Office Security Center
기기관리 마스터 : 취약기기 Zero 도전!

기술컨택센터(26.03.13)

AhnLab

Table of Contents

AhnLab

설치파일 배포

01 조직도 등록을 통한 설치파일 배포하기

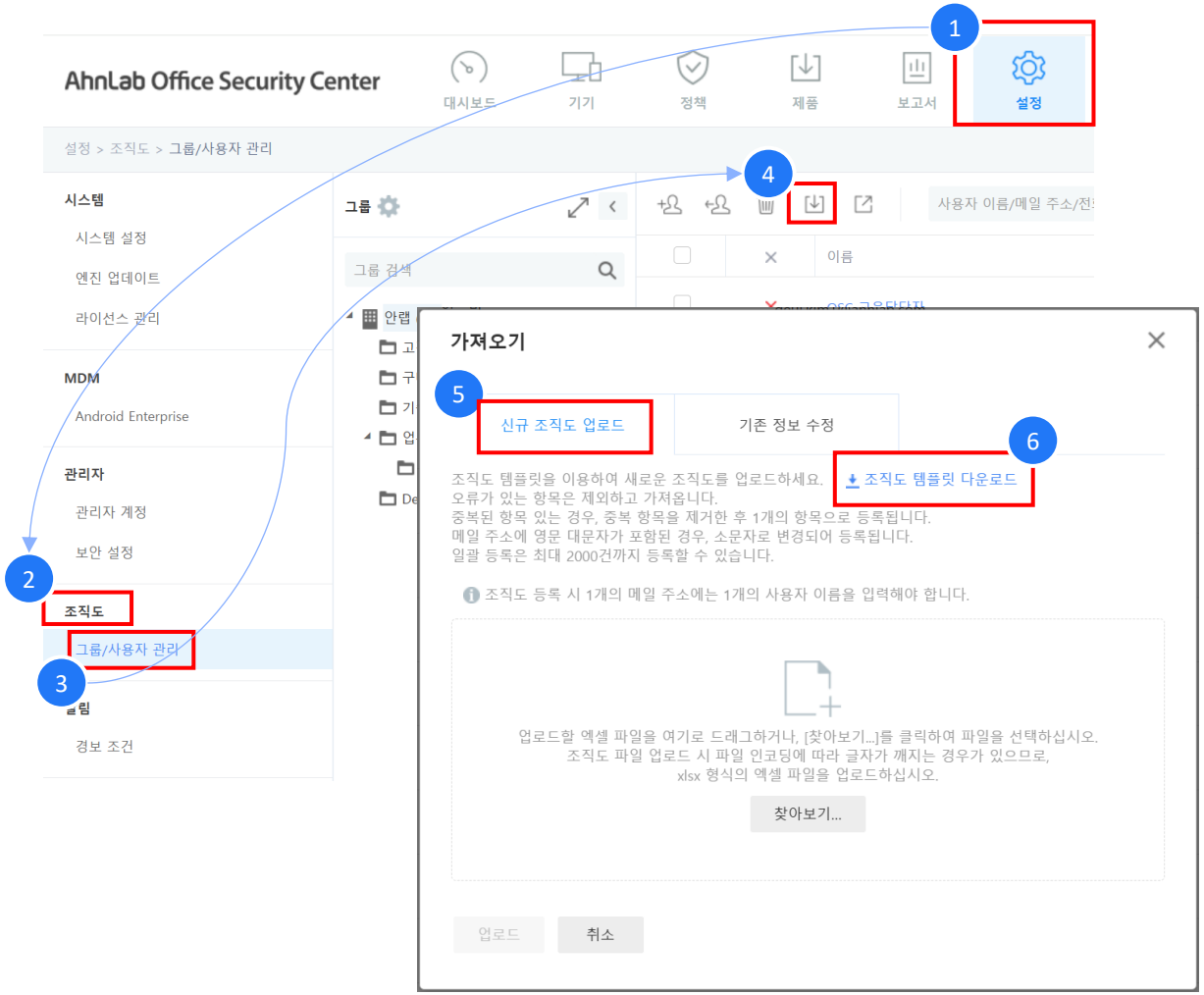
02 설치파일 직접 다운로드 하기

03 Office Security Agent 역할

AhnLab

1. 조직도 템플릿 다운로드 하기

✓ 직원 수가 일정 규모(20명)이상인 경우, 조직도 템플릿을 활용해 일괄 배포 방식이 이후 관리 측면에서 더욱 효율적입니다.
✓ 조직도를 등록하려면 사내에서 사용하는 개별 이메일 주소가 필요합니다.
✓ Office Security Center에 접속하신 후 [설정] 메뉴에서 아래 순서대로 선택하셔서 [조직도 템플릿]을 다운로드합니다.



2. 조직도 템플릿 파일 편집하기

1) 다운로드 받은 [조직도 템플릿] 파일 내용을 고객사 조직에 맞춰 편집합니다.

2) 템플릿 파일에 등록되어 있는 샘플과 같이 사용자 정보를 입력하고 파일을 저장합니다.

(필수 입력정보 : **이름, 메일주소**는 반드시 입력되어야 합니다)

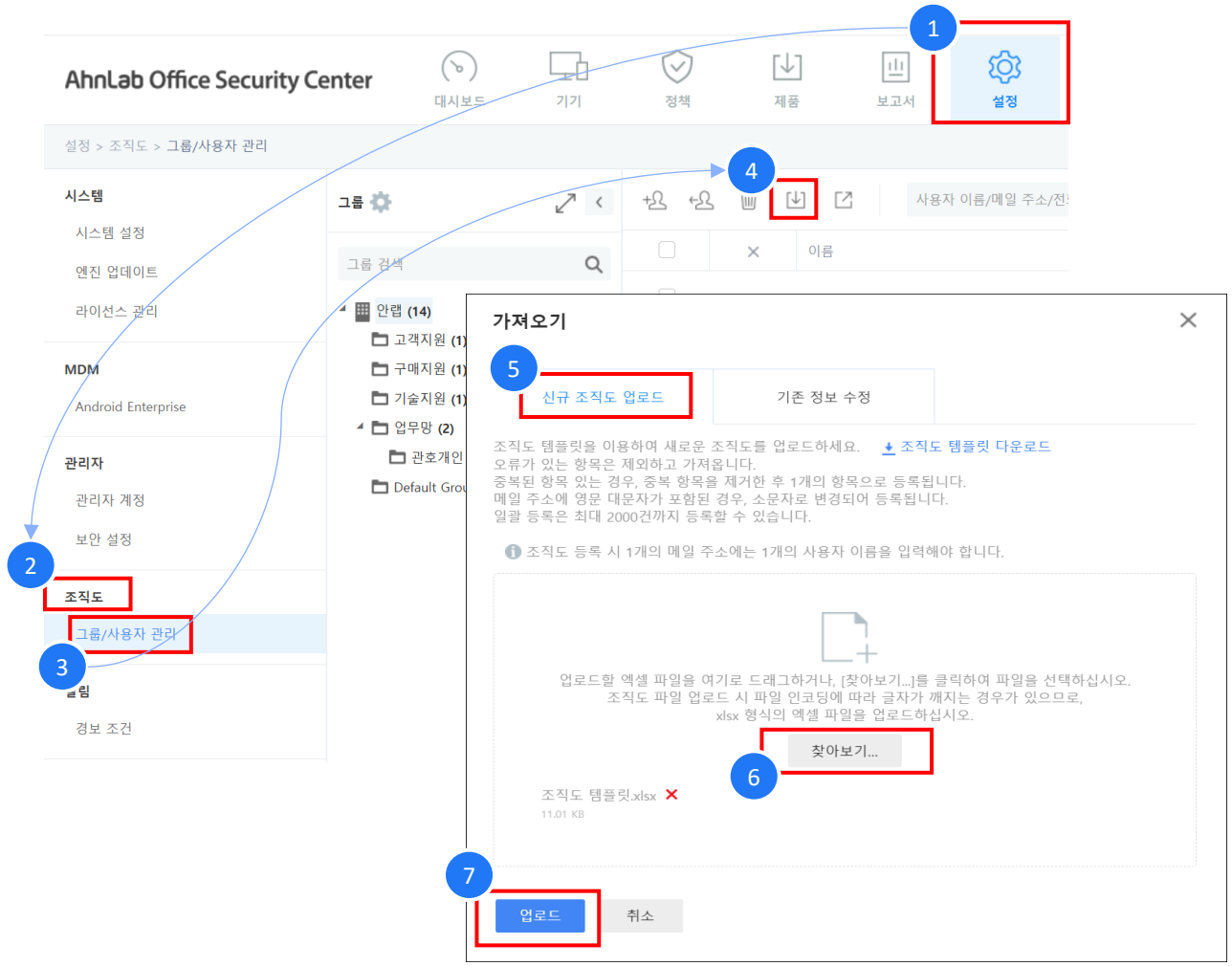
	A	B	C	D	E	F	G	H
1	** 조직도 템플릿 가이드 (본 가이드 내용을 삭제하지 마십시오.)							
2	1. 대상 목록 일괄 등록 시 한 번에 최대 2,000개 단위로 추가 업로드할 수 있습니다.							
3	2. 관리자 권한과 관리 대상은 대소문자 구분없이 영문 입력 문구 일치 시에만 적용됩니다.							
4	3. 관리자로 등록 시 대상자에게 계정 정보가 메일로 발송됩니다.							
5	4. 조직도 템플릿은 관리자 신규 추가만 가능합니다. 기존 관리자 정보를 변경하려면 사용자 정보 파일을 이용하십시오.							
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 주소는 사용자를 식별하는 고유 정보이므로, 하나의 이메일을 여러 사용자에게 중복 입력하는 것은 불가능합니다.
- ✓ 메일 주소에 대문자가 포함되어 있으면 자동으로 소문자로 변환되어 등록됩니다.
- ✓ 관리자 권한이 필요하지 않은 사용자의 칸은 비워두시기 바랍니다.

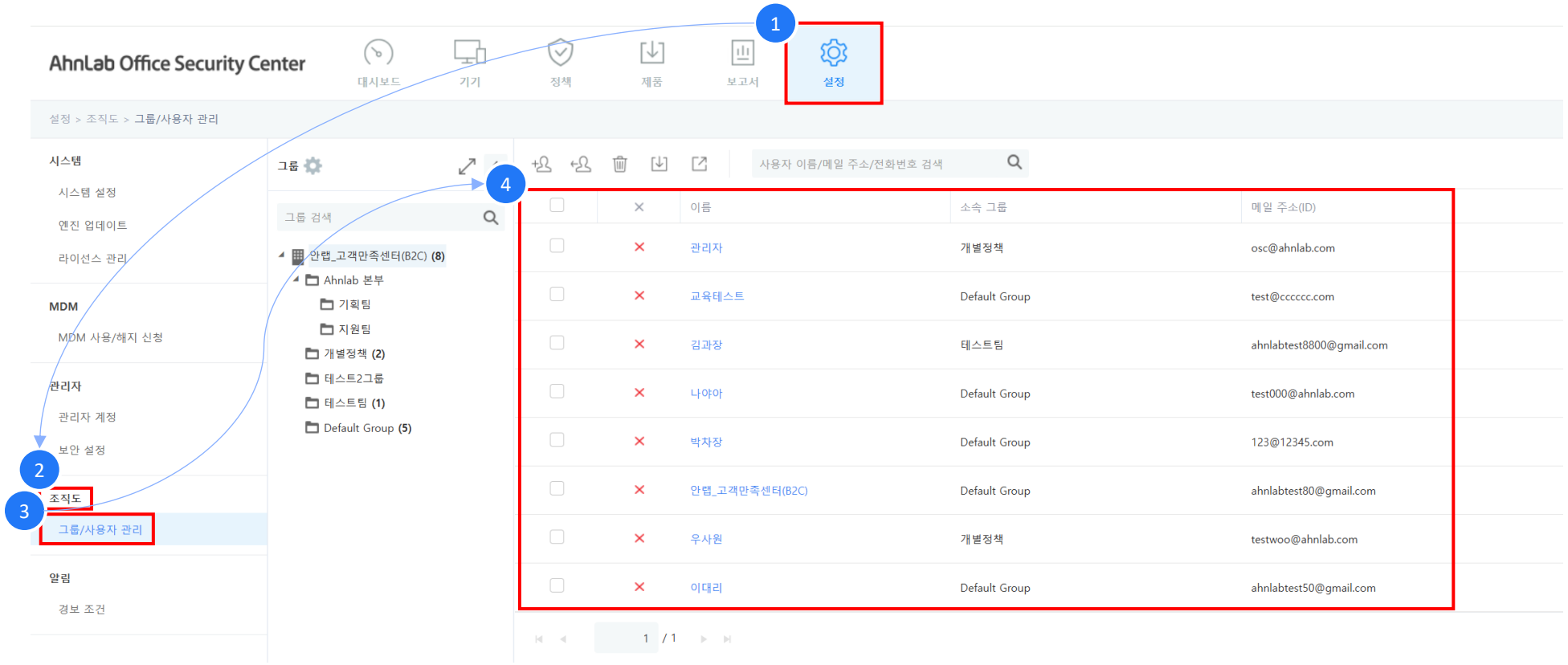
3. [조직도 템플릿] 파일 업로드 하기

✓ 편집이 완료된 조직도 템플릿 파일은 [설정]메뉴에서 아래 순서대로 선택하셔서 파일을 업로드 합니다.



4. 조직도 등록 결과 확인

✓ 템플릿으로 사용자 등록을 완료하면 입력한 그룹명, 이름, 이메일 주소, 전화번호, 내선, 사번 등이 시스템에 함께 등록됩니다.
✓ 그룹명을 입력하지 않은 경우, 소속 그룹은 Default Group으로 자동 등록 됩니다.
✓ [설정]메뉴에서 아래 순서대로 선택하셔서 조직도에 등록된 사용자 정보를 확인합니다.

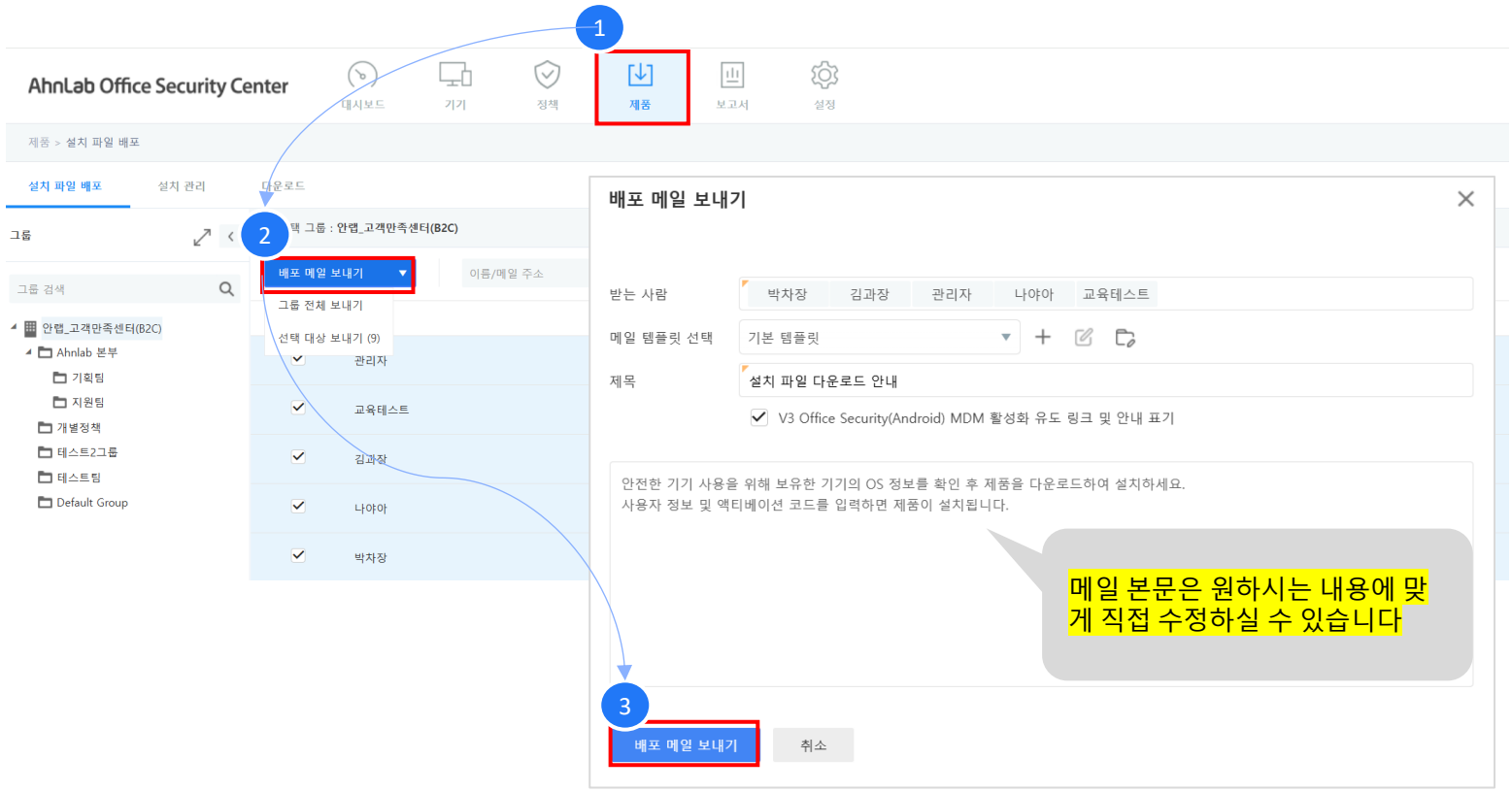


5. 설치파일 메일로 배포하기

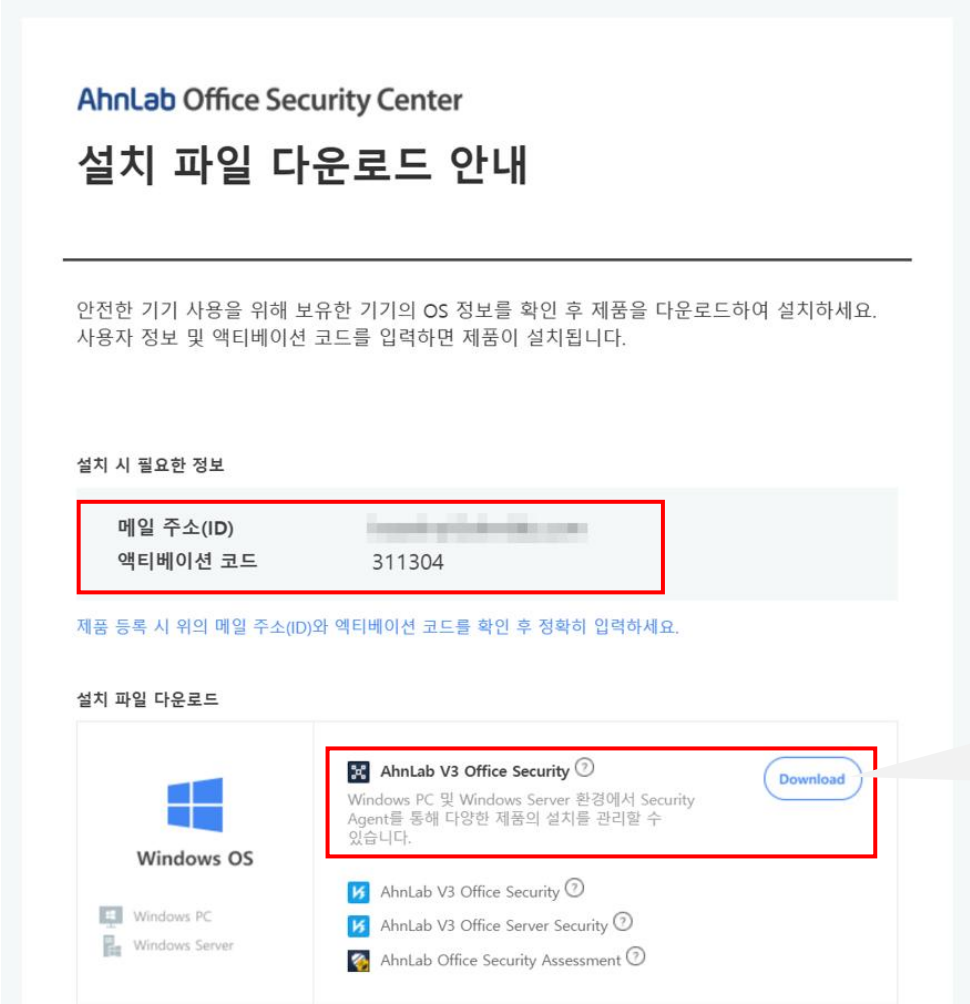
✓ 조직도에 등록된 사용자에게 Office Security Agent 다운로드 링크가 포함된 배포 메일을 발송하는 절차입니다.
✓ 아래 순서대로 제품에서 배포메일 보내기를 클릭하여 설치파일을 배포합니다.

① 설치파일을 배포하는 대상에 맞게 [그룹 전체 보내기] or [선택대상 보내기]를 선택합니다.
② [그룹 전체 보내기]를 선택 할 경우 조직도에 등록 된 모든 사용자에게 배포메일이 발송 됩니다.

✓ 설치파일 배포메일에는 보유 중인 모든 제품의 설치파일 다운로드 링크가 제공됩니다.



6. 사용자가 받게 되는 Office Security 설치 안내 메일



- ✓ 설치 안내 메일에는 수신자의 이메일 주소, 액티베이션 코드, 그리고 Office Security Agent 다운로드 링크가 포함됩니다.
- ✓ 해당 메일의 다운로드 링크는 기간제한 없이 언제나 접속해서 다운로드가 가능합니다.

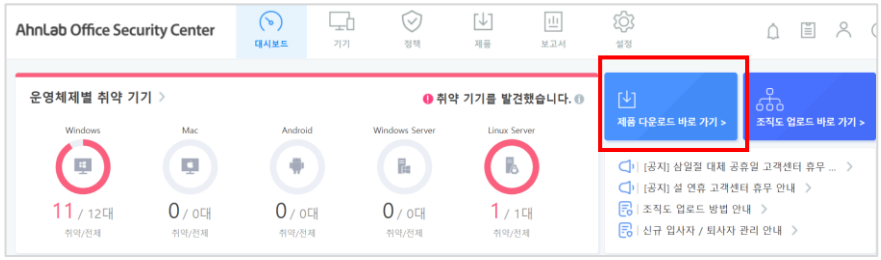
사용자는 [Download] 버튼을 클릭하여 Office Security Agent 파일을 내려받아 V3 제품을 설치할 수 있습니다.

관리자가 직접 설치파일을 다운로드하여 설치하는 방법

✓ 소규모 회사 또는 사내 이메일 미사용 시 관리자가 직접 설치파일을 내려받아 사내 PC에 설치할 수 있습니다.

- 관리자가 파일을 직접 다운로드 후 사내 공유(USB, 사내 게시판에 게시, 메일에 첨부하여 전달 등)
- 관리자가 사용자 PC에서 직접 Office Security Center에 로그인하여 설치파일 다운로드

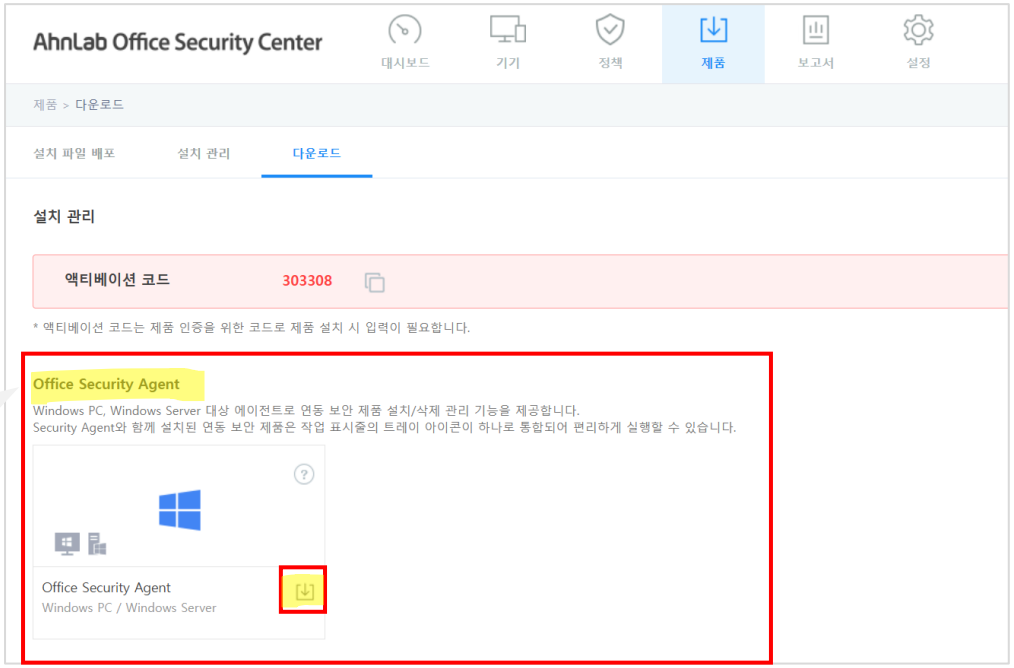
1) 대시보드 화면에서 다운로드 페이지로 바로 이동



✓ Office Security Agent 파일을 직접 다운로드하여 액티베이션 코드와 관리자 이메일 주소를 입력하여 설치를 진행합니다.

✓ 동일한 관리자 이메일로 여러 PC를 설치하는 경우, 설치 과정에서 기기 별칭을 입력하면 각 기기를 쉽게 구분하여 관리할 수 있습니다.

2) Office Security Agent 설치 파일 다운로드하기



Office Security Agent 역할

✓ Office Security Center(OSC)를 통해 사내 PC의 보안관리를 위해서는 Office Security Agent 를 꼭 설치해야 합니다.

✓ Agent는 PC와 Office Security Center 사이에서 정보를 연동하는 프로그램으로, Office Security Center의 관리 명령을 단말의 V3에 전달하고, 단말 V3의 정보를 다시 Office Security Center 로 보내는 통신 역할을 수행합니다.

✓ 작업표시줄 트레이 영역에 표시되는 Office Security Agent 아이콘 : 

✓ 참고로, Office Security Agent는 Windows PC와 Windows Server 환경만 지원하며, macOS와 Linux Server는 지원하지 않습니다.

사용자 PC의 운영체제에 맞는 V3 제품을 다운로드 및 설치하는 역할	• 자동으로 OS에 맞는 설치파일 다운로드 및 설치
Office Security Center에서 설정한 정책 및 원격 관리 명령을 V3에 전달하는 역할	• 원격 검사, 원격 업데이트의 명령 전달 • '기기 별칭' 정보를 PC로 전달하여 기기 관리 기능 제공
Office Security Agent가 설치된 PC의 정보 및 에이전트 로그를 OSC 서버로 전송하는 역할	• V3 진단 데이터를 서버로 전송 • PC의 앱 정보를 서버로 전송

- **OSC와 기기 내 Agent와의 정기적인 통신 주기**
  - 제품 라이선스/정책 주기 체크 : 120분
  - 기기 전송/원격 명령 주기 체크 : 15분
- **PC에서 OSC 명령을 확인하는 기준 : PC 부팅 이후(V3 서비스 시작 시점 기준)**
  - 원격 명령 실행 : 10분 이후
  - 정책 확인 : 10분 후 정책 체크 및 라이선스 인증 수행
  - V3 정보 전송 : 15분 후 V3 상태 및 기기정보 전송
- **PC가 꺼져 있는 상태에서 원격 검사 수행 주기**
  - 원격 명령은 24시간동안 유효
  - 그 사이 PC가 부팅되면 원격 명령을 수신
  - 24시간 이상 꺼져 있거나 네트워크 연결 문제로 24시간 경과 시 원격 명령은 수행되지 않음

Office Security Agent 역할

✓ Office Security Agent 설치 여부에 따른 기능 비교표

구분	설치됨	미 설치 (미 설치 환경)
OS별 V3 자동 설치 (Windows만 지원)	제공됨	제공되지 않음 (직접 다운로드 및 설치)
원격명령으로 제품 설치/제거	제공됨	제공되지 않음
설치된 앱 목록 조회	제공됨	제공되지 않음
기기 별칭 입력	제공됨	제공되지 않음 (기기 관리 수동 설정 가능)
업데이트·검사 명령 원격 실행	제공됨	제공됨
기기 등록해제	제공됨	제공됨
기기 상태 모니터링	제공됨	제공됨

상황별 기기 관리 방법

01 중복 라이선스가 발생된 경우

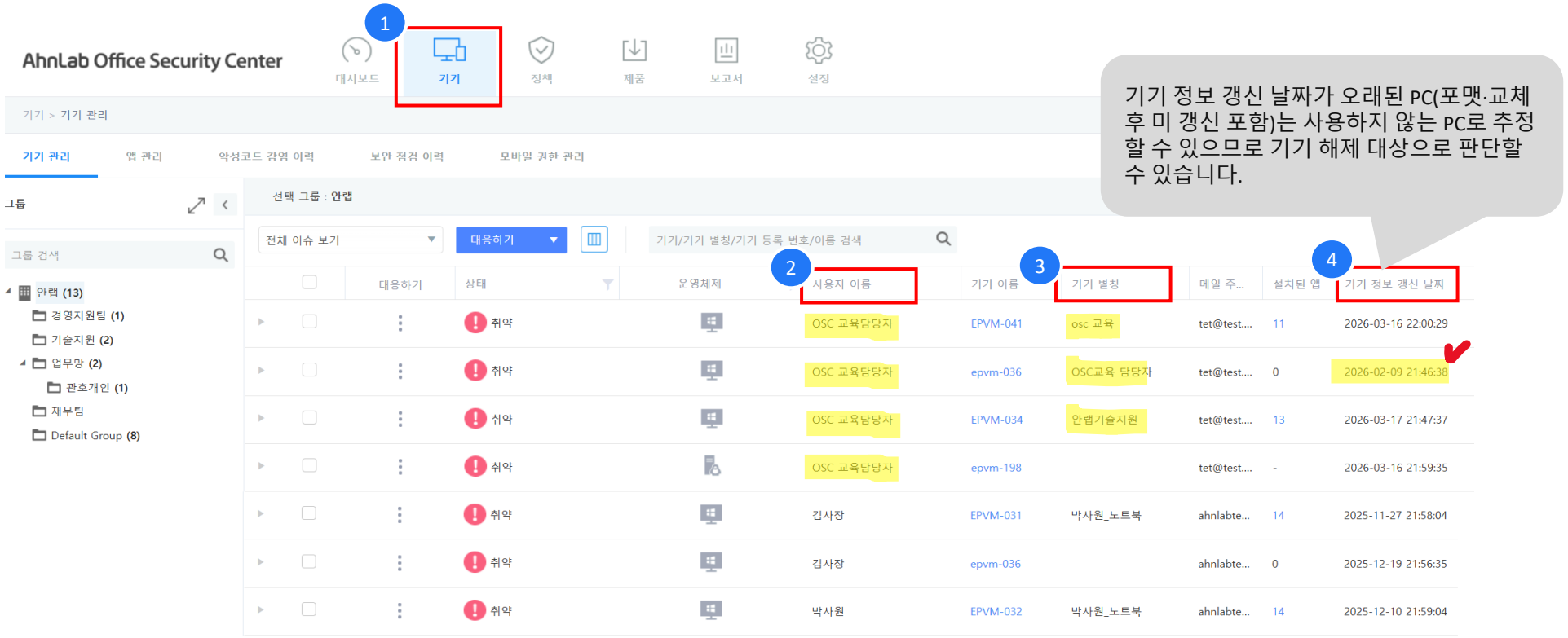
02 PC 사용자가 변경된 경우

03 PC 사용자 구분이 필요한 경우

AhnLab

1. 중복으로 등록된 기기 여부에 대한 정기적인 확인과 기기 해제조치

✓ PC 포맷 후 V3 Office Security를 재설치 할 경우 기존 설치정보를 삭제(기기 해제)하지 않으면 한 대의 PC에 라이선스는 2개를 사용하는 개념 - 중복 기기가 발생하게 됩니다.
✓ 라이선스 잔여수량 관리를 위해서는 정기적으로 중복 기기가 발생하는지 여부를 확인해서 정리하시길 권해드립니다.



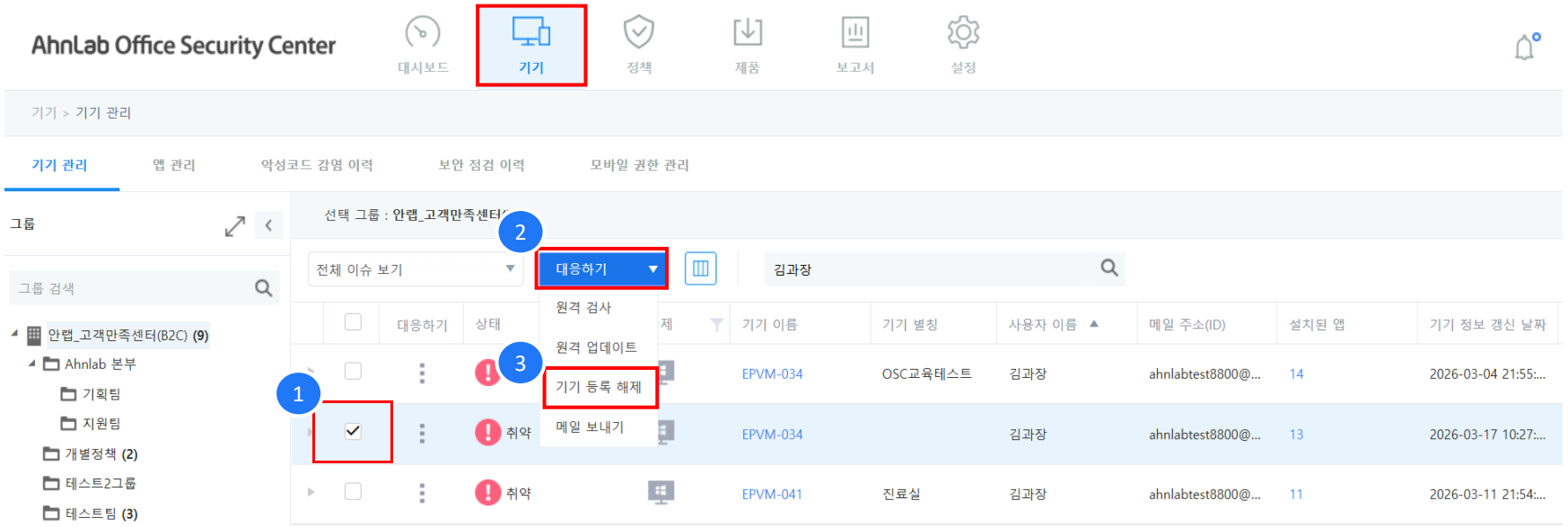
① 사용자 이름 기준으로 정렬 : 동일 이름으로 2개 이상 리스트가 나오는지 확인

② 기기별칭, 기기 정보 갱신 날짜의 정보 비교 :
- 별칭이 각각 다른 경우 : 한 사람이 여러대 PC를 사용하는 경우일 수 있음
- 기기 정보 갱신 날짜 비교 : 비 상식적으로 갱신 날짜가 오래된 기기는 포맷 전 PC 정보이거나 네트워크 연결 등 문제로 인해 정상 통신이 안되는 PC일 수 있음.
  - 중복기기 관점 및 정상 사용여부 관점에서 해당 사용자에게 확인 필요

③ 중복으로 판단되는 기기 : 기기 등록 해제 조치로 라이선스 최신화

2. 중복 기기 등록 해제 하기

✓ 중복 기기로 확인된 경우에는 아래 순서에 따라 기기 등록 해제를 진행합니다.

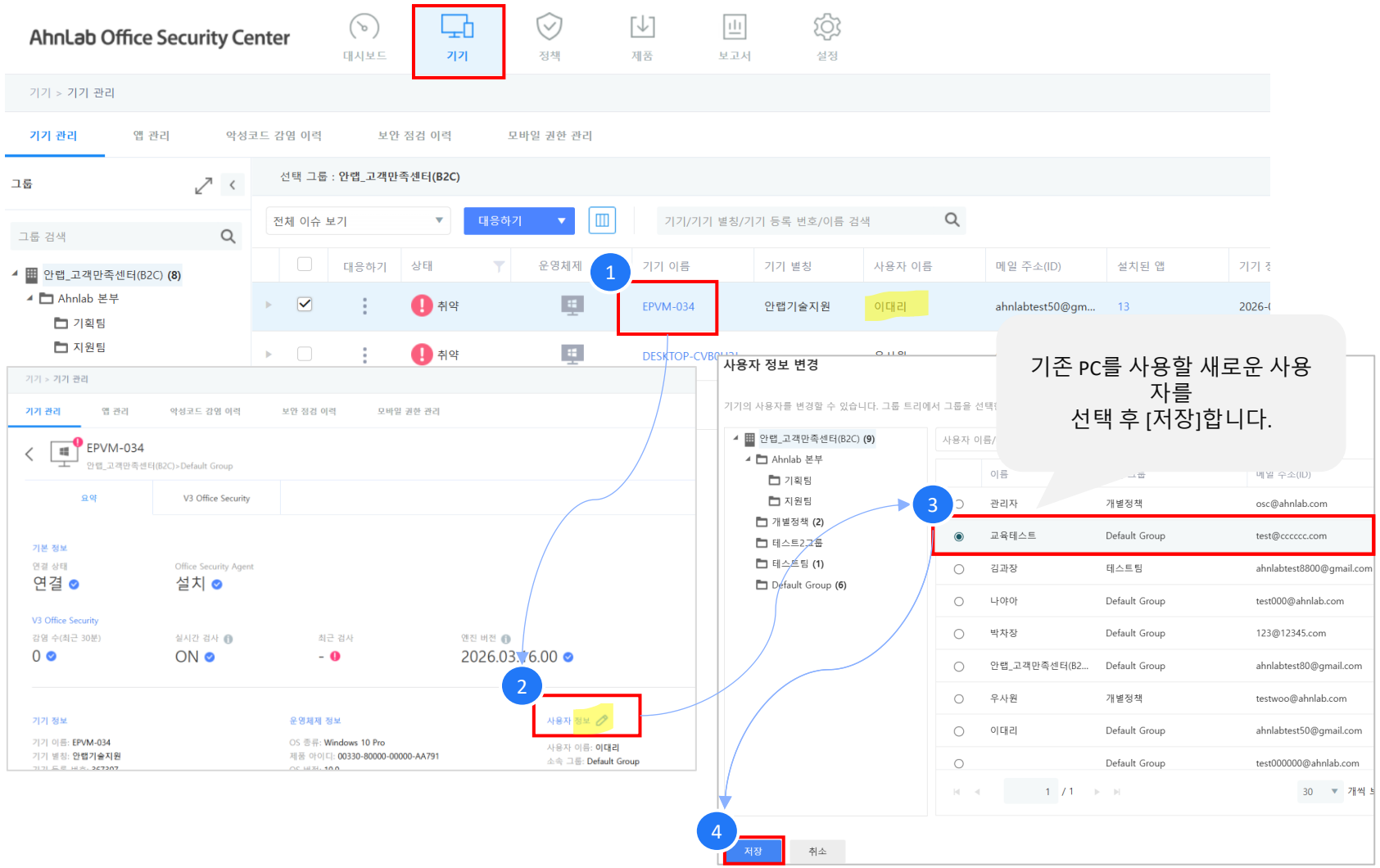


✓ 사용중인 PC를 [기기 등록 해제]할 경우 V3 Office Security 제품 사용이 중지됩니다.

✓ 따라서 중복 여부가 불명확한 경우에는 해당 사용자에게 직접 확인하여 미사용 PC에 한해서만 [기기 등록 해제]를 적용하는 것이 중요합니다.

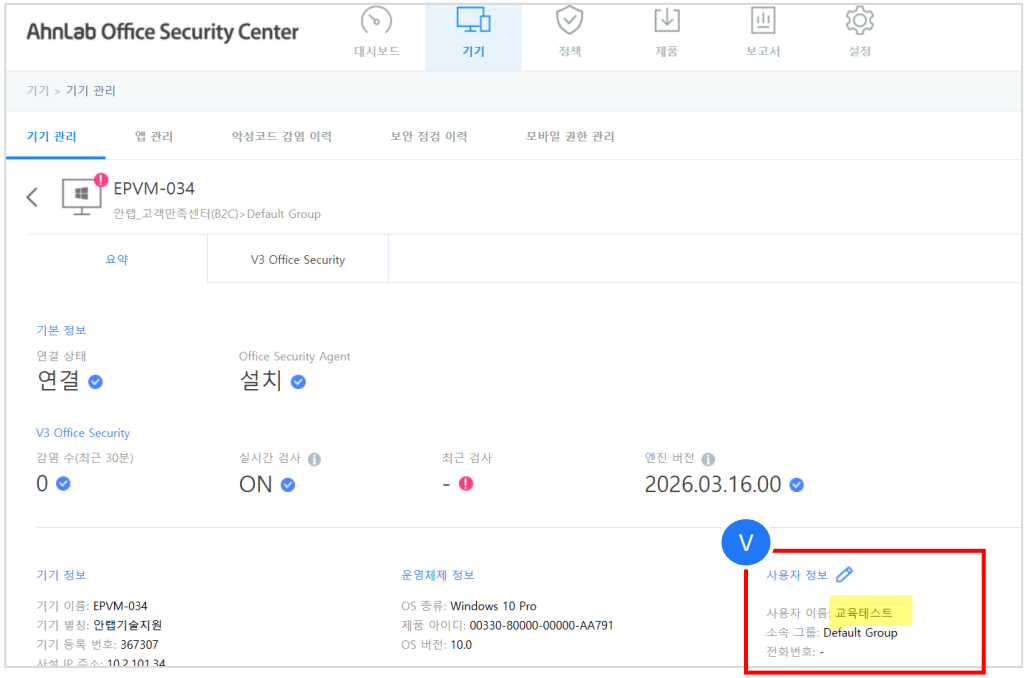
1. 기기의 사용자 정보 변경하기

✓ 퇴사자의 PC를 신규 입사자가 포맷없이 그대로 받아서 사용하는 경우 : 기기의 사용자 정보만 변경합니다. 이때 신규 입사자에 대해서는 설정 > 그룹/사용자 관리 메뉴에서 사용자 추가를 먼저 해놓습니다.
✓ 기타 이유로 A 직원의 PC를 포맷없이 B직원이 받아서 사용하는 경우 : 기기의 사용자 정보만 변경합니다.
✓ 기기의 사용자 정보를 변경하는 순서는 아래와 같습니다.

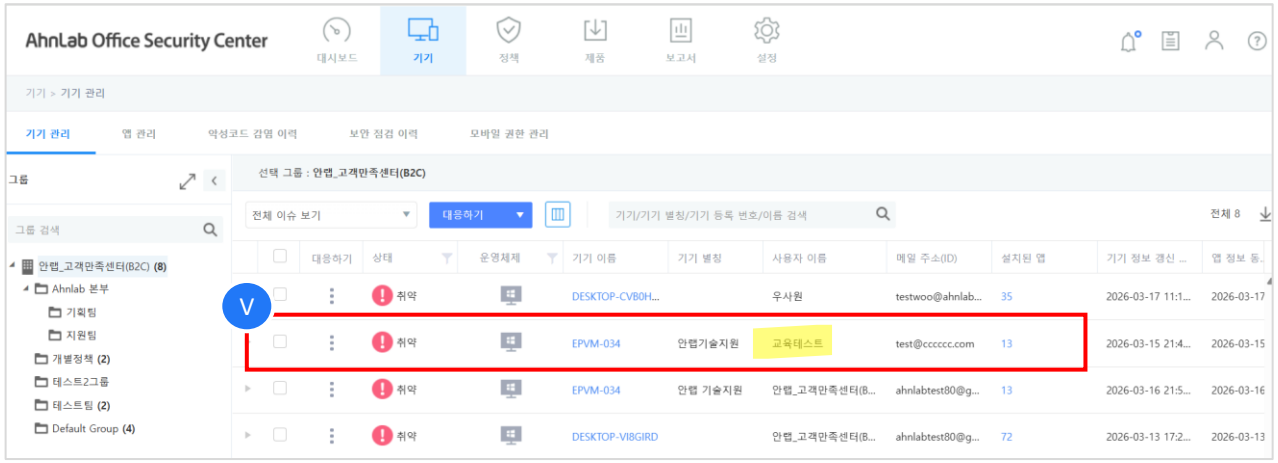


2. 기기의 사용자 정보 변경 결과 확인하기

✓ 사용자 정보가 정상적으로 변경되었는지 확인합니다.

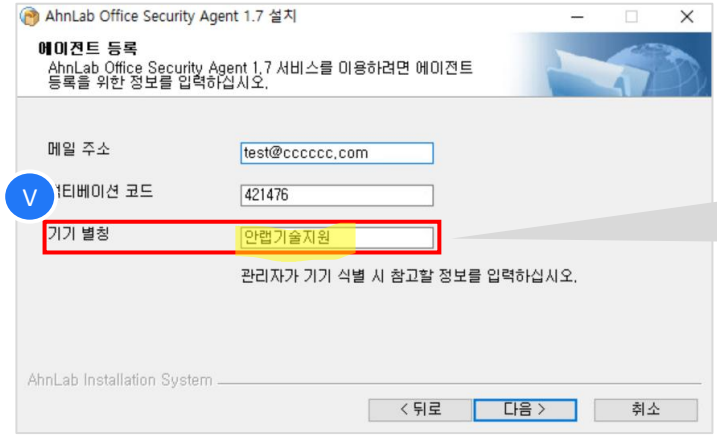


사용자 정보 변경이 아닌 실제 퇴사자가 발생한 경우에는,
P14 페이지의 '중복 기기 등록 해제하기'를 참고하여 해당 기기를 해제하고 라이선스를 회수해 주시기 바랍니다.

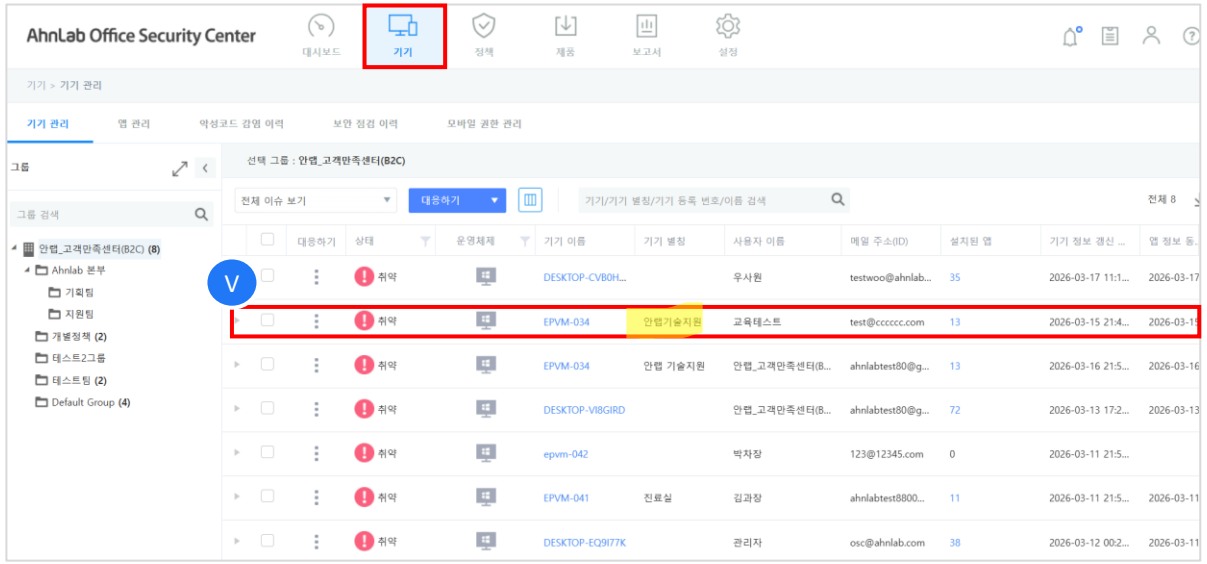


1. 기기 별칭 메뉴를 통해 PC 사용자 구분하기

✓ 동일한 사용자 정보(예: 동일 이메일)로 여러 PC에 Agent를 설치하면, 사용자 이름만으로는 각 PC를 구분하기 어렵습니다. 이런 경우에는 기기 별칭을 사용하면 쉽게 구분하실 수 있습니다.
✓ 이미 등록된 기기라도 Office Security Center 기기 관리 화면에서 언제든지 별칭을 추가하거나 수정할 수 있습니다.
✓ Agent 설치 과정에서 기기 별칭을 입력하면, Office Security Center 기기관리에서 해당 PC의 별칭을 확인할 수 있습니다.

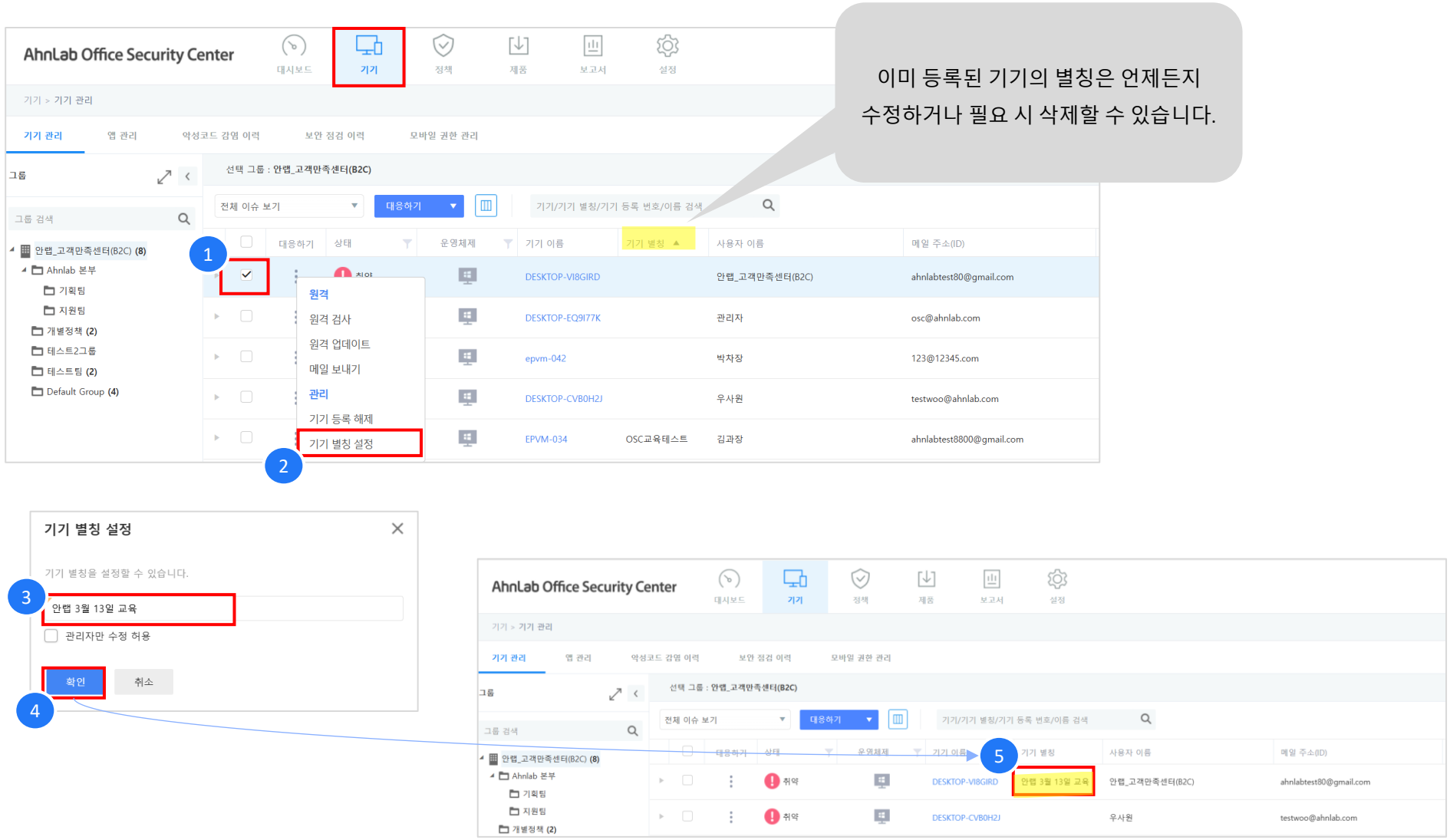


설치 과정에서 기기 별칭을 입력하지 못했더라도,
관리자가 OSC > 기기 관리 화면에서
언제든지 별칭을 추가하거나 수정할 수 있습니다.



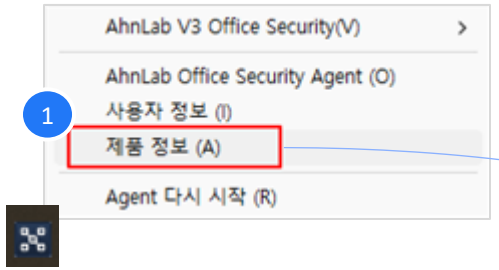
2. V3 Office Security 기기 별칭 설정 방법

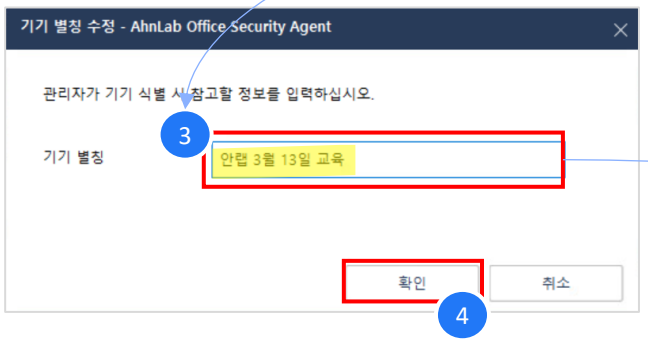
✓ 기기 별칭 설정은 아래 순서에 따라 설정하실 수 있습니다.

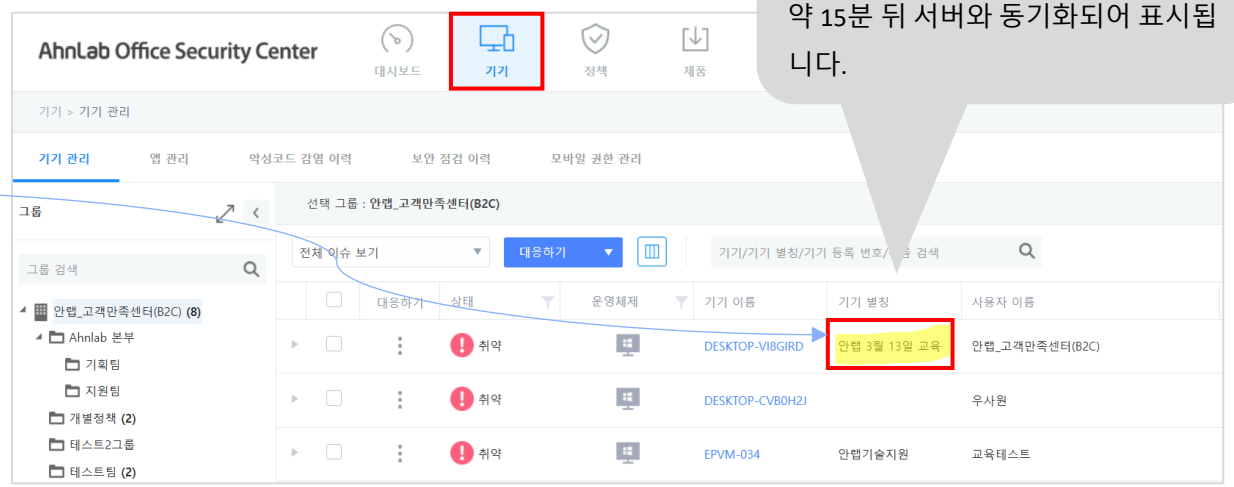


3. Office Security Agent 제품정보에서 기기 별칭 설정하기

✓ PC 사용자가 직접 기기 별칭 등록 가능 : 트레이에 있는 Office Security Agent 아이콘을 이용해 기기 별칭을 등록하거나 수정할 수 있습니다.



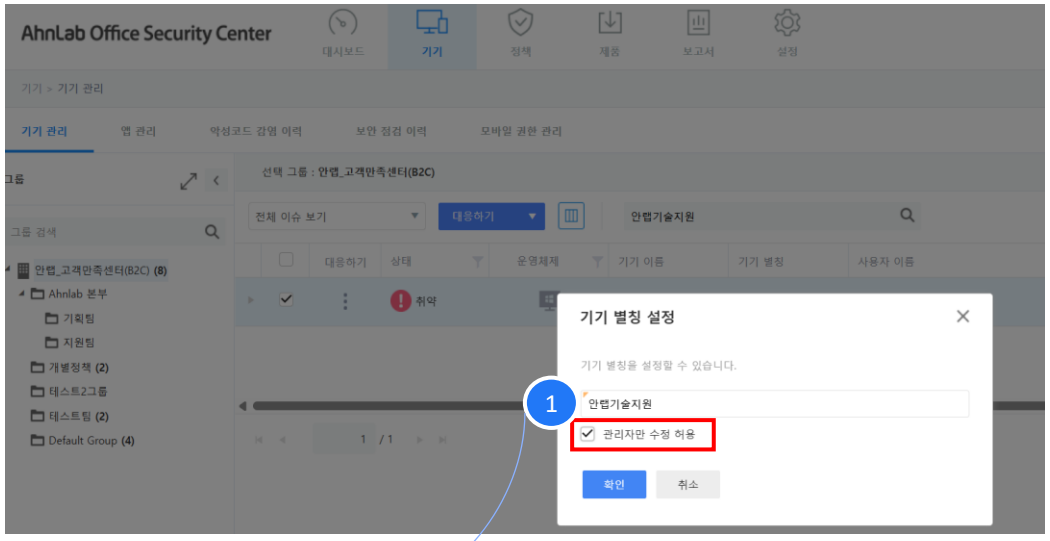




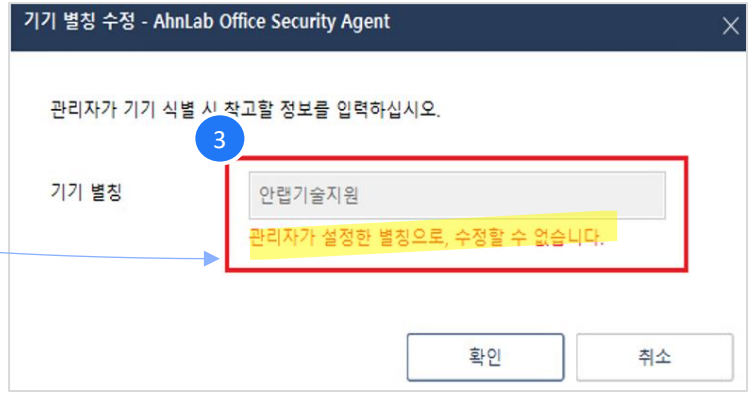
Office Security Agent는 15분 주기로 서버와 통신하므로, 기기 정보 변경 시 약 15분 뒤 서버와 동기화되어 표시됩니다.

4. 기기 별칭 설정에 대한 권한 제어 가능

✓ [관리자만 수정 허용]을 체크하면, 기기 별칭은 PC 사용자가 변경할 수 없으며 관리자만 수정 가능합니다.



Office Security Agent는 15분 간격으로 서버와 동기화 되므로, '관리자만 수정 허용' 설정은 최소 15분 ~ 최대 30분 이내에 사용자 PC에 반영됩니다.



취약 기기 파악 및 대응 가이드

AhnLab

취약 기기 판단 항목과 기준

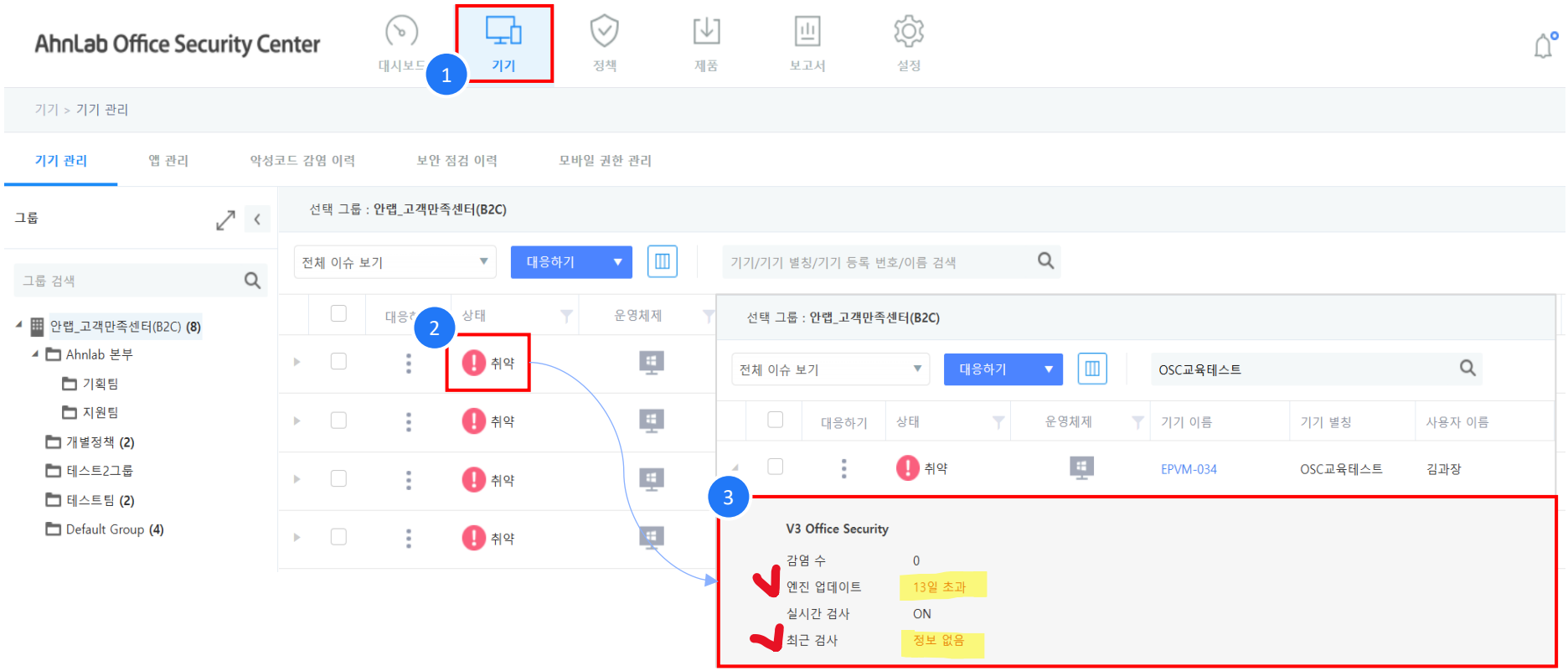
✓ 사내 PC에 대한 보안관리 포인트를 기준으로 취약한 기기를 구별해서 관리할 수 있습니다.
✓ 취약 기기를 구별하는 항목 및 취약에 대한 판단 기준은 다음과 같습니다.

1) 감염 수 : 최근 30분 이내 악성코드 감염(진단) 이벤트가 발생한 경우

2) 엔진 업데이트 : 최신 엔진이 7일 이상 업데이트되지 않은 경우

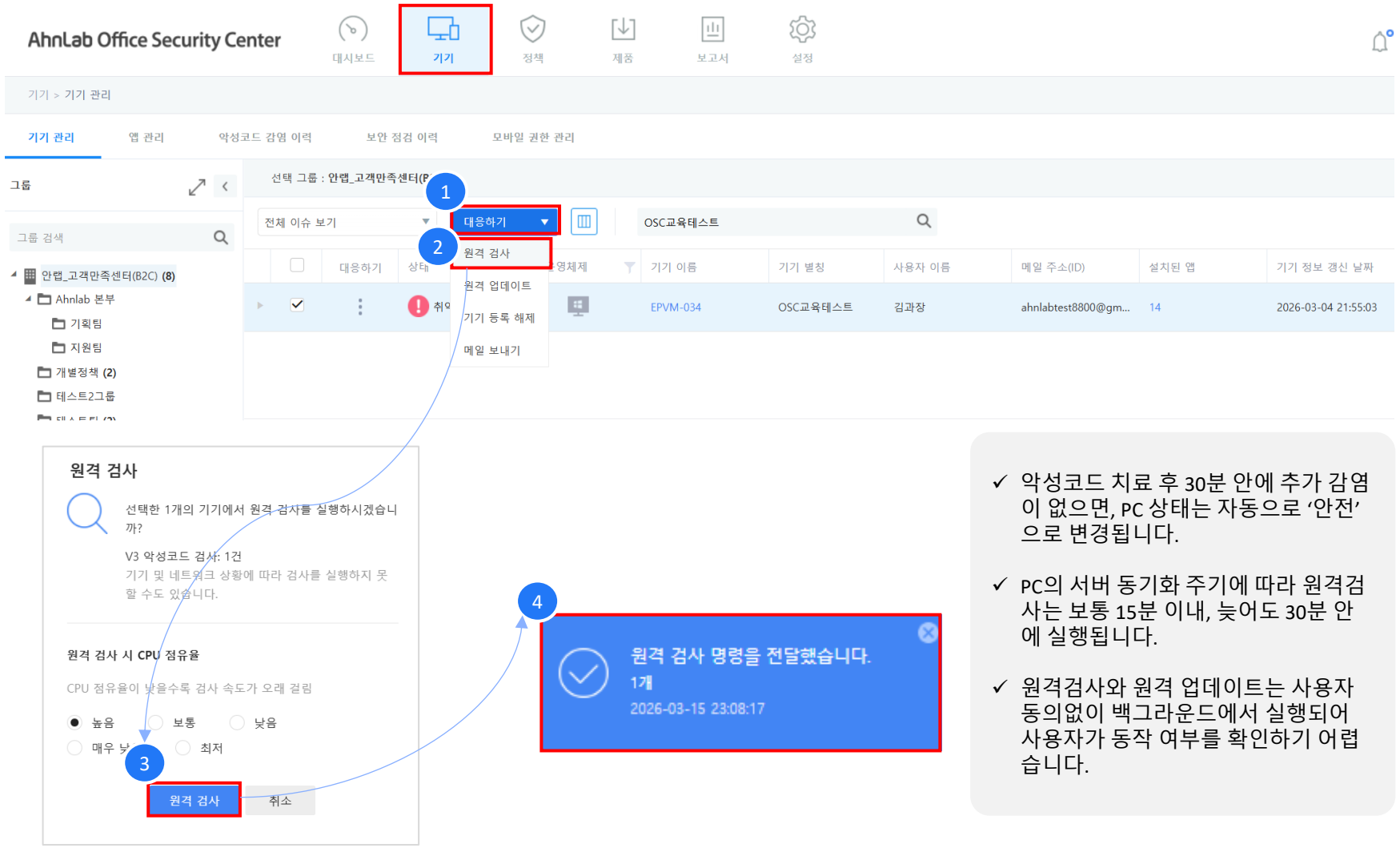
3) 실시간 검사 : 실시간 검사 기능이 OFF(비활성화) 상태인 경우

4) 최근 검사 : 바이러스(수동) 검사가 7일 이상 실행되지 않았거나, V3 최초 설치 후 한 번도 검사를 실행한 적이 없는 경우



1. 최근 30분 이내 악성코드 감염기록이 탐지된 경우

✓ 감염수가 표시된 경우는 실제 사용자 PC에서 악성코드가 진단되었음을 의미합니다.
✓ 최근 30분 이내에 악성코드를 탐지하거나 치료한 기록이 있으면, Office Security Center에서는 해당 PC를 '취약' 상태로 표시합니다.
✓ 기기 관리에서 감염된 기기로 표시된 PC가 있다면, 원격검사 기능을 사용해 즉시 검사 명령을 전달하시기 바랍니다.



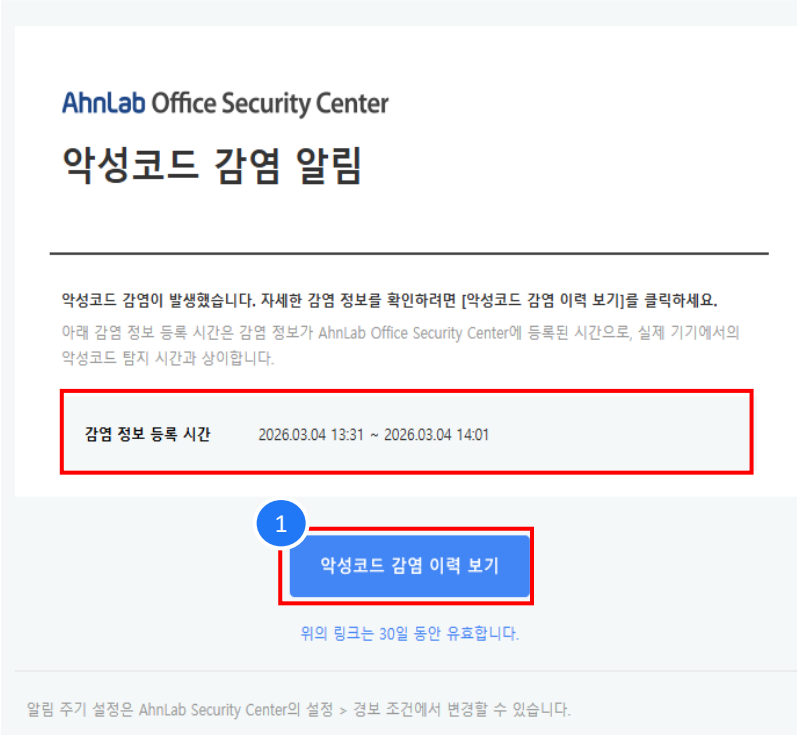
✓ 악성코드 치료 후 30분 안에 추가 감염이 없으면, PC 상태는 자동으로 '안전'으로 변경됩니다.

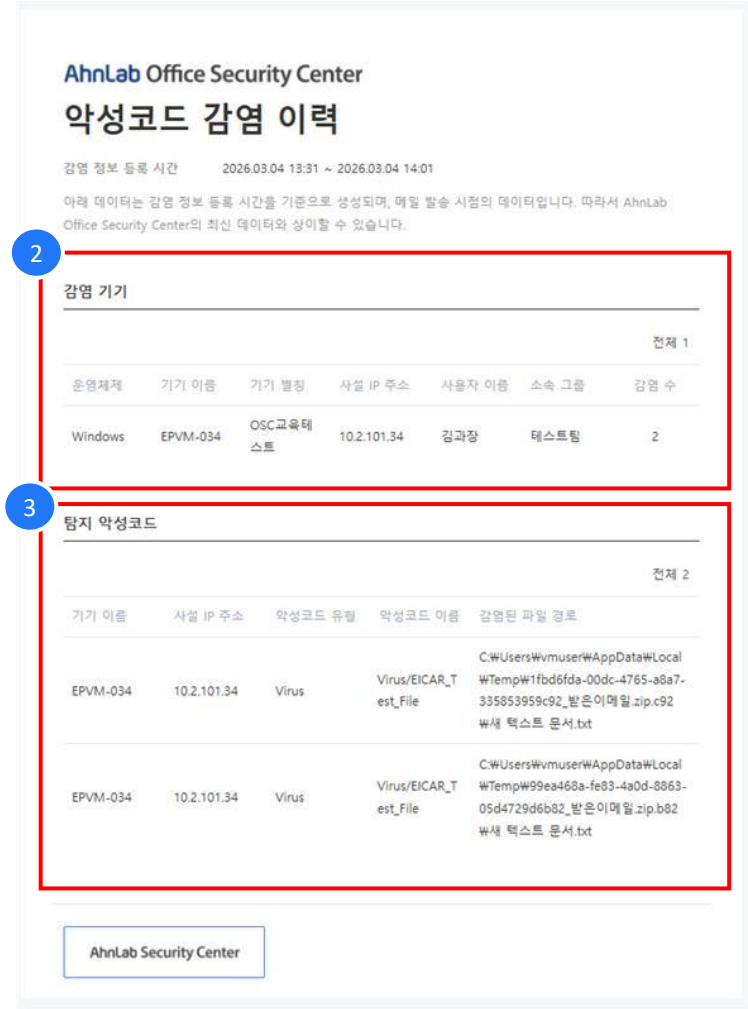
✓ PC의 서버 동기화 주기에 따라 원격검사는 보통 15분 이내, 늦어도 30분 안에 실행됩니다.

✓ 원격검사와 원격 업데이트는 사용자 동의없이 백그라운드에서 실행되어 사용자가 동작 여부를 확인하기 어렵습니다.

3. 악성코드 감염 알림 메일을 통해 실시간으로 사내 감염정보 확인하기(1/2)

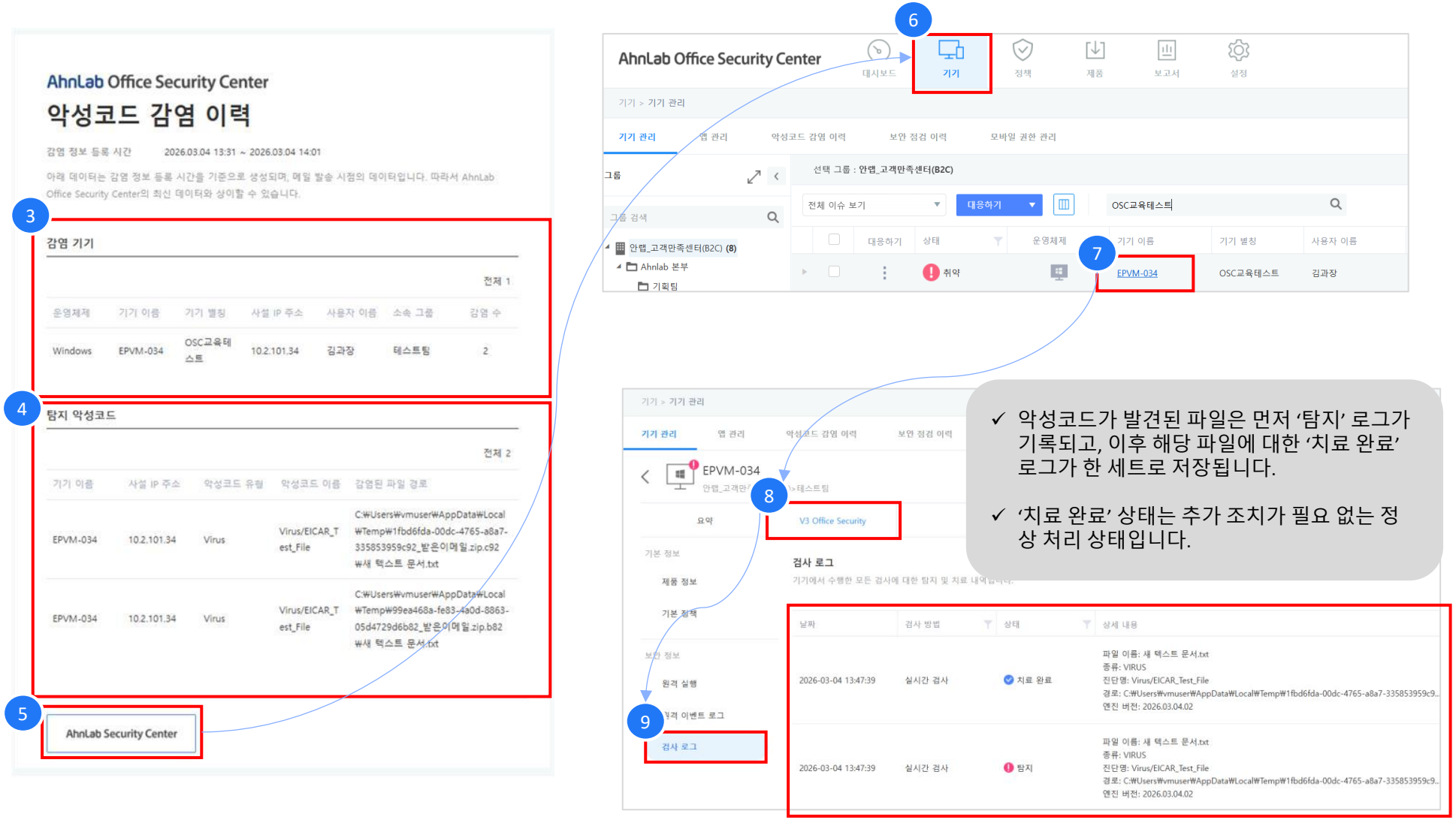
✓ 사용자 PC에서 악성코드가 진단되어 치료된 경우, 최대 30분 이내에 관리자 **이메일로 악성코드 감염 알림 메일이** 발송됩니다.
✓ 이메일에서는 감염된 기기명, 감염 정보 등록 시간, 악성코드 진단·치료여부 등 상세한 정보를 확인하실 수 있습니다.
✓ 악성코드 감염 알림 메일을 수신하였다면, 안내된 순서대로 진행하여 악성코드가 진단된 기기의 상세 정보를 확인할 수 있습니다.
✓ Office Security Center로 이동하여 감염된 기기에 [원격검사] 명령을 내리고 결과를 확인할 것을 권장합니다.





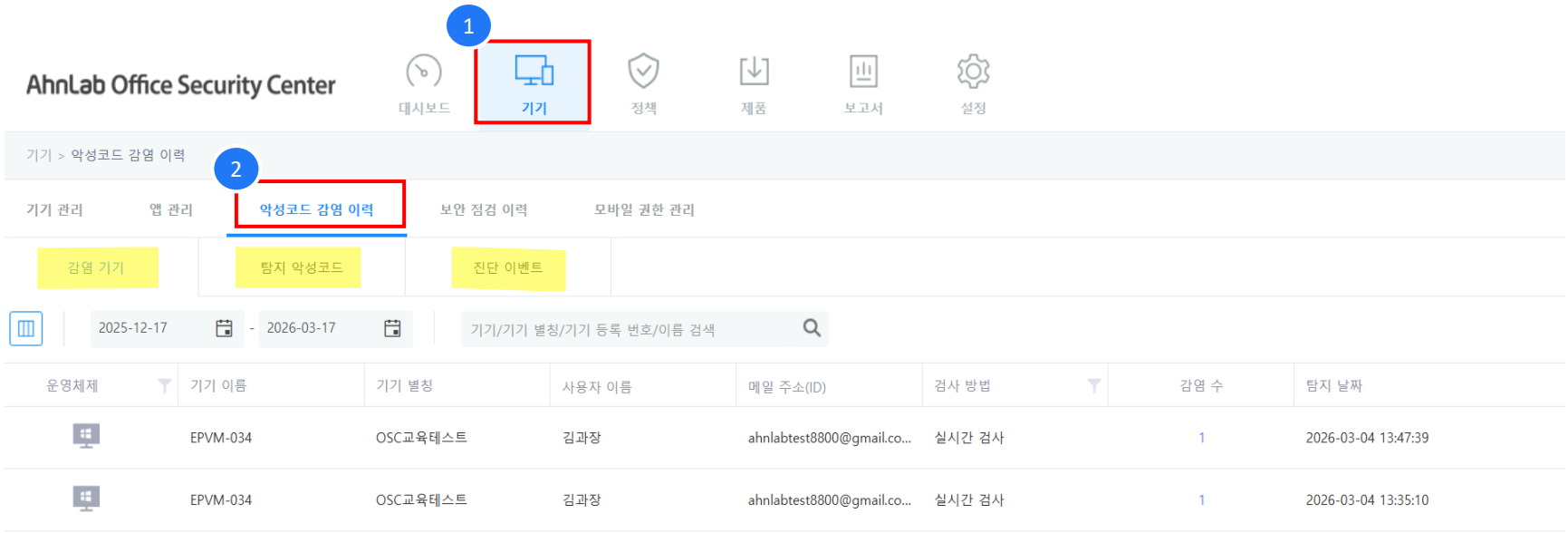
3. 악성코드 감염 알림 메일을 통해 실시간으로 사내 감염정보 확인하기(2/2)

✓ 악성코드 감염 알림 메일을 수신하면, 안내된 순서대로 진행하여 악성코드가 진단된 기기의 상세 정보를 확인할 수 있습니다.



4. 사내 전체 기기의 감염 이력을 조회하기

✓ 사내 전체 기기의 감염 이력 조회 방법은 다음과 같습니다.



1) 감염 기기: 관리자가 설정한 기간을 기준으로 감염된 기기의 상세 정보를 확인할 수 있습니다.

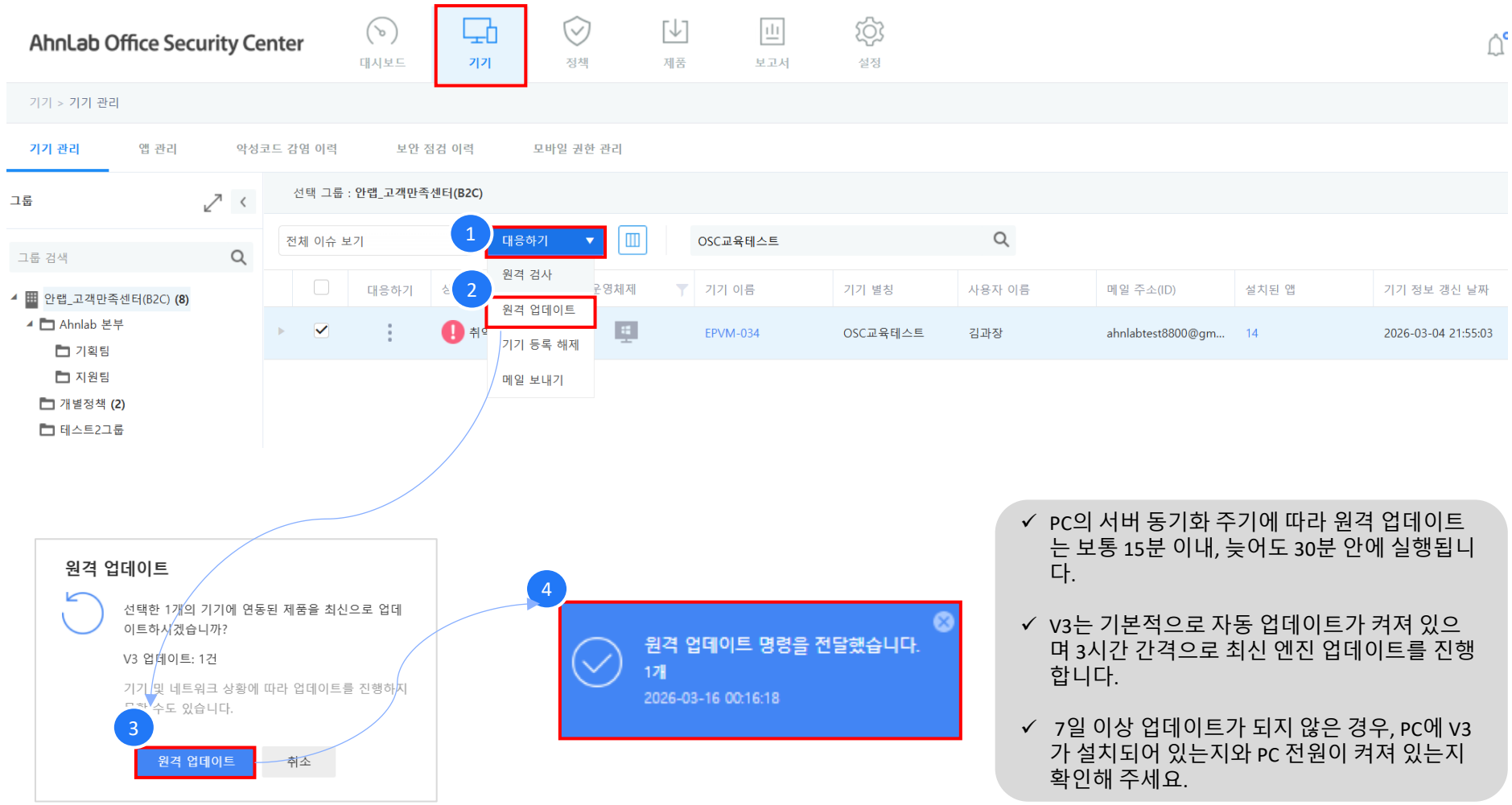
2) 탐지 악성코드: 관리자가 설정한 기간 동안 탐지된 악성코드의 상세 내역을 확인할 수 있습니다.

3) 진단 이벤트: 각 기기에서 발견된 악성코드에 대한 V3의 탐지 및 치료 이력을 확인할 수 있습니다.

✓ 감염 수(숫자)를 클릭하면 악성코드 이름과 감염 경로 등 상세 정보를 확인할 수 있으며, 진단된 목록은 엑셀로도 다운로드할 수 있습니다.

5. 엔진 업데이트가 취약인 경우

✓ 엔진 업데이트가 7일 이상 경과한 경우 오래된 엔진으로 판단하여 '취약' 상태로 분류됩니다.
✓ 최신 엔진으로 업데이트가 되지 않은 경우 신·변종 악성코드에 감염될 가능성이 있습니다.
✓ 기기 관리에서 엔진 업데이트가 7일 이상 경과한 PC가 있다면, [원격 업데이트] 명령을 통해 즉시 검사 명령을 전달해 주시기 바랍니다.



✓ PC의 서버 동기화 주기에 따라 원격 업데이트는 보통 15분 이내, 늦어도 30분 안에 실행됩니다.

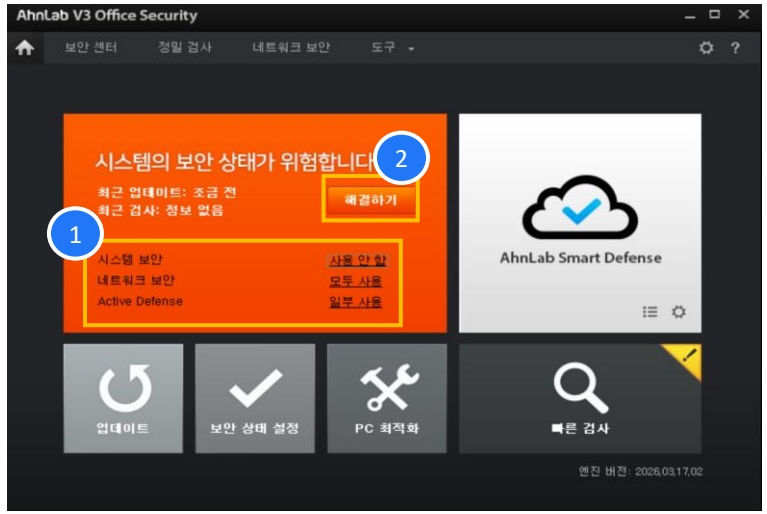
✓ V3는 기본적으로 자동 업데이트가 켜져 있으며 3시간 간격으로 최신 엔진 업데이트를 진행합니다.

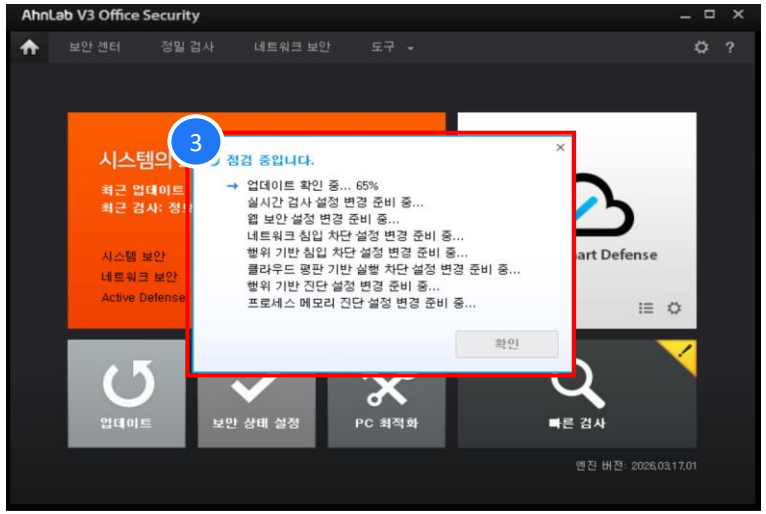
✓ 7일 이상 업데이트가 되지 않은 경우, PC에 V3가 설치되어 있는지와 PC 전원이 켜져 있는지 확인해 주세요.

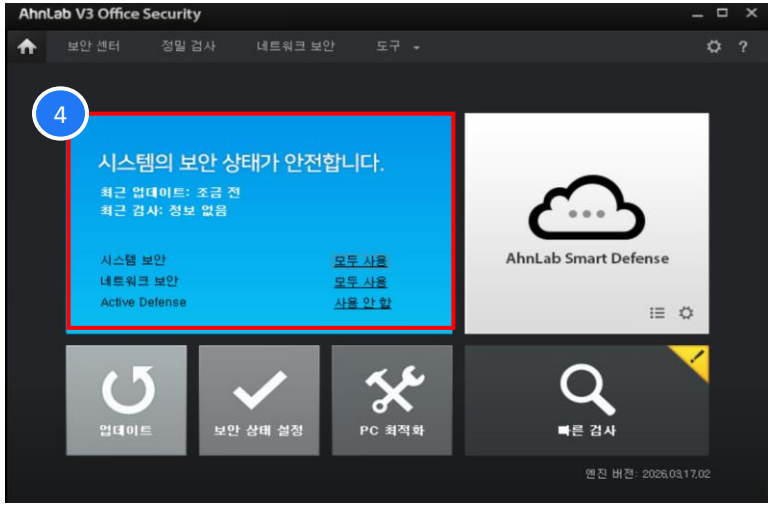
6. 실시간 검사가 OFF 상태로 표시되는 경우

✓ 실시간 검사가 꺼져 있으면 최신 엔진 상태와 관계없이 백신 기능이 작동하지 않아 '취약'으로 표시됩니다.
✓ 실시간 검사가 비활성화된 단말은 원격대응하기 기능으로 처리할 수 없습니다.
✓ **따라서 실시간 검사가 꺼져 있는 PC는 관리자가 직접 해당 PC에서 V3 실행 상태를 점검해 원인을 확인해 주셔야 합니다.**

실시간 검사가 꺼져 있는 PC에 대한 조치 가이드입니다.







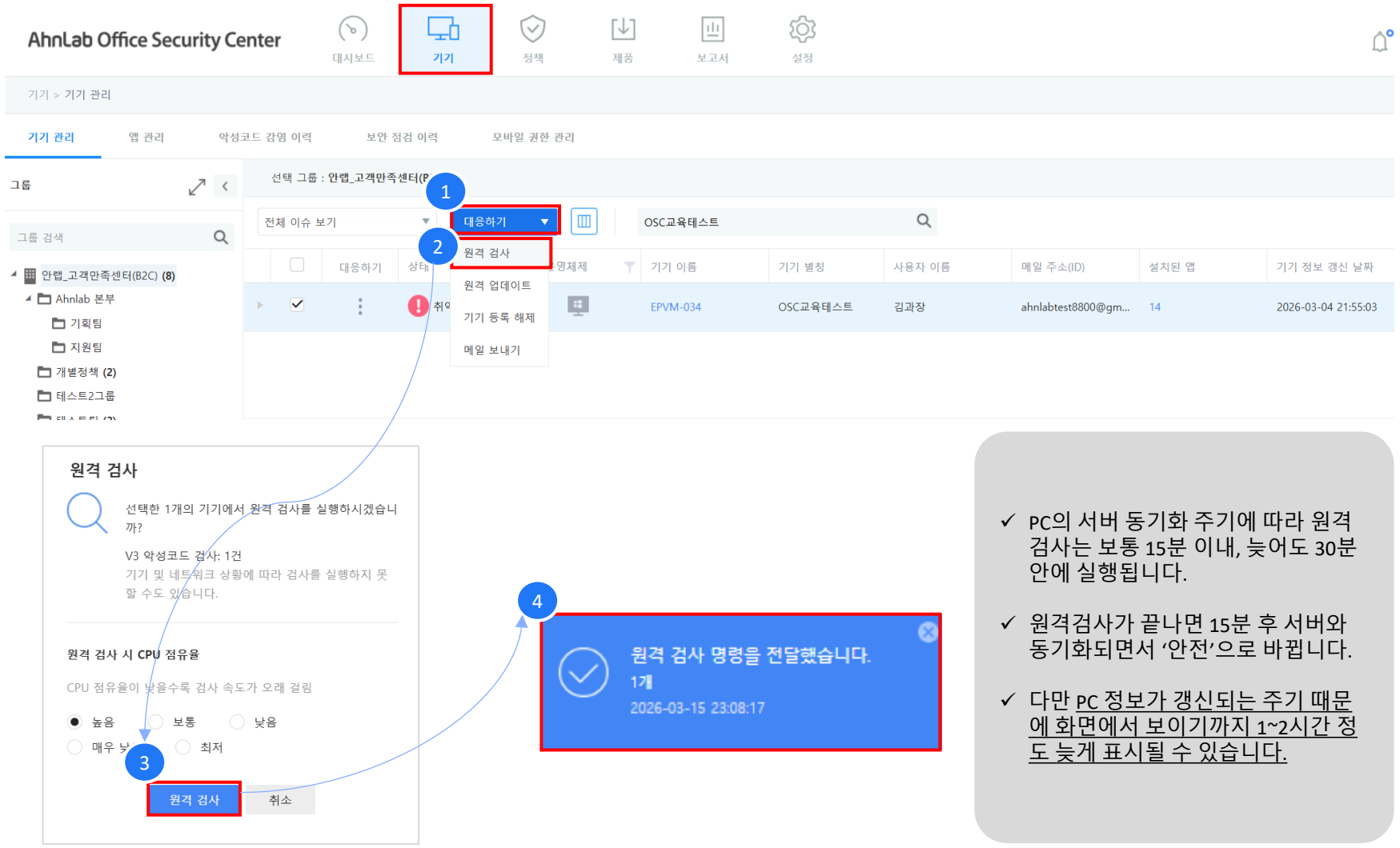
✓ '해결하기' 로 조치되지 않는 경우, 안랩 ASK에 문의를 등록하여 추가 조치 가이드를 받아 보시기 바랍니다.

✓ 안랩 ASK 문의 등록 바로가기
https://ask.ahnlab.com/hc/ko/requests/new

✓ 정상적으로 동작 중인 PC라면 실시간 검사가 꺼져 있는 경우에도 '실시간 검사 자동 재시작' 옵션에 따라 기본적으로 60분 후 자동으로 다시 활성화됩니다.

7. 최근 검사가 취약인 경우(1/2)

✓ 바이러스(수동) 검사가 7일 이상 실행되지 않는 경우 최근검사는 취약으로 표시됩니다.
✓ 실시간 검사는 실행 파일만 검사하므로, 보안을 위해 정기적으로 PC 전체에 대한 수동 검사가 필요합니다.
✓ 최근검사 취약 표시된 PC가 있다면, 원격검사 기능을 사용해 원격 검사 명령을 전달해 주시기 바랍니다.



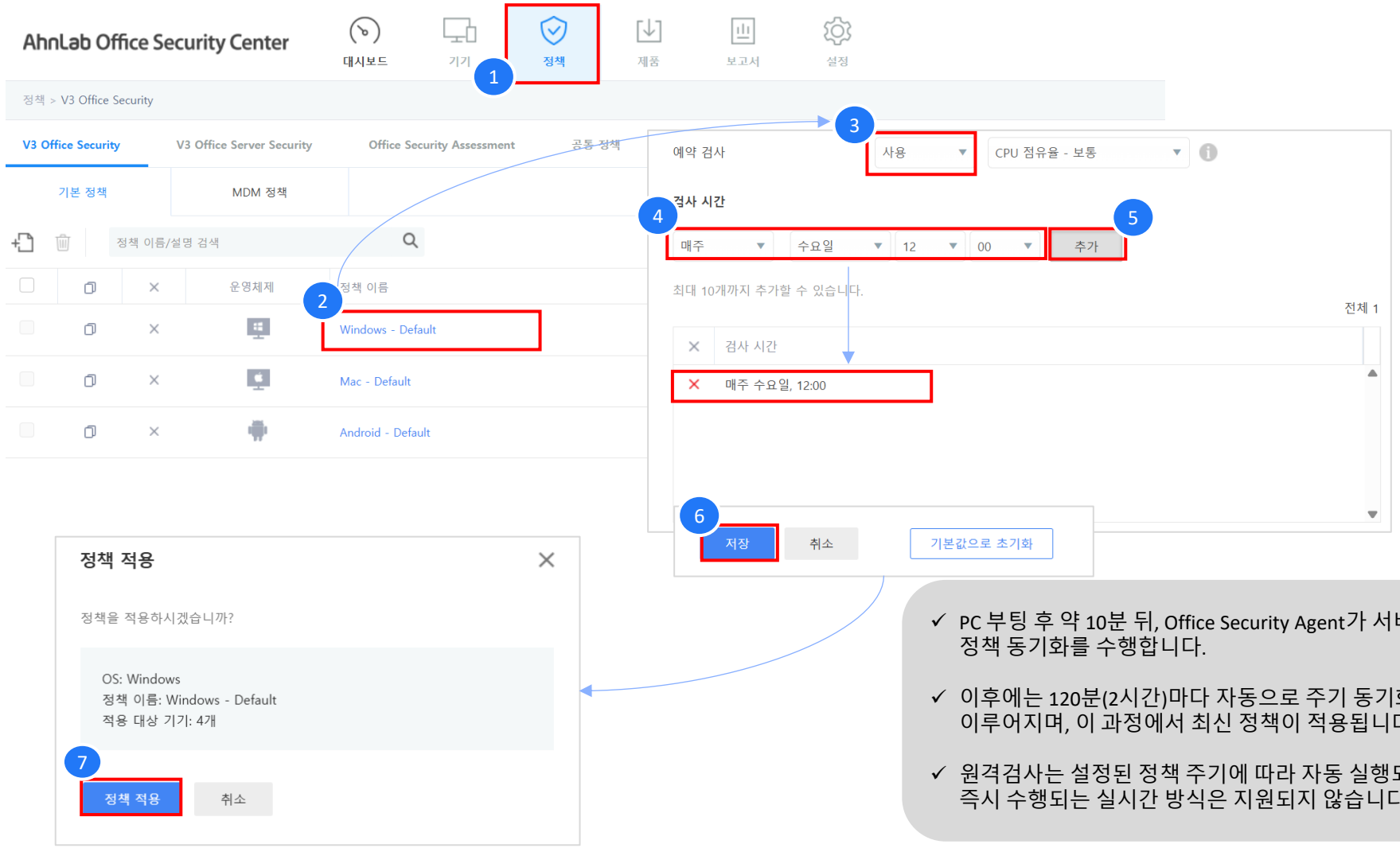
✓ PC의 서버 동기화 주기에 따라 원격 검사는 보통 15분 이내, 늦어도 30분 안에 실행됩니다.

✓ 원격검사가 끝나면 15분 후 서버와 동기화되면서 '안전'으로 바뀝니다.

✓ 다만 PC 정보가 갱신되는 주기 때문에 화면에서 보이기까지 1~2시간 정도 늦게 표시될 수 있습니다.

7. 최근 검사가 취약인 경우(2/2)

✓ 관리자가 반복적으로 취약 단말을 확인해 개별적으로 원격검사를 실행하는 방식은 운영 효율성이 낮습니다.
✓ 정책에서 '예약 검사' 기능을 활용하여 7일 이내 주기로 정기 예약검사를 설정한다면 사전 보안 대응이 가능합니다.
✓ 정책에서 '예약 검사'설정은 아래 순서대로 진행하시기 바랍니다.



✓ PC 부팅 후 약 10분 뒤, Office Security Agent가 서버와 정책 동기화를 수행합니다.

✓ 이후에는 120분(2시간)마다 자동으로 주기 동기화가 이루어지며, 이 과정에서 최신 정책이 적용됩니다.

✓ 원격검사는 설정된 정책 주기에 따라 자동 실행되므로, 즉시 수행되는 실시간 방식은 지원되지 않습니다

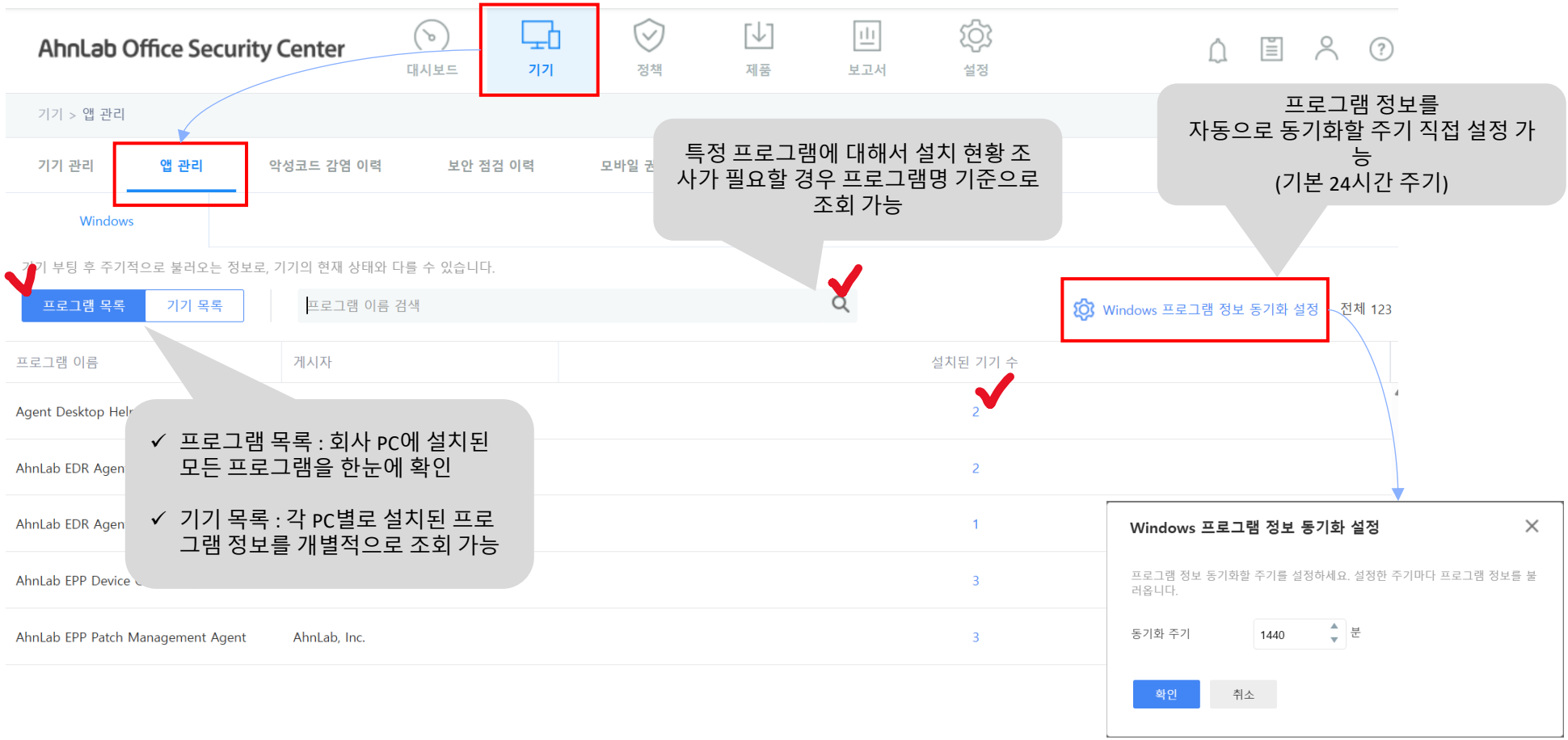
앱 관리

AhnLab

01
앱 관리 하기

1. 사내 PC에 설치된 앱 관리하기

✓ 회사 PC에 업무와 관련 없는 프로그램을 설치하면 보안 위험, 속도 저하, 관리 어려움 등이 생길 수 있습니다.
✓ Office Security Center의 앱 관리 기능을 통해 사내 PC에 설치된 프로그램을 한 번에 확인하고, 위험한 확장 프로그램도 빠르게 파악할 수 있습니다.
✓ 사내 PC에 불법 S/W 또는 취약점이 보고된 프로그램이 설치되진 않았는지 등을 확인하여 안전하게 관리할 수 있습니다.



01
앱 관리 하기

2. 앱 관리 기능 활용 해 보기

✓ 특정 프로그램이 악용되거나 취약점 이슈가 기사화 됐을 때 [앱 관리] 기능을 통해 빠르게 설치 여부를 확인할 수 있습니다.


브라우저 확장 프로그램 430만 건, 스파이웨어로 흑화

입력 : 2025-12-03 10:59

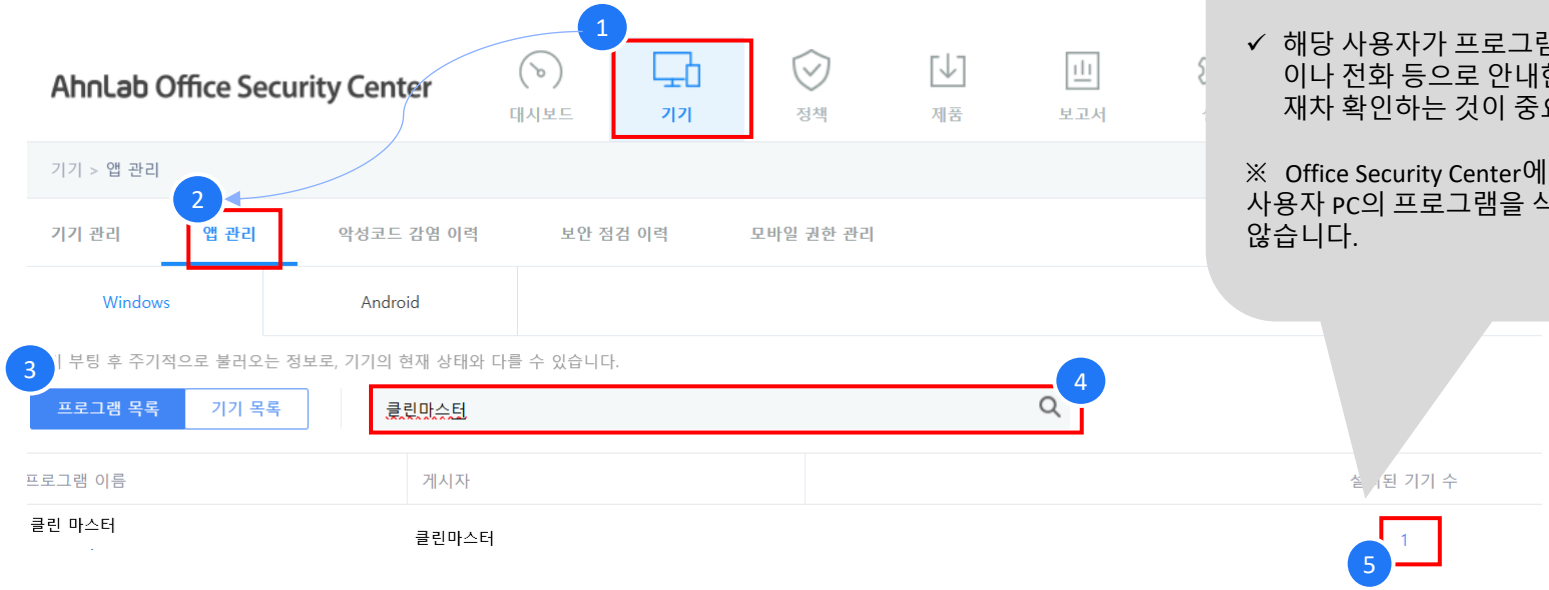
2026 SECURITY MARKET WHITE PAPER 보안뉴스와 시큐리티월드가 발행하는 '2026 보안시장 백서'
보안시장백서 한 권으로 꿰뚫는 대한민국 보안시장
구매신청 바로가기

확장 앱 마켓플레이스 사후 관리 부실 악용

[보안뉴스 김형근 기자] '셰이디판다'(ShadyPanda)라는 이름의 위협 행위자가 지난 7년 동안 430만 건 이상 설치된 크롬과 엣지 브라우저 확장 프로그램 공격 캠페인과 연루된 것이 밝혀졌다.

구글이 추천하고 검증까지 받아 의심 피해

특히 클린 마스터라는 확장 프로그램은 한때 구글이 추천하고 검증까지 받은 프로그램이다. 이로 인해 공격자들은 수년 후 악성 업데이트를 배포하면서도 의심을 피할 수 있었다.



✓ 설치된 기기수를 클릭하면 해당 프로그램이 설치된 기기목록을 확인할 수 있습니다.

✓ 해당 사용자가 프로그램을 삭제할 수 있도록 메일이나 전화 등으로 안내한 후 모두 삭제되었는지 재차 확인하는 것이 중요합니다.

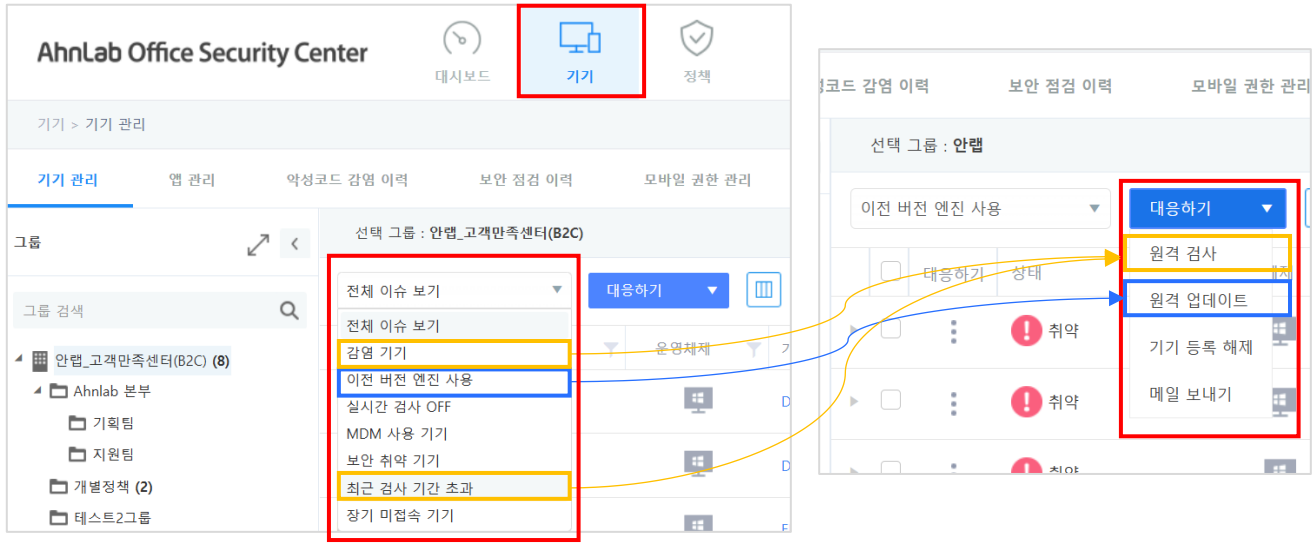
※ Office Security Center에서는 관리자가 원격으로 사용자 PC의 프로그램을 삭제하는 기능은 제공하지 않습니다.

FAQ

AhnLab

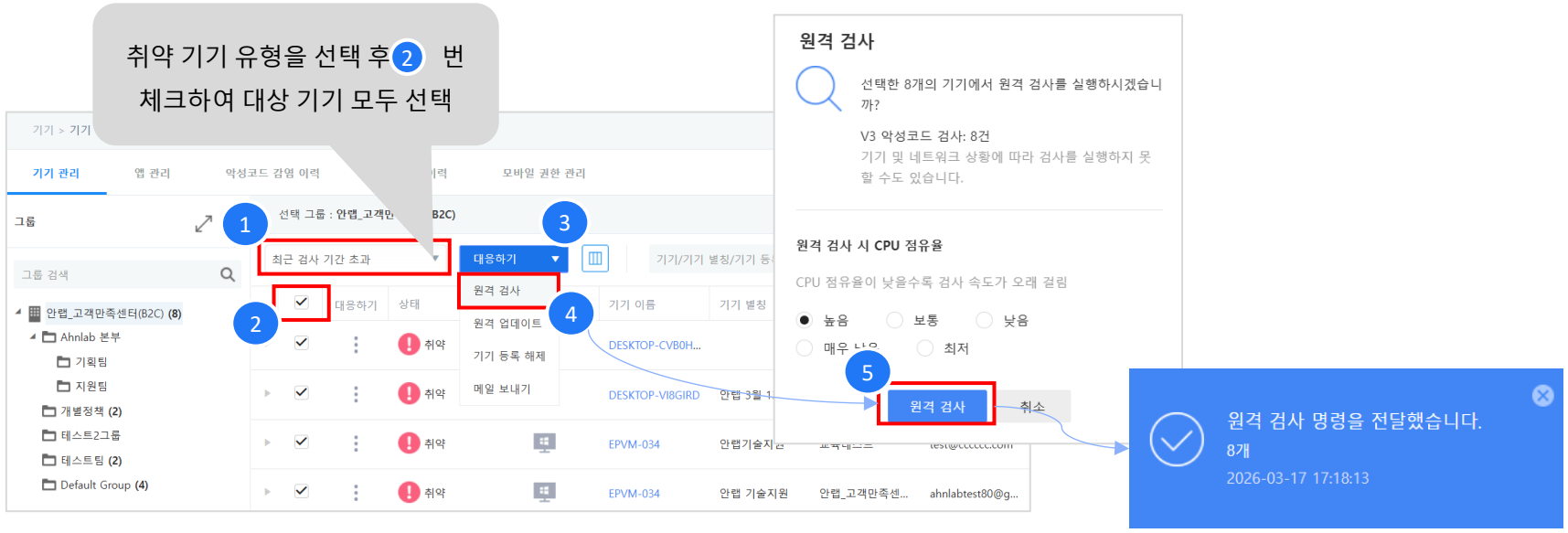
1. 취약 기기들 전체 대상으로 일괄 대응하기를 적용할 수 있나요?

✓ 취약 기기의 유형별로 일괄 대응하기가 가능합니다.



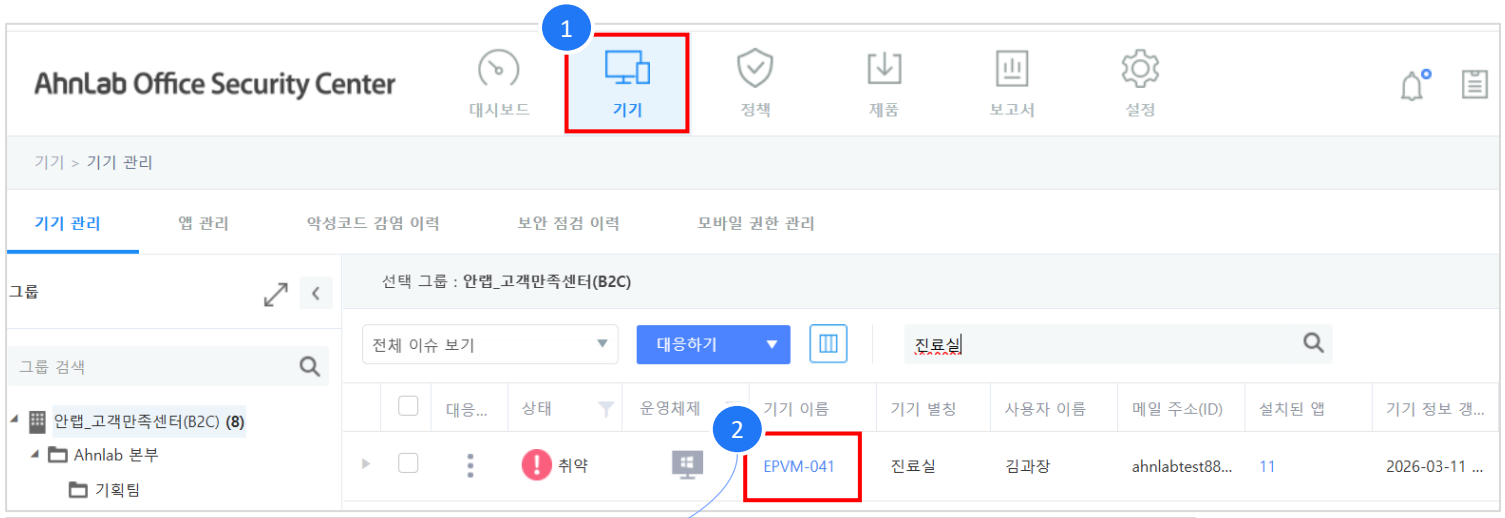
취약 유형 중 원격으로 대응 가능한 항목

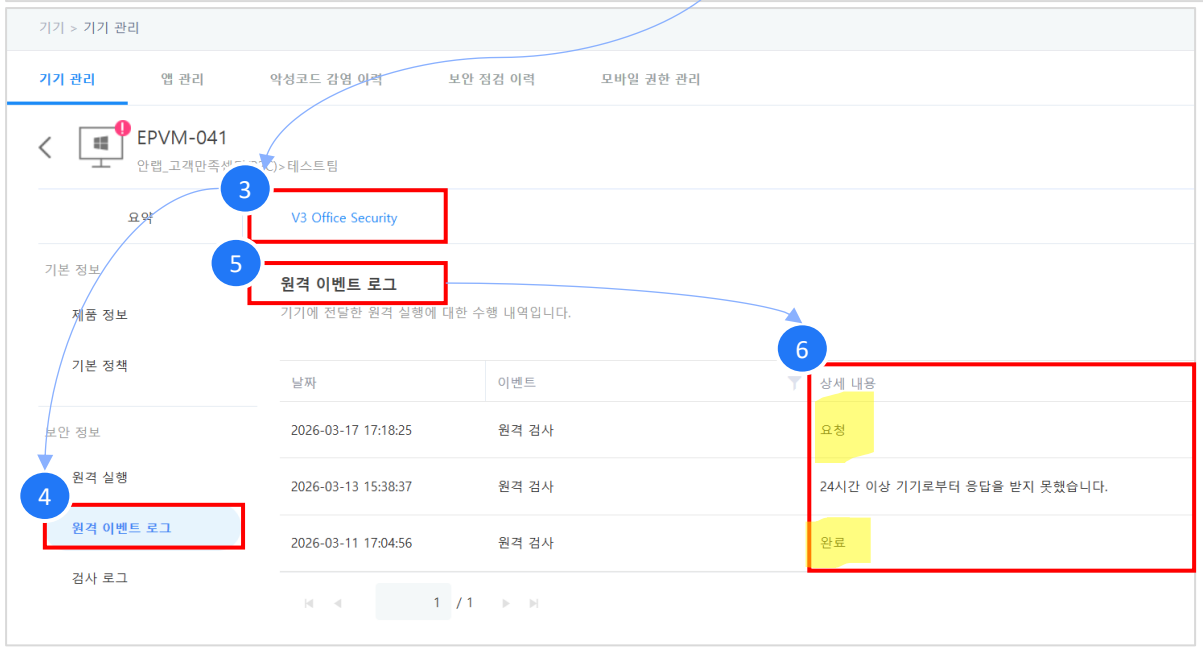
✓ 감염기기 → 대응하기 : 원격검사
✓ 이전 버전 엔진 사용 → 대응하기 : 원격 업데이트
✓ 최근 검사 기간 초과 → 대응하기 : 원격 검사



2. 원격검사 명령을 수행한 결과는 어디서 확인할 수 있나요?

✓ 개별 기기별로 원격 검사 명령 결과는 아래의 순서로 확인할 수 있습니다.

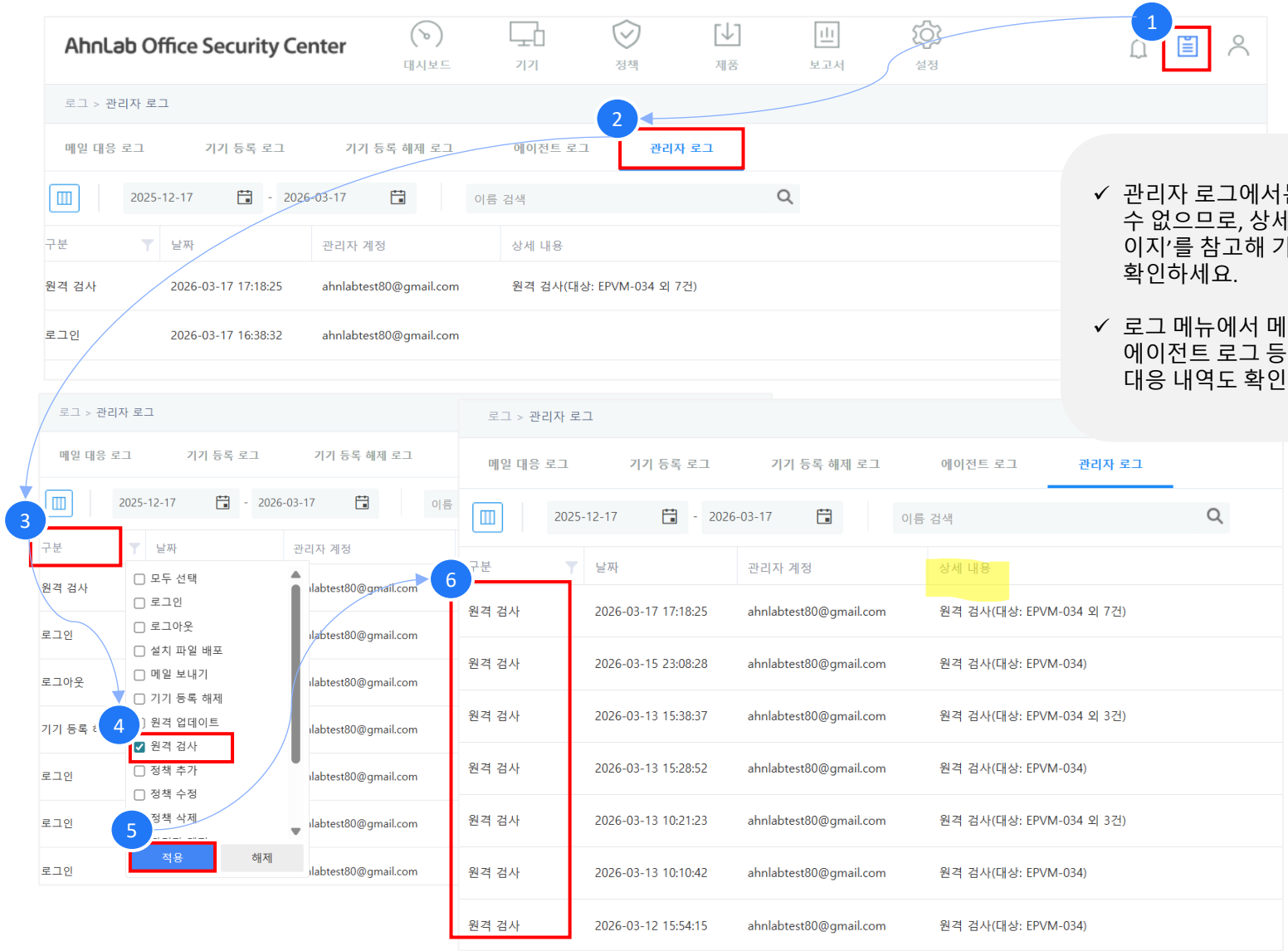




원격검사 명령을 보내면 상태가
'요청 → 실행 → 완료' 순서로 바뀌어
진행 상황을 쉽게 확인할 수 있습니다.

3. 관리자가 실행한 원격명령, 정책 적용, Agent 설치 요청 등의 대응 내역을 확인할 수 있나요?

✓ 아래 예시는 관리자 로그에서 전체 원격 검사 수행 기록을 확인하는 방법입니다.

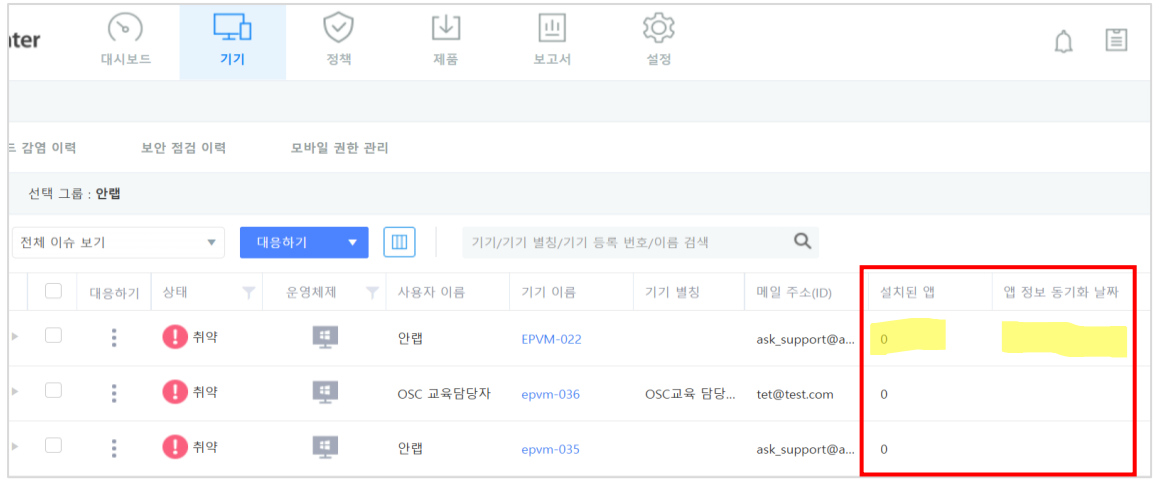


✓ 관리자 로그에서는 기기별 상세 내용을 볼 수 없으므로, 상세 로그가 필요하면 'P36 페이지'를 참고해 기기별 상세 로그 화면에서 확인하세요.

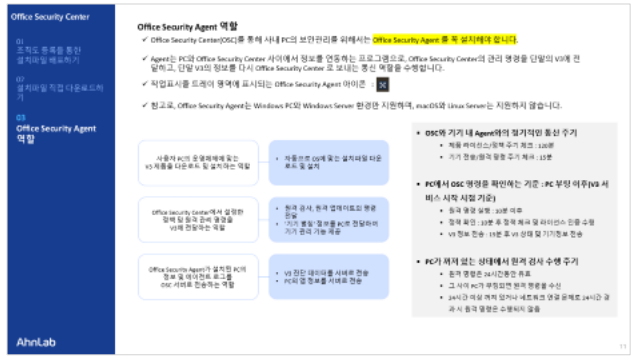
✓ 로그 메뉴에서 메일 대응, 기기 등록·해제, 에이전트 로그 등을 눌러 각 항목의 전체 대응 내역도 확인해 볼 수 있어요.

4. 기기관리에서 '설치된 앱'이 '0'으로 표시되고, '앱 정보 동기화 날짜'가 비어 있는 기기는 어떤 경우인가요?

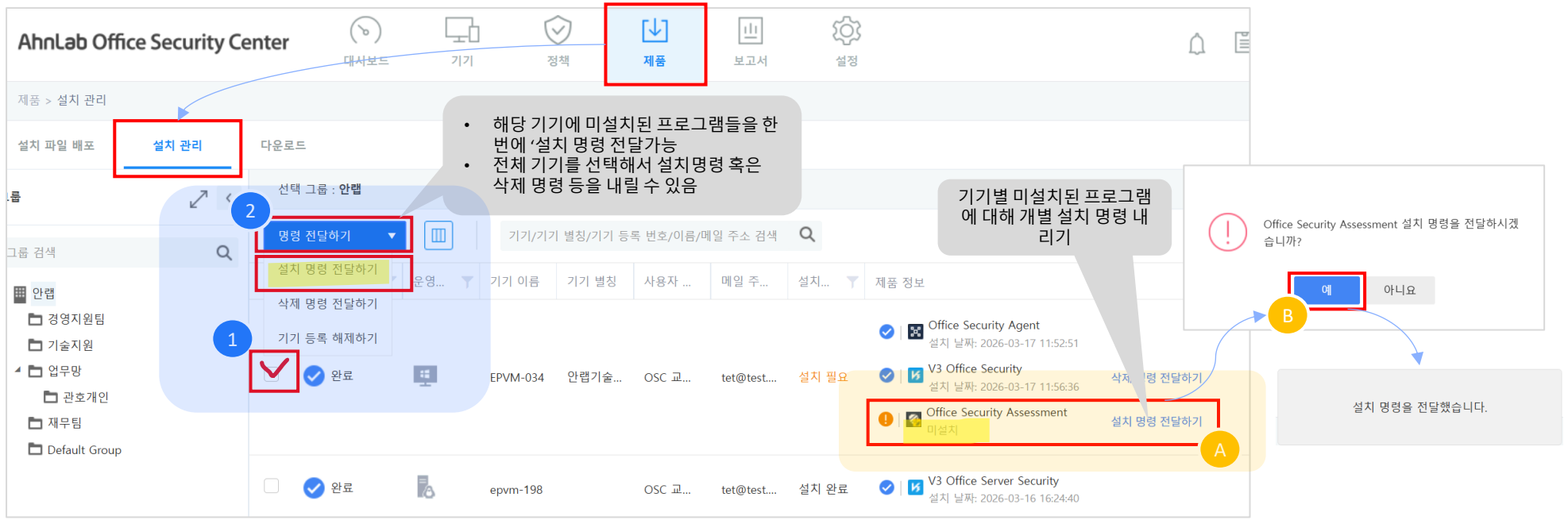
✓ 해당 PC에 Office Security Agent가 설치되어 있지 않아, 설치된 앱 정보를 가져오지 못한 경우입니다.



사내 PC에 설치되어 있는 프로그램 관리를 위해서는 Office Security Agent 를 설치하시길 권장합니다.

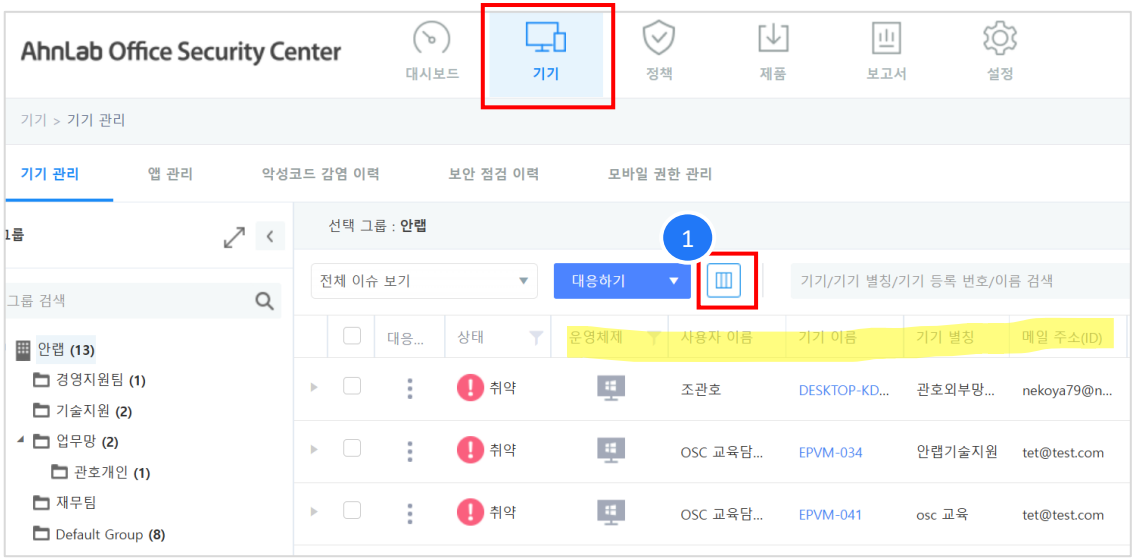


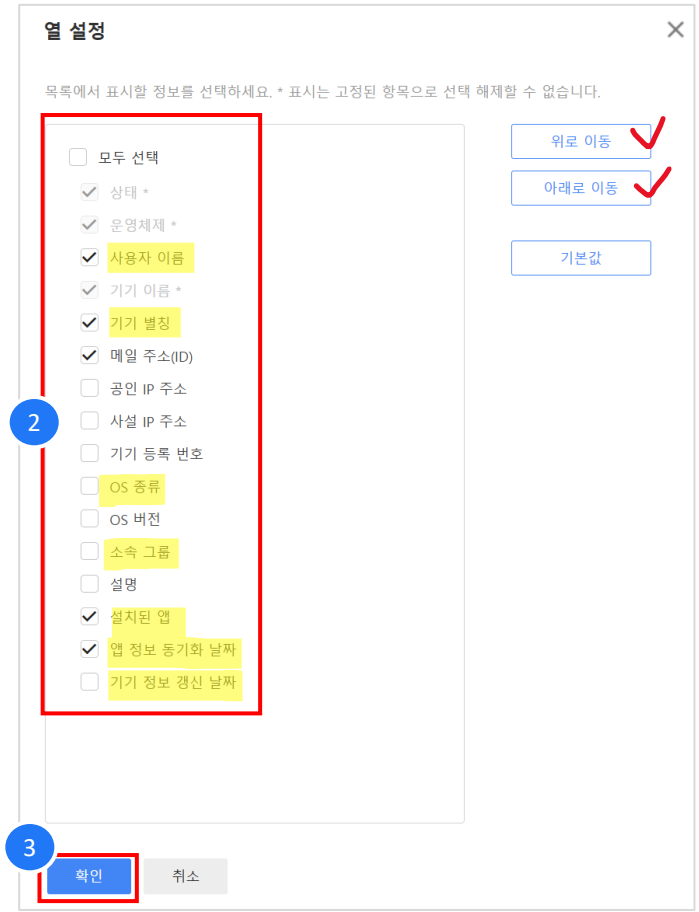
✓ Office Security Agent 를 원격으로 설치할 수 있는 방법은 2가지입니다.(PC의 서버 동기화 주기에 따라 15분~30분 안에 설치명령 전달)



5. 기기 목록에 표시되는 정보를 변경할 수 있나요?

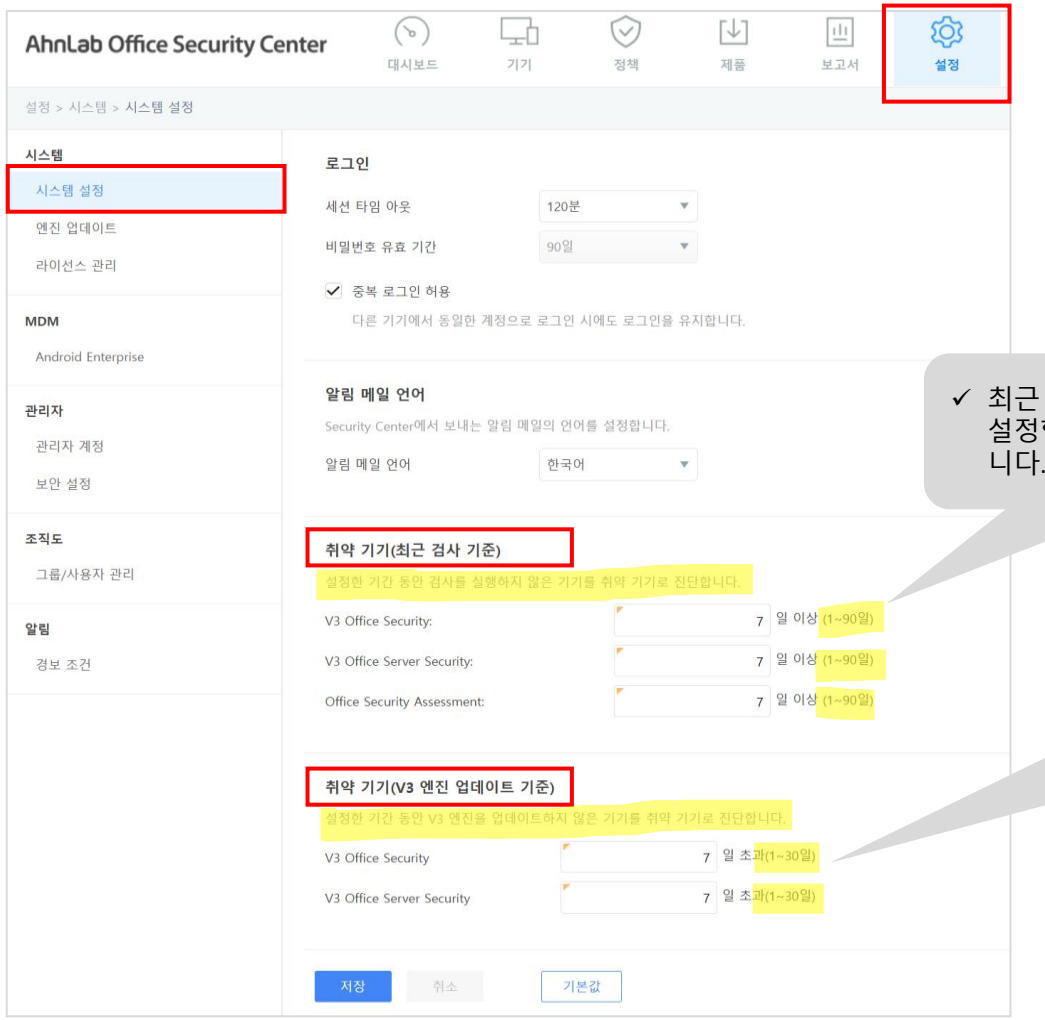
- ✓ [기기] 메뉴에서 관리자가 보고 싶은 정보를 선택할 수 있으며 정렬 순서도 변경할 수 있습니다.
- ✓ 관리자의 관점에서 기기 보안 현황을 파악하기 적절한 항목을 선택해 배열하시면 됩니다.
- ✓ 추천 항목 : 사용자 이름, 기기 별칭, OS 종류, 소속 그룹, 설치된 앱, 앱 정보 동기화 날짜, 기기 정보 갱신 날짜





6. 취약 기준 설정 하기

✓ 취약 기기로 판단하는 4가지 항목 중에서 최근 검사, 엔진 업데이트 항목은 관리자가 판단 기준일을 직접 설정할 수 있습니다.
✓ PC 전체검사에 대한 주기는 주 1회 검사를 권장하고 있으며 현재 기본값으로 설정된 상태입니다.
✓ V3 엔진 업데이트 역시 기본 7일로 설정되어 있습니다. 일반적으로 매일 매일 업데이트가 진행되지만 휴가, 출장, 공휴일 등으로 PC 전원이 OFF된 경우 등의 다양한 상황을 감안한 기준일이며, 회사 보안 정책에 따라 7일 이하로 설정하셔도 무방합니다.



✓ 최근 검사 기간을 1~90일 사이에서 설정할 수 있으며, 기본값은 7일입니다.

✓ V3 엔진 업데이트 취약 기준은 1~30일 사이에서 설정할 수 있으며, 기본값은 7일입니다.

✓ 악성코드에 효과적으로 대응하기 위해 취약 기기 기준은 기본값인 7일로 설정할 것을 권장합니다.

More security, More freedom

www.ahnlab.com

AhnLab