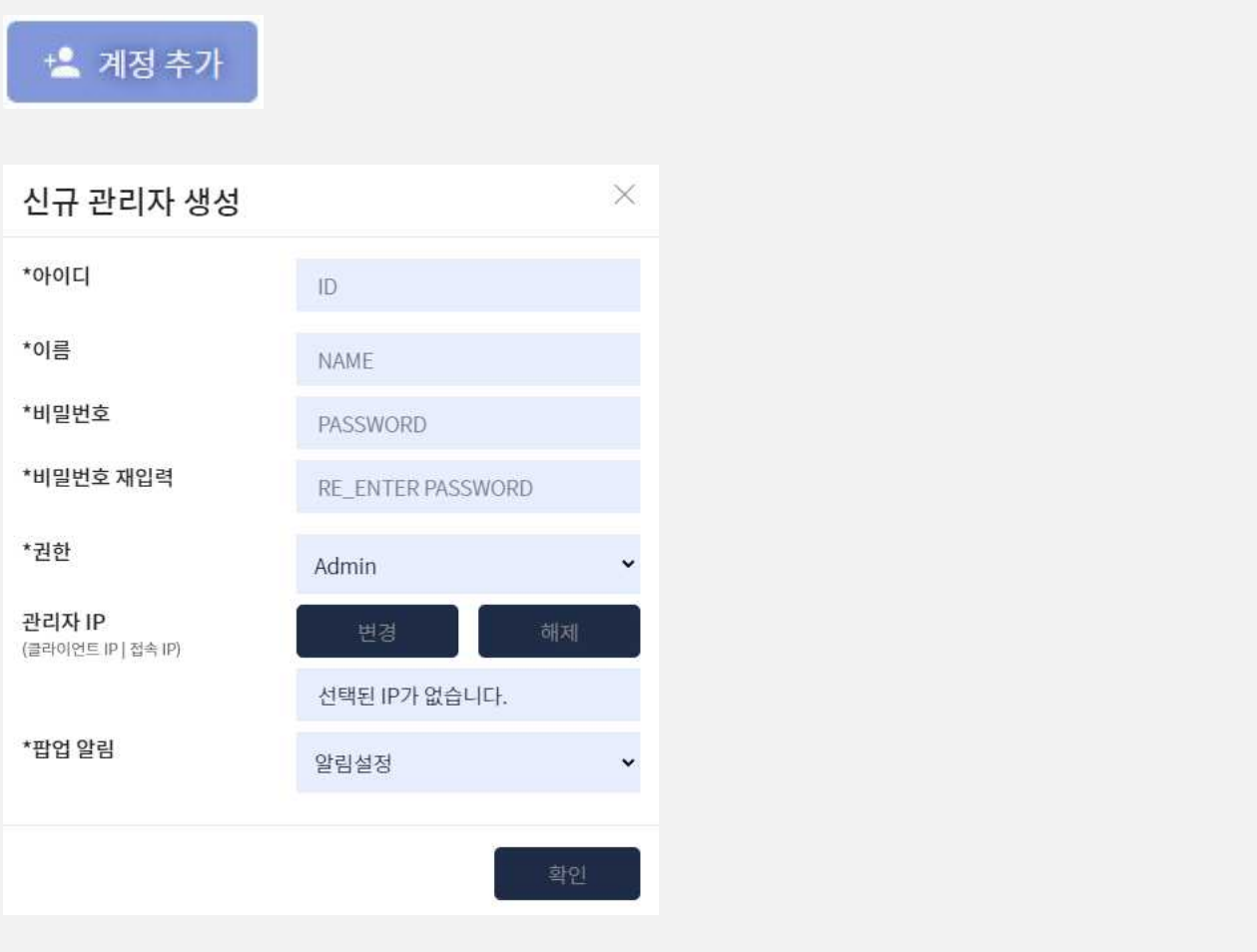
다운로드할 항목에 있는 다운로드 아이콘을 클릭하면 해당 백업 데이터가 SQL문으로 다운로드 할 수 있습니다.

계정 설정

본 솔루션에서 제공되는 관리자는 두가지 종류가 있습니다. 각종 환경설정 및 계정 추가/수정/삭제 할 수 있는 SuperAamin과 단순 모니터링할 수 있는 Admin입니다.

1. 계정추가

계정설정 메뉴에서 오른쪽 상단의 [계정추가] 버튼을 클릭하면 [신규 관리자 생성] 팝업창이 열립니다.
신규 관리자 계정을 생성하고 권한 및 IP, 팝업(관리자 전용 팝업) 설정을 진행합니다.



(1) 아이디

아이디는 [영어 대문자, 영어 소문자, 숫자]의 조합으로 구성되어야 하며 총 길이는 50자 이하여야 합니다.

(2) 비밀번호

아래의 모든 항목을 만족해야 패스워드를 생성할 수 있습니다.

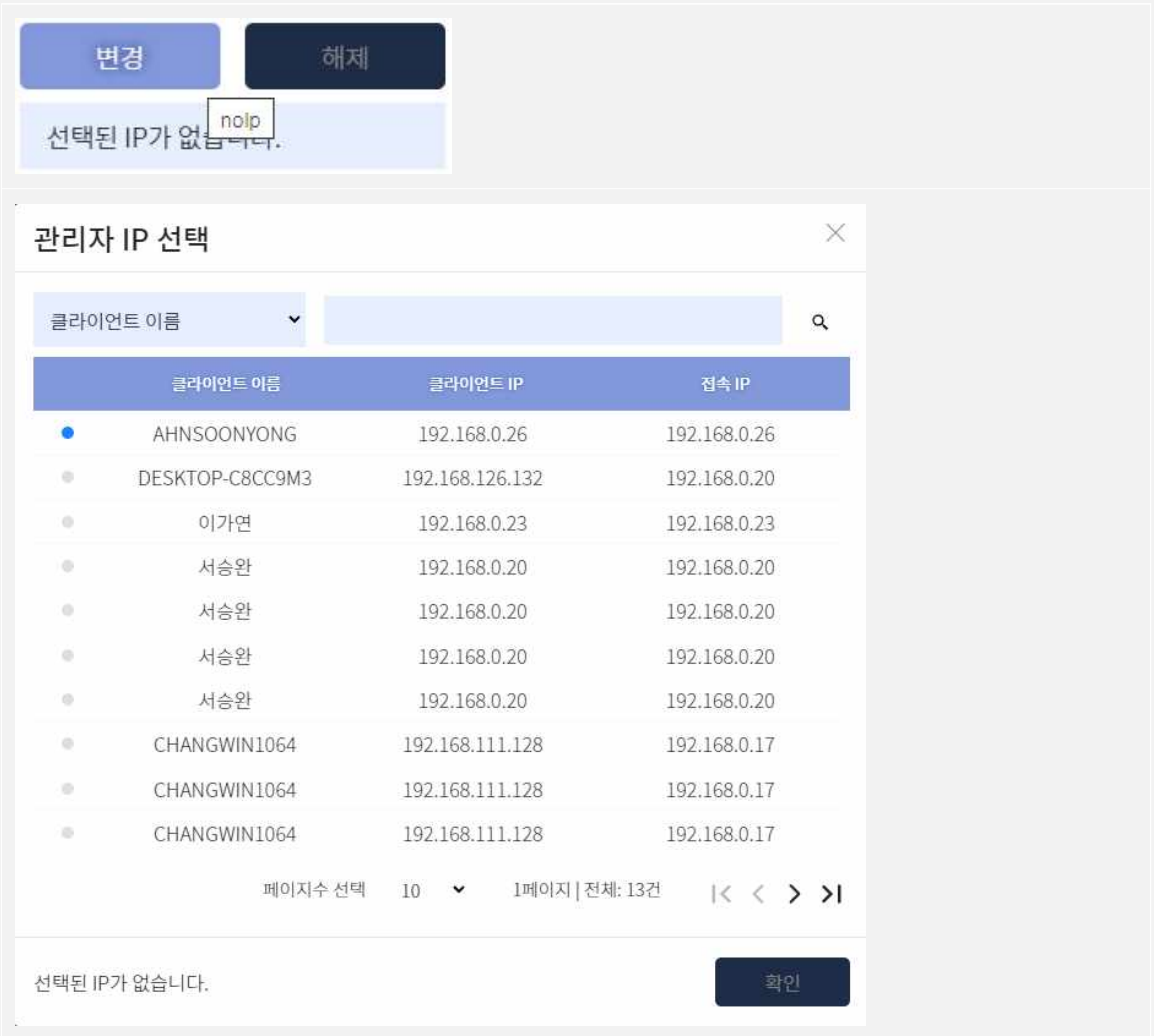
- 대문자, 소문자와 숫자, 특수문자가 포함되어야 합니다.
- 9자 이상 20자 미만이어야 합니다.
- 사용자 계정(아이디)가 포함된 패스워드는 사용할 수 없습니다.
- 동일한 단어를 연속적으로 3회 이상 반복할 수 없습니다.
- 연속적인 키보드 배열의 4자 이상을 패스워드로 할 수 없습니다.

(3) 권한

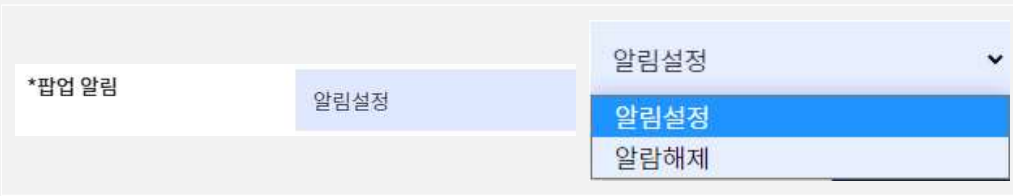
관리자의 권한은 Admin과 Super Admin 두가지 권한 중 하나를 선택할 수 있습니다. Super Admin은 2개의 계정까지 생성 할 수 있습니다. Admin권한은 정책 설정 등 주요한 설정 생성 및 변경 권한을 가지지 못합니다.

(4) 관리자IP

[변경] 버튼을 클릭하면 나타나는 팝업창 리스트에서 선택된 IP로 관리자 접속 가능합니다. IP를 변경할 때 [변경]버튼으로 나타나는 리스트로 선택하고, IP할당하지 않을 경우 이미 선택된 IP를 삭제하기 위하여 [해제]버튼을 클릭하면 선택된 IP가 삭제됩니다.



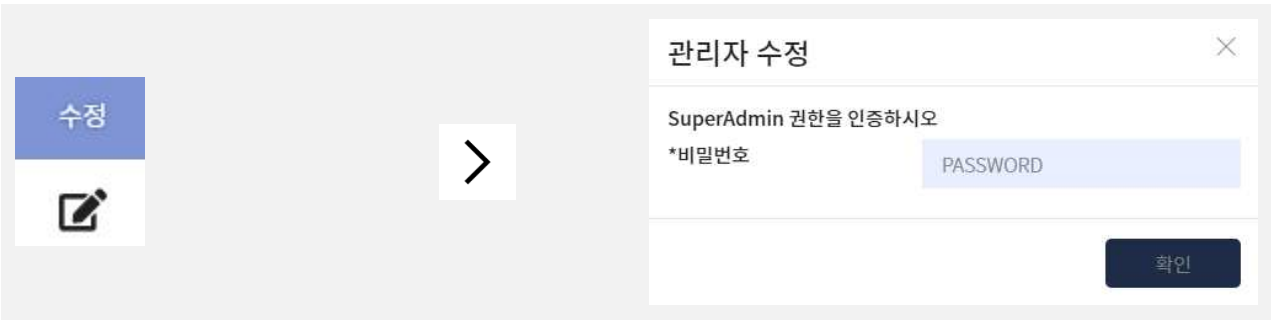
(5) 팝업 알림

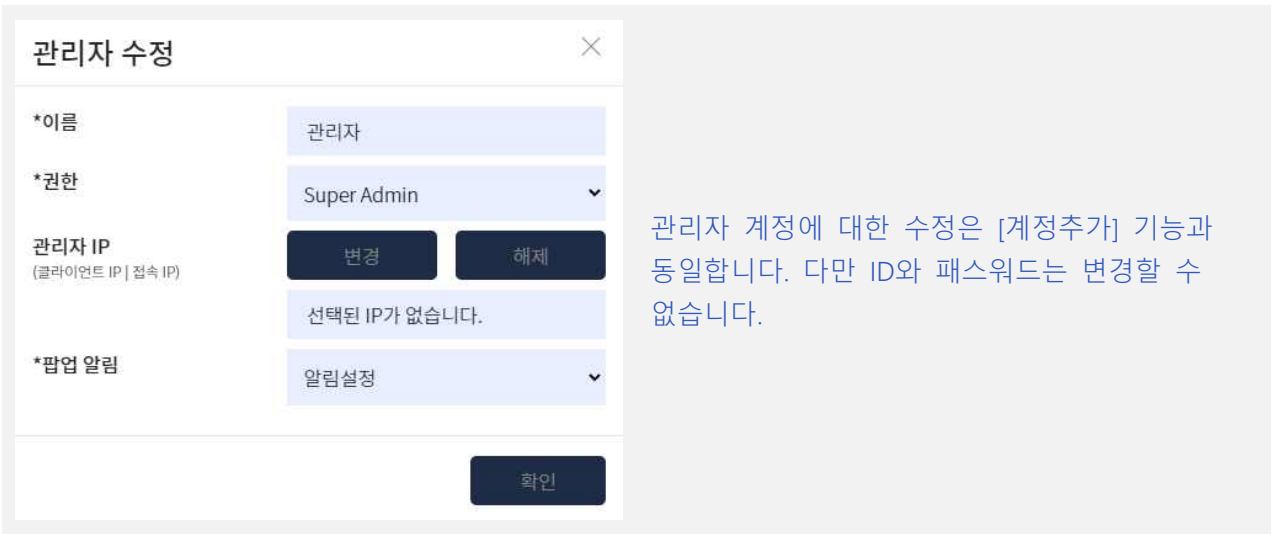


2. 계정 수정 및 삭제

(1) 계정 수정

한번 설정된 관리자 계정에 대한 수정은 매우 신중해야 하기 때문에 수정 기능 활성화를 위하여 권한 인증 단계를 통과해야 합니다.

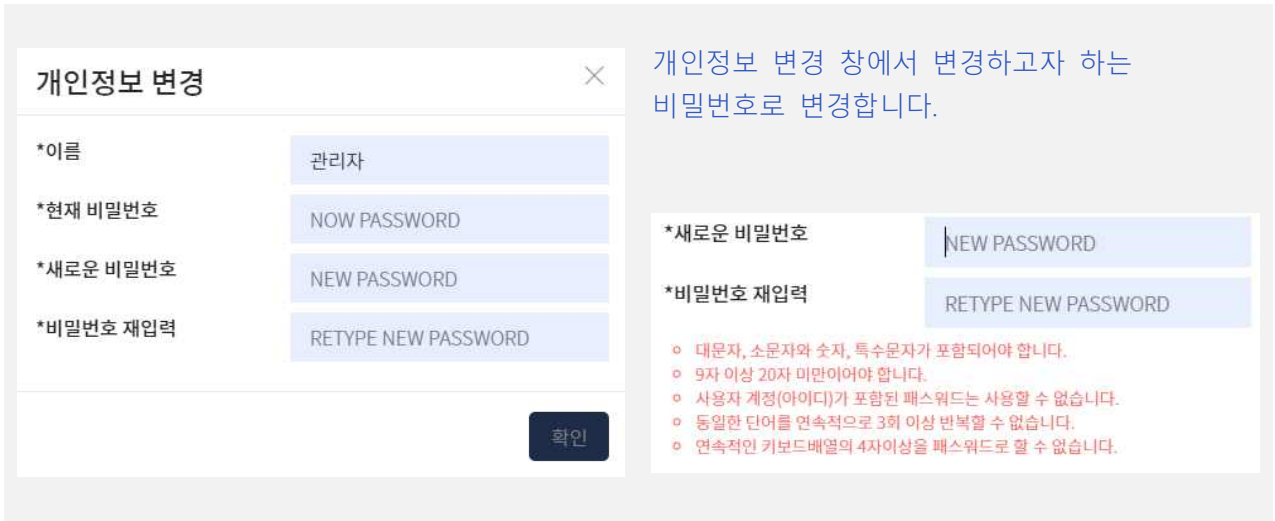




관리자 계정에 대한 수정은 [계정추가] 기능과 동일합니다. 다만 ID와 패스워드는 변경할 수 없습니다.

관리자의 비밀번호 변경을 위해서는 해당 관리자 계정으로 로그인 상태에서 관리자화면 우측 상단의 [관리자] 메뉴 중 [마이페이지]를 선택합니다.

비밀번호를 입력하면 개인정보 변경 창이 열립니다.

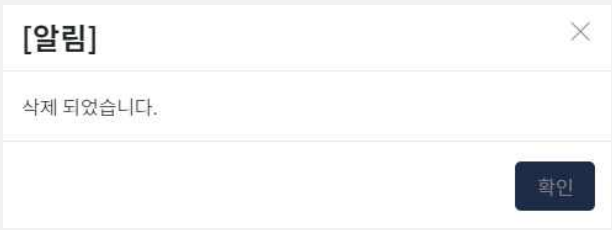


(2) 계정 삭제

최초 설치 시 생성된 admin계정은 권한과 관계없이 삭제할 수 없습니다.

권한이 admin인 경우 삭제 권한이 없습니다. 권한이 SuperAdmin인 경우만 삭제 할 수 있습니다.

설치 시 최초 생성되는 admin계정은 삭제할 수 없습니다.



SuperAdmin권한을 가지고 있는 관리자 계정으로 다른 관리자 계정을 삭제 할 수 있습니다. 이때도 최초 admin계정은 삭제 할 수 없습니다.

업데이트 설정

에이전트 업데이트는 파일 등록 후 [설정관리 – 운영환경설정]의 버전확인 주기에 설정된 시간 간격으로 자동 업데이트 됩니다.

1. 업데이트 파일 등록

업데이트 파일 등록을 위해서는 온전한 업데이트 파일과 업데이트 파일에 대한 유효성 검증 파일을 함께 등록하여야 하며, 사전에 정해진 규칙에 위배되는 경우 업데이트 파일이 등록되지 않습니다. 업데이트 파일은 독스토리의 개발사인 에스엠테크놀러지(주)에서 공식적으로 제공되는 파일만 등록 할 수 있습니다.

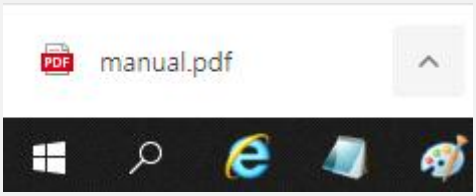
2. 자동업데이트 설정

업로드된 업데이트 파일에 대하여 [자동업데이트 설정]이 되어 있어야 업데이트 됩니다.

X 사용설명서/제품버전 정보

사용 설명서

DocStory매뉴얼 버튼을 클릭하시면 PDF파일로되어 있는 사용설명서를 다운로드 받으실 수 있습니다. 기본적인 내용은 설명서를 참고하시기 바랍니다.



버전 정보

독스토리 패키지에 포함되어 있는 주요 프로세스들의 버전 정보를 표기합니다.

Module Name	DsManager	**Version**	1.15.1.4
Module Name	DsAgent.exe	**Version**	1.15.1.4
Module Name	DocStoryService.exe	**Version**	1.15.1.4
Module Name	DsReset.exe	**Version**	1.15.1.4
Module Name	RSBDrvSvc.exe	**Version**	1.15.1.4
Module Name	SMTDsWatcher.exe	**Version**	1.15.1.4
Module Name	RSBUpdater.exe	**Version**	1.15.1.4

부록

로그 이벤트

데이터 보호 로그 이벤트

이벤트번호	이벤트 내용
601	백그라운드 접근 차단
602	백그라운드 접근 종료
603	백그라운트 접근 타임 아웃

데이터 정책설정 로그 이벤트

이벤트번호	이벤트 내용
101	보호대상 확장자 삭제
102	보호대상 확장자 삭제 실패
103	보호대상 확장자 추가
104	보호대상 확장자 추가 실패
105	보호대상 확장자 수정
106	보호대상 확장자 수정 실패
107	화이트리스트 등록(수동)
108	화이트리스트 등록 실패(수동)
109	화이트리스트 제외
110	화이트리스트 제외 실패
111	차단프로세스 제거
112	차단프로세스 제거 실패
113	화이트리스트 등록 설정
114	화이트리스트 등록 실패

클라이언트 로그 이벤트

이벤트번호	이벤트 내용
401	클라이언트 시작 알림
402	클라이언트 관리(활성화)
403	클라이언트 관리(비활성화)
404	업데이트 파일 정책 위반(보안정책 위반)
405	업데이트 파일 정책 위반(유효하지 않은 파일 등록)
406	업데이트 등록
408	에이전트 삭제/재설치

이벤트번호	이벤트 내용
409	업데이트 설정(허용)
410	업데이트 설정(비허용)
411	필터드라이버 무결성
412	무결성 실패
413	무결성 성공
414	업데이트 전자서명 검증 실패
415	업데이트 무결성 실패
416	설치 실패
417	구성요소 삭제 실패
418	드라이버 종료 실패
419	권한 복구
420	비활성화 실패
421	서비스 등록 실패
422	클라이언트 사용량 경고
423	무결성 복구
424	암호기능장애(암호화 기능 장애)
425	암호기능장애(복호화시 장애)
426	업데이트 전자서명 검증 성공
427	클라이언트 화이트리스트 등록
4011	클라이언트가 시작했습니다.
4021	활성화하였습니다.
4031	비활성화하였습니다.
4041	업데이트 파일 등록 중 보안 정책에 위반되어 중단되었습니다.
4051	유효하지 않은 업데이트 파일을 등록하여 중단되었습니다.'
4061	업데이트 파일이 등록되었습니다.
4081	에이전트 삭제/재설치로 인해 관리자 IP가 해제 되었습니다.
4091	업데이트 설정 정보를 "허용"으로 변경했습니다.
4101	업데이트 설정 정보를 "비허용"으로 변경했습니다.
4111	드라이버 파일 해쉬가 불일치 하여 복구했습니다.
4121	클라이언트 무결성 검증에 실패했습니다.
4131	클라이언트 무결성 검증에 성공했습니다.
4141	업데이트 파일의 전자서명 검증에 실패해 업데이트를 중단했습니다.
4151	업데이트 파일의 무결성 검증에 실패했습니다.
4161	설치 중 일부를 설치하는데 실패했습니다.
4171	구성요소 중 일부를 삭제하는데 실패했습니다.
4181	드라이버를 종료하는데 실패했습니다.
4191	권한무결성을 복구했습니다.
4201	클라이언트 비활성화를 실패했습니다.
4211	서비스 등록에 실패했습니다.

이벤트번호	이벤트 내용
4221	사용량(%s2%) : 남은 용량이 얼마 없습니다. 조치가 필요합니다.
4231	(comName(localIp|remoteIp))에서 contents 파일 해쉬가 불일치하여 복구했습니다.
4241	암호화시 장애가 발생하였습니다.
4251	복호화시 장애가 발생하였습니다.
4261	클라이언트가 업데이트 파일 전자서명 검증에 성공하였습니다.
4271	(프로세스 경로)를 화이트리스트로 등록하였습니다.

시스템 로그 이벤트

이벤트번호	이벤트 내용
201	프로세스 실행중
202	무결성 실패
203	무결성 성공
204	프로세스 재실행
205	감사 기록 시작
206	감사 기록 종료
207	dbms 계정 생성
208	dbms 계정 생성 실패
209	암호기능장애(암호화 기능 장애)
210	암호기능장애(복호화시 장애)
213	보안관리(데이터 복원)
214	보안관리(데이터 백업)
215	사용량 경고(80%)
216	사용량 경고(90%)
217	무결성 검증 실행
219	업데이트 설정 실패(허용)
220	업데이트 파일 등록 실패(버전확인)
221	데이터 백업 실패
222	클라이언트 관리(활성화)
223	클라이언트 관리(비활성화)
224	업데이트 파일 정책 위반(보안정책 위반)
225	업데이트 파일 정책 위반(유효하지 않은 파일 등록)
226	업데이트 등록
227	업데이트 설정(허용)
228	업데이트 설정(비허용)
229	클라이언트 삭제요청 승인
230	클라이언트 삭제요청 거절

이벤트번호	이벤트 내용
231	클라이언트 삭제요청 목록 삭제
241	라이선스 삭제
2011	통신 서버와 웹 어플리케이션 서버가 정상적으로 실행중입니다.
2021	관리자모듈 무결성 검증에 실패했습니다. 조치가 필요합니다.
2031	관리자모듈 무결성 검증에 성공했습니다.
2041	일부 프로세스가 종료되어 재실행되었습니다.
2051	감사 기록 기능이 시작되었습니다.
2061	감사 기록 기능이 종료되었습니다.
2071	dbms default 계정을 생성했습니다.
2081	dbms default 계정 생성에 실패하였습니다.
2091	암호화시 장애가 발생하였습니다.
2101	복호화시 장애가 발생하였습니다.
2131	보안관리 데이터를 복구 하였습니다.
2141	보안관리 데이터를 백업 하였습니다.
2151	사용량(80%) : 서버에 남은 용량이 얼마 없습니다. 조치가 필요합니다.
2161	사용량(90%) : 서버에 남은 용량이 부족하여 용량 확보를 위해 일부 로그가 삭제되었습니다.
2171	무결성 검증을 실행했습니다.
2191	이미 업데이트 설정 정보가 '허용'인 업데이트 파일이 존재합니다.
2201	등록된 동일한 업데이트 파일이 존재하여 업데이트 파일 등록에 실패하였습니다.
2211	요청한 백업 기간에 해당하는 로그가 존재하지 않습니다.
2221	활성화하였습니다.
2231	비활성화하였습니다.
2241	업데이트 파일 등록 중 보안 정책에 위반되어 중단되었습니다.
2251	유효하지 않은 업데이트 파일을 등록하여 중단되었습니다.'
2261	업데이트 파일이 등록되었습니다.
2271	업데이트 설정 정보를 "허용"으로 변경했습니다.
2281	업데이트 설정 정보를 "비허용"으로 변경했습니다.
2291	[List] 클라이언트 삭제요청 승인이 완료되었습니다.
2301	[List] 클라이언트 삭제요청 거절이 완료되었습니다.
2311	[List] 클라이언트 삭제요청 목록을 삭제 하였습니다.
2411	클라이언트 라이선스를 삭제하였습니다.

운영환경 설정 로그 이벤트

이벤트번호	이벤트 내용
501	클라이언트 로그 내용 변경
502	클라이언트 로그 제목 변경
503	로그 보존 일수 설정
504	클라이언트 로그 표시 시간 변경
505	프로세스 차단 한계수 설정
506	클라이언트 삭제 권한 설정(자유삭제)
	클라이언트 삭제 권한 설정(삭제제한)
507	프로세스 차단 기능 설정(차단)
	프로세스 차단 기능 설정(미차단)
508	무결성 확인 주기
509	클라이언트 로그 설정(표기)
	클라이언트 로그 설정(미표기)
510	운영환경설정 초기화
511	업데이트 주기 설정
512	인증서 검증 타임아웃 시간 변경
5011	클라이언트 로그 내용을 변경했습니다.
5021	클라이언트 로그 제목을 변경했습니다.
5101	운영환경설정 초기화를 완료했습니다.
5111	업데이트 주기를 변경했습니다.
5121	value + (으)로 변경했습니다.

계정 설정 이벤트

이벤트번호	이벤트 내용
301	중복 로그인(동일 계정)
302	중복 로그인(동일 권한)
303	로그인
304	로그아웃
305	관리자 세션 종료
306	로그인 실패
307	관리자 계정 변경(권한)
308	관리자 계정 변경(알람)
309	관리용 IP 해제
310	관리용 IP 변경
311	관리자 계정 보안 경고
312	관리자 계정 삭제
313	관리자 계정 추가

이벤트번호	이벤트 내용
314	로그인 차단
315	허용되지 않은 IP
316	관리자 계정 패스워드 변경
317	관리자 계정 패스워드 변경 실패
318	관리자 계정 이름 변경
319	관리자 계정 변경(알람)
320	관리자 계정 변경(권한)
321	default 사용자 계정 삭제 실패
322	현재 로그인 계정 삭제 시도 실패
3011	동일 계정을 다른 사용자가 로그인 했습니다.
3021	동일 권한의 다른 사용자[아이디]가 로그인 했습니다.
3031	로그인하였습니다.
3041	로그아웃하였습니다.
3051	관리자가 오랫동안 아무 작업을 하지 않아 보안을 위해 세션을 자동으로 종료합니다.
3061	로그인 시도하였습니다.
3071	Admin 권한으로 변경되었습니다.
3081	알람설정으로 변경되었습니다.
3091	관리자 클라이언트 설정이 해제 되었습니다.
3101	관리자 IP가 변경 되었습니다.
3111	관리자 계정의 세션이 탈취된 것으로 판단되어 세션을 강제 종료합니다.
3121	write 관리자 계정을 삭제했습니다.
3131	tester 관리자 계정을 추가했습니다.
3141	오류회수 초과로 관리자 계정 로그인이 차단되었습니다.
3151	허용되지 않은 IP에서 관리자 계정으로 로그인 시도하였습니다.
3161	관리자 계정 패스워드가 변경되었습니다.
3171	관리자 계정 패스워드 변경에 실패하였습니다.
3181	관리자 계정 이름이 변경되었습니다.
3191	알람해제로 변경되었습니다.
3201	Super Admin 권한으로 변경되었습니다.
3211	default 사용자 계정 삭제에 실패하였습니다.
3221	현재 로그인 계정 삭제에 실패하였습니다.