



Anti-Ransomware Endpoint Security

사용자 매뉴얼

Windows PC Agent

Windows Server Agent

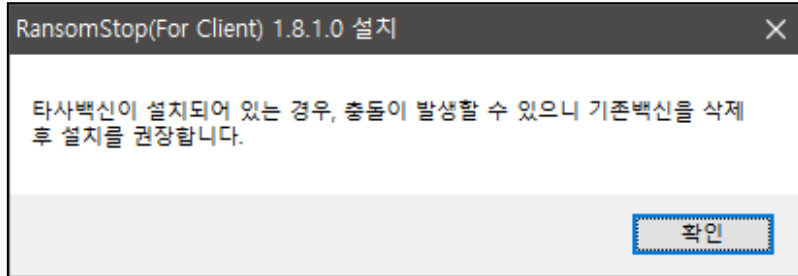
Ver. 1.8

2021. 04

INDEX

1. 설치 전 유의사항	2
2. 설치하기	2
2.1 설치하기	2
2.2 인증하기	3
3. 주요기능	5
3.1 실시간보호	5
3.2 로그	6
3.3 설정	8
3.4 차단정보 및 탐지정보	11
4. 기타기능	12
4.1 버전 업데이트	12
4.2 라이선스 만료	13
4.3 RSM 접속정보 변경	13
4.4 사용자인증 해제	13
5. 에이전트 삭제하기	14

1. 설치 전 유의사항

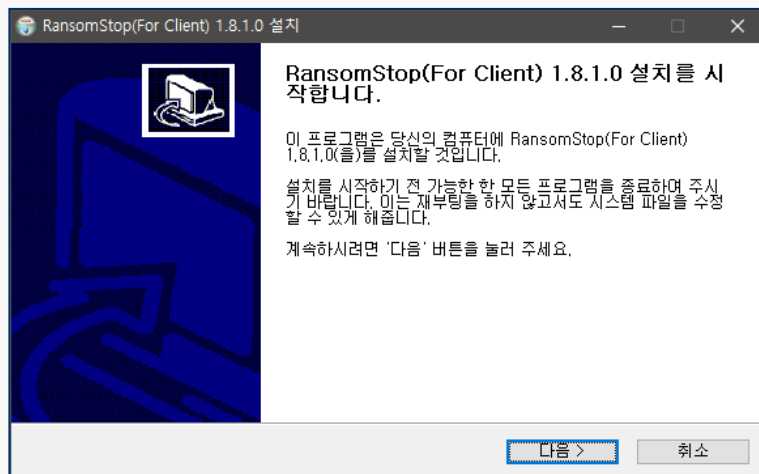


최근 보안의 위험성이 대두되어 대다수 보안제품들은 디지털서명이 된 프로세스에 대해 실행을 허용하고 있으나 타사 제품들의 정확한 기준을 알 수 없어 상호간의 문제점이 발생할 수도 있는 관계로 가급적 타사 보안제품의 삭제 후 설치를 권장합니다.

2. 설치하기

2.1 설치하기

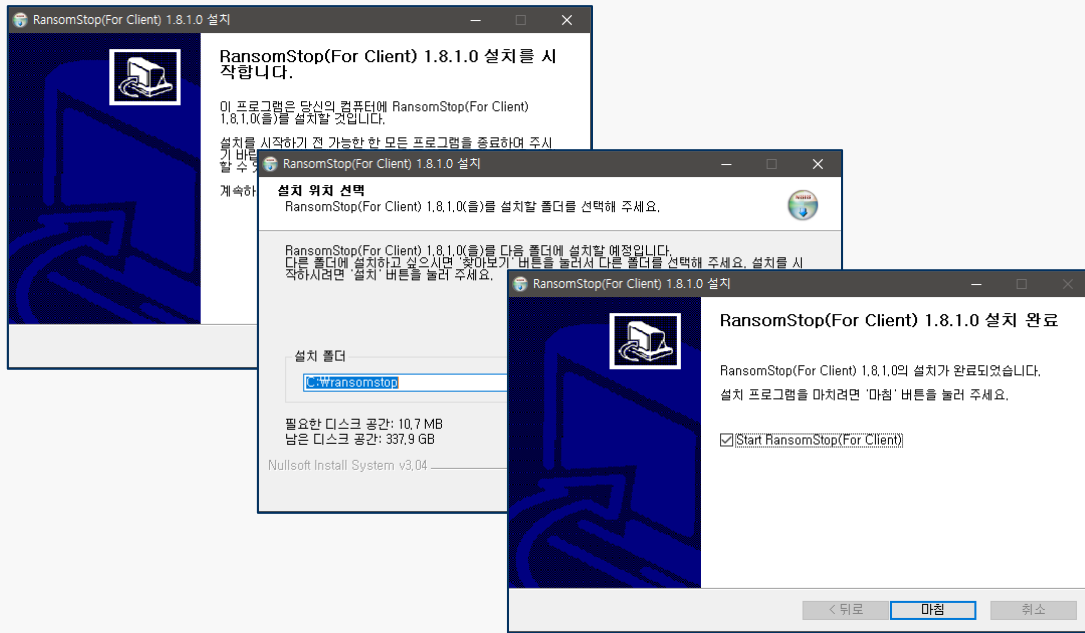
설치파일을 더블 클릭하여 설치합니다.



○ 설치파일명 안내

- PC용 제품 : RansomStop_[버전]_Pro_Client_Setup.exe
- 서버용 제품 : RansomStop_[버전]_Pro_Server_Setup.exe

설치는 기본적으로 C:\Wransomstop 위치에 설치가 됩니다.



2.2 인증하기

설치 완료 후 최초 구동시에는 사용자 인증을 수행하게 됩니다.

2.2.1 RSM 서버URL 설정



기본값으로 상기의 IP, PORT로 입력이 되어 있습니다.

관리자 또는 담당자에게 전달받은 도메인 또는 IP와 PORT를 입력 후 “저장” 버튼을 클릭합니다.

2.2.2 라이선스 확인

정보

RSM URI: 저장

사용자 정보

E-Mail:

이름:

라이선스 확인

사용자 등록

다음에 묻지 않기

상기에서 “저장” 버튼을 눌러 RSM서버와 통신이 성공하면 “라이선스확인” 버튼이 활성화 됩니다.
“라이선스 확인” 버튼을 클릭합니다.

2.2.3 사용자 등록

정보

RSM URI: 저장

사용자 정보 : 라이선스 체크가 완료되었습니다.

E-Mail:

이름:

라이선스 확인

사용자 등록

다음에 묻지 않기

정보

RSM URI: 저장

사용자 정보 : 라이선스 체크가 완료되었습니다.

E-Mail:

이름:

라이선스 확인

사용자 등록

다음에 묻지 않기

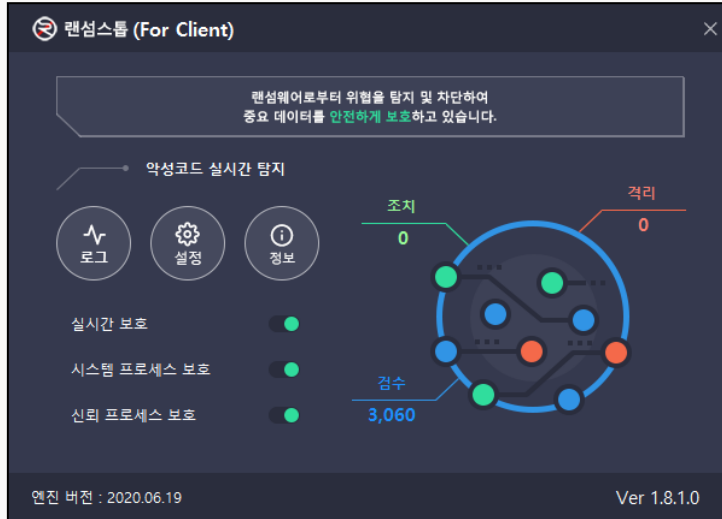
상기에서 “라이선스 확인” 버튼을 눌러 라이선스 체크가 완료되면 사용자정보 입력란이 활성화 됩니다.

관리자 또는 담당자에게 전달받은 이메일주소와 이름을 입력 후 “사용자등록” 버튼을 클릭 합니다.

(사용자 정보는 보통 회사 이메일 주소와 본명 또는 사번입니다.)

*무인증 버전(_SI)에 경우 사용자 정보와 이메일 주소 기본값이 자동으로 생성되어 입력됩니다.

3. 주요기능

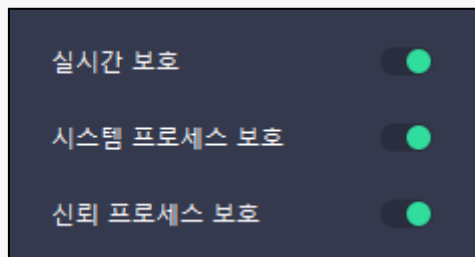


랜섬스톱 메인화면의 모습이며, 에이전트가 구동될 때마다 화면 우측의 조치, 검수, 격리 건수는 0으로 초기화 됩니다.

메인화면은 실시간보호, 로그, 설정, 정보의 3가지 부가적인 기능을 제공합니다.

각각의 항목을 클릭하시면 관련 기능의 이용이 가능합니다.

3.1 실시간보호



- 실시간보호

랜섬웨어에 대한 실시간 보호를 수행합니다.

- 시스템 프로세스 보호

시스템 프로세스 보호를 수행합니다..

○ 신뢰 프로세스 보호

신뢰 프로세스 보호를 수행합니다.

3.2 로그

3.2.1 일반(시스템)로그

시간	로그유형	설명
2020-06-19, 09:09:27	Protection Started	
2020-06-19, 09:09:24	Protected Stopped	
2020-06-19, 09:07:03	RansomStop Started	
2020-06-19, 09:07:02	Protection Started	
2020-06-19, 09:07:02	Service Started	

에이전트의 시작과 종료, 서비스 시작과 종료, 보호기능의 시작과 종료 등 에이전트 동작 관련 로그를 출력합니다.

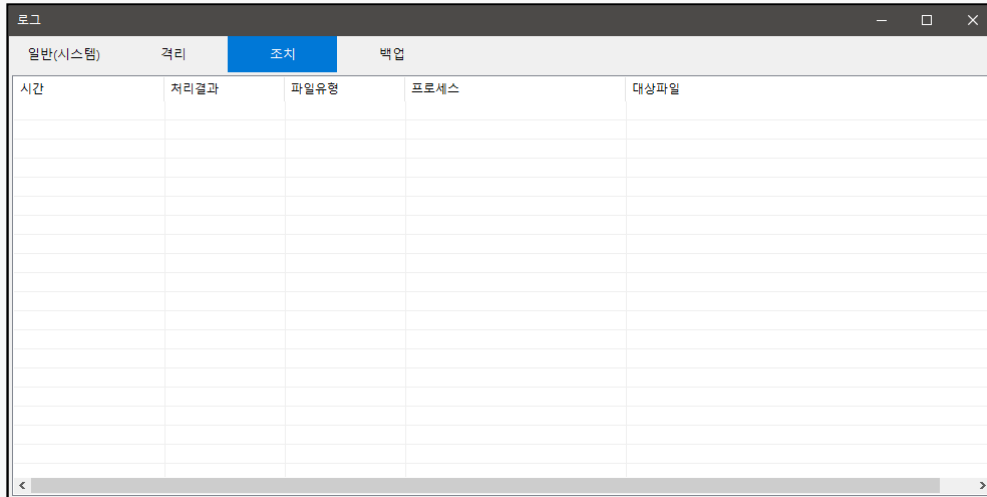
3.2.2 격리로그

시간	격리	프로세스	격리정보
2020-06-19, 09:46:43	변경	C:\PROGRAM FILES\DAUMW...	대상- C:\PROGRAM FILES\DAUMW\POTPLAYER\POTPLAYER64...

멀웨어로 탐지 또는 의심되는 프로세스의 격리 로그를 출력합니다.

정책적으로 차단된 프로세스의 정보도 이곳에서 확인 가능합니다.

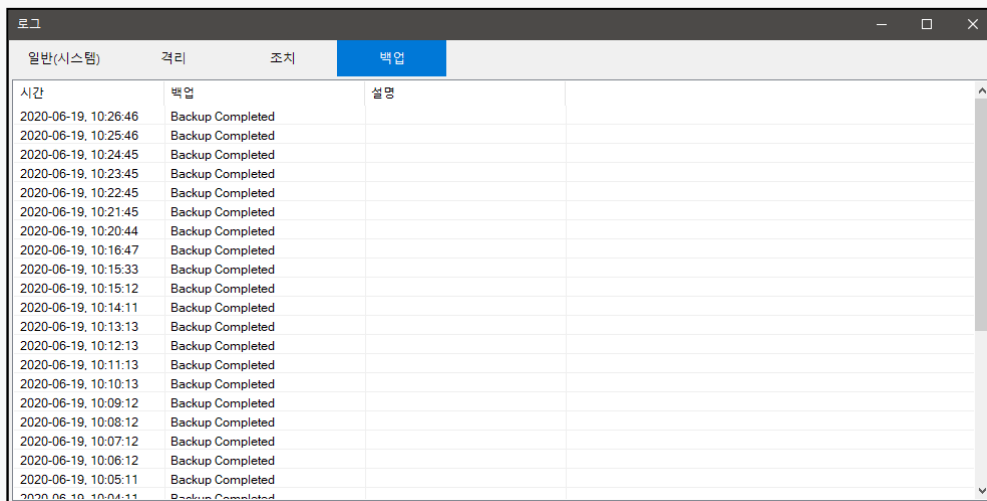
3.2.3 조치로그



시간	처리결과	파일유형	프로세스	대상파일
----	------	------	------	------

격리된 프로세스에 대한 조치 로그를 출력합니다.

3.2.4 백업로그



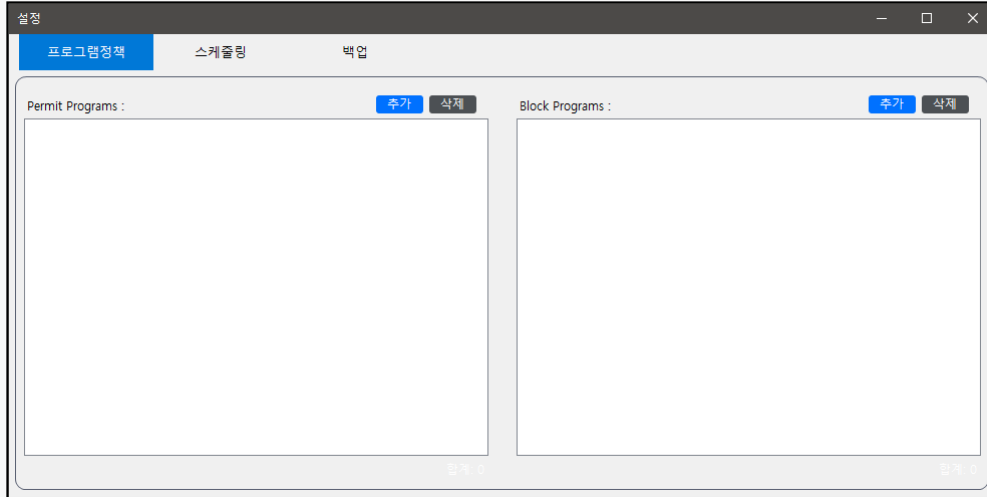
시간	백업	설명
2020-06-19, 10:26:46	Backup Completed	
2020-06-19, 10:25:46	Backup Completed	
2020-06-19, 10:24:45	Backup Completed	
2020-06-19, 10:23:45	Backup Completed	
2020-06-19, 10:22:45	Backup Completed	
2020-06-19, 10:21:45	Backup Completed	
2020-06-19, 10:20:44	Backup Completed	
2020-06-19, 10:16:47	Backup Completed	
2020-06-19, 10:15:33	Backup Completed	
2020-06-19, 10:15:12	Backup Completed	
2020-06-19, 10:14:11	Backup Completed	
2020-06-19, 10:13:13	Backup Completed	
2020-06-19, 10:12:13	Backup Completed	
2020-06-19, 10:11:13	Backup Completed	
2020-06-19, 10:10:13	Backup Completed	
2020-06-19, 10:09:12	Backup Completed	
2020-06-19, 10:08:12	Backup Completed	
2020-06-19, 10:07:12	Backup Completed	
2020-06-19, 10:06:12	Backup Completed	
2020-06-19, 10:05:11	Backup Completed	
2020-06-19, 10:04:11	Backup Completed	

사용자가 설정한 스케줄링(주기적인 백업)의 실행 결과 로그를 출력 합니다.

스케줄링 설정은 [3.3.2.1 스케줄링 설정](#)을 참조하세요.

3.3 설정

3.3.1 프로그램정책



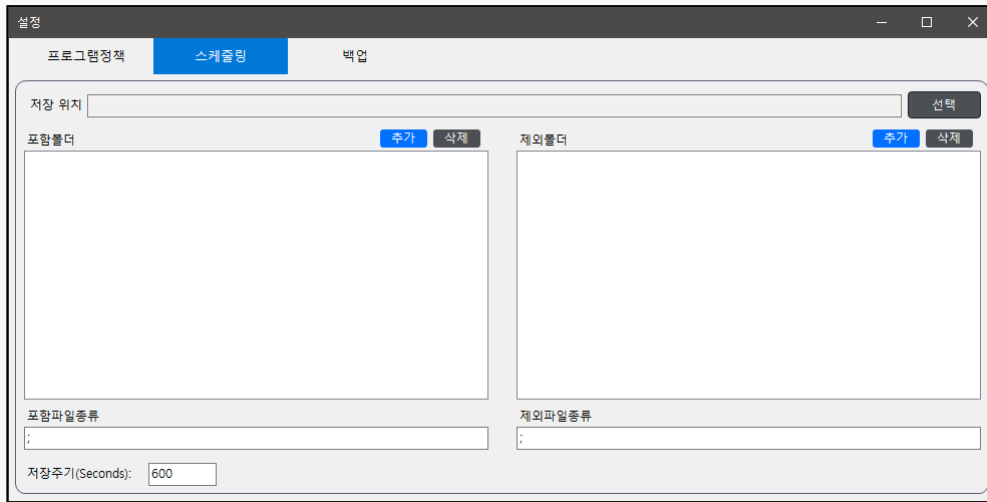
프로그램 정책은 에이전트가 설치된 PC에 국한하는 정책입니다.

우측은 허용할 프로그램, 좌측은 차단할 프로그램을 등록합니다.

이와 별도로 에이전트는 RSM서버를 통해 상위정책을 전달받으며, 이는 에이전트 개별정책보다 우선합니다.

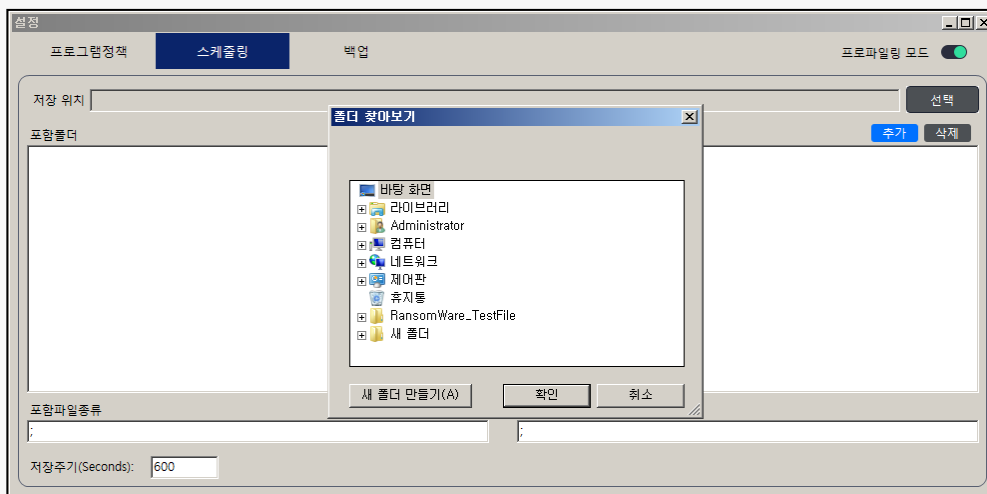
허용할 프로그램 또는 차단할 프로그램의 설정은 각각의 “추가” 버튼을 클릭하여 파일탐색기를 이용해 해당 프로그램이 위치한 경로의 실행파일을 선택해 주시면 됩니다.

3.3.2 스케줄링



스케줄링은 사용자가 설정한 경로의 특정 파일형식을 주기적으로 백업하는 기능입니다.

3.3.2.1 스케줄링 설정



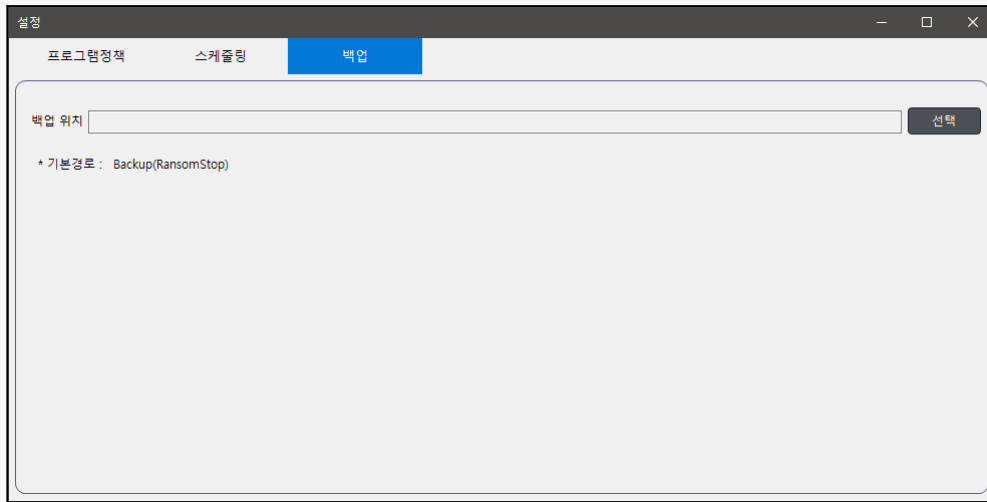
상단의 저장위치 우측의 “선택” 버튼을 눌러 저장할 경로를 설정합니다.

주기적으로 백업할 대상 폴더(디렉토리)를 “추가” 버튼을 이용해 선택합니다.

백업 대상 파일형식은 세미콜론(;)으로 구분하여 입력합니다.

저장주기는 최소60초이상으로 초단위로 입력합니다.(기본값 600초)

3.3.3 백업

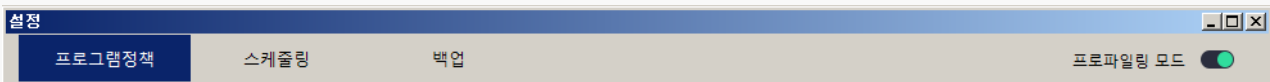


멀웨어 탐지 또는 의심되는 프로세스의 격리가 발생시 백업(보호소)의 경로 설정입니다.

설치시 기본 백업 위치은 C:\WBackup(RansomStop) 입니다.

변경을 원하시는 경우 백업위치 우측의 “선택”버튼을 이용해 원하는 경로를 선택하시면 변경됩니다.

3.3.4 프로파일링 모드

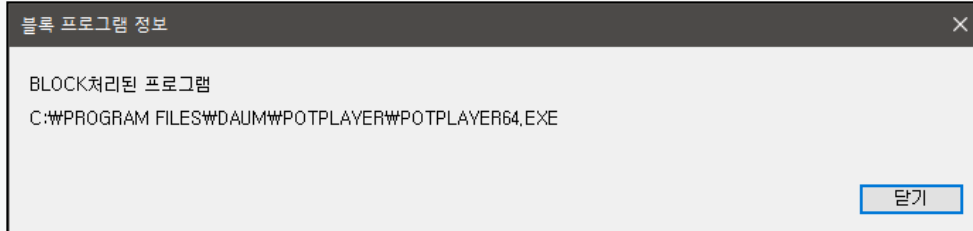


프로파일링 모드는 설치 이전에 프로그램 환경과 예상치 않는 충돌을 사전에 예방하기 위해 설정하는 모드입니다. 프로파일링 모드 설정시 RansomStop은 현재 운영중인 프로세스에서 이상행위를 탐지후 로그만 수집하며, 격리/조치 처리를 하지 않습니다.

최초 설치시 프로파일링 모드로 1주간 운영 후, 사용이 잦고 안전성이 확인된 충돌 프로세스는 3.3.1 프로그램 정책 > Permit Program에 허용 프로세스로 등록 후 프로파일링 모드를 해제 후 사용 합니다.

3.4 차단정보 및 탐지정보

3.4.1 차단정보



랜섬스톱이 시스템을 실시간 감시 중 비인가 프로세스(프로그램)의 탐지시 탐지 알림창과 함께 해당 프로세스는 종료됩니다.

해당내역은 로그 > [격리로그](#)에서 확인이 가능합니다.

3.4.2 탐지정보

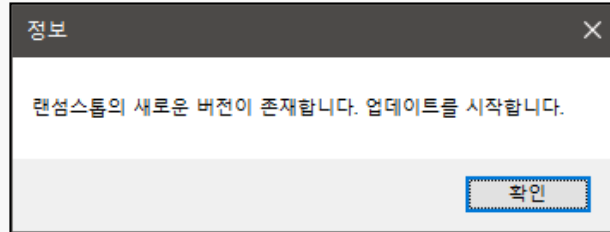


랜섬스톱이 시스템을 실시간 감시 중 이상행위 탐지시 탐지 알림창과 함께 해당 프로세스는 종료됩니다.

해당내역은 로그 > [격리로그](#) 또는 [조치로그](#)에서 확인이 가능합니다.

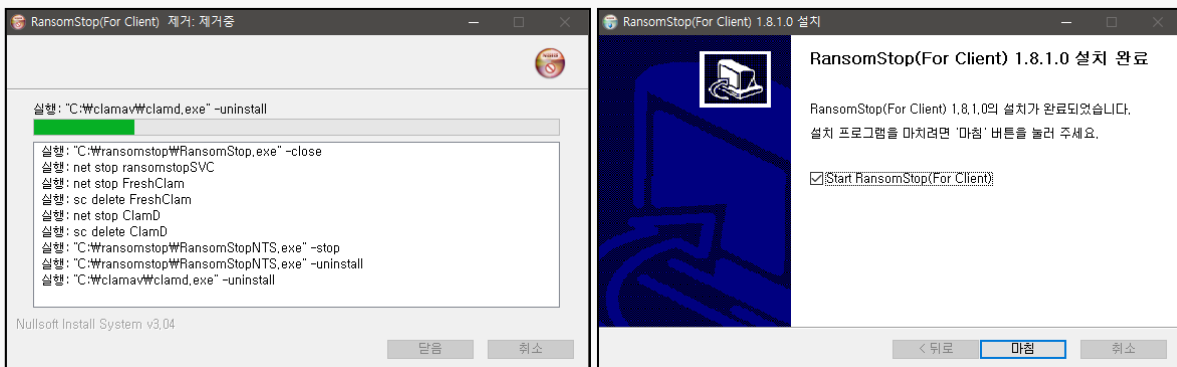
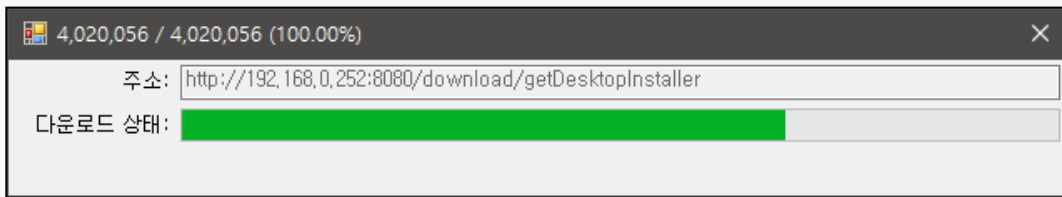
4. 기타기능

4.1 버전 업데이트



랜섬스톱은 RSM서버와의 통신을 통해 주기적으로 버전 업데이트 확인을 수행합니다.

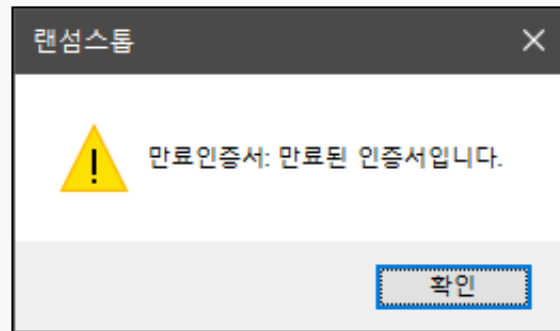
업데이트가 필요한 경우 업데이트 안내창으로 안내 후 업데이트를 진행합니다.



업데이트는 업데이트 파일의 다운로드, 기존 버전삭제, 상위버전 설치의 순서로 진행되며,

설치 완료 후 라이선스 체크, 사용자인증 등의 절차 없이 기존버전의 인증정보를 이용해 재실행 됩니다.

4.2 라이선스 만료



사용중인 라이선스의 기간경과 같이 만료된 경우 에이전트 구동시 라이선스 만료 안내창이 출력됩니다.

에이전트의 문제가 아니므로 관리자나 담당자에게 문의 바랍니다.

4.3 RSM 접속정보 변경

최초 설치시 입력한 RSM의 접속정보(IP, PORT)는 추후 에이전트 상에서 변경이 불가능합니다.

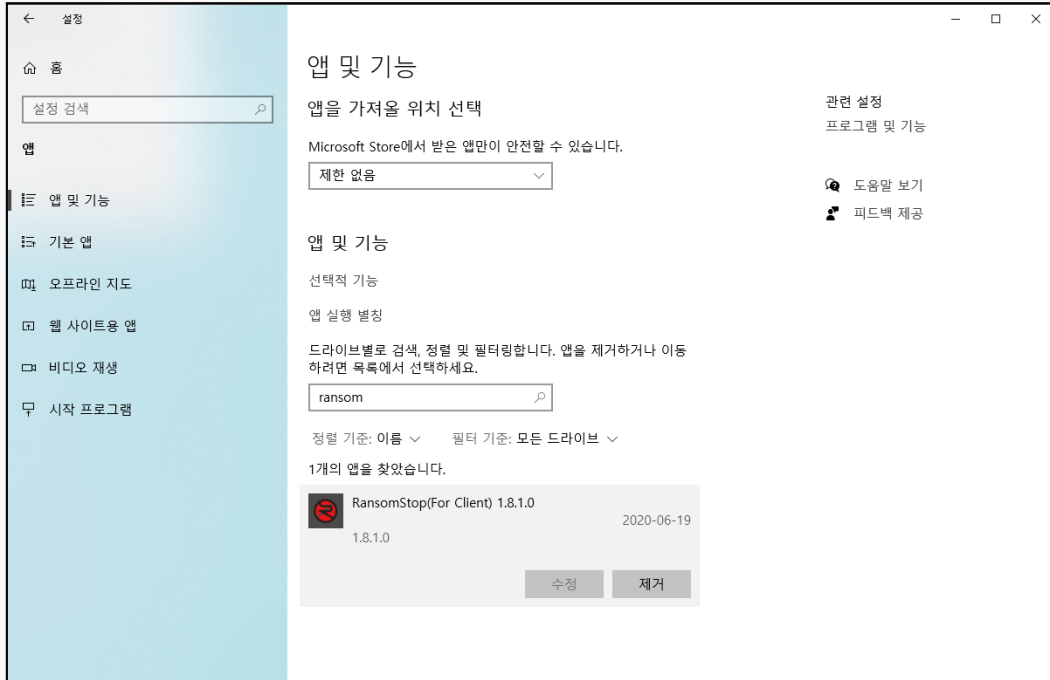
변경이 필요시 관리자나 담당자에게 문의 바랍니다.

4.4 사용자인증 해제

최초 설치시 입력한 사용자정보(이름, 이메일주소)는 추후 에이전트 상에서 변경이 불가능합니다.

사용자정보의 변경이 필요한 경우 관리자나 담당자를 통해 에이전트 인증해제 요청 바랍니다.

5. 에이전트 삭제하기



에이전트의 삭제가 필요한 경우 (윈도우10 기준) 시작버튼 > 제어판 > 앱으로 이동하여 “RansomStop ...”을 선택 후 하단의 “제거” 버튼을 클릭 합니다.

이후 화면상에 보이는 보안코드 4자리를 입력란에 입력 후 “다음” 버튼을 클릭해 삭제를 진행합니다.

