AhnLab Office Security Center 이용 가이드

(Office Security Center 이용 안내 문서)

More security,
More freedom

AhnLab

Office Security Center 이용 가이드

본 가이드 문서는 AhnLab Office Security Center(V3 Office Security)에 대한 활용 방법을 안내하기 위해 제작된 자료 입니다.

해당 문서에서는 제품을 적극적으로 활용 중인 기업들의 운영 사례를 바탕으로, 보다 효과적인 보안 환경 구축에 도움이 될 수 있는 실무형 팁과 정책 방향을 제시합니다.

보안 정책의 정답은 하나로 고정되어 있지 않으므로, 본 문서에서 소개하는 다양한 운영 방안을 참고하셔서 귀사의 보안 정책 수립 및 개선에 활용하시기 바랍니다.

가이드 문서 이용 과정에서 문의사항이 있으실 경우, 아래 기재된 연락처로 문의해 주시기 바랍니다.

고객지원

- 홈페이지: https://www.ahnlab.com
- AhnLab Office Security Center 관리자 페이지 : https://osc.ahnlab.com/
- AhnLab 고객기술지원 : https://ask.ahnlab.com/hc/ko
- 온라인 고객지원: 안랩 홈페이지 > 고객지원 > 온라인 고객지원 > 1:1 상담
- 기업고객 기술지원: 1577-9431(평일 오전 9시~오후 8시, 토/공휴일 제외)

줄인말 정리 :

Office Security Center => OSC

V3 Office Security => V3 OS

Table of Contents

AhnLab

Table of Contents

AhnLab

제품 배포 및 설치 과정

AhnLab

라이선스 구매 후 배포 방법

✅ 제품 구매 후 설치 과정 안내

제품을 구매한 후에는 **사용자가 V3를 사용 할 수 있도록 제품을 배포하는 절차**가 필요합니다.

이를 위해 **Office Security Agent** 설치가 필요합니다.

❓ 여기서 잠깐 : 왜 V3가 아닌 Office Security Agent를 설치 할까요?

✅ Office Security Agent 주요 기능은 다음과 같습니다.

1) 사용자 PC에 V3 자동 설치

- PC의 **운영체제를 감지**하여 자동으로 **OS에 맞는 V3 버전을 다운로드 및 설치하는 역할을 담당** 합니다.

2) 관리자가 설정 한 정책 및 관리 명령을 V3에 전달

- 관리자가 설정한 각종 정책을 PC로 전달하여 V3에 즉시 적용합니다.
- 원격 검사, 원격 업데이트 등 관리자가 내린 **원격 명령을 V3에 전달하는 역할**을 수행합니다.

3) Office Security Center 연동

- Office Security Agent가 설치된 PC의 정보와 에이전트 로그를 서버로 전송합니다.
- V3 진단 데이터를 서버로 전송하여 **각종 보고서를 생성**할 수 있습니다.
- 관리자가 지정한 **'기기 별칭' 정보를 PC로 전달**하여 기기 관리 기능을 제공합니다.

▲트레이 아이콘

그러면 사용자 PC에 Office Security Agent를 배포하는 방법에 대해 알아보겠습니다.

사내 메일 이용 여부에 따른 배포방법 차이

제품 구매 후 사용자에게 Office Security Agent를 배포하고 설치하는 방법에 대해 알아 보겠습니다.

다음에서 설명하는 두 가지 방법 중 사내 환경에 맞는 방법을 참고하여 주시기 바랍니다.

✅ 1. 사내 메일이 없는 경우 – 설치 대상자가 적은 경우

1) 설치 파일 전달

- 관리자가 Office Security Agent 설치 파일을 다운로드하여 사용자에게 직접 전달하거나 사용자 PC에서 직접 다운로드 진행 (예: 게시판, 메신저 등 내부 커뮤니케이션 도구를 활용 하여 설치 파일을 전달 할 수도 있습니다.)

2) 설치 정보 관리

- 설치 시 필요한 메일주소(관리자 메일주소) 및 엑티베이션 코드를 전달하여 입력
- 설치 과정에서 '기기 별칭'에 구분 할 수 있는 정보(실사용자 이름 또는 장소)를 입력 사용자 관리

✅ 2. 사내 메일이 있는 경우 – 설치 대상자가 많은 경우

1) 설치 파일 전달

- 먼저 **조직도**에 사용자를 등록
- 등록된 사용자에게 설치 파일 다운로드 링크가 포함된 **배포 메일전달**
- **사용자는 배포메일의 다운로드 링크를 통해 설치파일을 다운로드**

2) 설치 정보 관리

- 설치 시 사용자의 이메일 정보를 기반으로 인증이 진행
- 설치가 완료되면 설치 기기 목록에 해당 사용자 이름이 자동 등록 됩니다.

1. 사내메일이 없는 경우 설치파일 배포

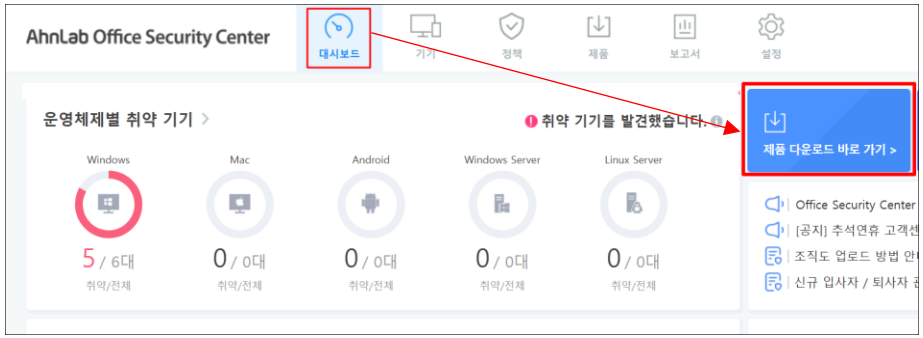
✅ 1. 사내 메일이 없는 경우

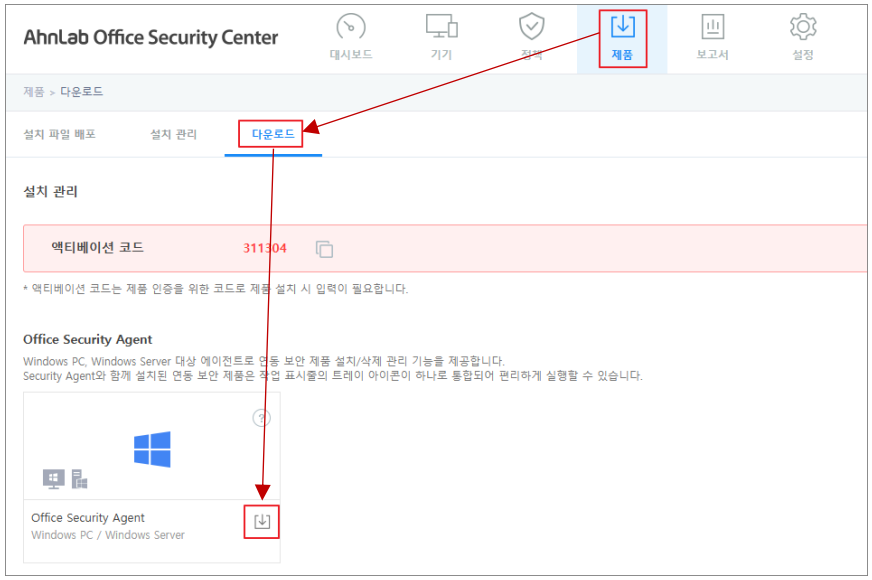
1. 설치파일 전달 방식
사내 메일을 사용하지 않는 경우, 다음 두 가지 방법 중 하나로 설치 파일을 제공 할 수 있습니다.

- 관리자가 설치 파일을 직접 다운로드 해 사용자에게 전달(예: 사내 게시판, 메신저 등 커뮤니케이션 도구 활용 가능)
- 관리자가 사용자 PC에서 Office Security Center 페이지에 로그인하여 직접 다운로드

2. 설치파일 다운로드 위치
아래 경로를 통해 설치파일(Office Security Agent)을 다운로드 할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 대시보드 > 제품 다운로드 바로가기
- Office Security Center 관리자 페이지 로그인 > 제품 > 다운로드





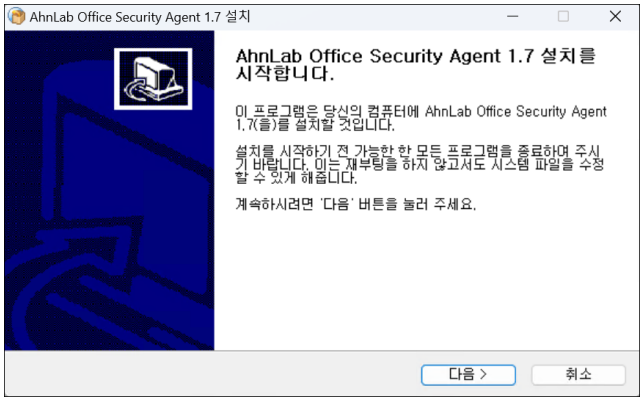
Office Security Agent 설치 과정

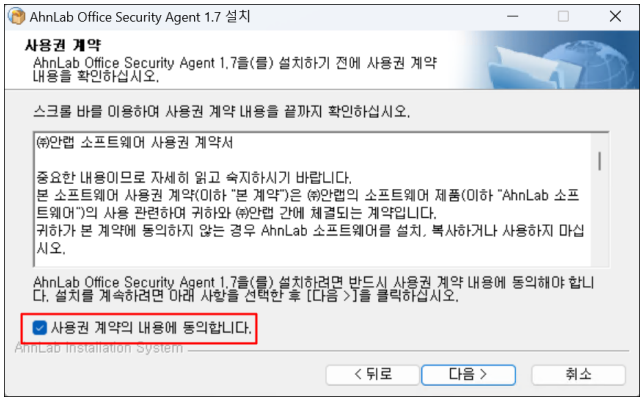
✅ 1. 사내 메일이 없는 경우

3. 제품 설치과정

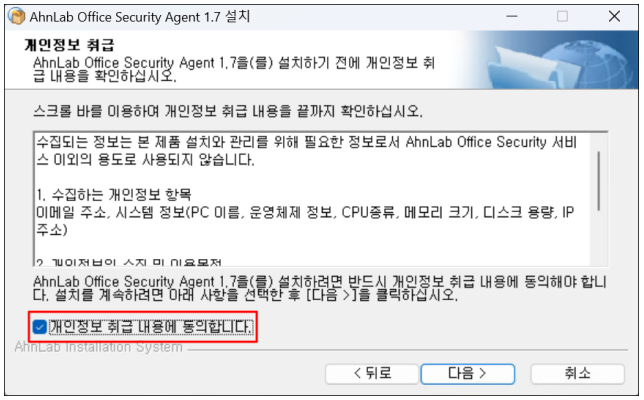
- 다운로드 완료 된 os_agent_setup.exe 파일을 실행하면 Office Security Agent 설치과정이 시작 됩니다.

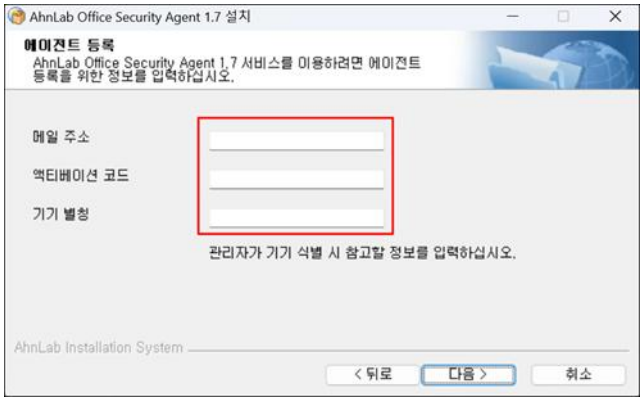
- 설치가 시작되면 [다음], 사용권 계약서에는 동의 체크박스를 체크 하고 [다음]을 클릭합니다.





- 개인정보 취급에서 동의 체크박스 후 [다음]을 클릭합니다.





Office Security Agent 인증 정보 입력

✅ 1. 사내 메일이 없는 경우

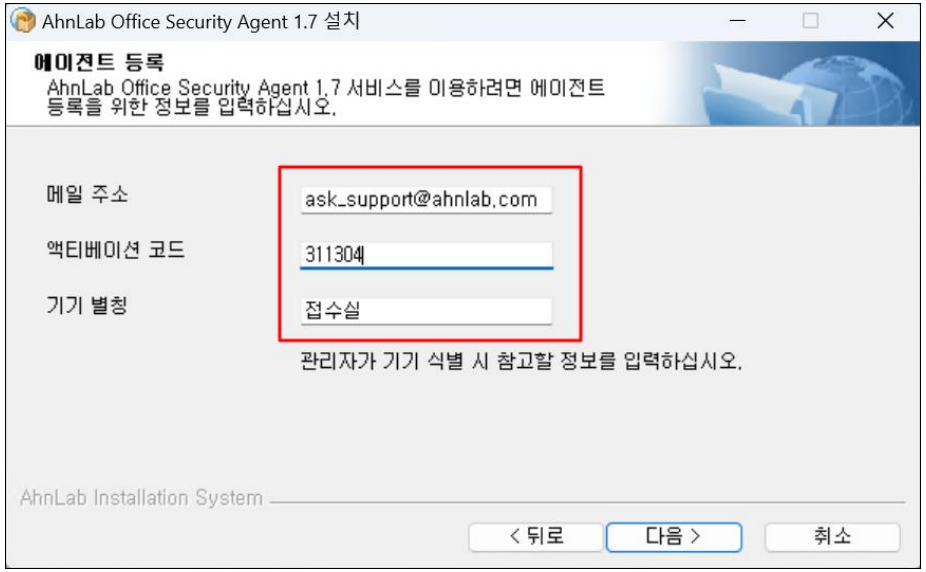
4. 에이전트 등록 정보 입력

- **사용자 개인 사내 메일주소 정보가 없으므로 메일주소 항목에는 대표 관리자 이메일 주소를 입력 합니다.**
- **Office Security Center 페이지에서 엑티베이션 코드를 확인하여 입력합니다.**

- 엑티베이션 코드 확인 위치

- Office Security Center 관리자 페이지 로그인 > 대시보드 페이지 하단
- Office Security Center 관리자 페이지 로그인 > 제품 > 다운로드 페이지

- **기기 별칭 항목에는 제품을 실제 사용할 사용자 이름을 입력합니다.(사용자가 특정되지 않는 공용 PC인 경우 사용 장소를 입력하셔도 됩니다.)**



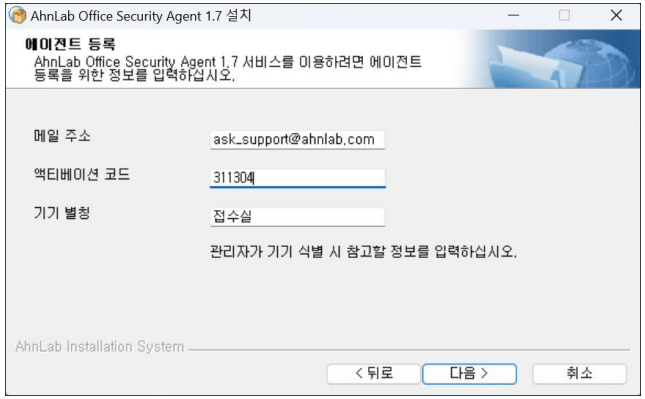
※ 기기 별칭을 입력하지 않을 경우 추후 **PC 교체나 포맷 등의 경우에 기기 정보 등록 해제 시** 기기 정보 확인에 어려움이 발생할 수 있습니다.

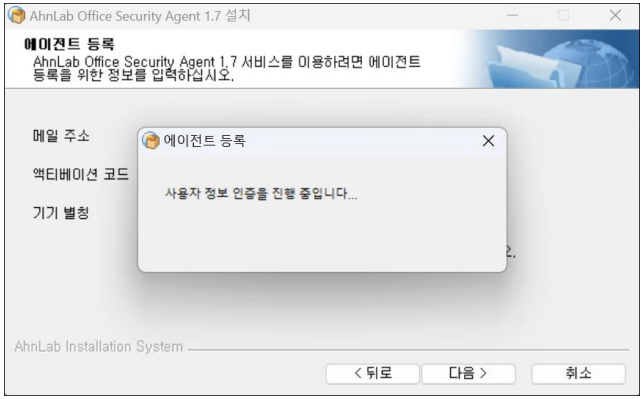
Office Security Agent 인증 및 설치 경로 지정

✅ 1. 사내 메일이 없는 경우

5. 에이전트 등록 과정

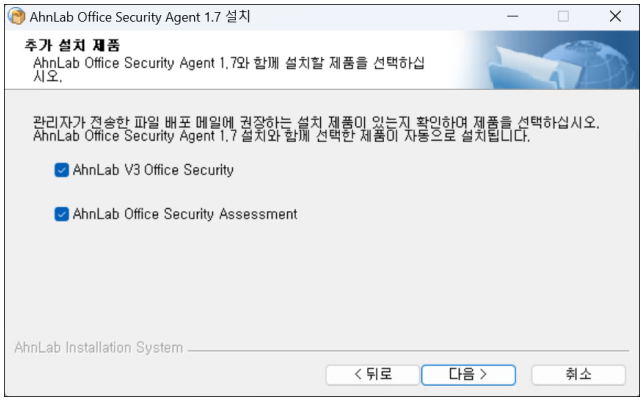
- 올바른 정보가 입력되었다면 인증이 진행 됩니다.

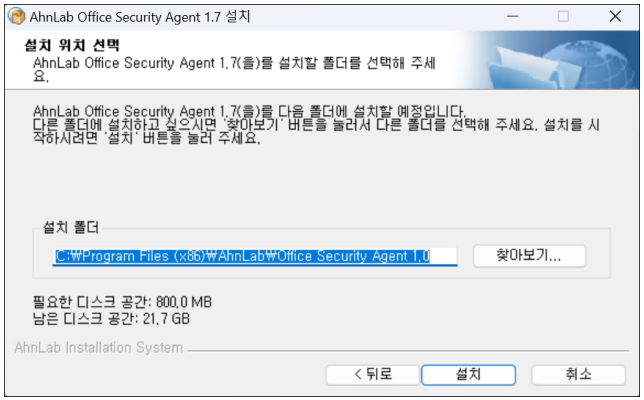




6. 보유제품 설치 여부 체크

- Agent 설치 시 함께 설치할 제품(V3)이 체크되었는지 확인 후 [다음], 설치 폴더 지정에서는 [설치]를 클릭하면 파일 복사가 진행 됩니다.



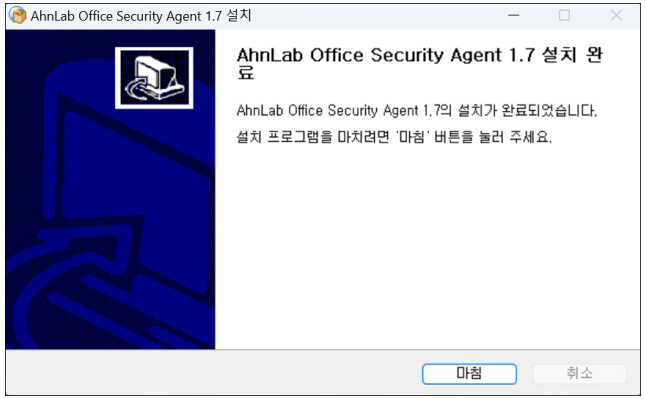


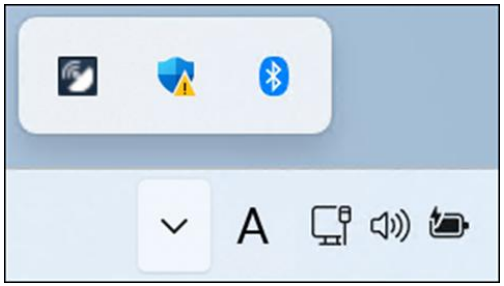
Office Security Agent 및 V3 설치 완료

✅ 1. 사내 메일이 없는 경우

7. Office Security Agent 설치 마침

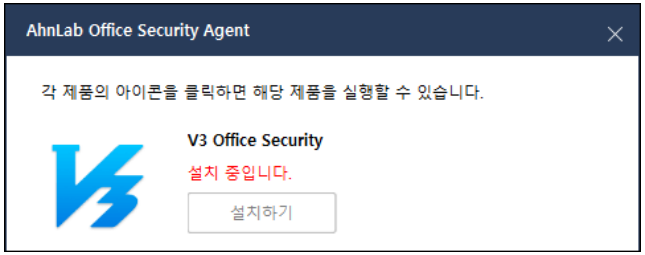
- **설치가 마무리 되고 [마침]을 누르면 시스템 트레이에 다음과 같은 Office Security Agent 아이콘이 표시 되고 보안제품 설치 안내창이 나타납니다.**

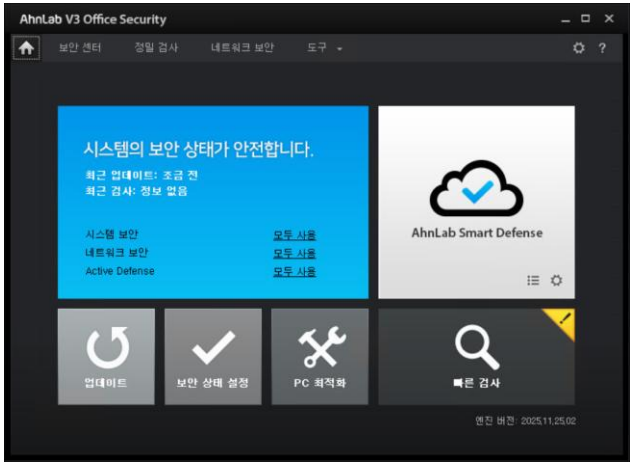




8. Office Security Agent를 통한 V3 설치 진행

- **Agent가 사용자 PC에 설치 된 OS를 감지하여 자동으로 V3를 설치**합니다.
  ※ V3 설치는 백그라운드로 진행 되며 설치 과정이 화면에 표시되지 않습니다.





- 백그라운드를 통한 V3 설치가 마무리 되면 V3가 팝업되어 표시 되며 마무리 됩니다.

설치 완료 후 기기 정보 확인

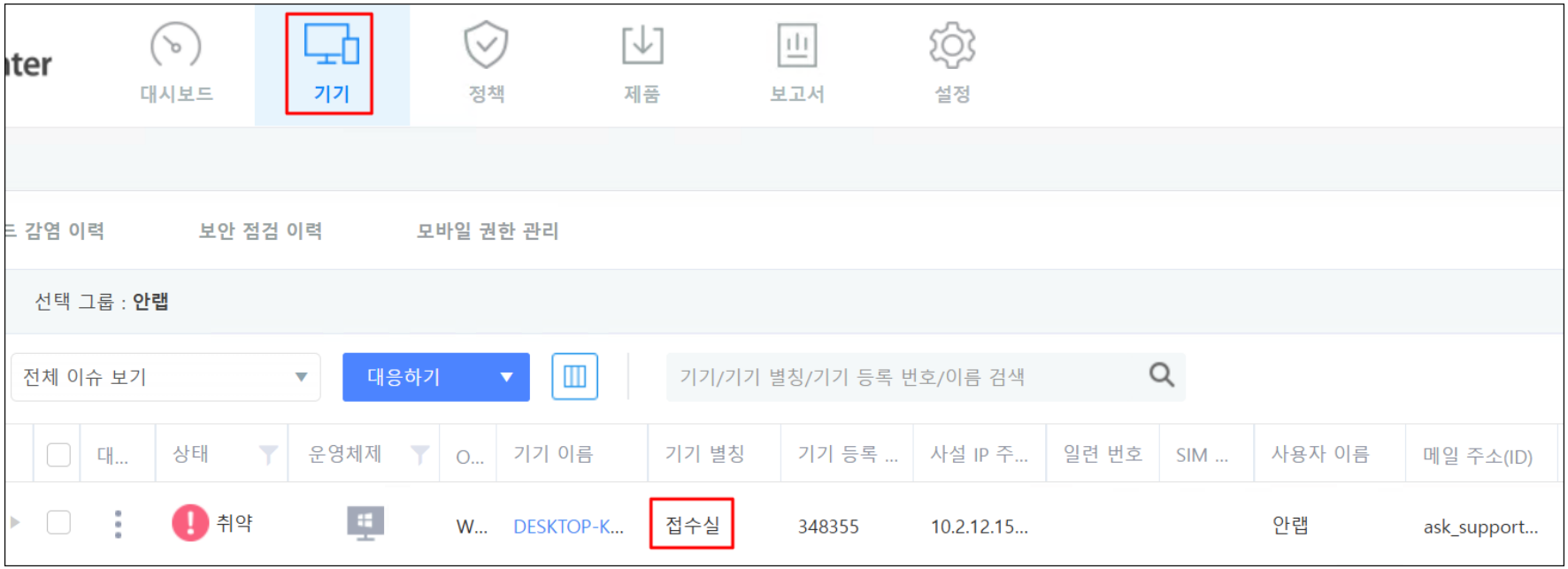
✅ 1. 사내 메일이 없는 경우

9. 설치 정보 확인

- **설치 된 기기 정보는 다음의 메뉴를 통해 확인 할 수 있습니다.**

- Office Security Center 관리자 페이지 로그인 > 기기

- **설치 과정에서 입력한 기기 별칭 및 기기 등록번호 등을 확인 할 수 있습니다.**



※ 기기 별칭을 입력 할 경우 PC 포맷 , PC 교체 시 기기 정보가 특정되어 변경 된 기기 정보를 수월하게 관리 할 수 있습니다.

다음은 사내 메일을 활용하고 있는 경우 배포 및 설치과정에 대해 알아보겠습니다.

2. 사내 메일이 있는 경우 설치파일 배포

✅ 2. 사내 메일이 있는 경우

1. 설치파일 제공 방법

사내 메일을 활용하고 계신 경우 사용자에게 **Office Security Agent 설치파일 다운로드 링크가 포함 된 안내 메일을 발송** 할 수 있습니다.

Agent 설치파일 배포 순서는 다음과 같습니다.

① Office Security Center 조직도에 사용자를 등록

② 사용자에게 Agent 설치파일 다운로드 링크가 포함 된 배포메일 발송

③ 수신 된 배포메일의 Office Security Agent 링크를 통해 설치파일을 다운로드

※ 조직도에 등록 된 사용자만 제품 설치가 가능하며, 등록되지 않은 사용자는 설치가 허용되지 않습니다.

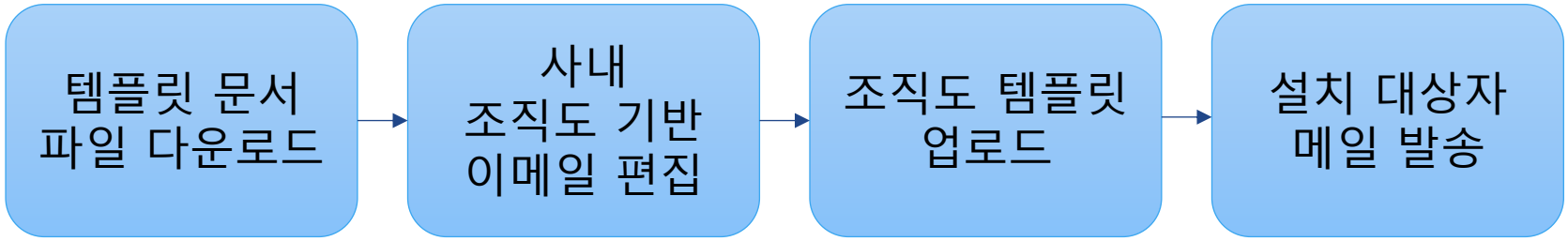
2. 사내 메일이 있는 경우 설치파일 배포

✅ 2. 사내 메일이 있는 경우

2. 조직도 등록

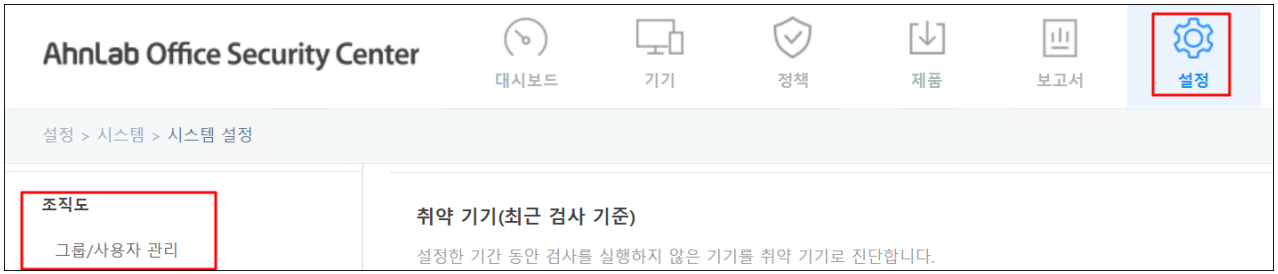
설치파일 배포를 위해 조직도에 사용자를 추가하여 설치 할 대상을 지정 할 수 있습니다. (V3 제품 설치를 허용 할 사용자를 추가 하는 과정)

제품 설치를 위한 조직도 등록 및 배포방법의 순서는 다음과 같습니다.



사내 조직도 등록을 위한 조직도 등록 방법에 대해 알아보겠습니다.

Office Security Center 관리자 페이지 로그인 > 설정 > 조직도 > 그룹/사용자 관리



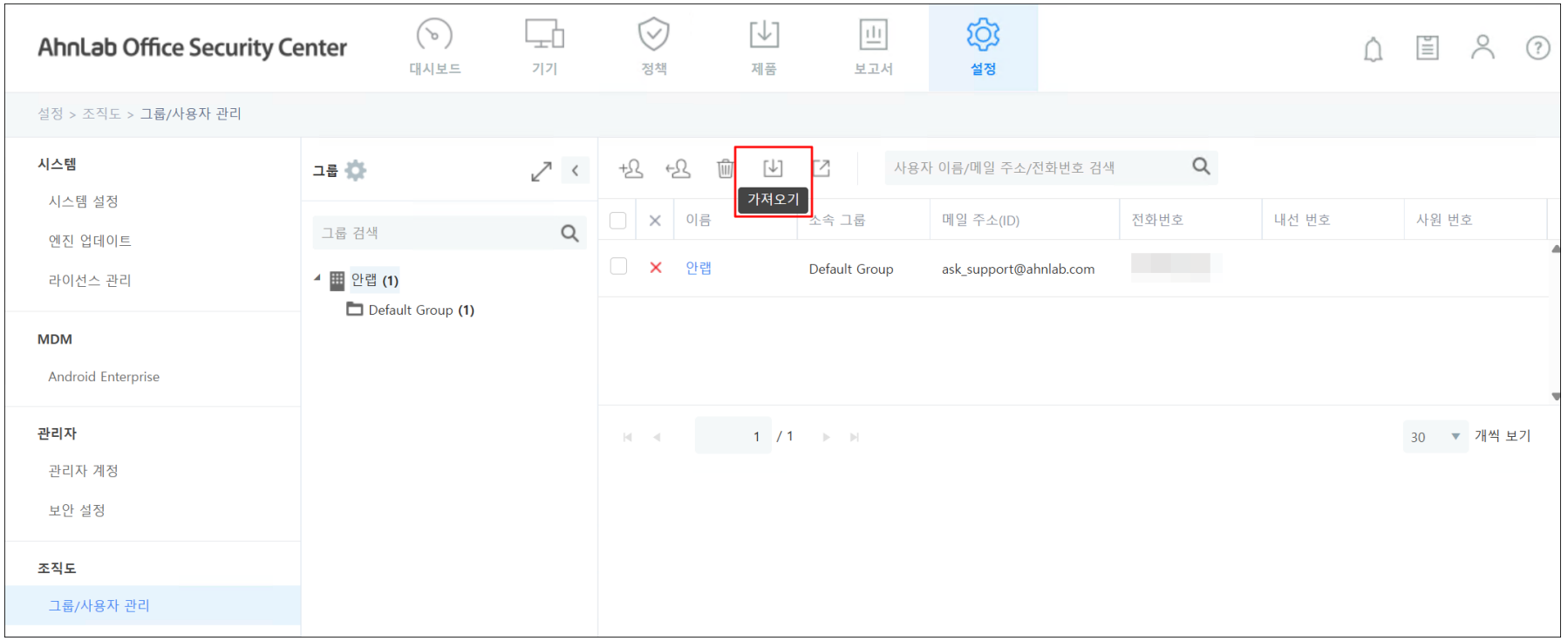
조직도 템플릿 다운로드

✅ 2. 사내 메일이 있는 경우

3. 조직도에 사용자 등록

V3 설치를 위해 Office Security Agent 설치 안내 메일 수신 할 사용자를 조직도에 등록하는 방법 입니다.

- Office Security Center 로그인 > 설정 > 조직도(그룹/사용자 관리) >  [가져오기] 버튼을 클릭



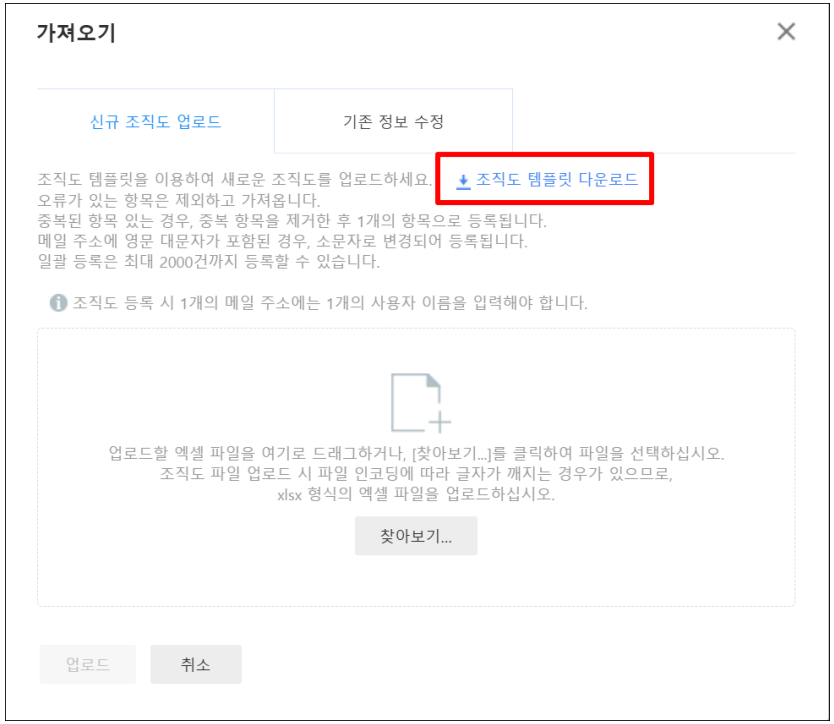
조직도 템플릿 편집

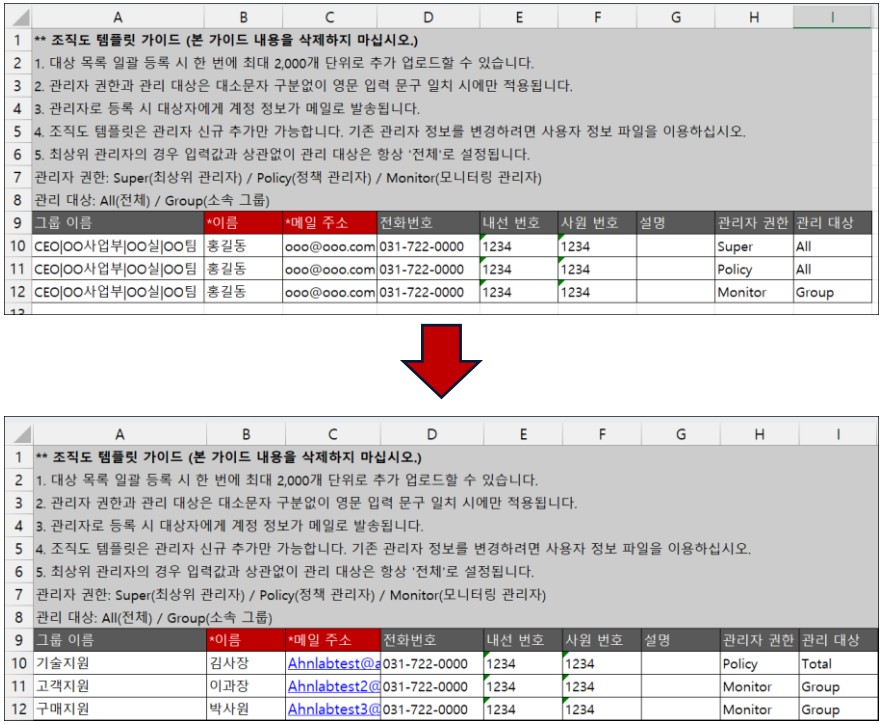
✅ 2. 사내 메일이 있는 경우

3. 조직도에 사용자 등록

- [조직도 템플릿 다운로드]를 통해 템플릿 파일을 다운로드 받고 내용을 편집합니다.

※ 템플릿 파일에 등록되어 있는 샘플과 같이 사용자 정보를 입력하고 저장 합니다. (필수 입력정보 : **이름, 메일주소**는 반드시 입력되어야 합니다)





	A	B	C	D	E	F	G	H	I
1	** 조직도 템플릿 가이드 (본 가이드 내용을 삭제하지 마십시오.)								
2	1. 대상 목록 일괄 등록 시 한 번에 최대 2,000개 단위로 추가 업로드할 수 있습니다.								
3	2. 관리자 권한과 관리 대상은 대소문자 구분없이 영문 입력 문구 일치 시에만 적용됩니다.								
4	3. 관리자로 등록 시 대상자에게 계정 정보가 메일로 발송됩니다.								
5	4. 조직도 템플릿은 관리자 신규 추가만 가능합니다. 기존 관리자 정보를 변경하려면 사용자 정보 파일을 이용하십시오.								
6	5. 최상위 관리자의 경우 입력값과 상관없이 관리 대상은 항상 '전체'로 설정됩니다.								
7	관리자 권한: Super(최상위 관리자) / Policy(정책 관리자) / Monitor(모니터링 관리자)								
8	관리 대상: All(전체) / Group(소속 그룹)								
9	그룹 이름	*이름	*메일 주소	전화번호	내선 번호	사원 번호	설명	관리자 권한	관리 대상
10	CEO|OO사업부|OO실|OO팀	홍길동	ooo@ooo.com	031-722-0000	1234	1234		Super	All
11	CEO|OO사업부|OO실|OO팀	홍길동	ooo@ooo.com	031-722-0000	1234	1234		Policy	All
12	CEO|OO사업부|OO실|OO팀	홍길동	ooo@ooo.com	031-722-0000	1234	1234		Monitor	Group

	A	B	C	D	E	F	G	H	I
1	** 조직도 템플릿 가이드 (본 가이드 내용을 삭제하지 마십시오.)								
2	1. 대상 목록 일괄 등록 시 한 번에 최대 2,000개 단위로 추가 업로드할 수 있습니다.								
3	2. 관리자 권한과 관리 대상은 대소문자 구분없이 영문 입력 문구 일치 시에만 적용됩니다.								
4	3. 관리자로 등록 시 대상자에게 계정 정보가 메일로 발송됩니다.								
5	4. 조직도 템플릿은 관리자 신규 추가만 가능합니다. 기존 관리자 정보를 변경하려면 사용자 정보 파일을 이용하십시오.								
6	5. 최상위 관리자의 경우 입력값과 상관없이 관리 대상은 항상 '전체'로 설정됩니다.								
7	관리자 권한: Super(최상위 관리자) / Policy(정책 관리자) / Monitor(모니터링 관리자)								
8	관리 대상: All(전체) / Group(소속 그룹)								
9	그룹 이름	*이름	*메일 주소	전화번호	내선 번호	사원 번호	설명	관리자 권한	관리 대상
10	기술지원	김사장	Ahnlabtest@a	031-722-0000	1234	1234		Policy	Total
11	고객지원	이과장	Ahnlabtest2@	031-722-0000	1234	1234		Monitor	Group
12	구매지원	박사원	Ahnlabtest3@	031-722-0000	1234	1234		Monitor	Group

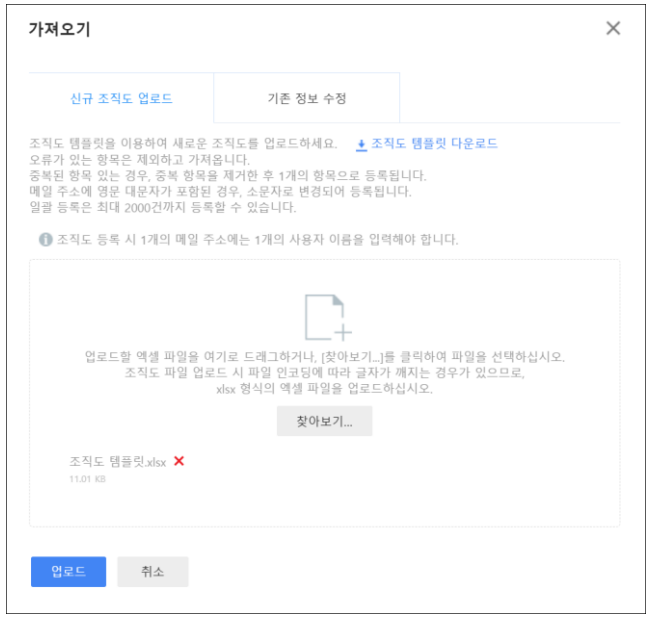
※ 이메일 주소의 경우 사용자를 구분하는 고유정보 입니다. 동일 이메일 주소를 여러 명의 사용자에게 중복하여 입력할 수 없습니다.

조직도 템플릿 업로드

✅ 2. 사내 메일이 있는 경우

3. 조직도에 사용자 등록

- 편집이 완료 된 조직도 템플릿 파일은 [찾아보기]를 눌러 [업로드] 합니다.



조직도 등록 확인

✅ 2. 사내 메일이 있는 경우

3. 조직도에 사용자 등록

- 템플릿을 통해 사용자 등록 완료 시 입력 한 **그룹 이름, 이름, 메일주소, 전화번호, 내선번호, 사원번호 등**이 등록 됩니다.

	A	B	C	D	E	F	G	H	I
1	** 조직도 템플릿 가이드 (본 가이드 내용을 삭제하지 마십시오.)								
2	1. 대상 목록 일괄 등록 시 한 번에 최대 2,000개 단위로 추가 업로드할 수 있습니다.								
3	2. 관리자 권한과 관리 대상은 대소문자 구분없이 영문 입력 문구 일치 시에만 적용됩니다.								
4	3. 관리자로 등록 시 대상자에게 계정 정보가 메일로 발송됩니다.								
5	4. 조직도 템플릿은 관리자 신규 추가만 가능합니다. 기존 관리자 정보를 변경하려면 사용자 정보 파일을 이용하십시오.								
6	5. 최상위 관리자의 경우 입력값과 상관없이 관리 대상은 항상 '전체'로 설정됩니다.								
7	관리자 권한: Super(최상위 관리자) / Policy(정책 관리자) / Monitor(모니터링 관리자)								
8	관리 대상: All(전체) / Group(소속 그룹)								
9	그룹 이름	*이름	*메일 주소	전화번호	내선 번호	사원 번호	설명	관리자 권한	관리 대상
10	기술지원	김사장	Ahnlabtest@a	031-722-0000	1234	1234		Policy	Total
11	고객지원	이과장	Ahnlabtest2@	031-722-0000	1234	1234		Monitor	Group
12	구매지원	박사원	Ahnlabtest3@	031-722-0000	1234	1234		Monitor	Group

배포메일 발송

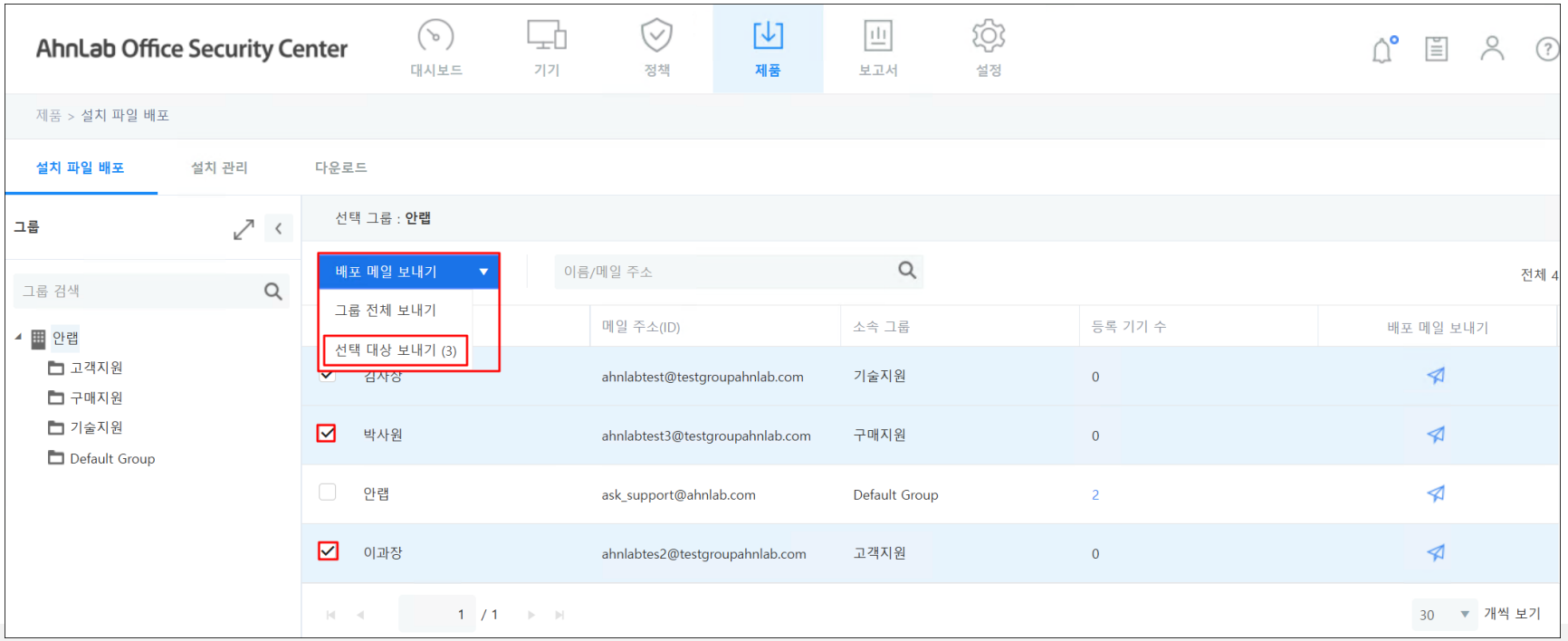
✅ 2. 사내 메일이 있는 경우

4. 배포메일 발송

조직도에 등록 된 사용자에게 Office Security Agent 다운로드 링크가 포함 된 배포메일을 발송하는 과정 입니다.

1. Office Security Center 관리자 페이지 로그인 > 제품 메뉴로 이동합니다.
2. 제품 설치가 필요한 사용자를 선택 합니다.
3. [배포 메일 보내기] > **[그룹 전체 보내기] 또는 [선택 대상 보내기]**를 선택 합니다.

※ 그룹 전체 보내기를 선택 할 경우 조직도에 등록 된 모든 사용자에게 배포메일이 발송 됩니다.



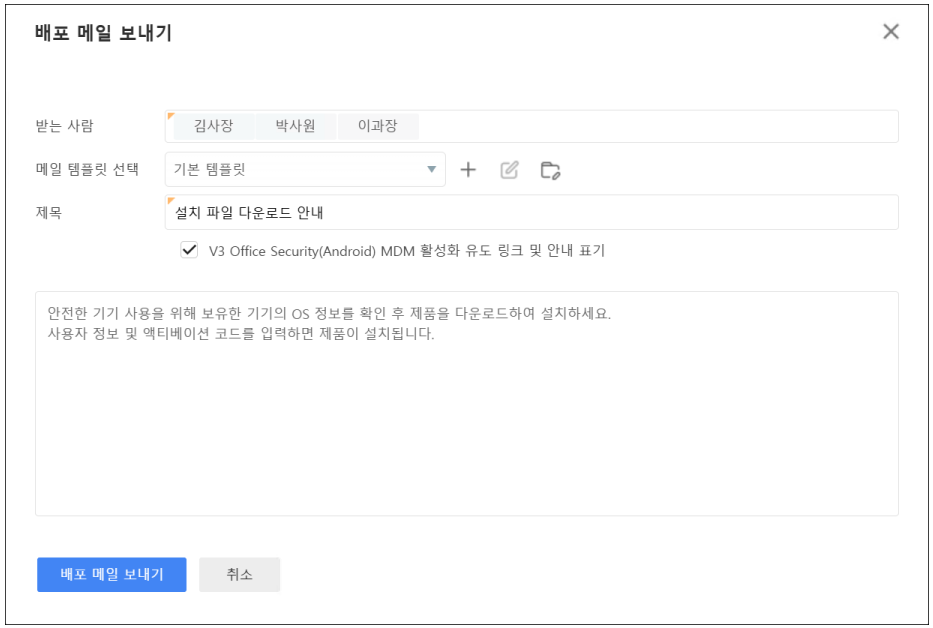
배포메일 발송

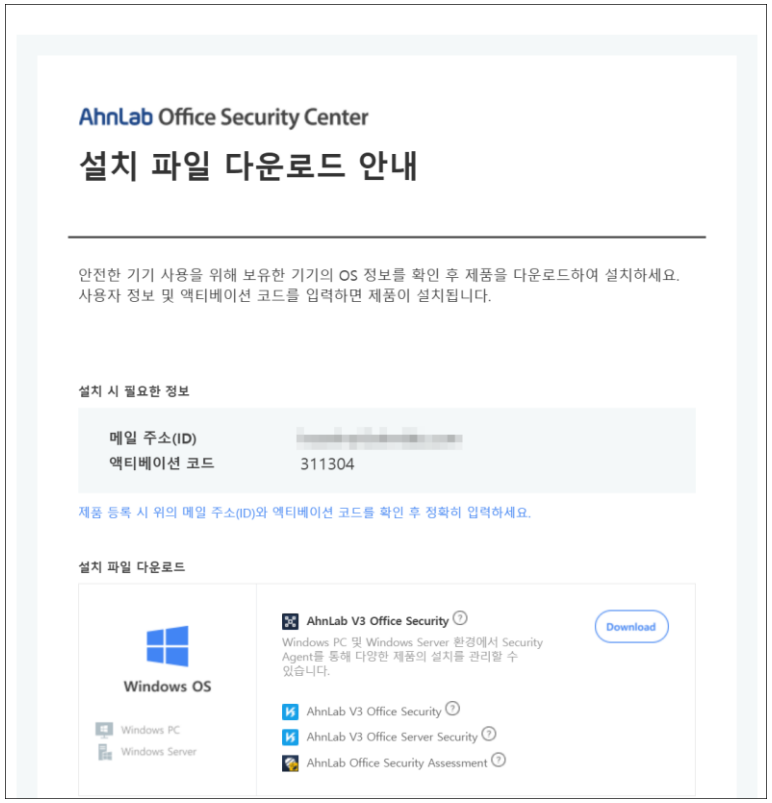
✅ 2. 사내 메일이 있는 경우

4. 배포메일 발송

- 배포 메일 보내기 창의 내용을 편집할수 있으며 편집할 내용이 없다면 [배포메일 보내기]를 눌러 사용자들에게 메일을 발송 합니다.

- 실제 발송 된 메일에는 수신자의 **메일 주소, 액티베이션 코드 , Office Security Agent 다운로드 링크**가 포함 된 메일이 수신 됩니다.
  ※ 보유 한 라이선스의 종류에 따라 배포메일 발송 시 전달되는 내용은 다를 수 있습니다.



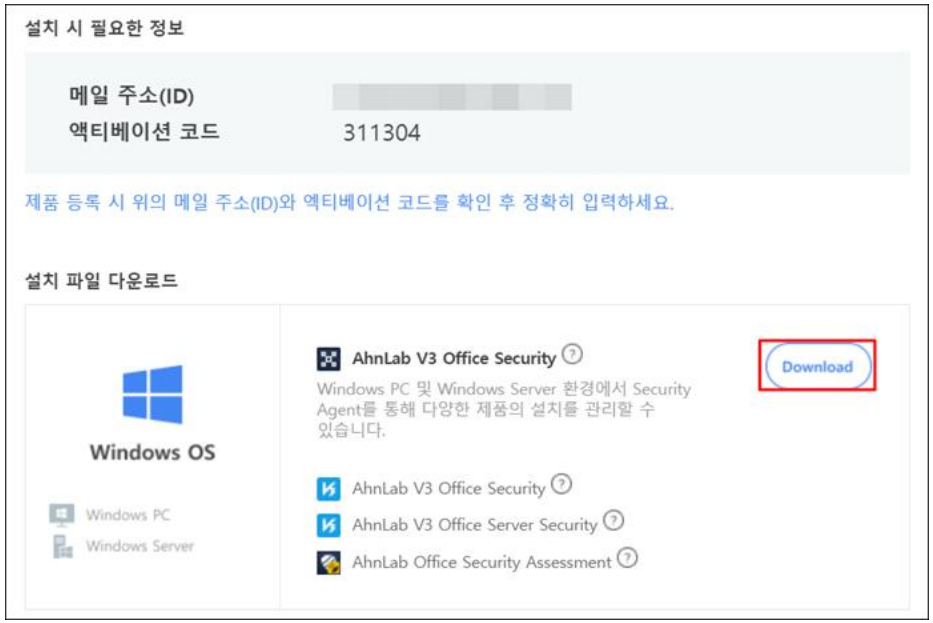


Agent 설치파일 다운로드

✅ 2. 사내 메일이 있는 경우

5. 설치파일 다운로드 후 실행

- 수신 된 메일에서 [Download] 버튼을 눌러 Office Security Agent 설치파일을 다운로드 합니다.
- 다운로드 완료 된 파일을 실행 합니다.

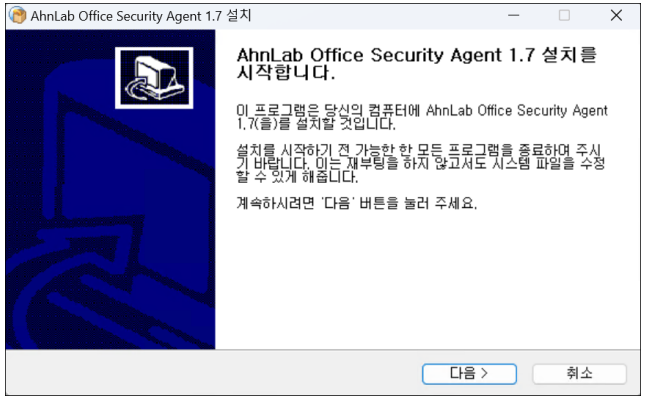


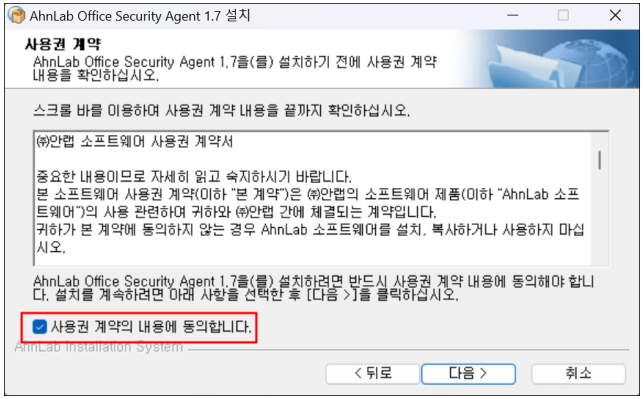
배포메일 발송

✅ 2. 사내 메일이 있는 경우

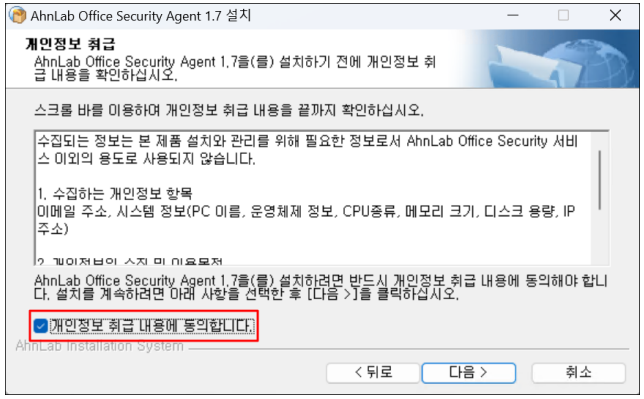
6. 제품 설치 과정

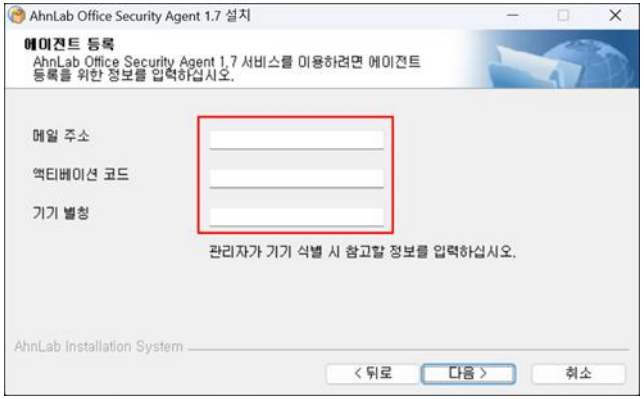
- **Agent 설치가 시작되면 [다음], 사용권 계약서에는 동의 체크박스를 체크 하고 [다음]을 클릭합니다.**





- **개인정보 취급에서 동의 체크박스 후 [다음]을 클릭합니다.**





Agent 인증 정보 입력

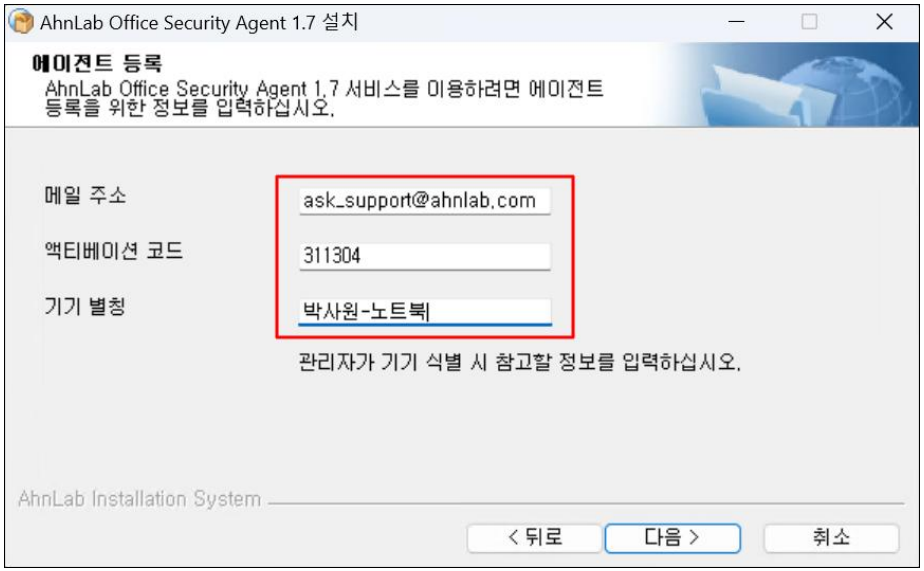
✅ 2. 사내 메일이 있는 경우

7. 에이전트 등록 정보 입력

- 메일 주소 항목에는 메일을 수신 한 **본인의 이메일 주소**를 입력 합니다.
- Office Security Center 페이지에서 엑티베이션 코드를 확인하여 입력합니다.

- 엑티베이션 코드 확인 위치
- 수신한 배포메일 본문에 본인 이메일주소와 엑티베이션 코드가 표시되어 있습니다.

- 기기 별칭의 경우 한 명의 사용자가 여러 대의 PC를 사용할 경우 기기 구분을 위한 별칭을 입력합니다.(필수 입력 값이 아닙니다)



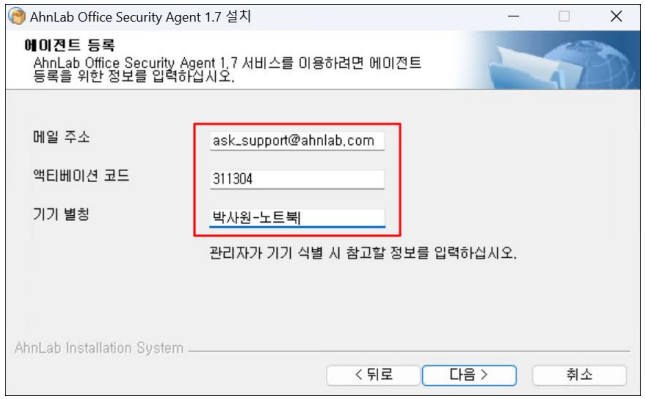
- ※ 조직도에 등록되지 않은 이메일 주소를 입력 할 경우 [코드 : 68] 오류가 발생하며 설치가 진행되지 않습니다.

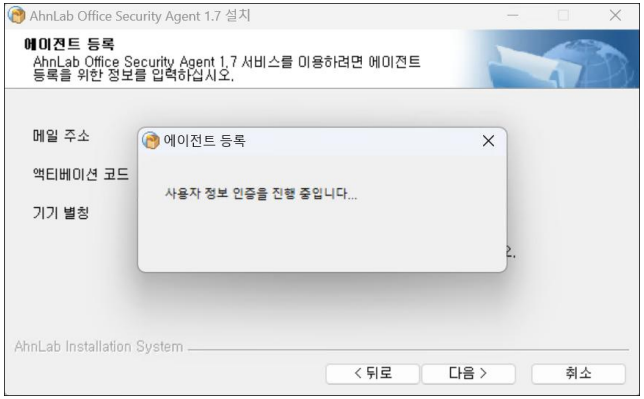
Agent 인증 정보 입력

✅ 2. 사내 메일이 있는 경우

8. 에이전트 등록 정보 입력

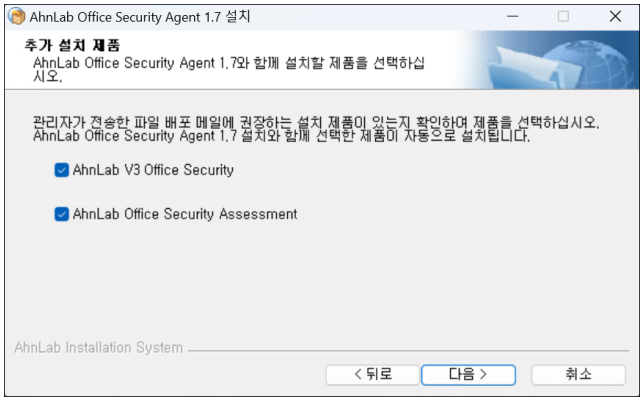
- 올바른 정보가 입력되었다면 인증이 진행 됩니다.

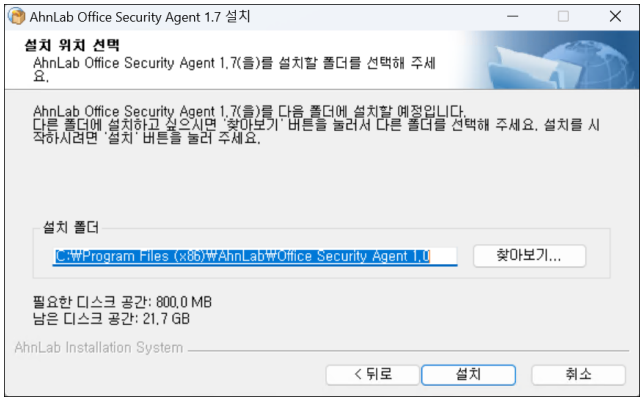




9. 보유제품 설치 여부 체크

- Agent 설치 시 함께 설치할 제품(V3)이 체크되었는지 확인 후 [다음], 설치 폴더 지정에서는 [설치]를 클릭하면 파일 복사가 진행 됩니다.



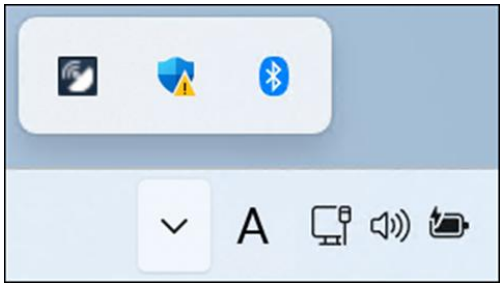


Agent 인증 정보 입력

✅ 2. 사내 메일이 있는 경우

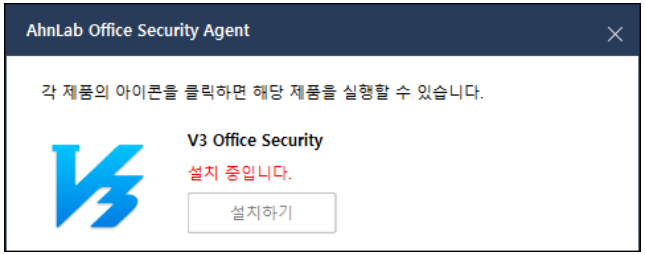
10. Office Security Agent 설치 마침

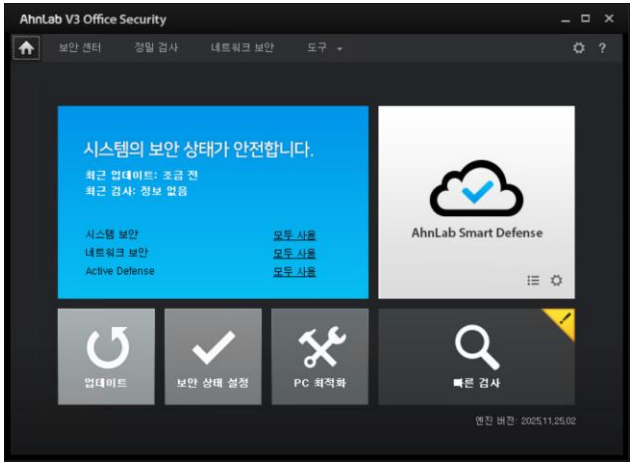
- **설치가 마무리 되고 [마침]을 누르면 시스템 트레이에 다음과 같은 Office Security Agent 아이콘이 표시 되고 보안제품 설치 안내창이 나타납니다.**



11. Office Security Agent를 통한 V3 설치 진행

- 잠시 후 **Agent가 사용자 PC에 설치 된 OS를 감지하여 자동으로 V3를 설치**합니다.
  ※ V3 설치는 백그라운드로 진행 되며 설치 과정이 화면에 표시되지 않습니다





- 백그라운드를 통한 V3 설치가 마무리 되면 V3가 팝업되어 표시 되며 마무리 됩니다.

설치 완료 후 기기 정보 확인

✅ 2. 사내 메일이 있는 경우

12. 설치 정보 확인

- 설치 된 기기 정보는 다음의 메뉴를 통해 확인 할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 기기

- 설치 시 입력한 메일주소를 통해 사용자 이름, 메일주소가 조직도에 등록 된 정보와 매칭되어 자동으로 입력 됩니다.
- 한 명의 사용자가 여러 대의 PC를 사용하는 경우도 있을 수 있으므로 기기 별칭 입력을 통해 기기를 구분할 수 있도록 사용을 권장합니다.

기본 관리 정책

AhnLab

사내 보안 정책 수립

✅ 제품 설치 후 관리 정책

제품의 배포가 완료 된 이후 일반적으로 관리자가 다음과 같은 궁금증을 가질 수 있습니다.

- 설치된 백신을 사용자들이 잘 사용하고 있는지 어떻게 확인할 수 있나?
- V3를 잘 사용할 수 있는 방법(정책)은 어떤 게 있나?
- 클라우드형 제품(SaaS)인데 관리자가 어떠한 방법으로 사용자를 관리 할수 있나?
- 얼마나 주기적으로 관리를 해주어야 할까?

몇 가지 관리 포인트를 지정하여 사내 보안 정책 수립을 통해 안전한 사용 환경을 구축 하실 수 있습니다.

다음으로 보안정책 수립 시 참고할 **체크포인트**에 대해 몇가지 알아보겠습니다.

사내 보안 정책 수립

✅ 제품 설치 후 관리 정책

다음의 스텝을 참고하여 사내 보안정책 수립을 고려 해 볼 수 있습니다.

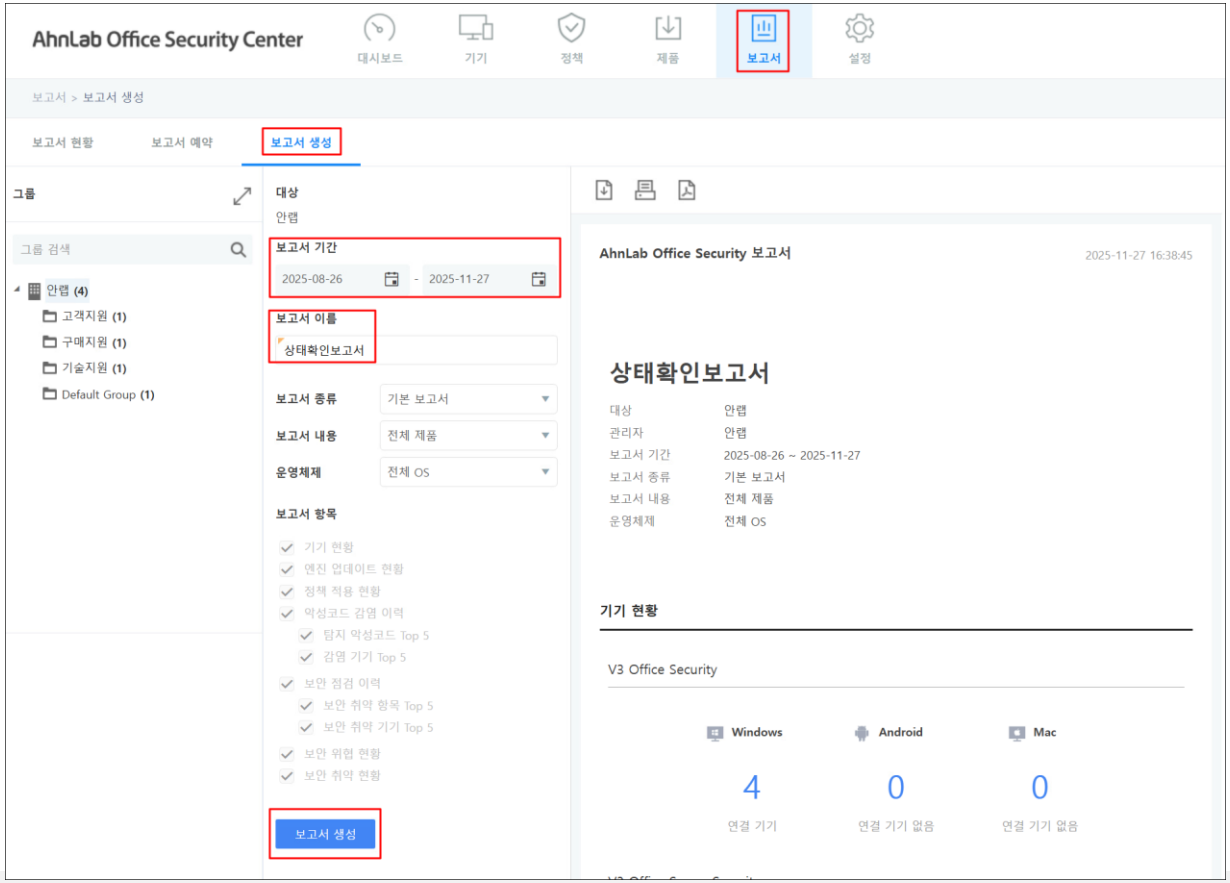
1. 관리가 필요한 **대상 PC(취약 기기) 확인**
2. 어떠한 사유로 **관리 대상(취약) 상태**로 분류 되었는지 **원인 확인**
3. 취약점을 해소하는 관리자의 **관리 업무 수행**
4. 취약점 조치 이후 상태가 안전으로 변경 되었는지 **상태 확인**
5. **정기 보고서(주간 보고서)** 수신을 통한 모니터링

보고서를 통한 보안상태 확인

✅ 1. 관리 대상 기기 확인

1) Office Security Center 보고서를 통한 관리 대상 기기 확인 방법

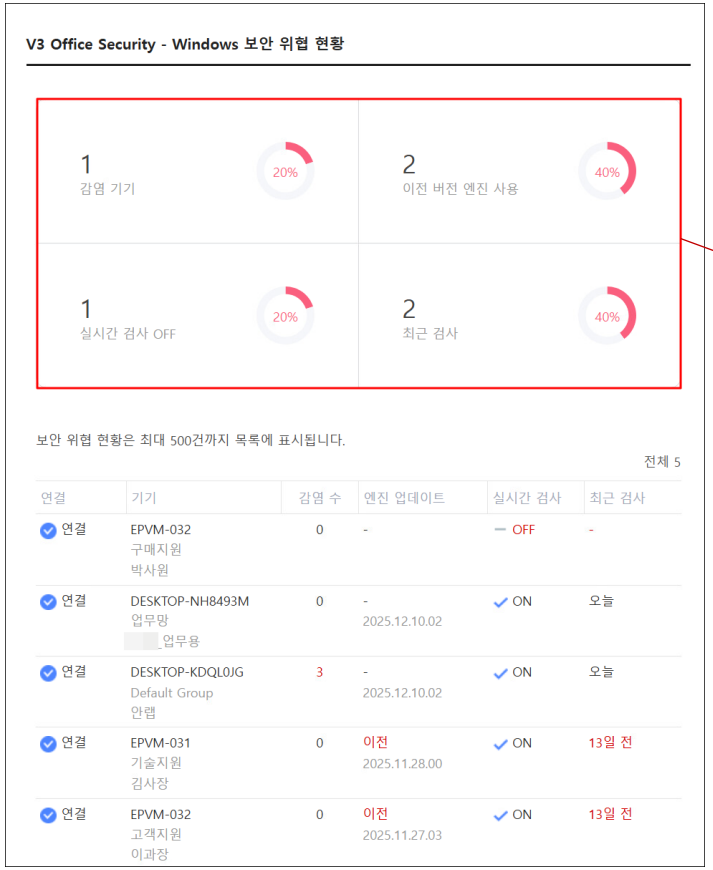
- Office Security Center 관리자 페이지 로그인 > 보고서 > 보고서 생성 > 보고서 기간 선택 및 이름 입력 > 보고서 생성 클릭



보고서를 통한 보안상태 확인

✅ 1. 관리 대상 기기 확인

- 보고서의 내용을 통해 기기의 보안 위협 현황(취약) 상태를 확인 할 수 있고 관리 대상 기기를 확인 할 수 있습니다.
- 취약한 사용자 정보를 확인하여 조치가 필요한 내용을 확인합니다.



V3 Office Security - Windows 보안 위협 현황

1 감염 기기 (20%)	2 이전 버전 엔진 사용 (40%)
1 실시간 검사 OFF (20%)	2 최근 검사 (40%)

보안 위협 현황은 최대 500건까지 목록에 표시됩니다.

전체 5

연결	기기	감염 수	엔진 업데이트	실시간 검사	최근 검사
연결	EPVM-032 구매지원 박사원	0	-	OFF	-
연결	DESKTOP-NH8493M 업무망 _업무용	0	- 2025.12.10.02	ON	오늘
연결	DESKTOP-KDQL0JG Default Group 안랩	3	- 2025.12.10.02	ON	오늘
연결	EPVM-031 기술지원 김사장	0	이전 2025.11.28.00	ON	13일 전
연결	EPVM-032 고객지원 이과장	0	이전 2025.11.27.03	ON	13일 전

보고서를 통해 **관리 대상 기기(취약)**로
확인되는 사용자 정보는 아래 4가지 입니다.

1. **감염 기기 :**
   30분 이내에 악성코드 감염이 발생한 경우
2. **이전 버전 엔진 사용 :**
   엔진 업데이트를 진행한지 7일을 초과
3. **실시간 검사 OFF :**
   실시간 검사 기능이 OFF 상태인 경우
4. **최근 검사 :**
   바이러스 검사를 수행한지 7일을 초과한 경우

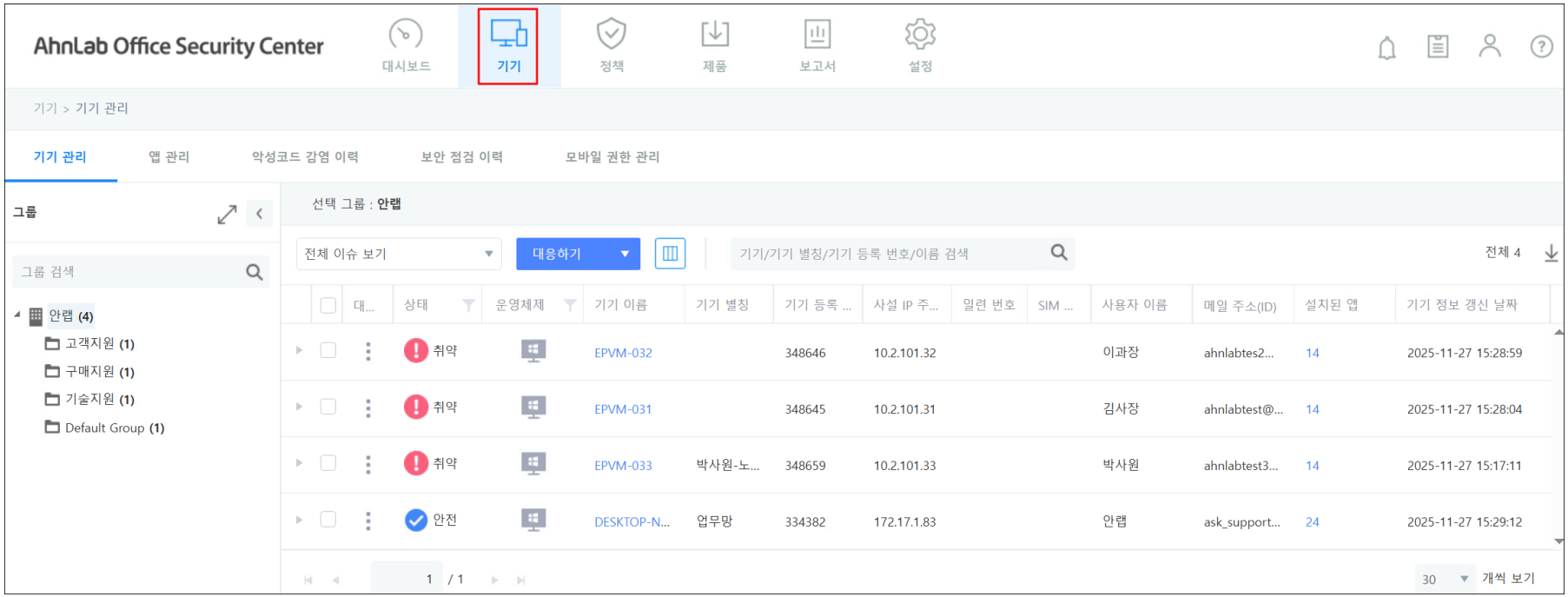
OSC 기기 목록 확인을 통한 보안 상태 확인

✅ 1. 관리 대상 기기 확인

2) 설치된 기기 목록을 통한 관리대상 기기 확인

- Office Security Center 관리자 페이지 로그인 > 기기
- 설치 된 기기 목록 중 상태가 '취약' 으로 분류 된 기기가 관리대상 기기 입니다.

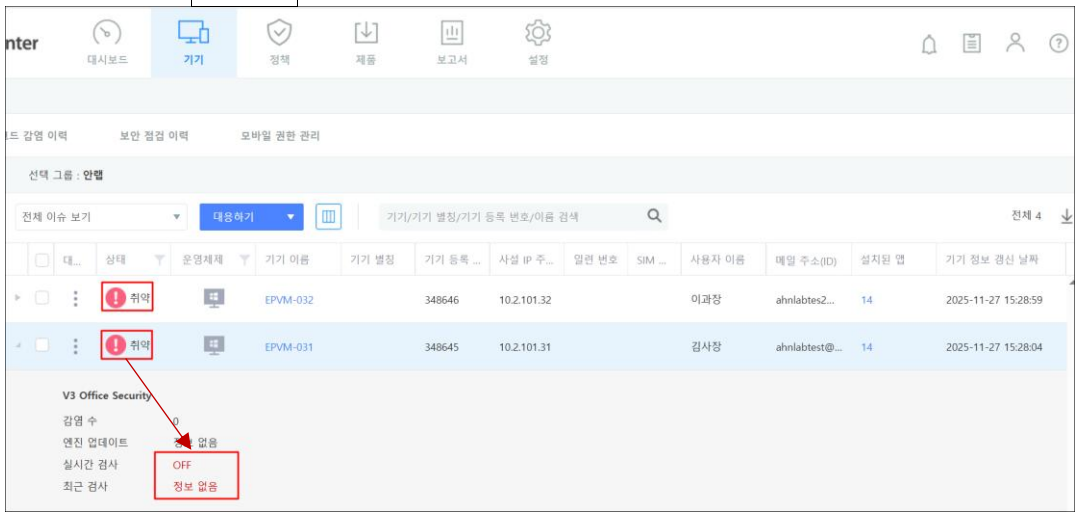
  - 설치 된 전체 기기 목록을 확인 할 수 있으며 기기의 상태(취약 또는 안전)를 확인 할 수 있습니다.



취약 사유 확인

✅ 2. 취약 사유 확인

- 관리대상 기기가 확인되었다면 제품의 상태가 취약으로 표시되는 원인에 대해 확인합니다.
- 상태 하단의 취약 을 클릭하면 각 기기가 취약으로 표시되는 원인을 확인 할 수 있습니다.



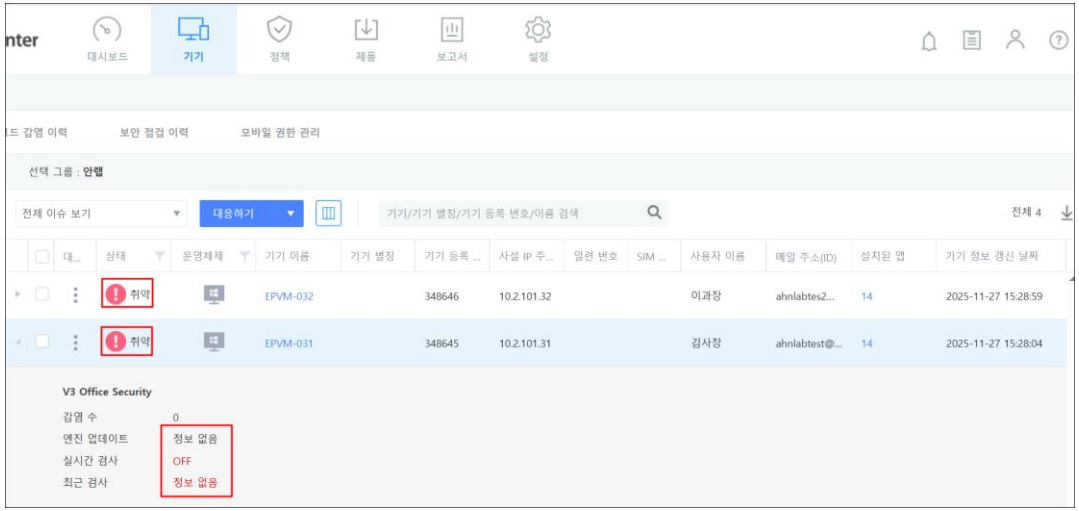
취약으로 표시되는 기기의 사유는 다음과 같습니다.

1. **바이러스를 검사한지 7일을 초과한 경우** (V3 설치 후 한번도 검사를 진행하지 않은 경우)
2. 최근에 **엔진 업데이트를 진행한지 7일을 초과** 한 경우
3. **실시간 검사 기능이 OFF** 상태인 경우
4. **30분 이내에 악성코드 감염이 발생한 경우**(30분 이내에 악성코드가 진단 된 경우)

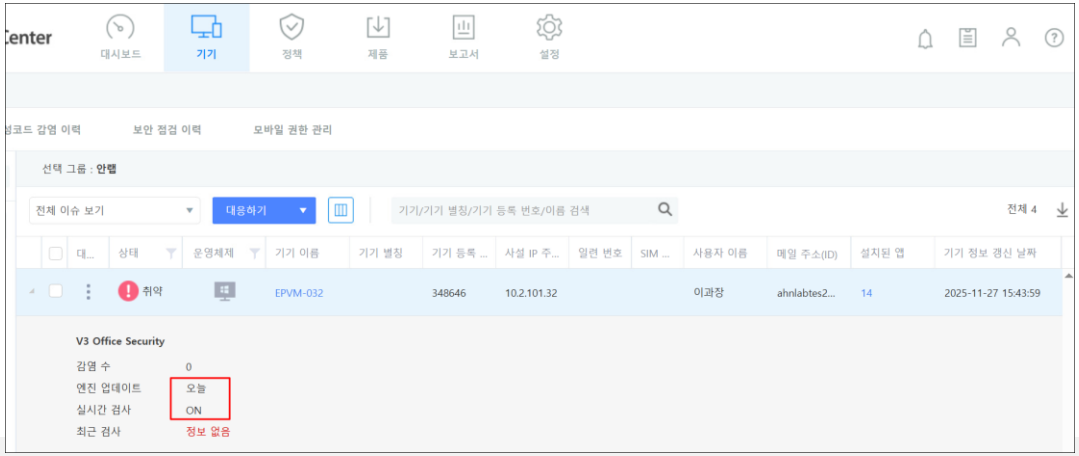
취약 기기 정보 확인(최초 설치 후)

✅ 2. 취약 사유 확인

- 제품 설치 후 PC에 설치 된 Office Security Agent는 **V3의 동작 상태를 확인하여 15분마다 서버로 전송** 합니다.
- 제품 최초 **설치 후 15분 이내의 PC는 V3의 상태가 취약**으로 표시 될 수 있습니다.



제품 설치 후 15분이 지나 지 않은 경우
엔진 업데이트 및 실시간 검사 기능의 동작 상태가
확인되지 않아 정보 없음으로 표시 되는 상태



설치 후 15분이 지나 엔진 업데이트 및
실시간 검사 기능이 ON 상태로 변경 되었음을 확인

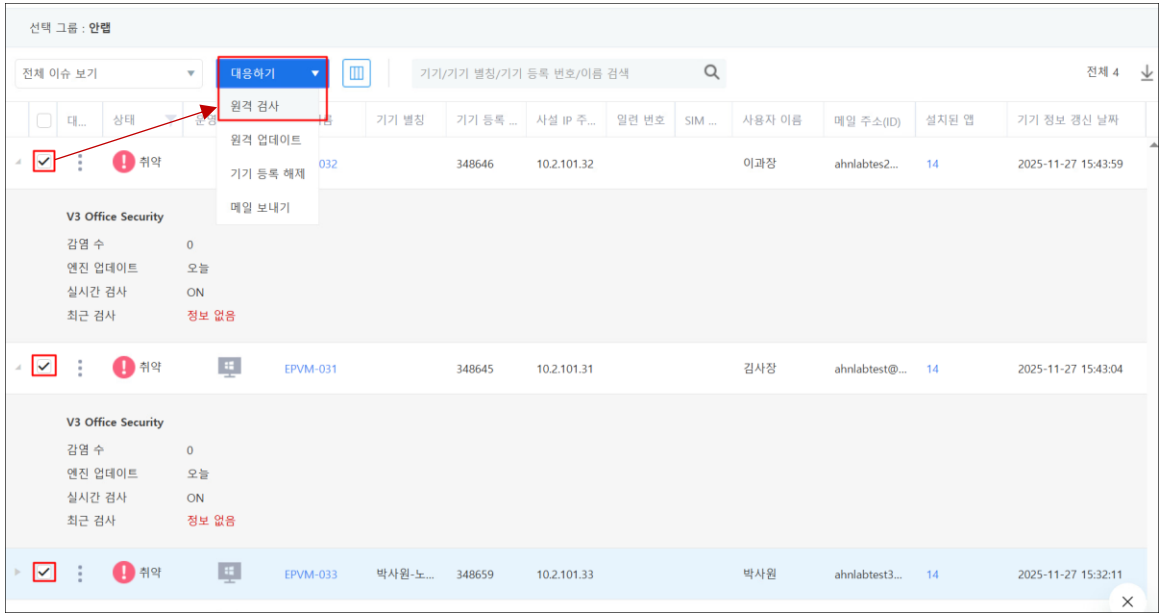
취약 : 최근 검사 7일초과 원격 검사 명령

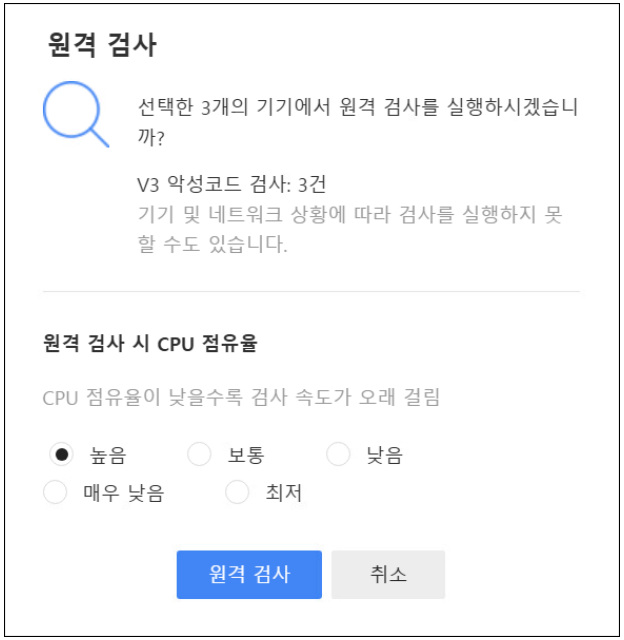
✅ 3. 취약 기기 [원격 검사] 조치

- **<u>설치 이후 바이러스 검사가 진행되지 않아 취약(검사 7일 초과)</u>**으로 분류 되었습니다.
- 관리자는 사용자 PC에서 바이러스 검사가 진행 될 수 있도록 [대응하기] 원격 명령을 통해 바이러스 수동검사를 진행할 수 있습니다.

- V3 Office Security는 아래와 같은 방법으로 **<u>관리자가 [원격 검사] 명령</u>**을 통해 최근 검사로 인한 취약 기기를 조치 할 수 있습니다.

1. [정밀 검사]가 필요한 기기 체크박스 체크
2. [대응하기]를 눌러 [원격 검사]를 클릭
3. 원격 검사 시 CPU 점유율을 선택(기본값 높음)
4. 사용자 PC에 원격 검사 명령 전달(15분 이내)
5. 원격 명령을 받은 사용자 PC에서 [원격 검사] 수행 후 검사 결과 서버 전송





검사가 완료되면 상태가 '취약 ' 에서 안전으로 변경 됩니다.

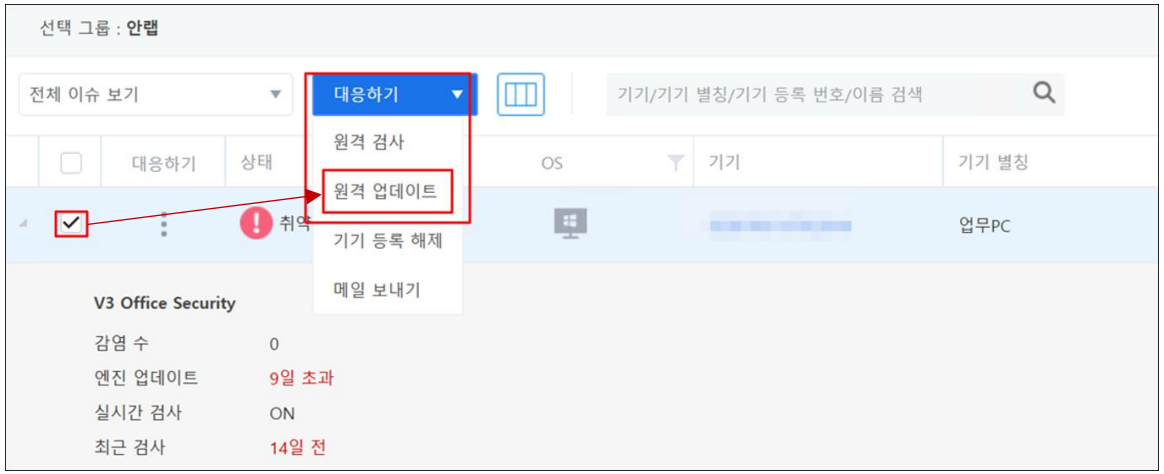
취약 : 최근 업데이트 7일 초과 원격 업데이트 명령

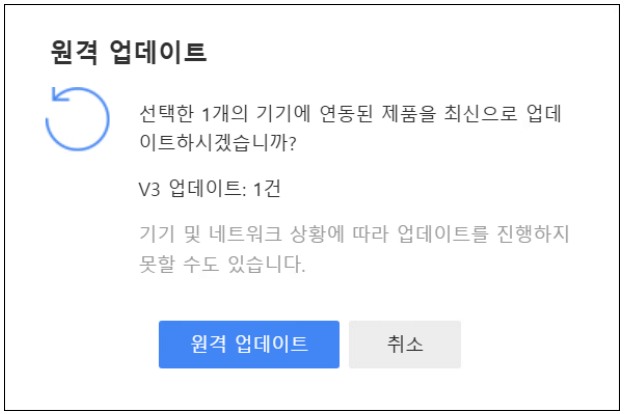
✅ 3. 취약 기기 [원격 업데이트] 조치

- 엔진 **업데이트가 진행 된 지 7일을 초과 한 경우도 취약**으로 분류 됩니다.

- 아래와 같은 방법으로 [원격 업데이트] 명령을 통해 최근 검사로 인한 취약 기기를 조치 할 수 있습니다.

1. [엔진 업데이트]가 필요한 기기 체크박스 체크
2. [대응하기]를 눌러 [원격 업데이트]를 클릭
3. 사용자 PC에 원격 검사 명령 전달(15분 이내)
4. 원격 명령을 받은 사용자 PC에서 [엔진 업데이트] 수행 후 엔진버전 업데이트 결과 서버 전송





- ※ V3 제품의 경우 [자동 업데이트] 옵션이 기본으로 활성화 되어있습니다. (3시간 마다 최신 엔진 업데이트 시도)

- ※ 7일 이상 업데이트가 진행되지 않았다면, 실제 PC에 V3가 설치 되어있는지, 사용자의 PC가 켜져 있는지 확인하여 주시기 바랍니다.

취약 : 30분 이내에 발견된 악성코드가 있는 경우

✅ 3. 취약(감염) 기기 추가 검사 모니터링

- 사용자PC에서 **30분 이내에 진단 된 악성코드가 있는 경우** 취약으로 분류 됩니다.

- 감염이 확인 된 PC에서 정밀검사를 수행 합니다.
- [정밀 검사] 또는 [원격 검사]를 통해 치료가 완료되고 30분 이내에 추가 악성코드가 발견되지 않는 경우 자동으로 상태가 안전으로 변경 됩니다

※ 악성코드가 발견 된 PC에서 추가 정밀검사를 권장 합니다.
※ 진단 된 악성코드가 치료불가 상태이거나 동일한 악성코드가 재진단 될 경우 안랩 기술지원센터를 통한 문의가 필요합니다.

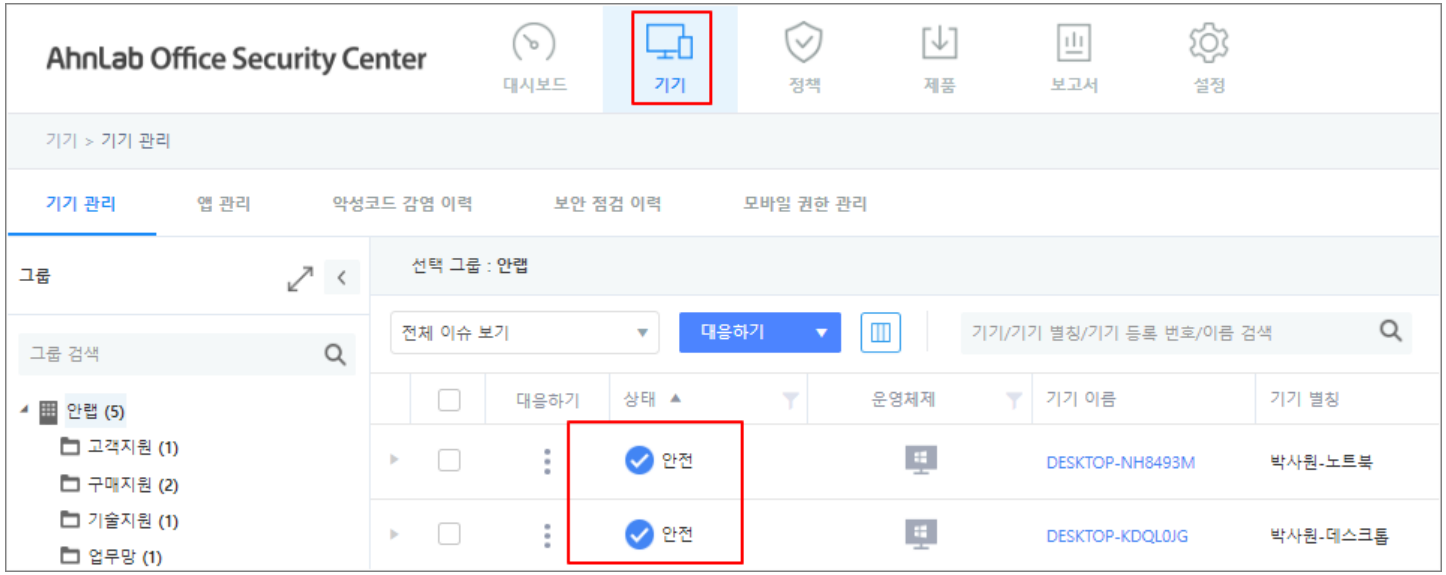
상세 감염정보 및 치료 상태 확인 방법은 본 가이드 55페이지 **[악성코드 감염 알림 메일을 수신했습니다.]** 내용을 참고 부탁드립니다.

취약기기 조치방법(동영상) :
https://ask.ahnlab.com/hc/ko/articles/40481352624921

기기 상태 '안전 ' 확인

✅ 4. 조치 후 상태 '안전' 변경 확인

- 원격 검사 및 원격 업데이트 등을 통해 기기의 취약 사유를 조치한 이후 기기 상태를 확인하면 '안전 ' 으로 상태가 변경 된 것을 확인 할 수 있습니다.



※ 사용자 PC의 상태 정보는 서버에 주기적으로 전송 됩니다. (검사 결과 정보는 실시간으로 전송되지 않습니다.)

※ 검사 완료 후 검사 완료 '안전' 상태를 서버로 정보 전송하기까지 **최대 30분까지 소요** 될 수 있습니다.

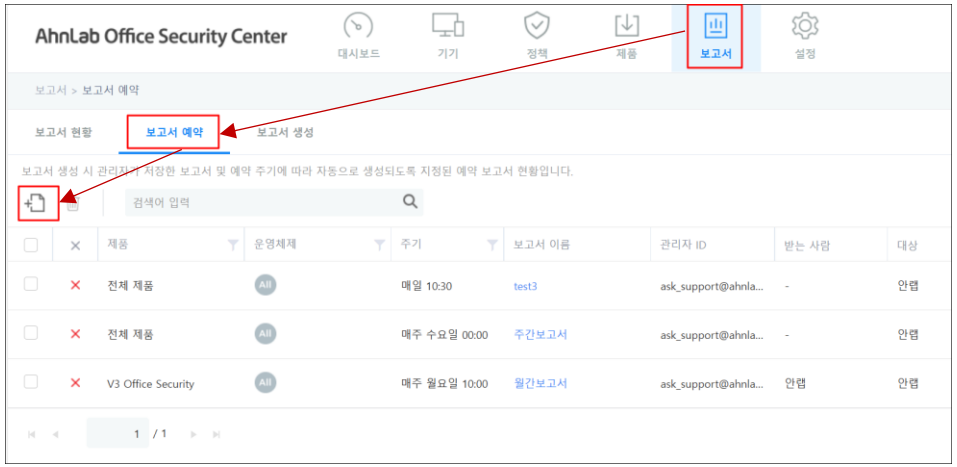
정기 보고서 예약 기능 활용

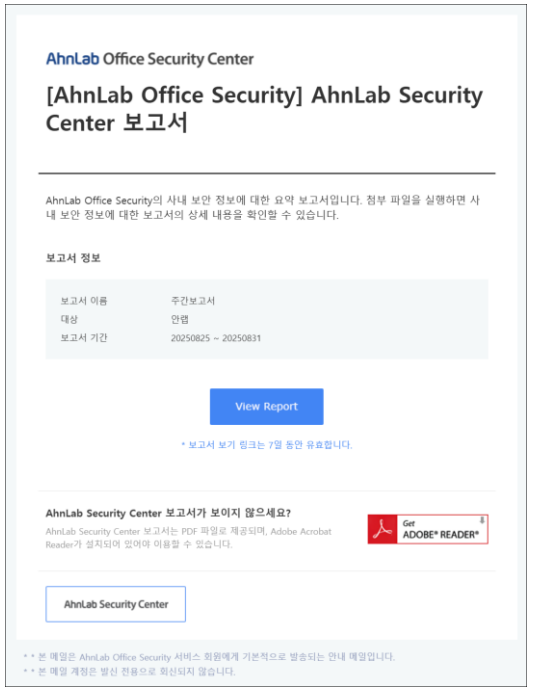
✅ 5. 주기적인 상태 모니터링

기본 제공되는 보고서 예약 기능을 통해 Office Security Center 관리자 페이지에 매번 접속하지 않아도 정기적으로 보고서를 메일로 받아 현황을 확인할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 보고서 > 보고서 예약
- 취약 기기의 기준이 7일이므로 **[주간보고서]**를 예약하여 최소 주 1회 이상 주간보고서를 참고하여 관리가 필요한 기기 목록 점검을 권장 드립니다.

※ 보고서는 1년간의 데이터를 서버에 보관하고 있습니다. 필요한 경우 감사 증적용으로도 활용이 가능합니다.(인쇄하거나 PDF 파일로 저장 가능합니다)





추천 정책

V3를 효과적으로 사용할 수 있도록 정책을 추천드립니다

AhnLab

추천 정책1(예약검사 설정)

✅ 1. V3를 효과적으로 사용할 수 있는 방법(정책)

V3가 설치되어 있지만 잘 사용하려면 어떻게 해야 하나? 라는 고민이 드신다면 다음과 같은 정책을 활용 해 볼 수 있습니다.

최근 7일 이내에 수동 검사가 진행되지 않을 경우 상태가 [취약]으로 변경 됩니다. 매번 직접 검사가 번거롭다면 다음의 방법을 참고해주세요.

- Office Security Center 관리자 페이지 로그인 > 정책 > V3 Office Security > Windows – Default(또는 사용중인 정책)
- 예약검사 설정을 통해 주기적으로 검사 수행하여 보안상태를 안전 상태로 유지 할 수 있습니다.
- 매일, 매주(요일 선택 가능), 매월(날짜 선택 가능) 예약검사를 지정할 수 있습니다.
- ※ 7일 이내 주기적인 검사를 위해 검사주기는 최소 **주1회 이상 예약 검사 설정을 권장** 드립니다.

추천 정책2(삭제 방지 설정)

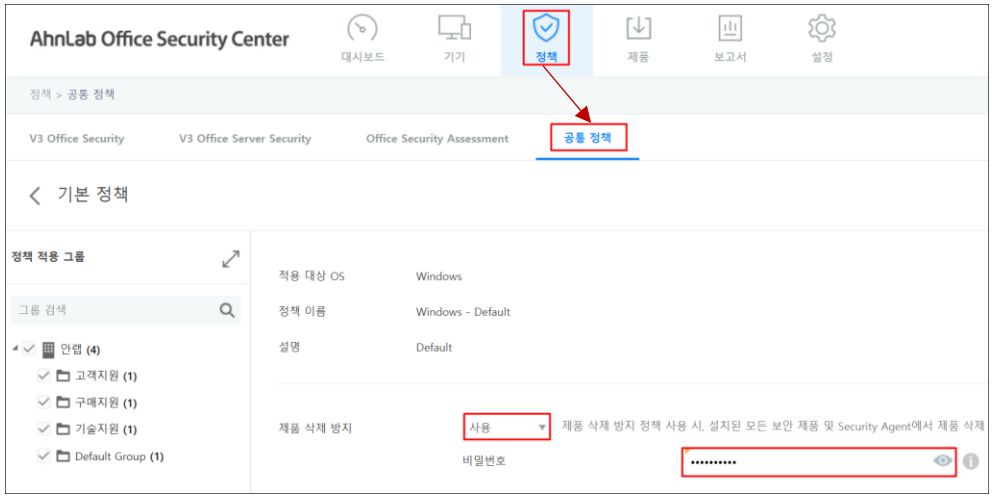
✅ 2. V3를 효과적으로 사용할 수 있는 방법(정책)

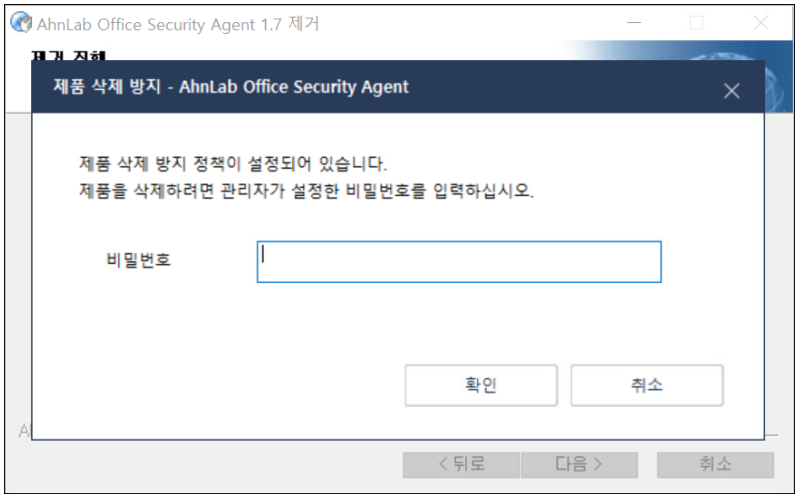
사용자가 번거롭다며 V3를 지우려고 시도합니다.

사용자가 임의로 제품을 삭제하지 못하도록 차단하려면 다음의 방법을 참고하여 주세요.

- Office Security Center 관리자 페이지 로그인 > 정책 > 공통 정책> Windows – Default(또는 사용중인 정책)
- 제품 삭제 방지 : 사용으로 변경 후 비밀번호를 입력하고 저장 합니다.

  ※ 제품을 삭제하려고 시도하면 관리자가 지정한 비밀번호를 넣어야만 삭제가 허용 됩니다.





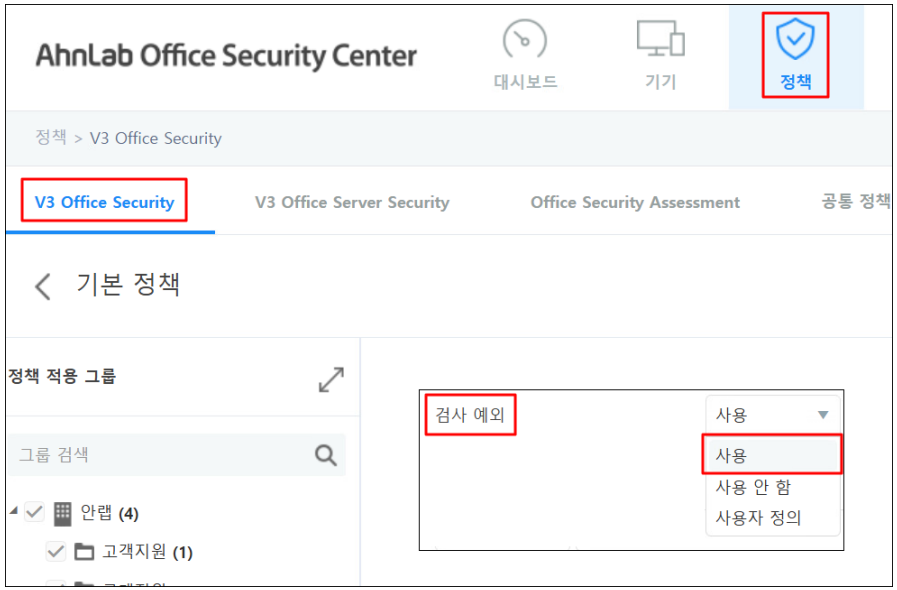
추천 정책3(검사 예외 설정)

✅ 3. V3를 효과적으로 사용할 수 있는 방법(정책)

사내에서 사용중인 **프로그램을 V3가 검사하지 않도록 예외처리**를 해야 할 경우 아래와 같은 방법으로 검사 예외대상을 지정 할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 정책 > V3 Office Security > Windows – Default(또는 사용중인 정책)
- 검사 예외 옵션 [사용] : 관리자가 미리 지정 해 놓은 파일은 V3가 검사하지 않습니다.

※ 사전에 검사 예외대상을 파악하여 관리자가 직접 경로 및 파일명을 지정해주어야 합니다.



사용자가 직접 검사 예외대상 추가를 허용하려면 다음 페이지를 참고하여 주시기 바랍니다.

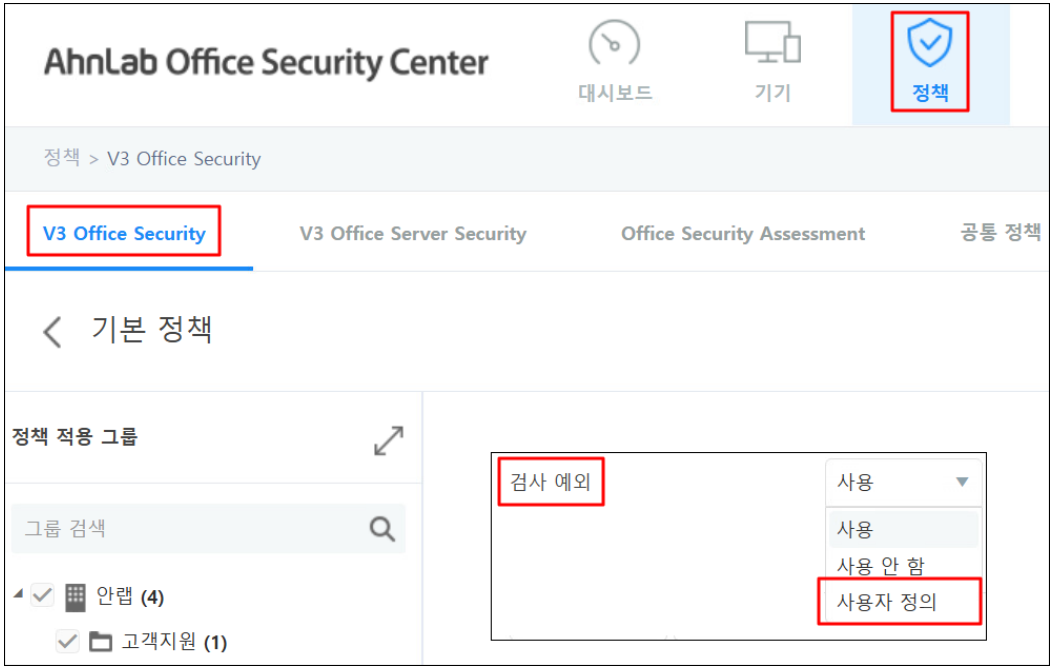
추천 정책3(검사 예외 설정)

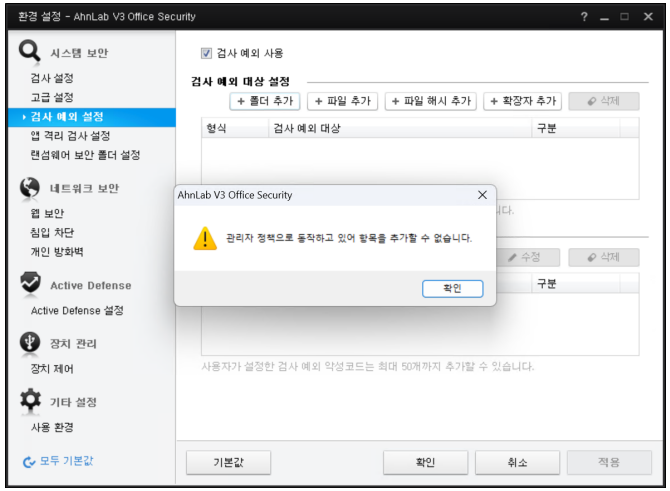
✅ 3. V3를 효과적으로 사용할 수 있는 방법(정책)

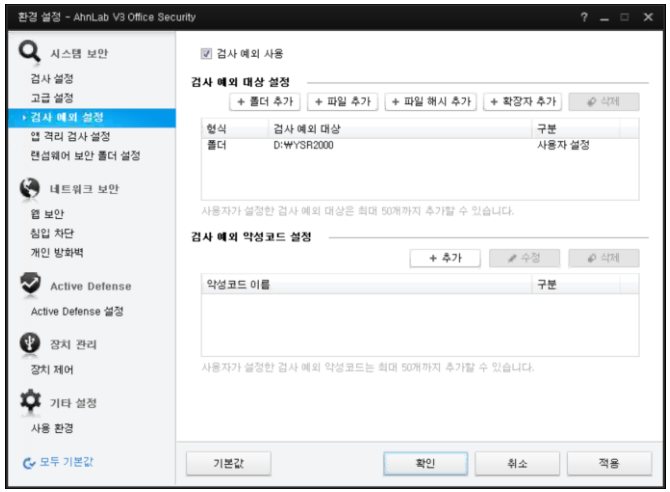
검사 예외 옵션이 [사용] 인 상태에서 사용자가 직접 검사 예외 경로를 직접 추가하려고 할 경우

- **관리자 정책으로 동작하고 있어 항목을 추가할 수 없습니다.** 오류가 발생합니다.

- 사용자가 직접 검사 예외 대상을 추가 할 수 있도록 허용하려면
- **검사 예외 옵션을 [사용자 지정]으로 변경** 해야 합니다.







추천 정책4(USB 장치 제어 설정)

✅ 4. V3를 효과적으로 사용할 수 있는 방법(정책)

개인정보 유출 방지 및 USB 장치를 통한 악성코드 감염을 막기 위해 사용자 PC에서 USB 장치를 사용하지 못하도록 차단하고 싶습니다.

※ Autorun 바이러스 유형의 경우 USB 장치를 연결하는 것 만으로도 USB 내 바이러스가 자동 실행되어 바이러스에 감염 될 수 있습니다.

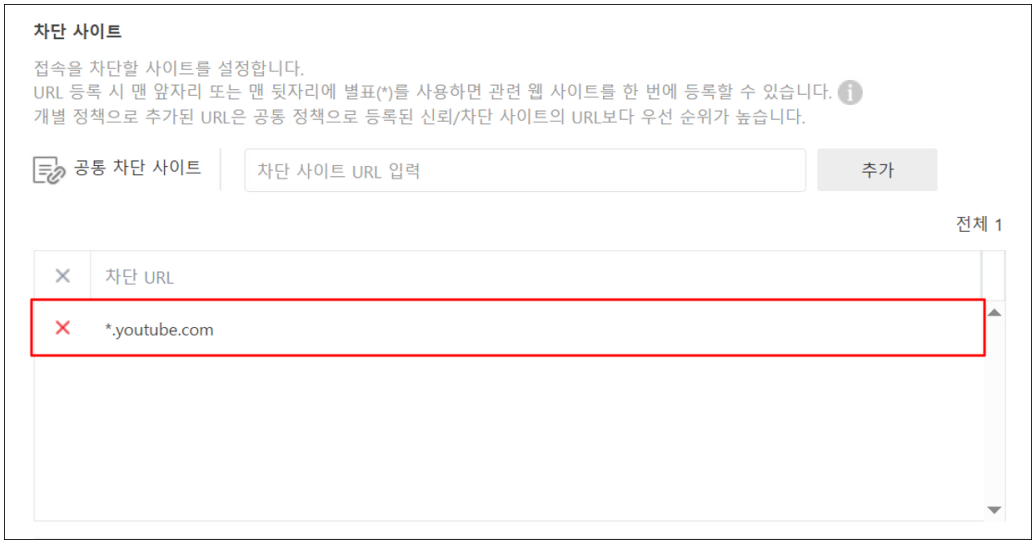
- Office Security Center 관리자 페이지 로그인 > 정책 > V3 Office Security > Windows – Default(또는 사용중인 정책)
- 장치 제어 [사용] – USB 장치 [차단] 인 경우에도 필요 시 프린터 및 USB 포트를 사용하는 미디어 장치를 허용하거나 차단 할 수도 있습니다.

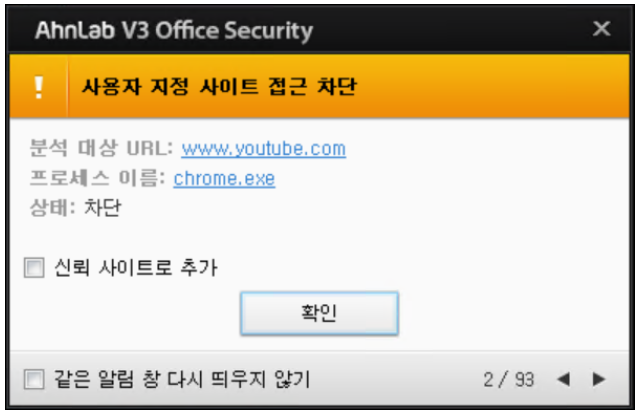
추천 정책5(차단 사이트 설정)

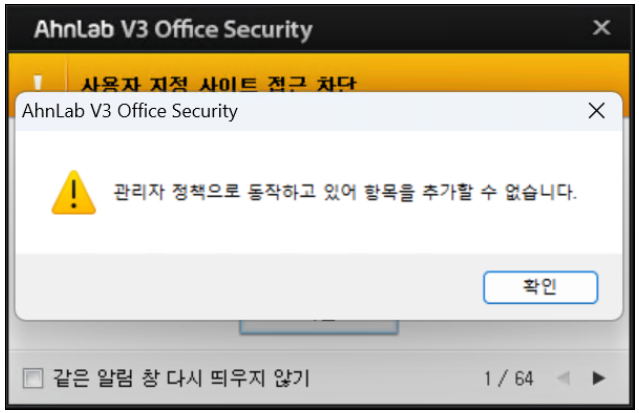
✅ 5. V3를 효과적으로 사용할 수 있는 방법(정책)

업무에 불필요한 사이트를 접속하지 못하도록 차단하고 싶습니다.

- Office Security Center 관리자 페이지 로그인 > 정책 > V3 Office Security > Windows – Default(또는 사용중인 정책)
- 차단 사이트에 차단하고자 하는 URL을 추가
- 사용자가 신뢰 사이트로 추가를 시도할 경우 **'관리자 정책 차단' 알림** 창을 띄웁니다.







※ 위의 차단 URL 주소는 차단 예시로 입력 된 주소 입니다.
※ 일부 HTTP3 프로토콜로 동작하는 사이트의 경우 차단 기능이 동작하지 않을 수 있습니다.

관리자 체크 포인트

관리자가 참고하면 좋은 관리 포인트를 소개해 드립니다

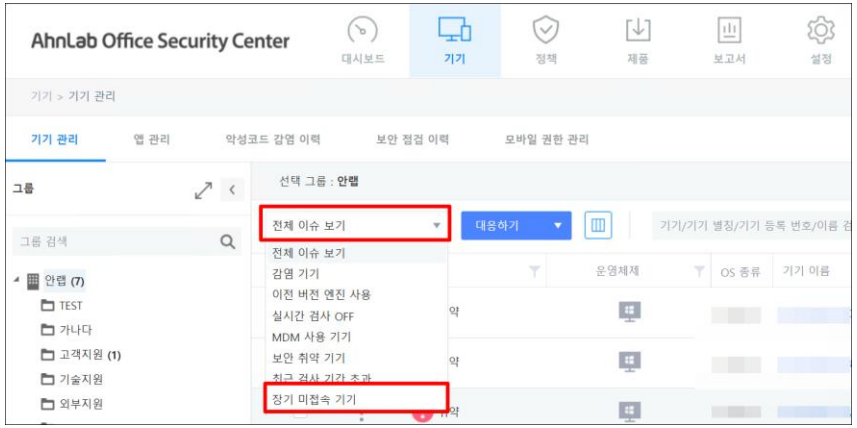
AhnLab

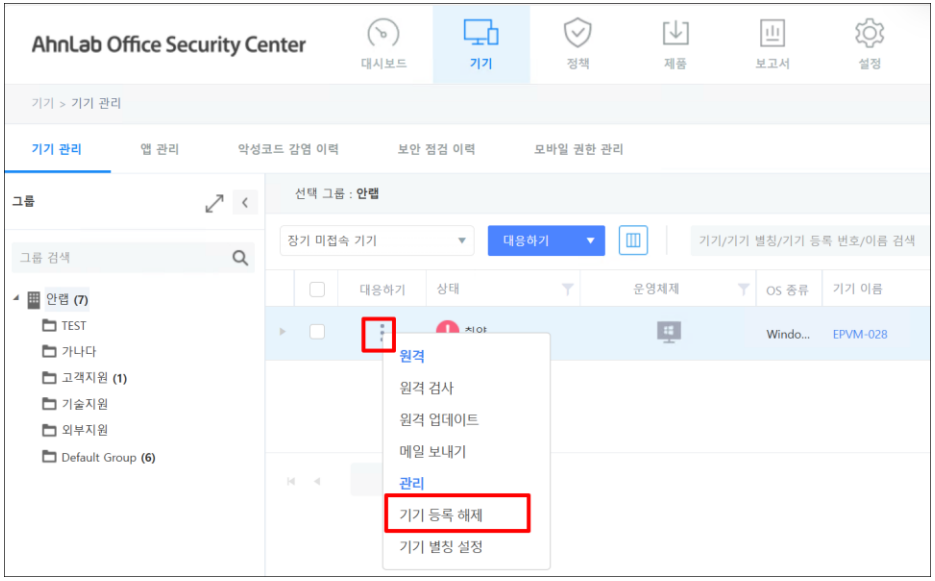
장기 미접속 기기 관리

✅ 1. 추가 체크 포인트

PC가 인터넷에 연결 되지 않았거나, 전원이 꺼져 있는 상태로 장기간(90일) 서버와 통신이 이루어지지 않는 기기는 장기 미접속 기기로 전환 됩니다.

- Office Security Center 관리자 페이지 로그인 > 기기 > 기기 관리 > [전체 이슈 보기] > [장기 미접속 기기] 클릭
- 90일 이상 사용하지 않은 기기목록이 sort 되어 보여집니다





- 장기 미접속 기기의 경우 실제 사용하지 않지만 사용 기기 목록에 등록되어 라이선스를 정상적으로 사용하고 있는 기기로 간주 됩니다.
- 따라서 해당 기기에서 더 이상 제품을 이용하지 않는다면 기기 등록 해제를 통해 라이선스를 회수 할 수 있습니다.

장기 미접속 기기의 주요 사유 :

- PC 포맷 또는 교체 과정에서 기존 사용하던 PC 정보를 삭제하지 않은 경우
- 실제로 PC 사용을 오랫동안 하지 않고 방치한 경우

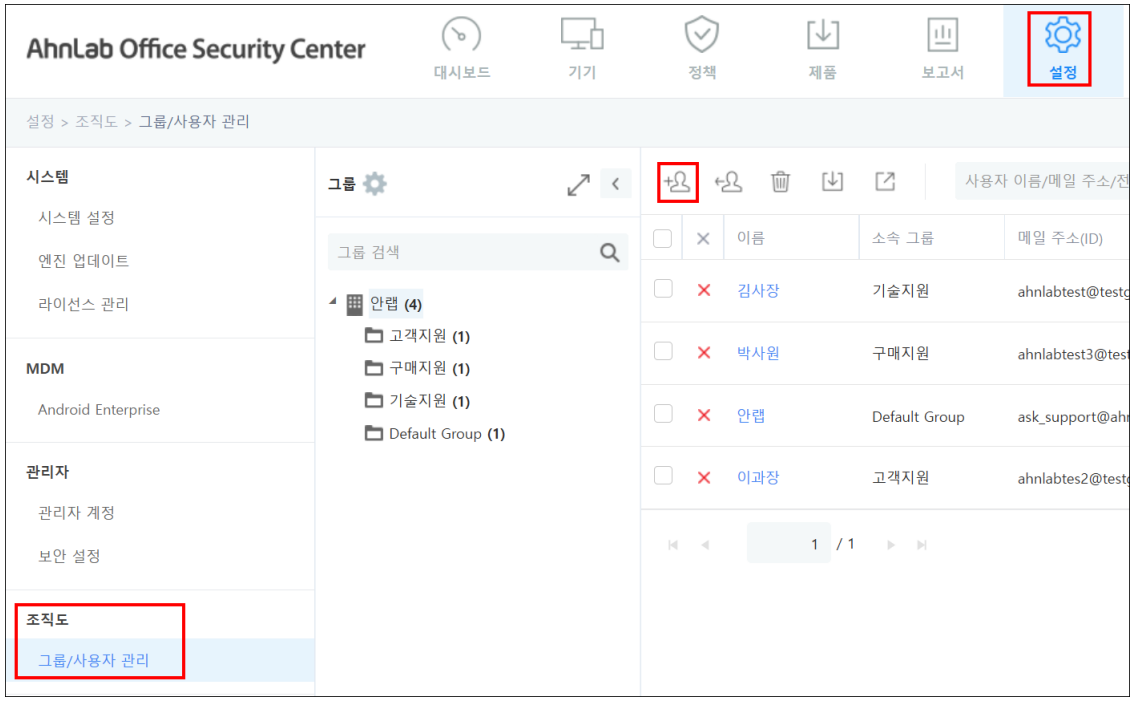
※ 장기 미접속 기기를 켜서 업데이트를 진행 할 경우 다시 **'기기 정보 갱신 날짜'**가 갱신 됩니다.

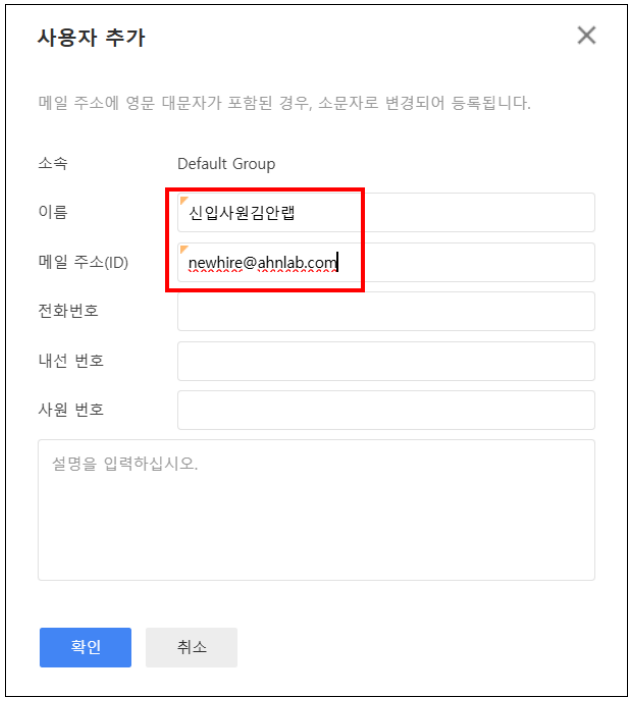
개별 사용자 추가

✅ 2. 추가 체크 포인트

조직도를 사용하는 기업의 경우 신규입사자 발생 시 사용자 정보를 간단하게 추가 할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 설정 > 조직도(그룹/사용자 관리)
- 사용자를 추가 하려면  사용자 추가 버튼을 클릭 합니다.
- 추가하려는 사원의 이름 및 메일주소를 넣고 확인을 눌러 손쉽게 사용자를 추가 할 수 있습니다.



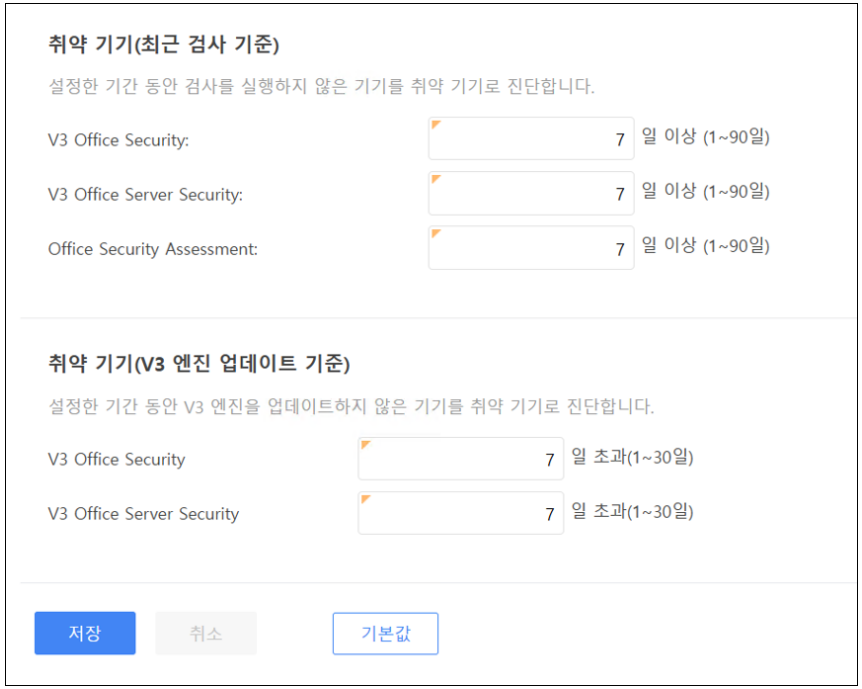


취약 상태 기준 설정

✅ 3. 추가 체크 포인트

설치 된 기기가 취약으로 변경되는 기준을 변경 할 수 있습니다.

- Office Security Center 관리자 페이지 로그인 > 설정 > 시스템 > 시스템 설정
- 최근 검사 및 최근 업데이트가 7일을 초과 할 경우 취약으로 변경 됩니다.
- 취약으로 변경되는 기준을 완화하고 싶은 경우 날짜를 수정하여 변경 할 수 있습니다. (추천하지 않음)

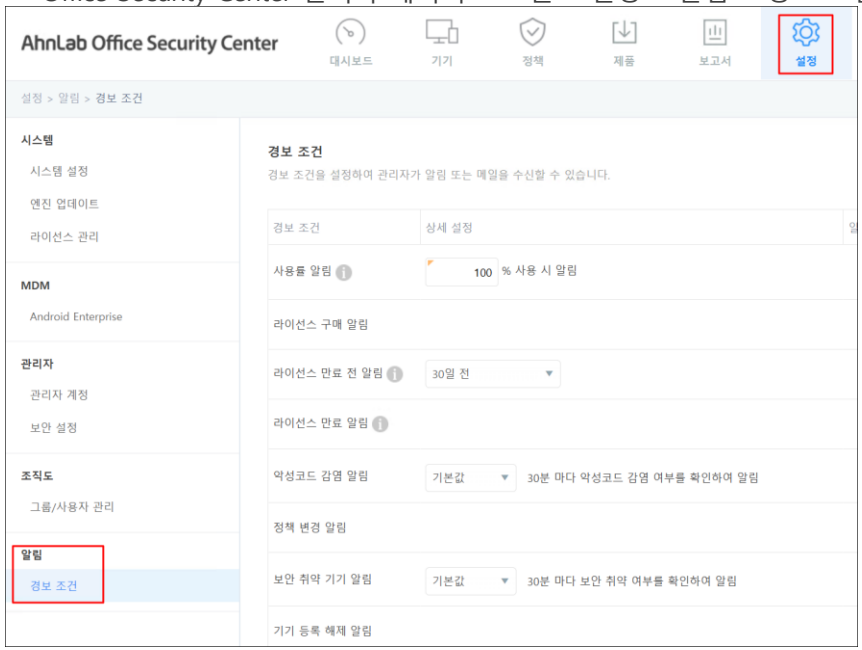


경보 알림메일 설정

✅ 4. 추가 체크 포인트

관리자가 설정한 조건에 해당하는 상황에 알림 및 메일을 받아볼 수 있습니다. (수신대상 선택가능)

- Office Security Center 관리자 페이지 로그인 > 설정 > 알림 > 경보 조건



주요 알림

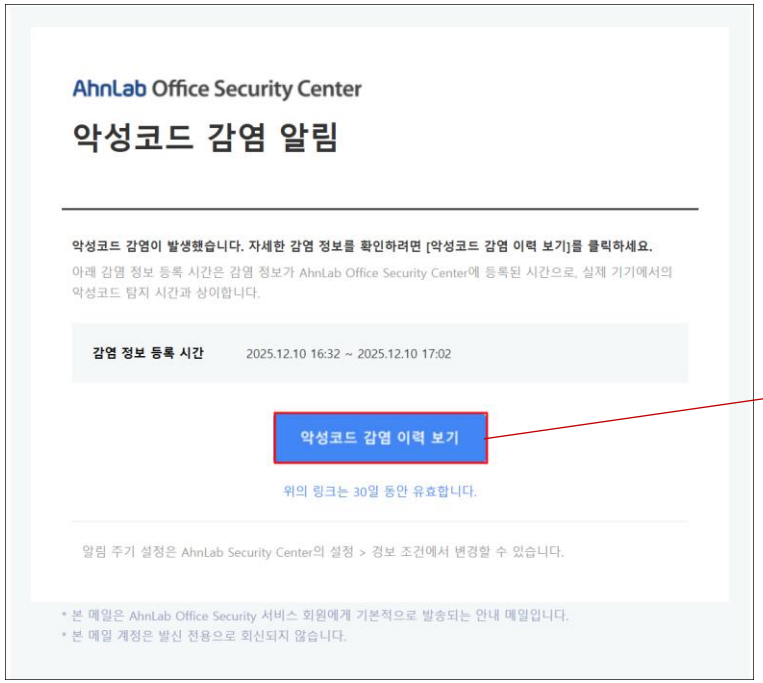
- 라이선스 만료 전 알림 : 라이선스 만료일이 다가오면 알림을 받을 수 있습니다.
- 악성코드 감염 알림 : **30분 이내에 악성코드가 진단된 기기가 있을 때** 알림을 수신 합니다.
- 보안 취약 기기 알림 : **등록 기기가 보안 점검 결과 취약**일 때 알림을 받을 수 있습니다.
- 기기 등록 해제 알림 : 관리자가 **등록 된 기기를 해제** 했을 때 알림을 수신 할 수 있습니다.

★악성코드 알림메일 설정

✅ 5. 추가 체크 포인트

악성코드 감염 알림 기능은 **바이러스에 감염 된 사용자가 있을 경우 관리자가 즉시 알림 메일을 수신** 하는 기능으로 반드시 설정하셔서 이용 하실 것을 권장 드립니다.

- Office Security Center 관리자 페이지 로그인 > 설정 > 알림 > 경보 조건 > 악성코드 감염 알림 > 수신자 선택
- 관리가 조치가 필요한 사용자를 즉시 확인하여 감염 된 PC를 조치 할 수 있습니다.



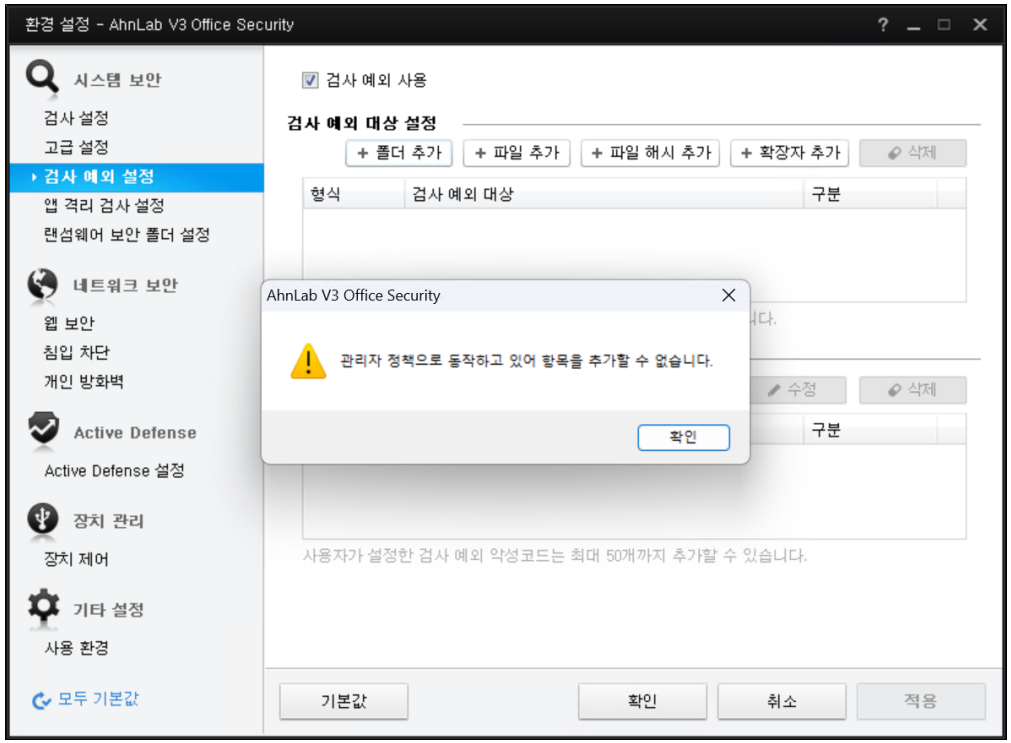
자주하는 질문

Office Security Center 사용 과정에서 발생 할 수 있는 FAQ를 모았습니다.

AhnLab

검사 예외 폴더 추가 시 '관리자 정책으로 동작...'

Q. 사내에서 사용중인 소프트웨어를 검사 예외 추가 하려는데 아래와 같은 알림이 나오고 추가되지 않습니다.

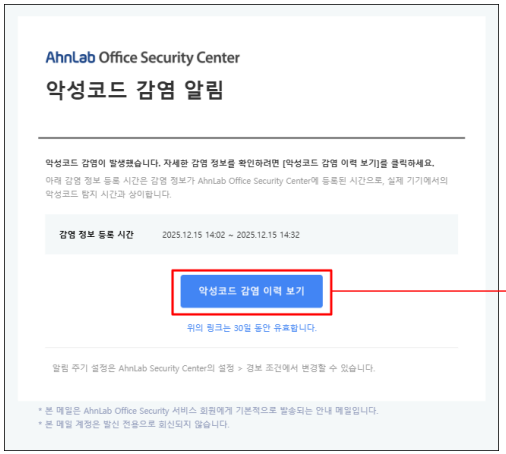


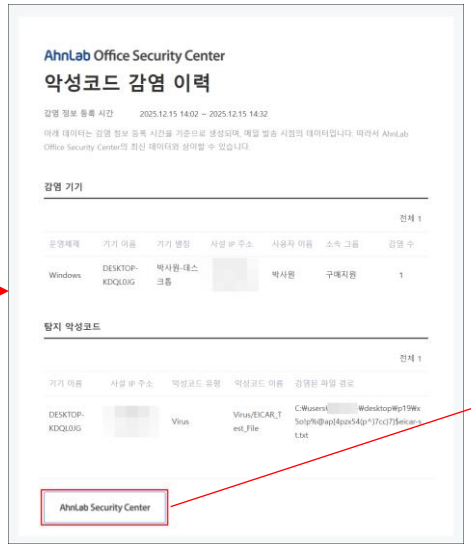
A. 사용자가 직접 검사 예외 대상 설정을 할 수 있도록 허용하려면 정책을 변경해야 합니다.

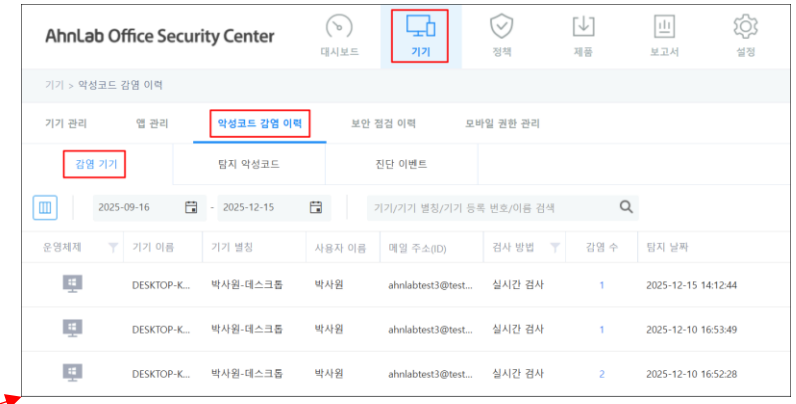
Office Security Center > 정책 > Windows Default 정책 > '사용'을 **[사용자 정의]**로 변경 후 저장하면 사용자가 직접 검사 예외 대상을 직접 추가 할 수 있습니다.

악성코드 감염 알림 메일을 수신했습니다.

Q. 악성코드 감염 알림 메일을 수신했습니다. 조치방법이 궁금합니다.





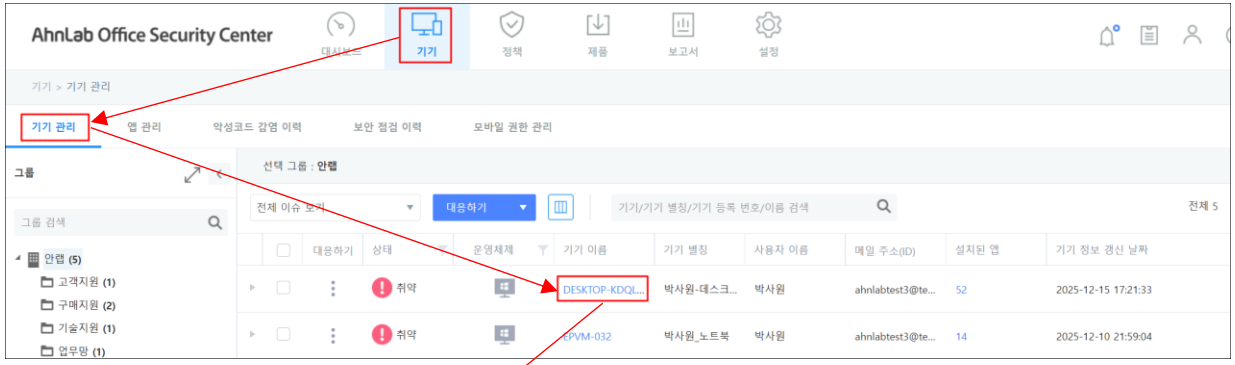


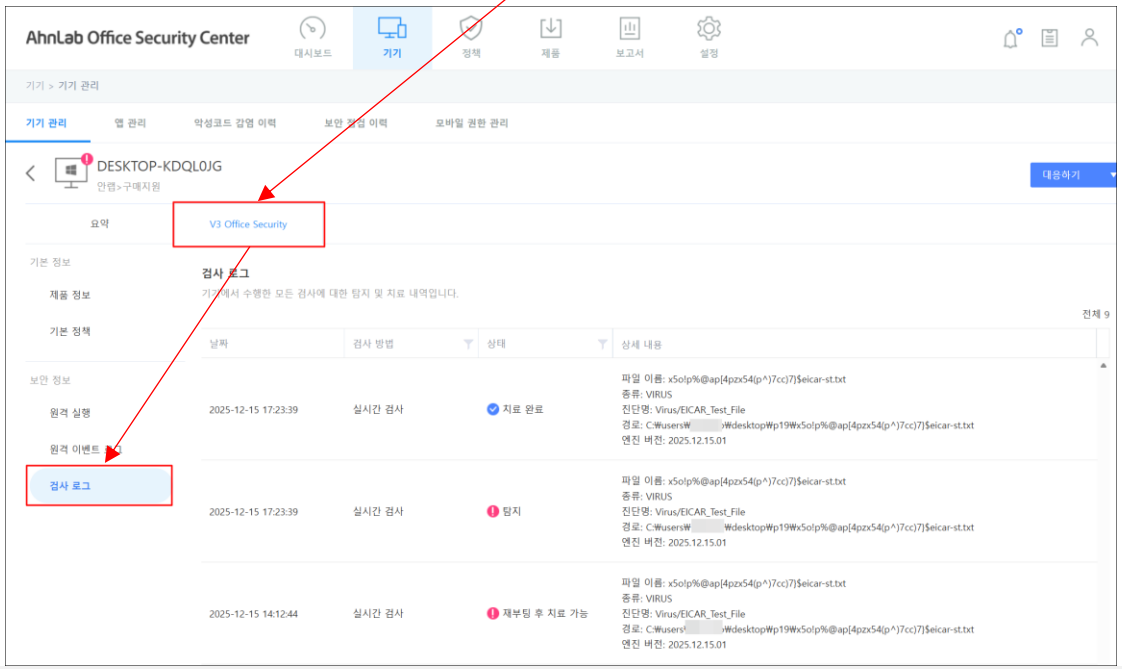
A. 악성코드 감염 알림 수신 시 위와 같은 [악성코드 감염 알림] 메일을 수신하게 됩니다.

- [악성코드 감염 이력 보기]를 통해 감염기기 및 감염 건수 등을 확인 할 수 있습니다.
- [AhnLab Security Center] 링크를 통해 감염이 발생 한 기기의 이름, 사용자 이름, 감염 건 수 등을 확인 할 수 있습니다.
  Office Security Center > 기기 > 악성코드 감염 이력 > 감염 기기 > 메뉴를 통해서도 동일하게 메뉴 이동이 가능합니다.
- 악성코드가 발견 된 기기에서 실제 악성코드가 치료되었는지 확인하려면 다음 페이지를 참고하여 주시기 바랍니다.

악성코드 감염 알림 메일을 수신했습니다.

A. 진단 된 악성코드의 상세 치료 상태 정보가 필요한 경우 아래의 순서로 이동하여 실제 치료 상태를 확인 할 수 있습니다.
Office Security Center 관리자 페이지 > 기기 > 기기 관리 > 감염기기명 클릭 > V3 Office Security > 검사 로그





악성코드 발견 시 검사 방법의 종류에 따라 실시간 검사, 예약검사, 원격 검사 등으로 표시합니다

악성코드가 발견 된 파일에 대해 먼저 **[탐지]** 로그가 남고 이후 해당 파일에 대한 **[치료 완료]** 로그가 하나의 세트로 기록 됩니다.

상태 값 설명 :
[치료 완료]별다른 조치가 필요하지 않습니다.

[재부팅 후 치료 가능] PC를 재부팅 하는 과정에서 바이러스가 치료 됩니다. (PC 재부팅 필요)

결과 확인 시 **동일한 악성코드가 [재감염]**, 또는 **[치료 불가]** 상태인 경우

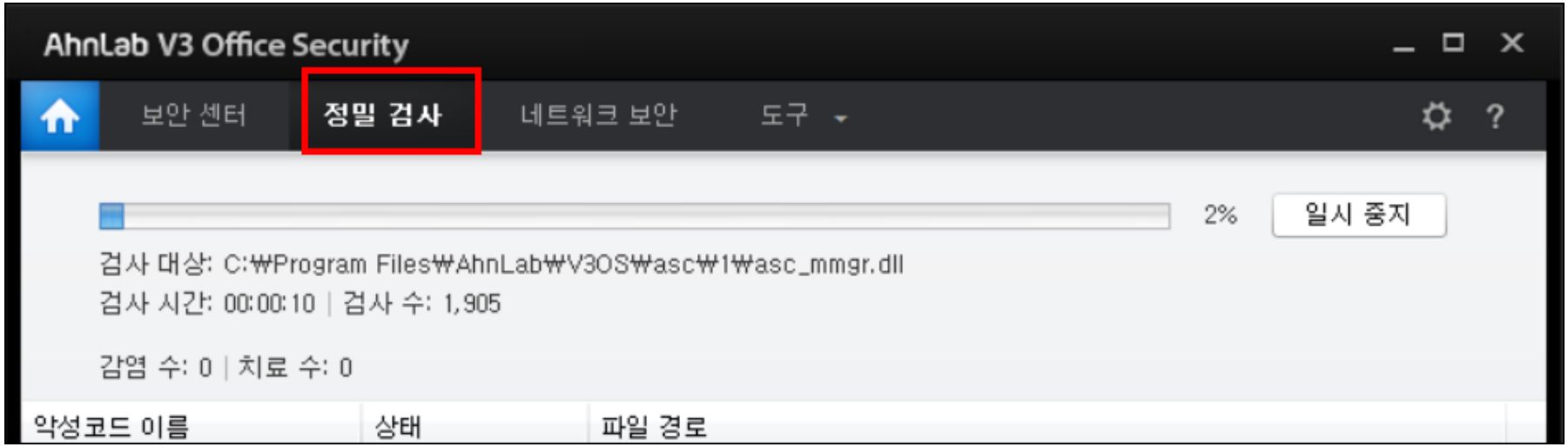
안랩 기술지원센터(1577-9431)로 문의 주셔서 조치 방법을 확인하여 주시기 바랍니다.

제품 최초 설치후 보안 상태가 '취약'으로 표시 됩니다.

Q. V3 Office Security를 신규 설치했는데 기기 목록에 상태가 '취약'으로 표시 됩니다.
어떤 조치를 취해야 하나요?

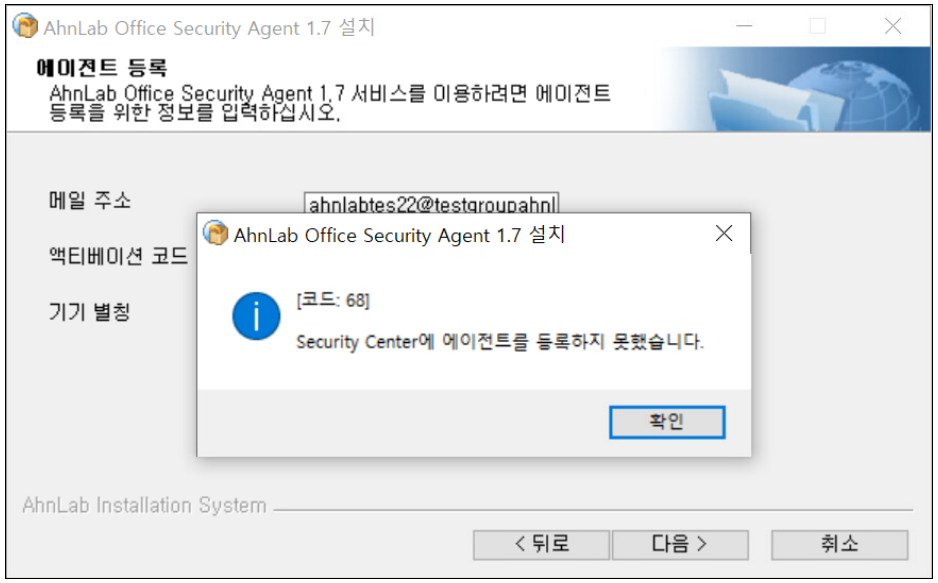
A. V3 Office Security 제품을 최초 설치한 상태는 검사가 진행되기 전 상태입니다.
아직 검사가 진행되지 않은 상태이므로 기기가 안전한 상태인지 확인되지 않은 상태로
'취약' 상태로 분류 됩니다.

V3로 '정밀검사'를 진행 하고 악성코드가 추가로 진단되지 않은 경우 15분 내로 **'안전'**으로 상태가 변경 됩니다.



'코드: 68 Security Center 에이전트 등록실패

Q. '코드: 68 Security Center에 에이전트를 등록하지 못했습니다.' 메시지가 발생하며 인증에 실패합니다.



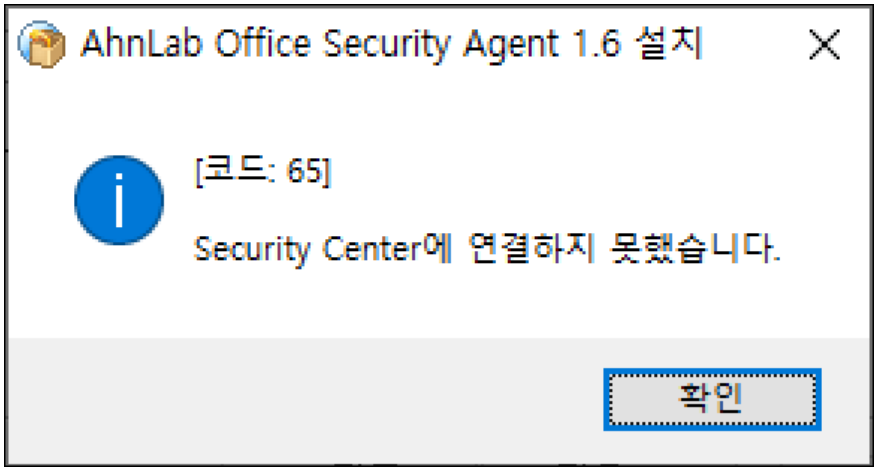
A.

1. 조직도에 등록 된 이메일 주소가 아닌 메일주소를 입력했을 경우 발생 할 수 있습니다.
   입력하신 메일 주소가 조직도에 등록된 이메일 주소인지 확인 합니다.

2. 엑티베이션 코드가 올바르게 입력되었는지 확인합니다.
   액티베이션 확인 방법 :
   1) 액티베이션 코드는 Office Security Center 관리자 페이지 [대시보드] 하단
   2) Office Security Center 관리자 페이지 로그인 > [제품] > [다운로드] 페이지에서 확인할 수 있습니다.

'코드: 65 Security Center에 연결하지 못했습니다.'

Q. '코드: 65 Security Center에 연결하지 못했습니다.' 메시지가 발생하며 설치가 진행되지 않습니다.

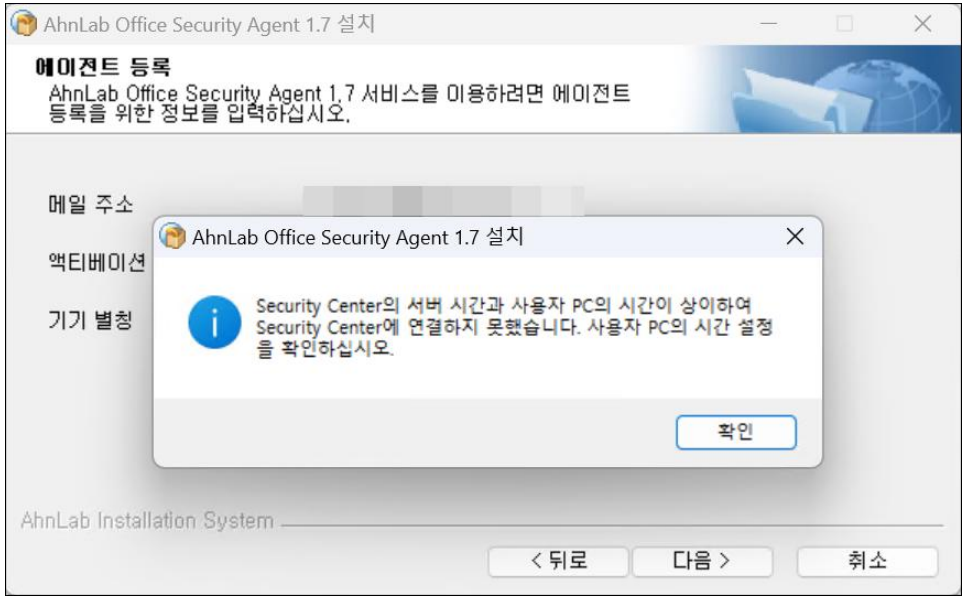


A. 네트워크 문제로 등록에 실패한 경우에 발생 할 수 있습니다.
인터넷 연결이 정상인지 확인이 필요합니다.

방화벽을 사용하여 외부 인터넷이 제한 된 경우 안랩업데이트 서버 목록을 방화벽에 예외처리 합니다.
안랩 업데이트 서버IP 리스트 문서요청 방법 : https://ask.ahnlab.com/hc/ko/articles/4413123350681

서버 시간과 사용자 PC의 시간이 상이 할 경우

Q. Office Security Agent 설치 시 서버 시간과 사용자 PC의 시간이 상이하다고 나옵니다.



A. Agent를 설치하는 PC의 시간이 **실제 시간과 30분 이상 차이가 나는 경우**에 발생합니다.
시스템의 날짜 및 시간이 정상적으로 설정된 상태인지 확인 후 현재 시간으로 변경해주십시오.

참고 링크 : MS 가이드 – 시스템의 날짜 및 시간 설정 방법

More security, More freedom

AhnLab