# Office Security Center

## 정책관리 마스터 : 보다 더 안전하게!

기술컨택센터



AhnLab

# Table of Contents





AhnLab

# 보안 정책의 이해

01 보안 정책 역할

02 정책 설정 메뉴 접속 방법

03 정책 옵션 정의

04 정책 즉시 업데이트



AhnLab

# 보안 정책 역할

## 기본 정책의 역할

*현관문 자물쇠처럼 기본 보안을 지켜줍니다*

- ✓ V3는 설치하는 순간부터 이미 알려진 바이러스를 자동으로 막아주는 방어막이 작동합니다
- ✓ 별도 설정 없이도 일반 업무 환경에서 무리 없이 충분한 보안 기능을 제공합니다
- ✓ 즉, 기본 설정만으로도 충분히 안전합니다

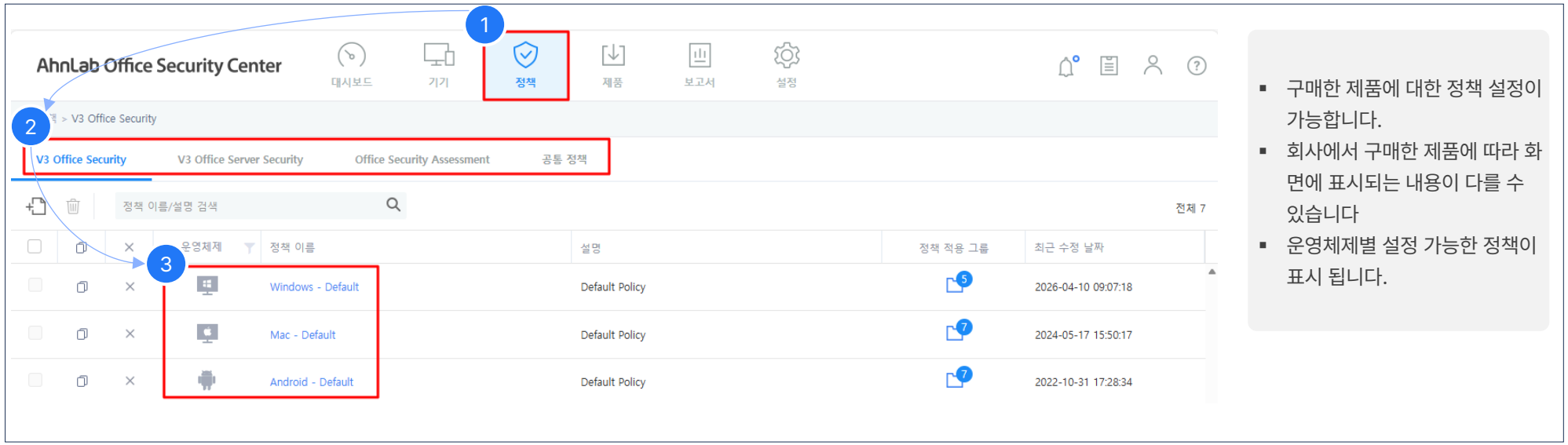
## 이번 교육에서 다룰 내용

*자물쇠에 보조 잠금 장치를 더하는 방법*

- ✓ 실제 현장에서 자주 요청되는 보안 설정을 적용하는 방법(엔지니어가 권장하는 보안정책 3가지)
- ✓ 업무에 큰 불편 없이 보안 사고 가능성을 줄여주는 설정
- ✓ 지금 바로 적용할 수 있는 유용한 보안 강화 포인트를 소개합니다

# 정책 설정 메뉴 접속 방법

- ✓ http://osc.ahnlab.com/ 주소로 접속하여 로그인 합니다.
- ✓ [정책] 탭을 클릭하여 Windows–Default 정책을 클릭




- 구매한 제품에 대한 정책 설정이 가능합니다.
- 회사에서 구매한 제품에 따라 화면에 표시되는 내용이 다를 수 있습니다
- 운영체제별 설정 가능한 정책이 표시 됩니다.

# 정책 옵션 정의

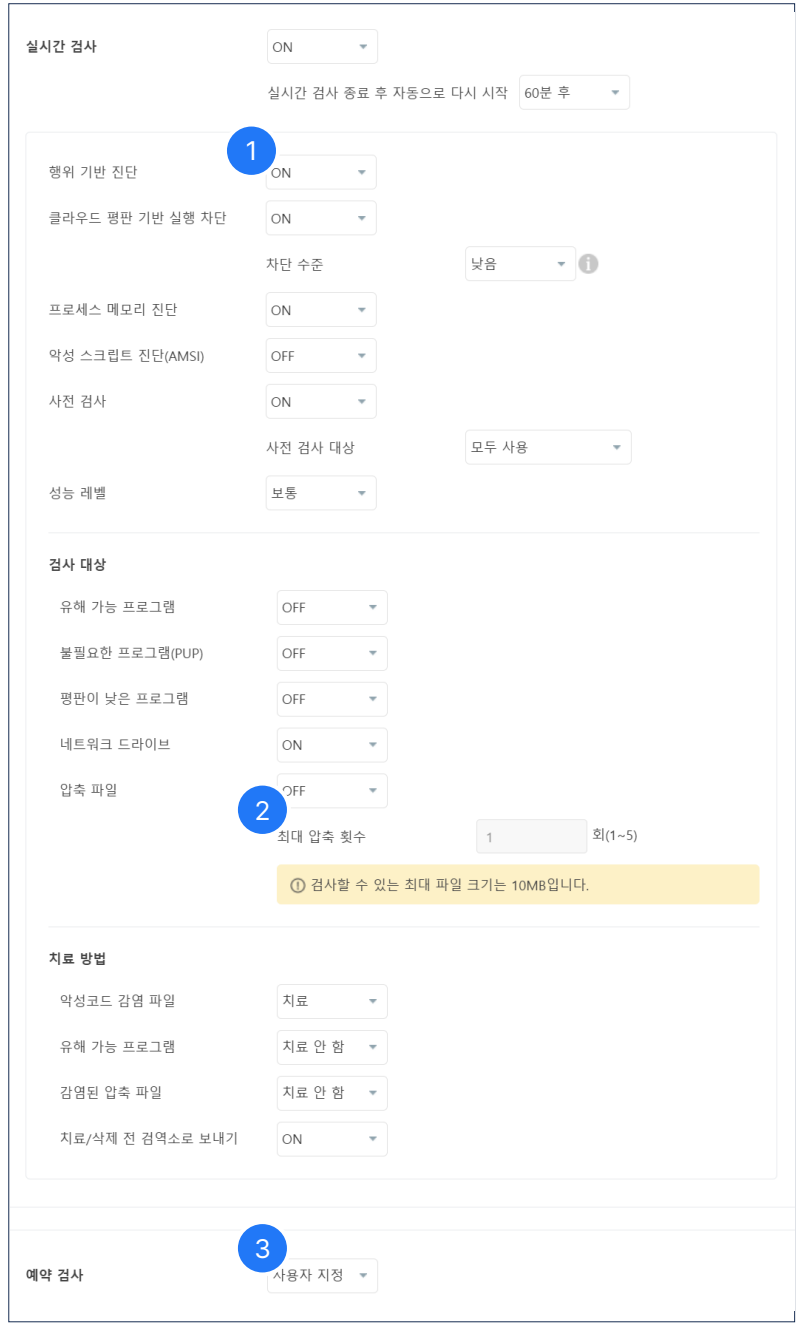
✓ 정책 ON, OFF, 사용자 지정 설정 차이점

1 **ON :** 관리자가 정한 규칙을 모든 PC에 적용합니다 (사용자가 변경 불가)

2 **OFF :** 보안 기능을 끄는 설정입니다

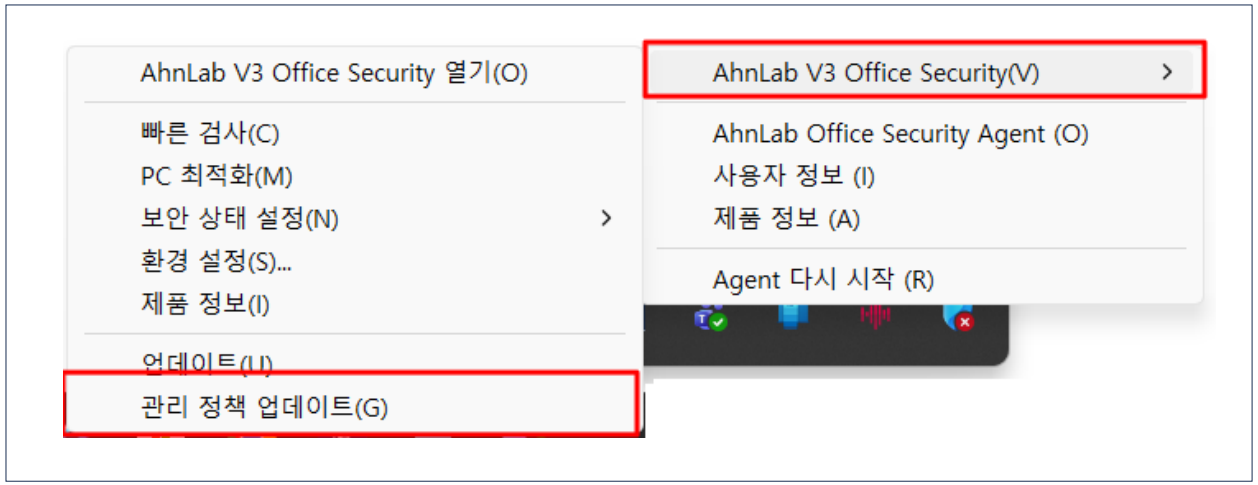
3 **사용자 지정 :** 관리자가 기능을 강제하지 않고, 사용자가 보안 기능을 직접 선택할 수 있도록 자율권을 제공합니다.

※ 업무 특성과 보안 요구 수준에 따라 맞는 적용 방식을 선택하는 것이 중요합니다.



# 정책 즉시 업데이트

- ✓ 관리자가 설정한 정책은 사용자 PC에 15분 주기로 전달 됩니다.
- ✓ 설정한 정책을 즉시 적용하려면 PC에서 Office Security Agent의 '관리 정책 업데이트'를 통해 즉시 정책을 적용 할 수 있습니다.



# 엔지니어가 추천하는 권장 정책

01 예약 검사 설정

02 V3 삭제 방지 기능

03 V3 환경 설정 제한 기능

04 자주 문의되는 정책 : 검사 예외 정책



AhnLab

## ① 예약 검사, 왜 필요할까요?

**? 백신을 잘 설치해서 쓰고 있는데, 왜 PC가 '취약'하다고 표시될까요?**

PC를 '안전' 상태로 유지하려면 아래 4가지 조건을 모두 만족해야 합니다. 이 중 3가지는 PC가 켜져 있으면 자동으로 관리되지만, 한 가지는 직접 검사를 실행해야만 충족됩니다.

| | | |
|---|---|---|
| **최근 감염 이력** | 최근 30분 내 악성코드가 진단된 적이 없어야 합니다 | 자동 관리 |
| **엔진 최신 상태** | 백신 엔진이 7일 이내에 자동 업데이트 되어야 합니다 | 자동 관리 |
| **실시간 검사 ON** | 실시간 검사 기능이 켜져 있어야 합니다 | 자동 관리 |
| **주기적인 검사 이력** | 바이러스 검사를 7일 이내에 한 번은 직접 실행해야 합니다 | 직접 검사 필요 |

즉, 일주일에 한 번 직접 검사를 실행하거나 — 미리 '예약 검사'를 설정해 두면,
신경 쓰지 않아도 이 조건이 자동으로 충족되어 PC를 항상 '안전' 상태로 유지할 수 있습니다.

## ② 예약 검사, 이런 효과가 있습니다

**예약 검사란?**
내가 정해 놓은 주기에 따라 자동으로 PC를 정기적으로 검사해 주는 기능입니다.

### 🚪 실시간 검사만으로는 부족

- 실시간 검사는 파일이 들어오는 순간만 확인
- 이미 숨어있는 악성코드 놓칠 수 있는 상태

### ⏰ 내가 정한 시간에 자동으로 검사

- PC 전체 또는 원하는 영역만 정밀하게 검사
- 따로 신경 쓰지 않아도 알아서 실행

### 🩺 꾸준한 검사로 안심하고 사용

- 숨어 있는 위협을 주기적으로 스캔
- 주기적인 검사로 PC가 '취약' 상태로 바뀌는 것을 예방

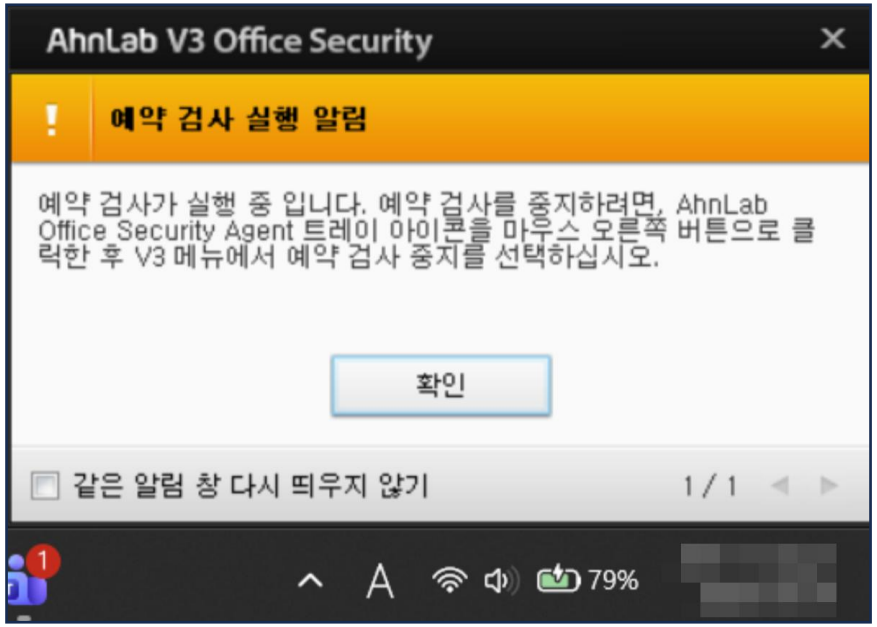
## ③ 예약 검사, 이렇게 설정하시면 됩니다

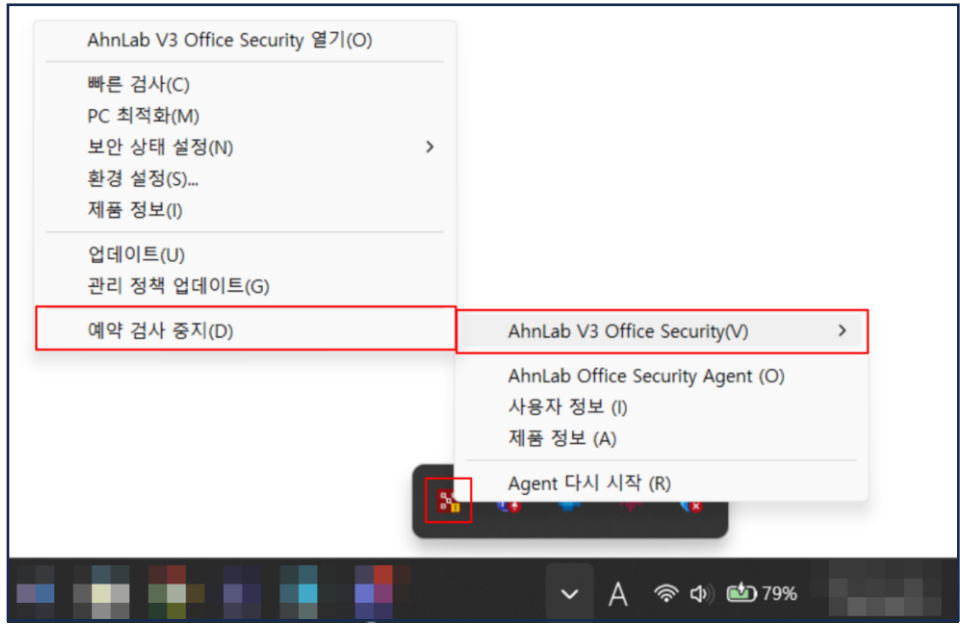
- ✓ 매일 / 매주(요일 선택) / 매월(날짜 선택) 중 원하는 주기로 설정할 수 있습니다.
- ✓ 검사는 주 1회 이상, PC를 잘 사용하지 않는 점심시간에 진행되도록 설정하는 것을 추천드립니다.
- ✓ 점심시간처럼 PC가 쉬는 시간에 진행되므로 CPU 사용률은 '보통' 또는 '높음'으로 설정해도 괜찮습니다.
- ✓ PC가 꺼져 있으면 예약 검사가 실행되지 않으니, 휴일은 검사일에서 제외하는 것이 좋습니다.


※ 예약 검사 시간에 PC 전원이 꺼져 있었다면, 24시간 이내에 다시 검사 일정이 전달됩니다.

## ④ 검사 중이라면, 이렇게 중지하시면 됩니다

- ✓ 예약 검사가 시작되면 PC 화면 우측 하단에 검사 실행 알림 창이 나타납니다.
- ✓ 중요한 업무 중이라 검사를 잠시 멈추고 싶다면, 화면 우측 하단 트레이의 백신 아이콘에서 '예약 검사 중지'를 선택하시면 됩니다.




※ 검사 도중 중지하면 다음 예약 주기가 될 때까지 추가 검사는 진행되지 않습니다.

## ① 삭제 방지, 왜 필요할까요?

**? 백신을 설치해 두었는데, 누군가 마음대로 지워버릴 수도 있지 않을까요?**

**★ 백신이 지워지면, 악성코드의 활동을 그대로 허용하는 셈이 됩니다 ★**

악성코드는 보통 이런 흐름으로 PC에 침투합니다. 백신이 살아있어야 각 단계를 차단할 수 있습니다.

| 침투 · 실행 | → | 권한 탈취 | → | 확산 · 공격 |
|---|---|---|---|---|
| 악성 사이트 · 첨부파일 차단 | | 비정상 권한 획득 탐지 | | 악성 행위 탐지 및 차단 |

그래서 본인이나 동료가 실수로, 혹은 악성코드가 의도적으로 백신을 지우지 못하도록 '삭제 방지 비밀번호'를 설정해 두는 것을 권장합니다.

## ② 삭제 방지, 이런 효과가 있습니다

**삭제 방지란?**
비밀번호를 입력해야만 백신을 삭제할 수 있도록 잠가두는 기능입니다.

### 🛡️ 외부에서의 백신 삭제 차단

- 악성코드가 몰래 백신을 지우려는 시도를 차단
- 사용자가 실수로 삭제하는 것도 방지

### 🔐 비밀번호는 안전하게 관리돼요

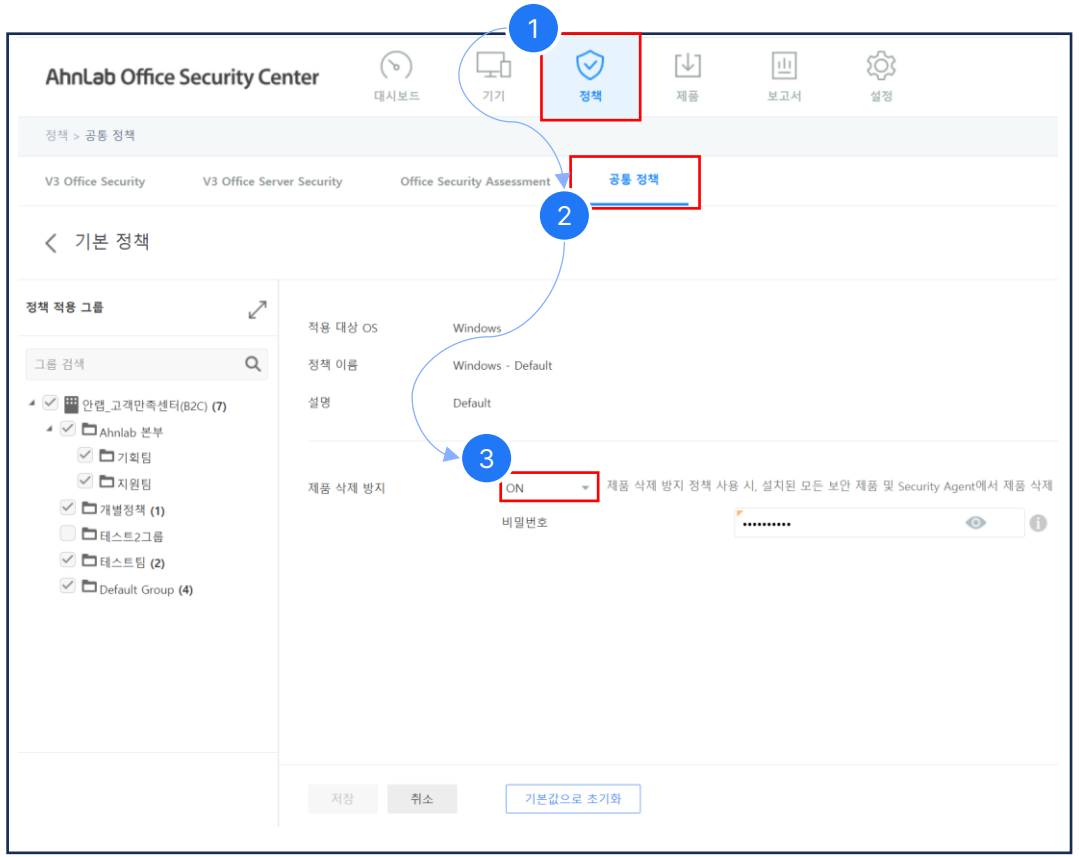
- 삭제 방지 비밀번호는 회사 관리자가 보관
- 주기적으로 변경하며 관리

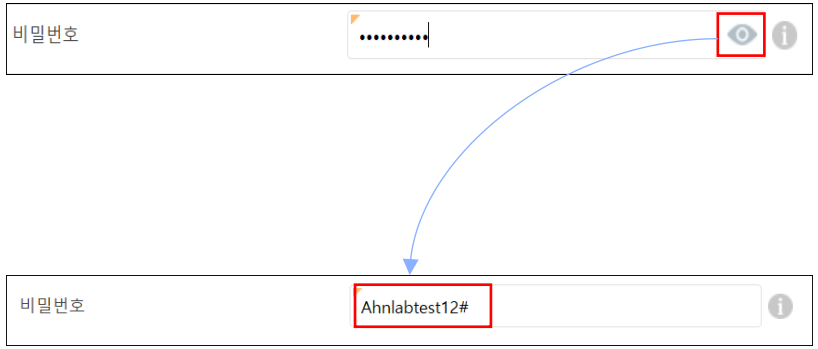
### 💻 정말 삭제가 필요할 때는

- 사용자는 관리자에게 요청하여 비밀번호를 받고 삭제 가능
- 잠시 삭제가 필요한 특수한 상황도 안내받아 삭제 진행 가능

## ③ 삭제 방지, 이렇게 설정하시면 됩니다

- ✓ 아래 순서로 삭제 방지를 설정 할 수 있습니다
- ✓ 이미 설정된 비밀번호는 아래 메뉴에서 다시 확인할 수 있습니다

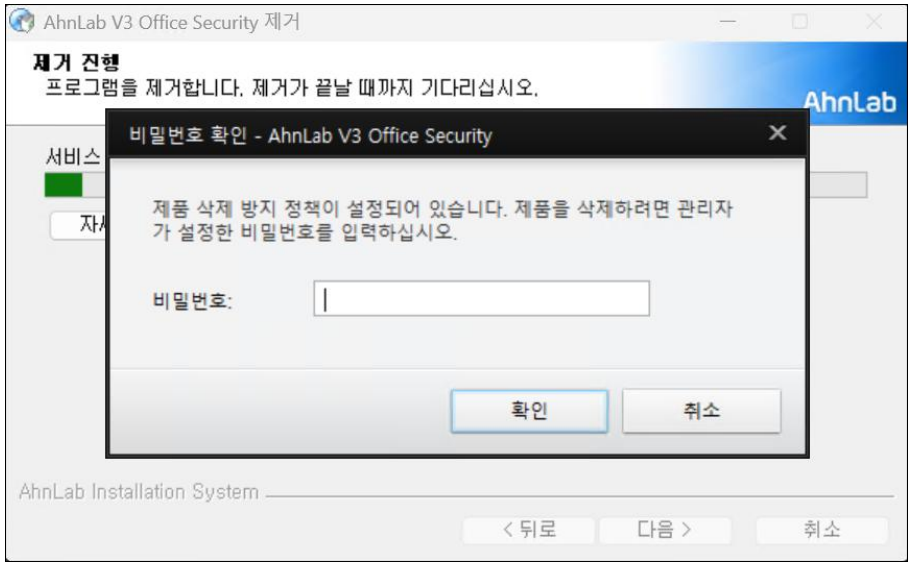


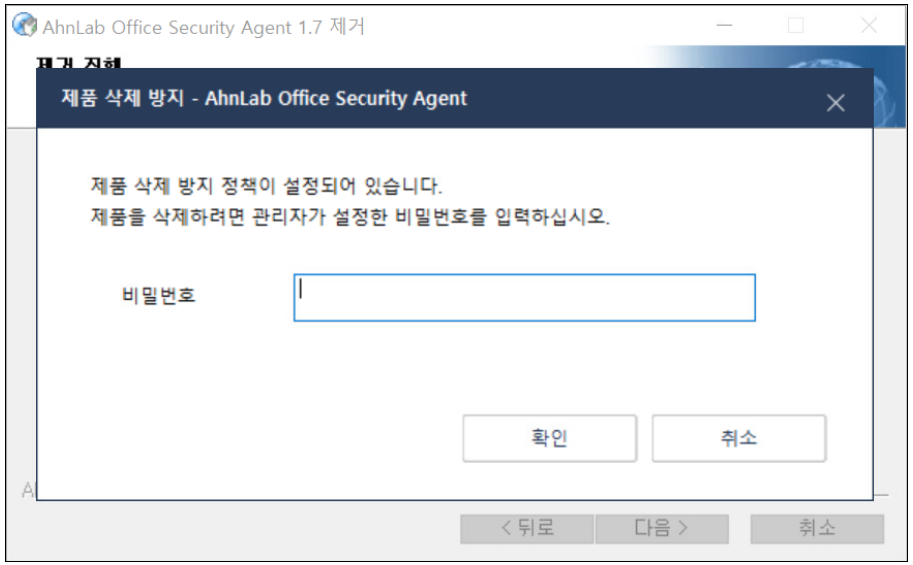




※ 비밀번호 입력란 클릭 후 오른쪽 끝 눈 모양 아이콘을 누르면 비밀번호를 확인할 수 있어요.

## ④ 삭제를 시도하면 이렇게 보입니다

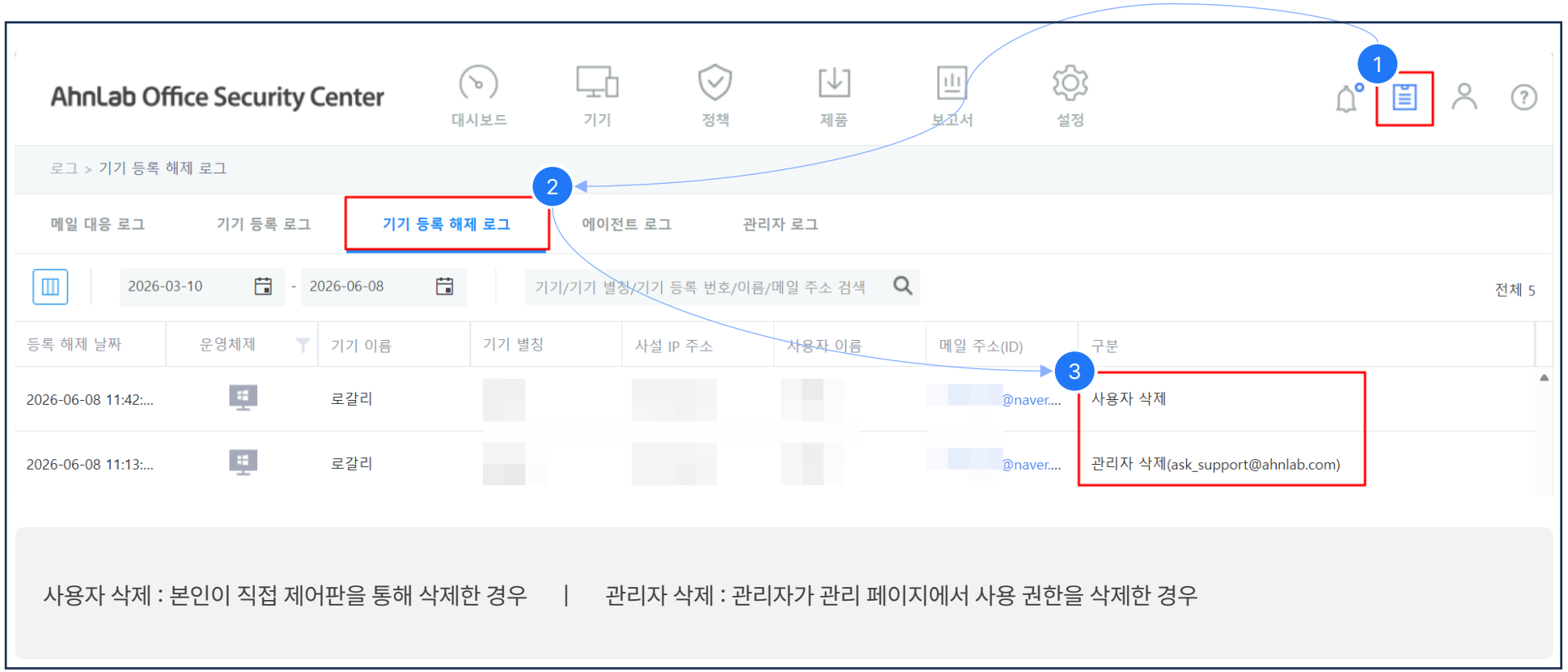
- ✓ 삭제 방지가 적용된 상태에서 백신을 삭제하려고 하면, 아래와 같은 비밀번호 입력창이 나타납니다.
- ✓ 정말 삭제가 필요하다면 관리자에게 문의해 비밀번호를 받은 뒤 진행하시면 됩니다.



## ⑤ 누가 기기 정보를 삭제했는지 궁금하십니까?

✓ 관리자는 로그를 통해 누가, 언제 백신을 삭제했는지 확인할 수 있습니다.

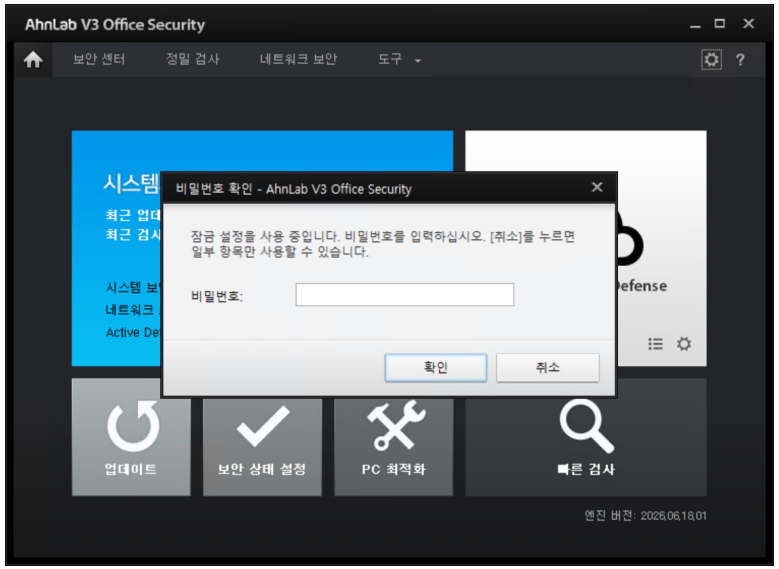


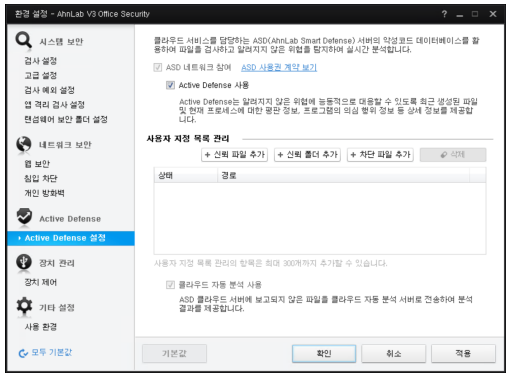

사용자 삭제 : 본인이 직접 제어판을 통해 삭제한 경우 | 관리자 삭제 : 관리자가 관리 페이지에서 사용 권한을 삭제한 경우

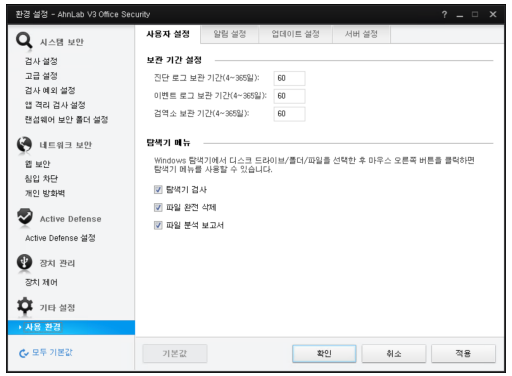
# ① 환경 설정 잠금, 왜 필요할까요?

**? 삭제는 막아뒀는데, 설정에서 기능을 잠깐 꺼버릴 수도 있지 않을까요?**

맞아요. 삭제 방지를 설정해도 '환경 설정 잠금'을 함께 켜두지 않으면, 백신의 기능들을 일시적으로 꺼버릴 수 있어요. 두 기능을 함께 사용해야 안전합니다.





비밀번호를 입력하지 않고 취소를 누르면, 로그 보관기간 설정 등 일부 메뉴만 볼 수 있고 변경은 할 수 없습니다.

## ② 환경 설정 잠금, 이런 효과가 있습니다

**환경 설정 잠금이란?**
비밀번호 없이는 백신의 설정을 끄거나 바꿀 수 없도록 잠가두는 기능입니다.

### ☣️ 백신 기능 OFF를 위한 접근 차단

- 바이러스가 임의로 백신 기능을 끄려는 시도를 차단

### ⚙️ 설정 변경엔 비밀번호가 필요

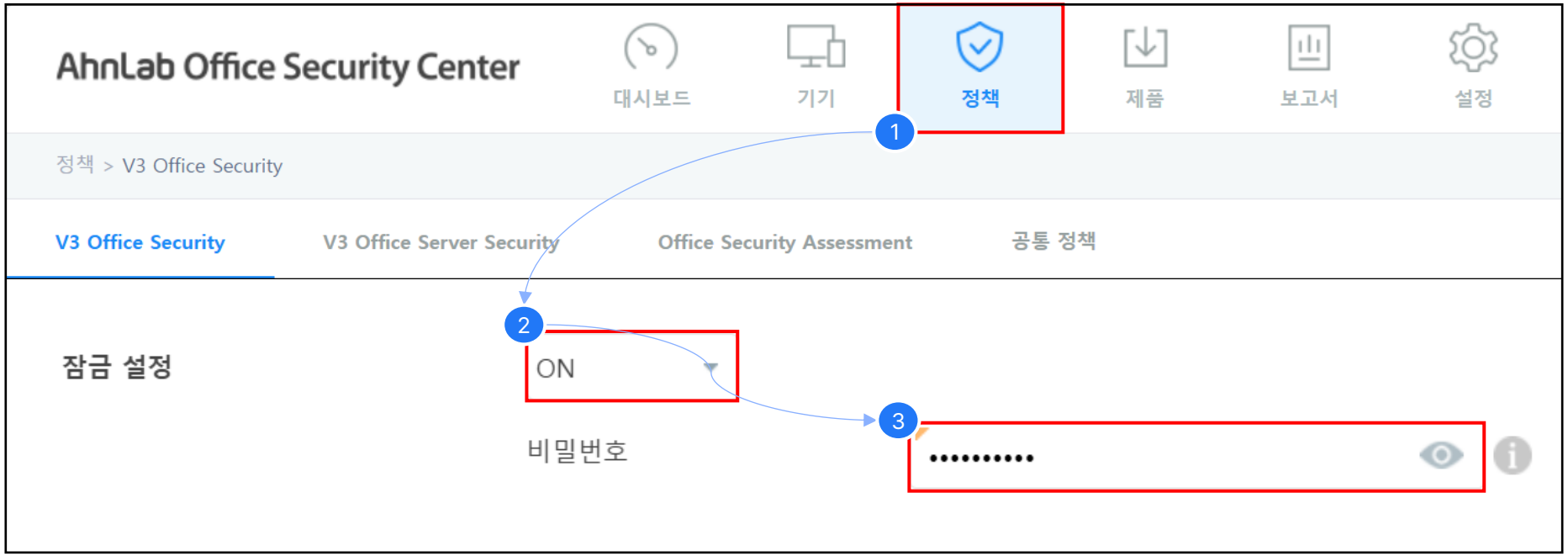
- 순간적으로 백신의 특정 기능을 OFF하는것을 방지
- 관리자가 정한 보호 수준이 그대로 유지

### 🔐 비밀번호는 안전하게 관리

- 잠금 비밀번호는 관리자가 보관
- 주기적으로 변경하며 관리

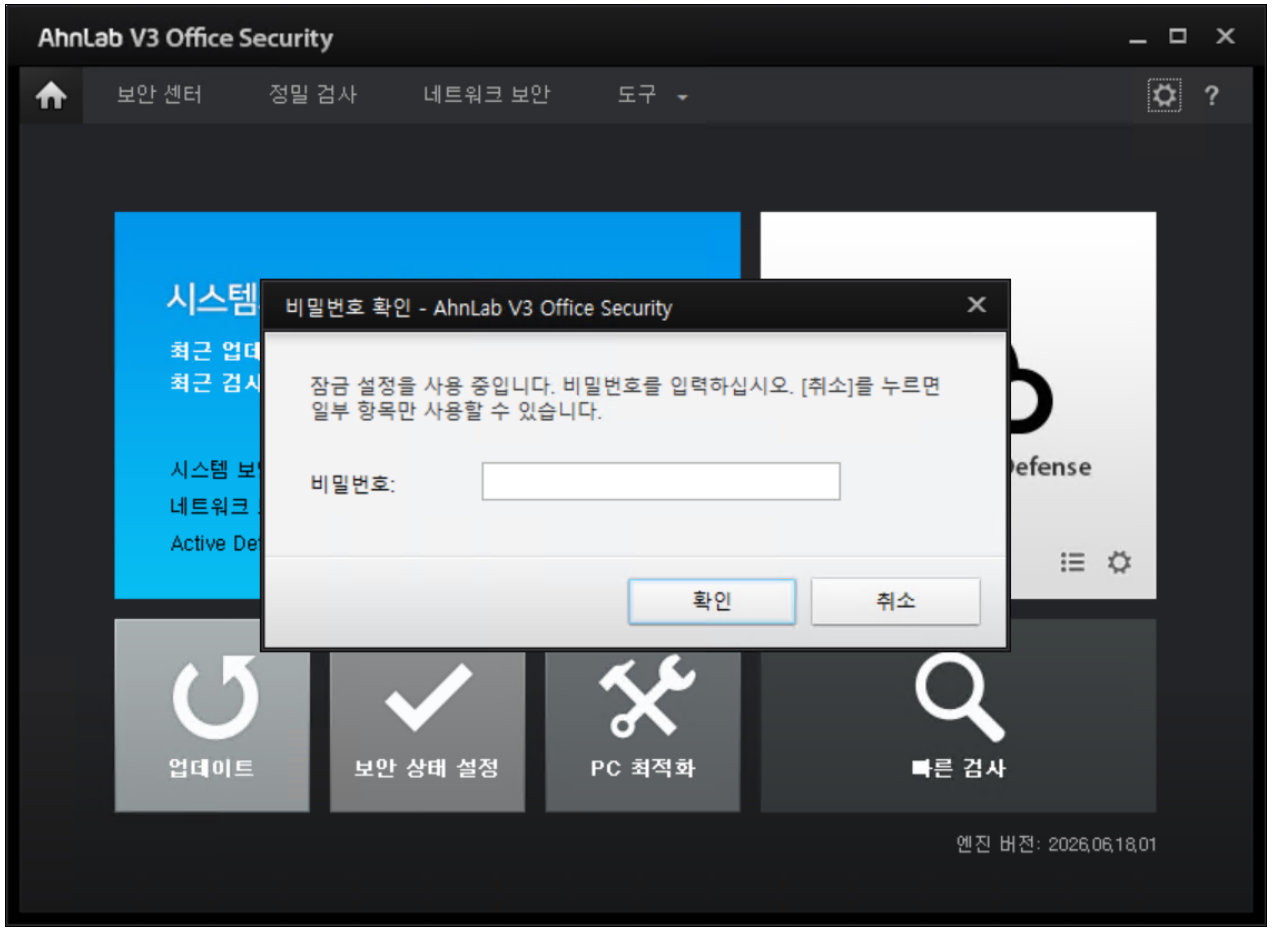
## ③ 환경 설정 잠금, 이렇게 설정하시면 됩니다

- ✓ 잠금설정을 사용으로 선택 한 뒤 비밀번호를 입력합니다.
- ✓ 비밀번호를 분실 했을 경우 우측의 눈동자 아이콘을 클릭하면 현재 설정 된 비밀번호를 확인 할 수 있습니다.



## ④ 설정 잠금 시 이렇게 동작합니다.

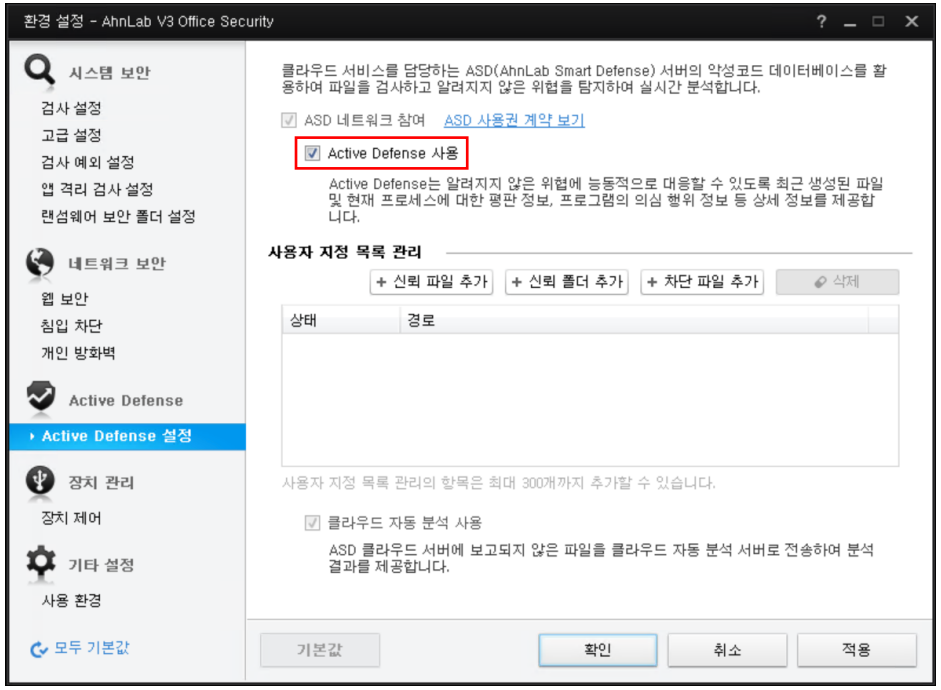
- ✓ 백신의 기능을 끄거나 설정을 바꾸려고 하면, 비밀번호 입력창이 먼저 나타납니다.
- ✓ 비밀번호를 모른다면 관리자에게 문의가 필요합니다. 설정 변경은 관리자를 통해서만 가능합니다.

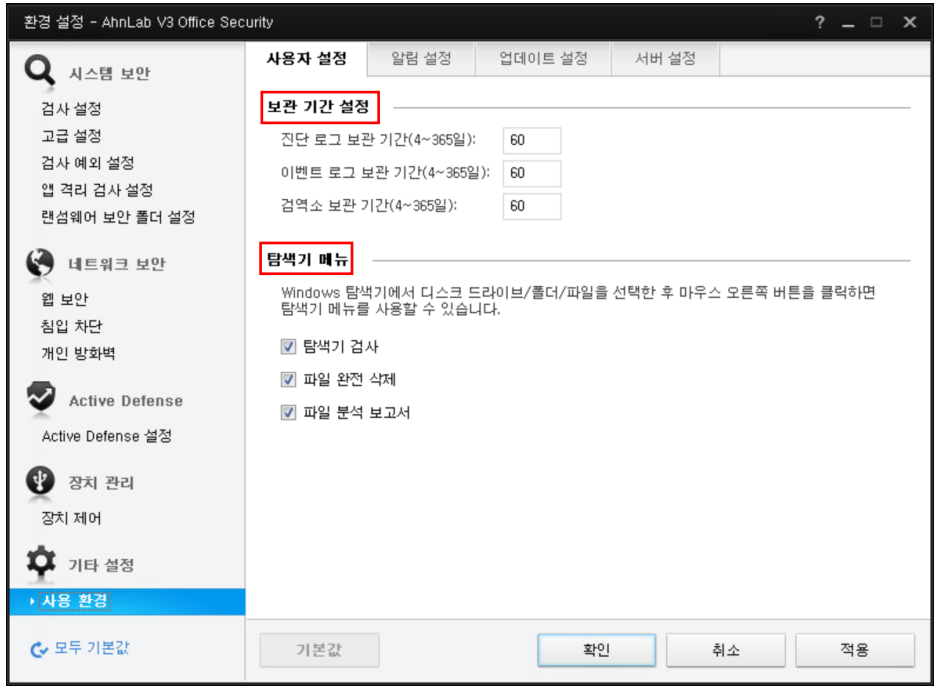


## ⑤ 잠금 설정을 해도 일부 항목은 허용됩니다

### 허용되는 항목

Active Defense, 보관기간, 탐색기 메뉴 – 탐색기 검사, 파일 완전 삭제, 파일 분석 보고서는 잠금 상태에서도 변경이 가능합니다.



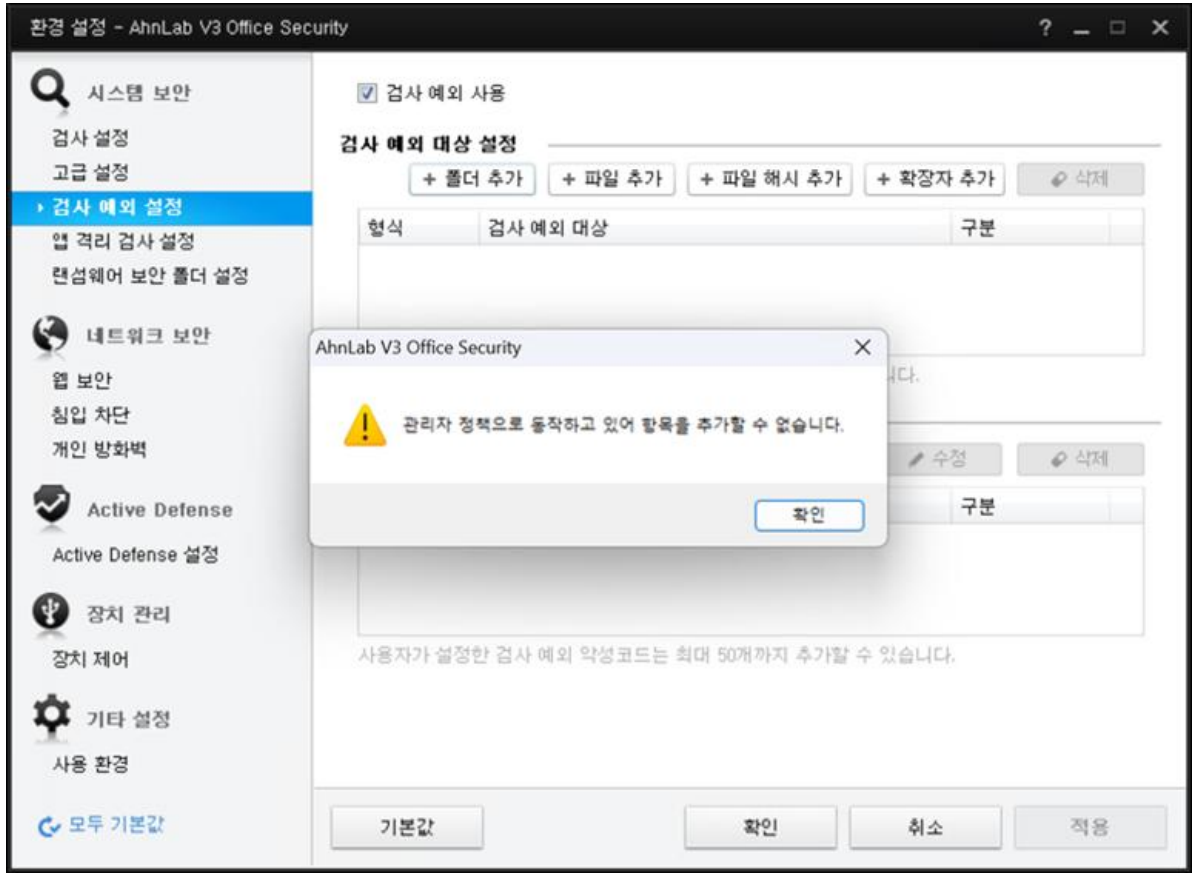




V3 환경 설정 제한 기능을 사용하더라도 일부 항목은 사용자가 수정이 가능하니 이를 참고하여 관리가 필요합니다.

## ① 검사 예외, 왜 필요할까요?

**? 업무용 프로그램 회사에서 '검사 예외로 등록해 달라'고 안내받았는데, 제가 직접 등록하려니 추가가 안 됩니다.**

- ✓ 기본적으로 검사 예외 정책은 관리자에 의해서 수정이 가능하게끔 설정 돼있습니다.
- ✓ 검사 예외가 필요할 시 사용자는 관리자에게 문의 후 수정이 필요합니다.



## ② 검사 예외, 이런 효과가 있습니다

**검사 예외란?**
신뢰할 수 있는 특정 파일이나 폴더를 바이러스 검사 대상에서 제외하는 기능입니다.

### 🔄 반복 검사를 줄여줍니다

- 자주 쓰는 프로그램을 매번 다시 검사하지 않습니다
- 검사 시간이 짧아지고 PC 속도가 빨라집니다

### 💻 프로그램이 실행을 막지 않습니다.

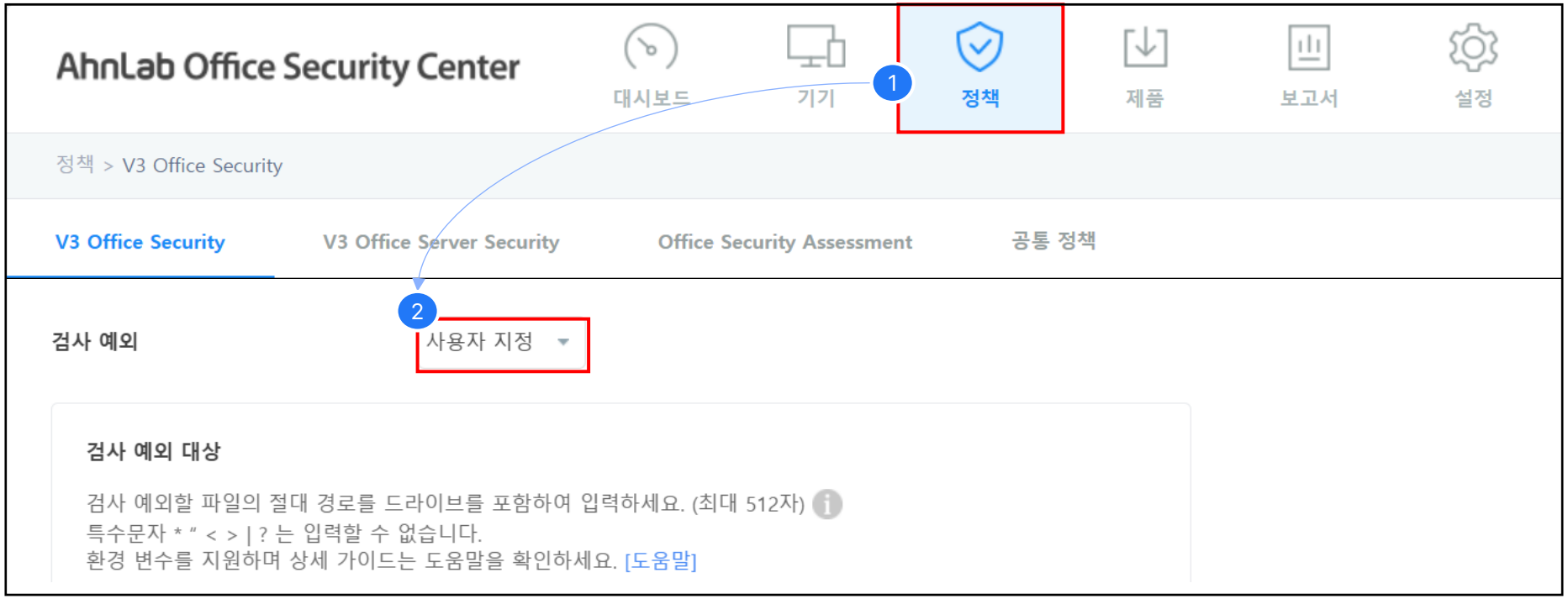
- 정상 프로그램이 악성코드로 잘못 인식되는 걸 막습니다
- 단, 과도한 사용은 보안 홀을 늘리므로 주의가 필요합니다.

### ⚠ 꼭 필요한 경우에만 등록!

- 예외로 등록한 경로는 검사하지 않습니다
- 너무 많이 등록하면 보호 기능이 약해질 수 있습니다

## ③ 검사 예외, 이렇게 설정하시면 됩니다

- ✓ 검사 예외 설정이 '**사용**'으로 설정되어 있으면, 예외 경로는 관리자만 등록할 수 있습니다.
- ✓ 직접 예외 경로를 등록하고 싶다면, 관리자에게 검사 예외 정책을 [사용자 정의]로 변경해 달라고 요청하면 됩니다.



## ④ 예외 대상 항목들

### 파일
특정 파일 하나를 정확한 경로로 지정해 예외 처리합니다
(예: C:\Program Files\회사프로그램\app.exe)

### 폴더
특정 폴더 안의 파일 전체를 예외 처리합니다
(윈도우 환경변수도 사용 가능 — 예: %ProgramData%)

### 확장자
특정 확장자를 가진 파일 전체를 예외 처리합니다
(단, exe·dll·ocx처럼 악성코드에 자주 쓰이는 확장자는 예외로 등록할 수 없습니다)

### 해시값(SHA-256)
특정 해시값을 가진 파일에 대해 예외 처리 합니다.
(특정 파일의 위치를 알 수 없는 경우 해시값을 참고하여 예외 처리 할 수 있습니다)

# 정책 복사 및 부서별 정책 적용

01 개별 정책 신규 생성

02 기존 정책 복사

03 권장 정책3 : 보안제품 삭제 방지 기능



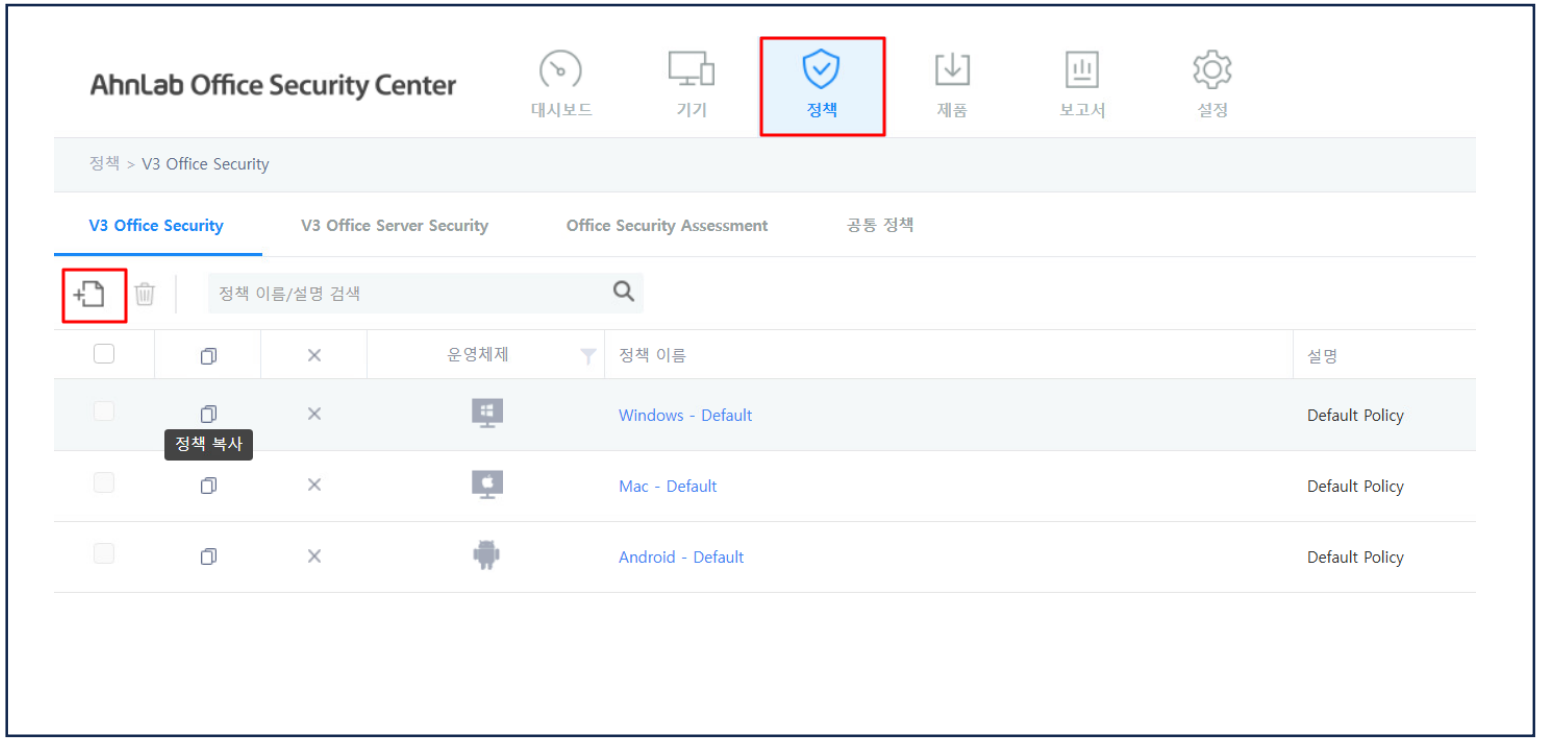
AhnLab

# 개별 그룹 정책 추가 – 신규 생성

## 신규 정책 생성

**장점:** 목적에 맞는 정책을 처음부터 설계하여 적용가능 / 불필요한 옵션 없이 깔끔하게 구성 가능

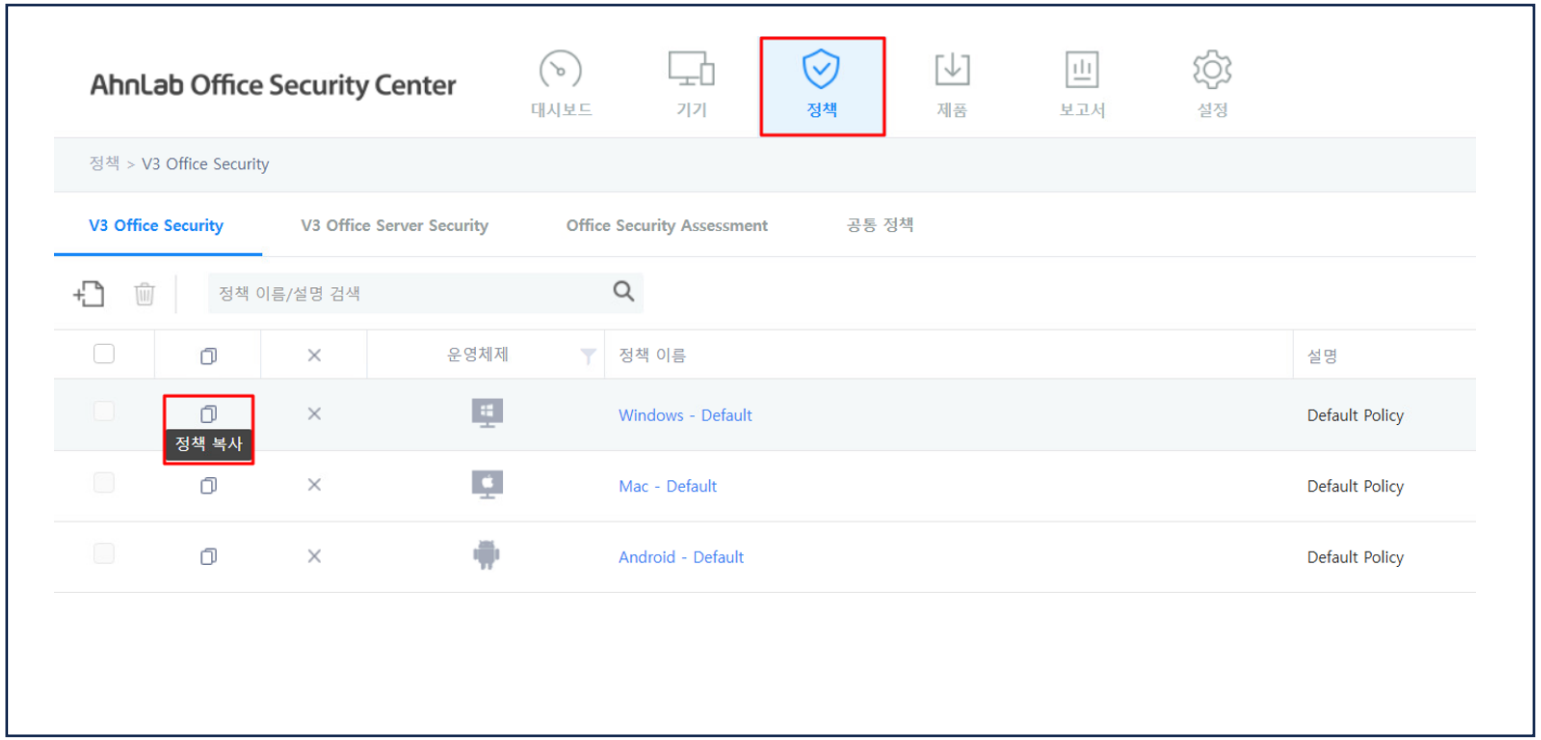
**유의:** 설정 항목이 많아 구성시간 소요 / 일부 보안 옵션 누락 시 보안 공백 발생가능성



# 개별 그룹 정책 추가 – 정책 복사

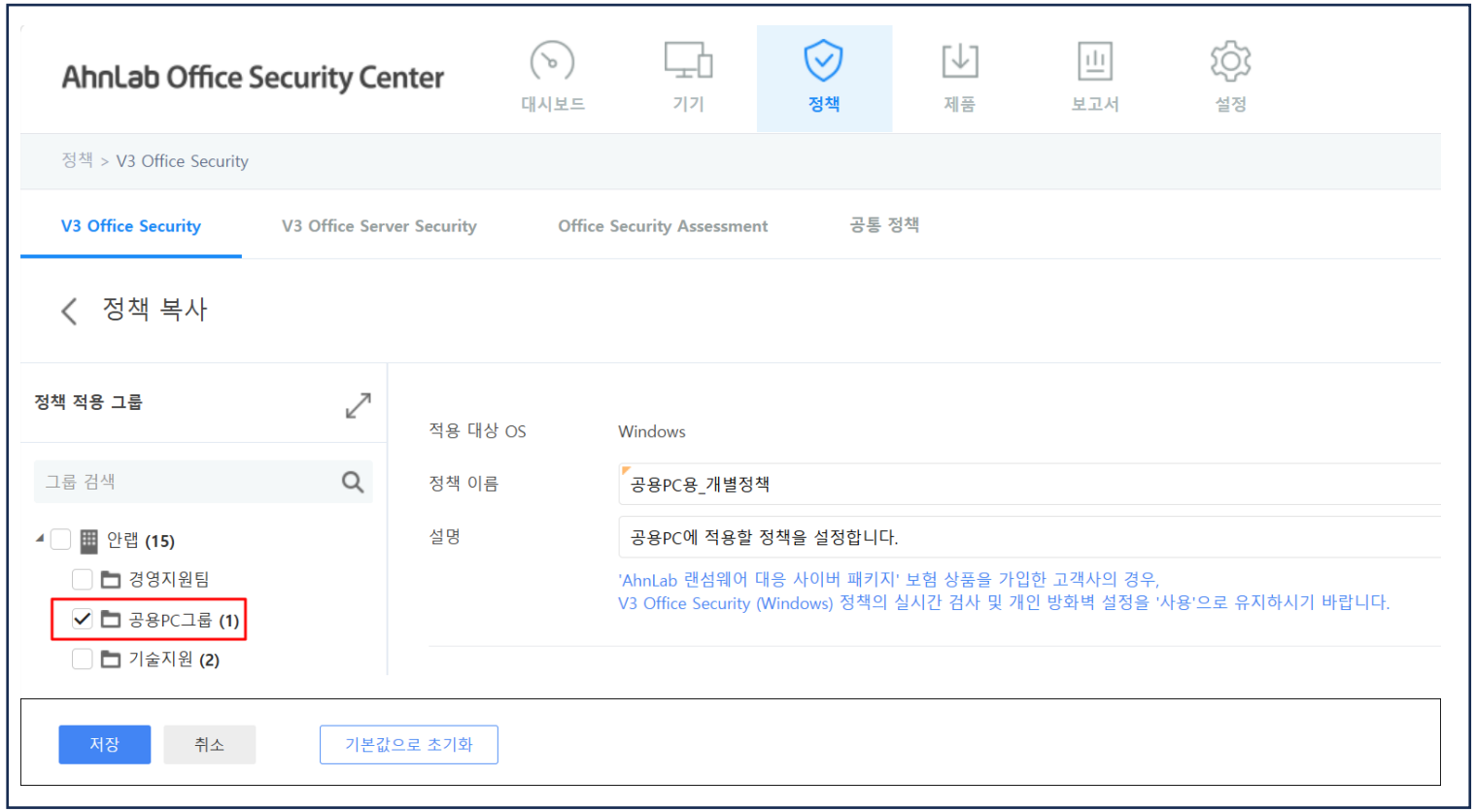
## 기존 정책 복사하여 정책 추가 (추천)

**장점:** 빠른 정책 생성 가능 / 이미 검증 된 설정을 그대로 활용하여 효율성 좋음
**유의:** 적용하려는 목적에 맞지 않는 불필요한 설정까지 함께 복사 될 가능성



## 생성 된 정책 적용 대상 선택

- ✓ 설정한 정책을 누구에게 적용 할 것인지?
- ✓ 정책을 적용 할 그룹을 선택하고 [저장] 합니다.
- ✓ 설정 된 정책은 정책 전달 주기(기본값 15분)에 마다 켜져 있는 PC에 정책을 전달 합니다.

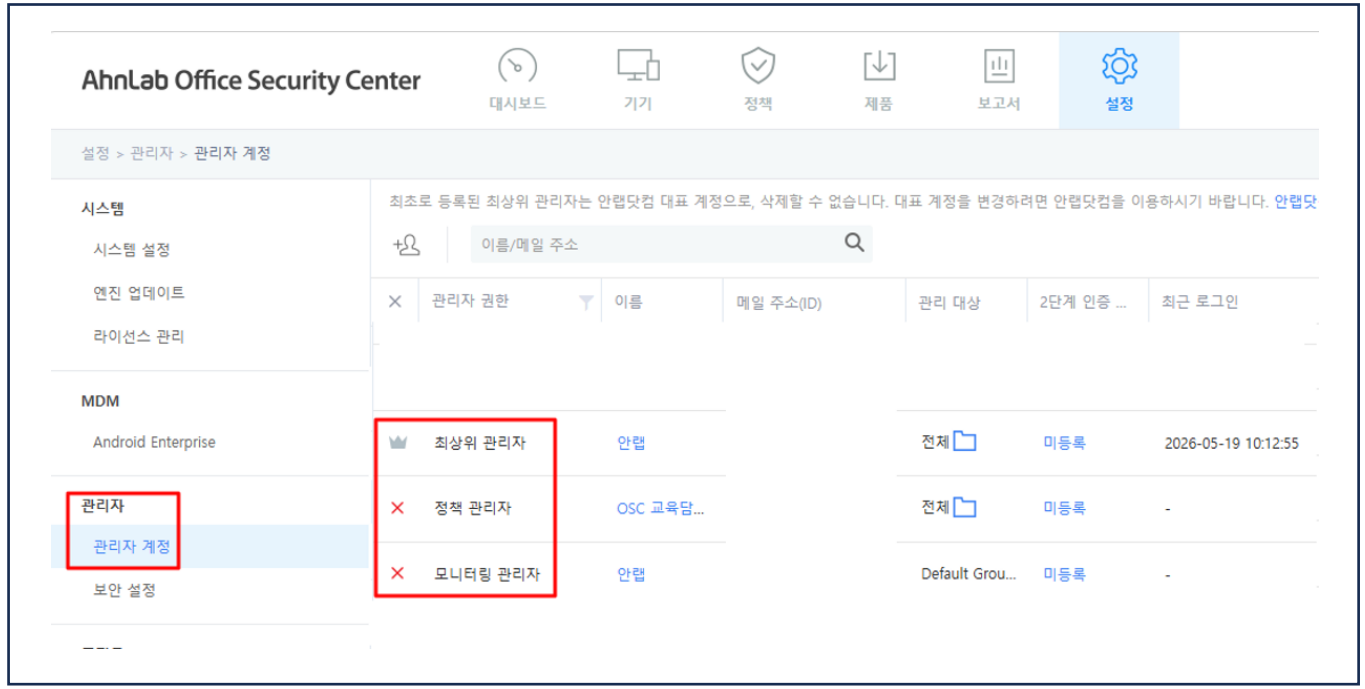


# 정책을 설정 할 수 있는 관리자

**최상위 관리자 :** 안랩닷컴 대표 계정으로 모든 권한을 보유합니다.
정책 수정 가능 여부 : O

**정책 관리자 :** 속한 그룹 또는 전체 그룹의 정책 설정 권한을 갖습니다.
정책 수정 가능 여부 : O

**모니터링 관리자 :** 속한 그룹 또는 전체 그룹의 사용현황 모니터링 기능을 제공합니다
정책 수정 가능 여부 : X



# 핵심 정리



AhnLab

# 마치며

1. '예약검사' 설정은 필수 권장 포인트(★)
2. 'V3 삭제 방지 기능 설정'을 통해 백신이 임의 삭제되지 않도록 설정
3. 'V3 환경 설정 방지 기능'을 통해 임의로 백신 기능 해제 방지
4. '검사 예외 설정'은 꼭 필요한 경우만 최소한으로
5. 개별정책을 추가하여 각 그룹별로 정책을 별도로 제공 할 수 있음
6. 정책은 최상위관리자 + 정책 관리자가 설정 가능(모니터링 관리자는 정책 변경 권한 없음)

# 보안 강화정책(부록)

01 악성 스크립트 진단(AMSI)

02 유해 가능 프로그램, 불필요한 프로그램(PUP)

03 개인 방화벽

04 압축 파일 검사

05 차단 사이트

06 Stable 엔진 사용



AhnLab

# 악성 스크립트 진단(AMSI)

**AMSI 악성 스크립트 차단 (권장 : 사용)**
요약 : AMSI는 눈에 보이지 않는 명령어(스크립트)를 실행할 때 악성 행위를 탐지하여 V3가 위협을 판단할 수 있도록 도와주는 기술입니다.

**✅ 장점 : 스크립트 기반 위협 대응 수준 강화**

- ✓ 파일 없이 몰래 실행되는 공격(파일리스 공격)도 잡아낼 수 있습니다
- ✓ 파일을 인질로 잡는 랜섬웨어처럼 눈에 안 보이는 방식의 공격을 막아줍니다
- ✓ 이메일 링크나 웹사이트를 통한 최신 공격에 더 잘 대응합니다

**⚠ 고려사항 : 오탐 여부 관련 사용자 문의 증가 가능성**

- 오피스 문서나 웹에서 사용하는 자동화 기능 실행 시 [확인] 창이 뜰 수 있습니다.
- 프로그램 개발 업무 시 일부 명령어 실행이 차단되어 불편할 수 있습니다.

# 유해 가능 프로그램, 불필요한 프로그램(PUP)

**유해 가능 프로그램, 불필요한 프로그램(PUP) (설정 : 사용)**
요약 : 바이러스는 아니지만 광고를 띄우거나 PC를 느리게 만드는 불필요한 프로그램을 차단하는 기능입니다.

### ✅ 장점 : 시스템 안정성 향상, 원치 않는 광고 팝업 차단 강화

- ✓ 허락 없이 내 PC를 원격으로 조종할 수 있는 프로그램을 미리 제거합니다
- ✓ 프로그램 설치 시 몰래 딸려오는 광고 프로그램을 제거합니다
- ✓ 쓸데없는 광고와 PC 자원을 낭비하는 프로그램을 차단하여 PC가 더 안정적으로 동작합니다

### ⚠ 고려사항 : 오탐 여부 관련 사용자 문의 증가 가능성 존재

- 일부러 설치한 프로그램이 위험하다고 잘못 판단될 수 있어 문의가 늘 수 있습니다
- 정상 프로그램에 딸려오는 부가 프로그램 설치가 막힐 수 있습니다

# 개인 방화벽 (Keyword : 개인 방화벽)

**개인 방화벽 (설정 : 사용)**

요약 : PC가 인터넷에서 주고받는 데이터를 감시하여 허가되지 않은 접근을 막아주는 보안 기능입니다. 윈도우 기본 방화벽보다 더 세밀하게 위협을 감지하고 차단합니다.

### ✅ 장점 : 프로그램 단위의 세세한 제어 기능을 제공

- ✓ PC 안팎으로 네트워크 연결을 시도하는 프로그램을 감시합니다
- ✓ 기본 방화벽보다 PC 안에서 실행되는 프로그램을 더 세밀하게 통제하고 기록합니다
- ✓ 수상한 통신이 발견되면 어떤 프로그램이 통신을 하는지 알려줍니다

### ⚠ 고려사항 : 방화벽 알림에서 '차단' 등록 시 네트워크 차단 가능성

- 실수로 정상 프로그램을 차단하면 해당 프로그램의 인터넷 접속이 막힙니다
- 잘 모르는 프로그램에 대해 허용할지 차단할지 문의가 늘 수 있습니다
- 실수로 차단한 프로그램을 다시 허용하는 방법 안내가 필요합니다

# 압축 파일 검사 (Keyword : 압축)

**압축 파일 (설정 : 사용)**
요약 : ZIP 같은 압축파일 안에 숨어있는 바이러스를 미리 찾아내어 실행 전에 차단하는 보안 기능입니다. 이중, 삼중으로 압축된 파일도 검사하도록 최대압축 2~3단계 검사를 권장합니다

## ✅ 장점 : 숨어있는 바이러스 사전 탐지

- ✓ 이메일 첨부파일이나 다운로드한 압축파일 속 숨은 바이러스를 찾아냅니다
- ✓ 실시간 검사가 꺼져 있을 때 들어온 바이러스도 발견할 수 있습니다
- ✓ 당장은 활동하지 않고 숨어있다가 나중에 실행되는 바이러스를 탐지합니다

## ⚠ 고려사항 : 압축을 풀면서 검사하기 때문에 PC가 잠시 느려질 수 있음

- 압축 해제 중 PC 성능이 일시적으로 떨어질 수 있습니다
- 여러 겹으로 압축된 파일은 검사 시간이 더 오래 걸릴 수 있습니다
- 비밀번호가 걸린 압축파일 / 너무 여러 겹으로 압축된 파일은 검사가 안 될 수도 있습니다

# 차단 사이트 – (Keyword : 차단 사이트)

**차단 사이트 (설정 : URL 등록)**
요약 : 바이러스 유포, 사기(피싱), 불법 사이트 등 위험한 웹사이트 접속을 미리 차단하여 PC 감염과 정보 유출을 예방하는 기능입니다

**✅ 장점 : 회사 차원에서 위험 사이트 접근을 일괄 차단**

- ✓ 바이러스가 많이 퍼지는 파일 공유 사이트를 차단합니다
- ✓ 출처를 알 수 없는 파일 다운로드를 차단합니다
- ✓ 실수로 위험한 링크를 클릭해도 접속이 차단되어 감염 사고를 줄여줍니다
- ✓ 회사 내부 문서가 외부로 유출되는 경로를 미리 차단합니다

**⚠ 고려사항 : 차단 해제 요청 및 예외 처리에 대한 운영 부담 증가**

- 일부 부서에서는 업무상 파일 공유 사이트가 필요할 수 있어 예외 처리가 필요합니다
- 정상적인 사이트가 잘못 차단되면 문의와 불만이 생길 수 있습니다

# 설정 – 엔진 업데이트 – Stable 엔진 사용 – (Keyword : Stable)

**Stable 엔진 사용 (설정 : 체크박스 체크)**
요약 : 충분히 테스트를 거친 안정적인 버전으로, 갑작스러운 변화 없이 안정적으로 동작하는 것에 중점을 둔 엔진입니다. 3일 전에 검증된 엔진이 제공됩니다

### ✅ 장점 : 운영 안정성 확보

- ✓ 업데이트로 인해 프로그램이 오작동하거나 충돌할 가능성이 줄어듭니다
- ✓ 충분히 검증된 방식을 사용하여 정상 파일을 바이러스로 잘못 잡는 경우가 줄어듭니다
- ✓ 보안도 중요하지만 업무 중단이 더 치명적인 환경에 적합합니다

### ⚠ 고려사항 : 신·변종 위협에 대한 초기 대응력은 상대적으로 낮을 수 있음

- 3일 전 엔진 제공으로 최신 위협 대응이 다소 늦을 수 있습니다
- 새로운 바이러스가 급증하면 최신 엔진보다 대응이 늦을 수 있습니다
- 새로운 위협이 급증할 때는 최신 엔진으로 전환을 검토해야 합니다

# More security, More freedom



AhnLab