

# Avira AntiVir Professional

사용자 매뉴얼

## 상표 및 저작권

### 상표

AntiVir 는 Avira GmbH 의 등록상표입니다.

Windows 는 미국 및 다른 나라에서 Microsoft Corporation 의 등록상표입니다.

다른 모든 브랜드 및 제품명은 해당 소유자의 상표 또는 등록상표입니다.

이 설명서에서는 보호되는 상표를 따로 표시하지 않습니다. 하지만 그렇다고 해서 그러한 상표를 마음대로 사용할 수 있는 것은 아닙니다.

### 저작권 정보

Avira AntiVir Professional 에는 타사에서 제공한 코드가 사용되었습니다.

그러한 코드를 사용할 수 있게 해준 저작권 소유자에게 감사드립니다. 저작권에 대한 자세한 내용은 Avira AntiVir Professional 도움말에서 타사 라이선스를 참조하십시오.

# 목차

<b>1</b>	<b>소개 .....</b>	<b>1</b>
<b>2</b>	<b>아이콘 및 강조 표시.....</b>	<b>2</b>
<b>3</b>	<b>제품 정보 .....</b>	<b>3</b>
3.1	배포 범위 .....	3
3.2	시스템 요구 사항.....	4
3.3	라이선스 및 업그레이드.....	4
3.3.1	라이선스 관리자.....	5
<b>4</b>	<b>설치 및 제거 .....</b>	<b>6</b>
4.1	설치.....	6
4.2	설치 변경 .....	10
4.3	설치 모듈.....	10
4.4	제거.....	12
4.5	네트워크에서 설치 및 제거.....	12
4.5.1	네트워크에서 설치.....	13
4.5.2	네트워크에서 제거.....	13
4.5.3	설치 프로그램용 명령줄 매개 변수.....	14
4.5.4	Setup.inf 파일의 매개 변수.....	15
<b>5</b>	<b>AntiVir Professional 개요.....</b>	<b>19</b>
5.1	사용자 인터페이스 및 작업.....	19
5.1.1	제어 센터 .....	19
5.1.2	구성 .....	21
5.1.3	트레이 아이콘.....	25
5.2	방법.....	26
5.2.1	라이선스 활성화.....	26
5.2.2	자동 업데이트 수행 .....	27
5.2.3	수동 업데이트 시작.....	28
5.2.4	온 디맨드 검사: 검사 프로필을 사용한 바이러스 및 맬웨어 검사.....	29
5.2.5	온 디맨드 검사: 끌어서 놓기를 사용한 바이러스 및 맬웨어 검사.....	30
5.2.6	온 디맨드 검사: 상황에 맞는 메뉴를 사용한 바이러스 및 맬웨어 검사 .....	31
5.2.7	온 디맨드 검사: 바이러스 및 맬웨어 자동 검사.....	31
5.2.8	온 디맨드 검사: 루트킷 및 활성화 맬웨어에 대한 대상 지정 검사.....	32
5.2.9	검색한 바이러스 및 맬웨어에 대응.....	33
5.2.10	격리: 격리된 파일(*.qua) 처리.....	37
5.2.11	격리: 격리 저장소의 파일 복원.....	38
5.2.12	격리: 의심스러운 파일을 격리 저장소로 이동.....	40
5.2.13	검사 프로필 검사 프로필의 파일 형식 수정 또는 삭제.....	40
5.2.14	검사 프로필 검사 프로필의 바탕 화면 바로 가기 만들기.....	40
5.2.15	이벤트: 이벤트 필터링.....	41
5.2.16	MailGuard: 검사에서 전자 메일 주소 제외 .....	41
5.2.17	FireWall: FireWall 의 보안 수준 선택.....	42

<b>6</b>	<b>검사 프로그램.....</b>	<b>44</b>
<b>7</b>	<b>업데이트.....</b>	<b>45</b>
<b>8</b>	<b>Avira FireWall :: 개요 .....</b>	<b>47</b>
<b>9</b>	<b>FAQ, 팁 .....</b>	<b>49</b>
9.1	문제 발생 시 도움말 .....	49
9.2	바로 가기 .....	53
9.2.1	대화 상자에서 .....	53
9.2.2	도움말에서 .....	54
9.2.3	제어 센터에서 .....	54
9.3	Windows 보안 센터 .....	56
9.3.1	일반 .....	56
9.3.2	Windows 보안 센터 및 AntiVir 프로그램 .....	56
<b>10</b>	<b>바이러스 및 기타.....</b>	<b>60</b>
10.1	확장된 위협 범주 .....	60
10.2	바이러스 및 기타 맬웨어.....	63
<b>11</b>	<b>정보 및 서비스.....</b>	<b>66</b>
11.1	연락처 주소.....	66
11.2	기술 지원.....	66
11.3	의심스러운 파일.....	67
11.4	가양성 보고.....	67
11.5	보안 강화를 위한 사용자 의견 보내기 .....	67
<b>12</b>	<b>참조: 구성 옵션.....</b>	<b>68</b>
12.1	검사 프로그램.....	68
12.1.1	검사 .....	68
12.1.1.1.	검색에 대한 작업 .....	71
12.1.1.2.	추가 작업 .....	74
12.1.1.3.	예외 .....	75
12.1.1.4.	추론 .....	76
12.1.2	신고 .....	77
12.2	Guard.....	78
12.2.1	검사 .....	78
12.2.1.1.	검색에 대한 작업 .....	80
12.2.1.2.	추가 작업 .....	83
12.2.1.3.	예외 .....	84
12.2.1.4.	추론 .....	88
12.2.2	ProActiv.....	89
12.2.2.1.	응용 프로그램 필터: 차단할 응용 프로그램.....	90
12.2.2.2.	응용 프로그램 필터: 허용된 응용 프로그램.....	90
12.2.3	신고 .....	91
12.3	MailGuard .....	92
12.3.1	검사 .....	93
12.3.1.1.	검색에 대한 작업 .....	94
12.3.1.2.	기타 작업 .....	96
12.3.1.3.	추론 .....	96

12.3.2	일반 .....	97
12.3.2.1.	예외 .....	97
12.3.2.2.	캐시 .....	98
12.3.2.3.	바닥글 .....	98
12.3.3	신고 .....	99
12.4	방화벽 .....	100
12.4.1	어댑터 규칙 .....	100
12.4.1.1.	들어오는 규칙 .....	102
12.4.1.2.	나가는 규칙 .....	110
12.4.2	응용 프로그램 규칙 .....	110
12.4.3	신뢰할 수 있는 공급자 .....	113
12.4.4	설정 .....	114
12.4.5	팝업 설정 .....	115
12.5	SMC 아래 방화벽 .....	117
12.5.1	일반 설정 .....	117
12.5.2	일반 어댑터 규칙 .....	118
12.5.2.1.	들어오는 규칙 .....	121
12.5.2.2.	나가는 규칙 .....	128
12.5.3	응용 프로그램 목록 .....	129
12.5.4	신뢰할 수 있는 공급자 .....	130
12.5.5	추가 설정 .....	130
12.5.6	표시 설정 .....	131
12.6	WebGuard .....	133
12.6.1	검사 .....	133
12.6.1.1.	검색에 대한 작업 .....	134
12.6.1.2.	잠긴 요청 .....	135
12.6.1.3.	예외 .....	137
12.6.1.4.	추론 .....	140
12.6.2	신고 .....	141
12.7	업데이트 .....	142
12.7.1	제품 업데이트 시작 .....	143
12.7.2	다시 시작 설정 .....	144
12.7.3	파일 서버 .....	145
12.8	일반 .....	146
12.8.1	이메일 .....	146
12.8.2	위협 범주 .....	147
12.8.3	암호 .....	148
12.8.4	보안 .....	150
12.8.5	WMI .....	151
12.8.6	디렉터리 .....	152
12.8.7	프록시 .....	153
12.8.8	경고 .....	153
12.8.8.1.	네트워크 .....	153
12.8.8.2.	전자 메일 .....	156
12.8.8.3.	음향 알림 .....	162
12.8.8.4.	경고 .....	162
12.8.9	이벤트 .....	163
12.8.10	보고서 제한 .....	163

# 1 소개

AntiVir 프로그램은 바이러스, 웜, 트로이 목마, 애드웨어와 스파이웨어 및 기타 위협으로부터 컴퓨터를 보호합니다. 이 설명서에서는 이러한 위협 요소를 바이러스 또는 맬웨어(유해 소프트웨어) 및 동의 없이 설치된 프로그램이라고 부릅니다.

또한 프로그램 설치 및 작업을 설명합니다.

그 밖의 옵션과 자세한 내용은 당사 웹 사이트를 참조하십시오.

<http://www.avira.kr>

Avira 웹 사이트에서 다음과 같은 혜택을 얻으실 수 있습니다.

- 다른 AntiVir 데스크톱 프로그램 관련 정보에 액세스
- 최신 AntiVir 데스크톱 프로그램 다운로드
- 최신 제품 설명서(PDF 형식) 다운로드
- 무료 지원 및 복구 도구 다운로드
- Avira 의 종합 기술 자료 및 문제 해결을 위한 FAQ 에 액세스
- 국가별 지원 연락처에 액세스

Avira 팀 드림

## 2 아이콘 및 강조 표시

다음 아이콘이 사용됩니다.

아이콘/지정	설명
✓	작업을 실행하기 전에 갖춰야 할 조건 앞에 표시됩니다.
▶	수행할 작업 단계 앞에 표시됩니다.
→	이전 작업 다음에 오는 이벤트 앞에 표시됩니다
경고	중요한 데이터 손실 위험에 대한 경고 앞에 표시됩니다.
참고	특히 중요한 정보에 대한 링크나 AntiVir 프로그램을 보다 손쉽게 사용할 수 있도록 도와주는 팁 앞에 표시됩니다.

다음 강조 표시가 사용됩니다.

강조 표시	설명
필기체	파일 이름 또는 경로 데이터
	표시되는 소프트웨어 인터페이스 요소(예: 창 제목, 창 필드 또는 옵션 상자)
굵게	클릭하는 소프트웨어 인터페이스 요소(예: 메뉴 항목, 섹션 또는 단추)

## 3 제품 정보

이 장에서는 AntiVir 제품의 구입 및 사용에 관한 모든 내용을 설명합니다.

- 참조: 배포 범위
- 참조: 시스템 요구 사항
- 참조: 라이선스
- 자세한 내용은

AntiVir 프로그램은 바이러스, 맬웨어, 사용자 동의 없이 설치된 프로그램 및 기타 위협으로부터 컴퓨터를 보호할 수 있는 포괄적이고 유연한 도구입니다.

▶ 다음 사항에 유의하십시오.

### 참고

대부분의 경우 중요한 데이터가 손실되면 막대한 결과가 초래됩니다. 가장 뛰어난 바이러스 차단 프로그램이라도 데이터 손실을 100% 막을 수는 없습니다. 따라서 보안을 유지하려면 정기적으로 데이터의 복사본(백업)을 만드십시오.

### 참고

프로그램이 바이러스, 맬웨어, 사용자 동의 없이 설치된 프로그램 및 기타 위협으로부터 효과적이고 안정적으로 보호하기 위해서는 최신 버전이어야 합니다. AntiVir 프로그램이 최신 버전으로 자동 업데이트되었는지 확인한 후 그에 따라 프로그램을 구성하십시오.

### 3.1 배포 범위

AntiVir 프로그램의 기능은 다음과 같습니다.

- 전체 프로그램을 모니터링, 관리하고 제어하는 제어 센터
- 사용하기 편리한 표준 및 고급 옵션 그리고 상황에 맞는 도움말을 이용하는 중앙 관리식 구성
- 알려진 모든 유형의 바이러스 및 맬웨어를 검사하는 검사 프로그램(온 디맨드 검사). 이 검사는 프로필을 통해 제어되며 구성 가능합니다.
- Windows Vista 사용자 계정 제어와 통합할 경우, 관리 권한이 필요한 작업을 수행할 수 있습니다.
- 모든 파일 액세스 시도를 지속적으로 모니터링하는 Guard(온 액세스 검사)
- 프로그램 작업을 영구적으로 모니터링하는 ProActiv 구성 요소(32 비트 시스템에만 해당되며, Windows 2000에서는 사용할 수 없음)
- 전자 메일 바이러스 및 맬웨어를 지속적으로 검사하는 MailGuard(POP3 검사 프로그램, IMAP 검사 프로그램 및 SMTP 검사 프로그램). 전자 메일 첨부 파일 검사가 포함됩니다.
- 인터넷에서 HTTP 프로토콜을 사용하여 전송된 데이터 및 파일을 모니터링하는 WebGuard(80, 8080, 3128 번 포트 모니터링)



- 통합 격리 저장소 관리로 의심스러운 파일 격리 및 처리
- 루트킷 차단 기능으로 컴퓨터 시스템에 설치된 숨겨진 맬웨어(루트킷) 검색  
Windows XP 64 비트에서는 사용할 수 없습니다.
- 검색된 바이러스 및 맬웨어에 대한 자세한 정보를 인터넷을 통해 직접 확인
- 인터넷 웹 서버 또는 인트라넷을 이용하는 단일 파일 업데이트 및 증분형 VDF  
업데이트에서 간단하고 신속하게 프로그램, 바이러스 정의 및 검색 엔진  
업데이트
- 편리하게 라이선스를 관리할 수 있는 라이선스 관리자
- 일회성 또는 되풀이 작업(예: 업데이트, 검사)을 계획할 수 있는 통합형  
스케줄러
- 추론 검사 방법을 비롯한 혁신적인 검사 기술(검사 엔진)을 통해 바이러스 및  
맬웨어에 대해 매우 높은 검색률 달성
- 중첩된 보관 검색 및 스마트 확장명 검색을 비롯한 모든 일반 보관 유형 검색
- 여러 개의 파일을 동시에 고속 검사하는 고성능 멀티스레딩 기능
- 인터넷 또는 다른 네트워크를 통한 무단 액세스 및 허가받지 않은 사용자의  
인터넷/네트워크 무단 액세스로부터 컴퓨터를 보호하는 Avira FireWall

### 3.2 시스템 요구 사항

시스템 요구 사항은 다음과 같습니다.

- Pentium 급 이상 컴퓨터(266MHz 이상)
- 운영 체제
- Windows XP, SP2(32 비트 또는 64 비트) 또는
- Windows Vista(32 비트 또는 64 비트, SP 1)
- Windows 7(32 비트 또는 64 비트)
- 150MB 이상의 하드 디스크 여유 공간(임시 보관을 위한 격리 저장소를  
사용할 경우 더 많은 공간 필요)
- Windows XP 의 경우 256MB 이상의 RAM
- Windows Vista, Windows 7 의 경우 1024MB 이상의 RAM
- 프로그램 설치: 관리자 권한 필요
- 모든 설치 공통: Windows Internet Explorer 6.0 이상 필요
- 인터넷 연결(설치 참조)

### 3.3 라이선스 및 업그레이드

AntiVir 제품을 사용하려면 라이선스가 필요합니다. 즉 사용권 계약에 동의해야  
합니다.

라이선스는 hbedv.key 파일 형태의 디지털 라이선스 코드를 통해 발행됩니다. 이 디지털 라이선스 코드는 개인 라이선스의 키 역할을 하며 여기에는 사용 가능한 프로그램 및 그 사용 기간에 대한 정확한 세부 정보가 포함되어 있습니다. 따라서 디지털 라이선스 코드는 둘 이상의 제품에 대한 라이선스도 포함할 수 있습니다.

인터넷 또는 프로그램 CD/DVD 를 통해 AntiVir 프로그램을 구입한 경우 전자 메일을 통해 디지털 라이선스 코드가 제공됩니다. 설치 과정에서 라이선스 키를 로드하거나 나중에 라이선스 관리자에서 설치할 수 있습니다.

### 3.3.1 라이선스 관리자

Avira AntiVir Professional 라이선스 관리자를 사용하면 Avira AntiVir Professional 라이선스를 매우 간단하게 설치할 수 있습니다.

#### Avira AntiVir Professional 라이선스 관리자



파일 관리자 또는 정품 인증 전자 메일에서 라이선스 파일을 두 번 클릭하여 선택하고 화면의 안내에 따라 라이선스를 설치할 수 있습니다.

#### 참고

Avira AntiVir Professional 라이선스 관리자는 해당 제품 폴더에 라이선스 파일을 자동으로 복사합니다. 라이선스가 이미 있는 경우 기존 라이선스 파일 대체 여부에 관한 메시지가 나타납니다. 이 경우 기존 파일을 새 라이선스 파일로 덮어씁니다.

## 4 설치 및 제거

이 장에서는 AntiVir 프로그램의 설치 및 제거에 관해 설명합니다.

- 참조: 설치: 조건, 설치 유형, 설치
- 참조: 설치 모듈
- 참조: 수정 설치
- 네트워크에서 설치 및 제거
- 참조: 제거: 제거

### 4.1 설치

설치하기 전에 해당 컴퓨터가 최소 시스템 요구 사항을 만족하는지 확인하십시오. 컴퓨터가 모든 요구 사항을 만족해야 AntiVir 프로그램을 설치할 수 있습니다.

#### 참고

설치 과정에서 복원 지점을 만들 수 있습니다. 복원 지점은 운영 체제를 설치 전 상태로 되돌리기 위해 만드는 것입니다. 그렇게 하려면 해당 운영 체제에서 복원 지점을 만들 수 있는지 확인해야 합니다.

Windows XP: 시스템 속성 -> 시스템 복원: **시스템 복원 사용 안 함** 옵션을 사용하지 않도록 설정합니다.

Windows Vista/Windows 7: 시스템 속성 -> 컴퓨터 보호: **보호 설정** 영역에서 해당 시스템이 설치된 드라이브를 강조 표시하고 **구성** 단추를 클릭합니다. **시스템 보호** 창에서 **시스템 설정 및 이전 파일 버전 복원** 옵션을 사용하도록 설정합니다.

#### 설치 유형

설치하는 동안 설치 마법사에서 설치 유형을 선택할 수 있습니다.

#### 빠른 설치

- 일부 프로그램 구성 요소는 설치되지 않습니다. 설치되지 않는 구성 요소는 다음과 같습니다.

Avira AntiVir ProActiv

Avira FireWall

- C:\Program Files 아래의 지정된 기본 폴더에 프로그램 파일이 설치됩니다.
- AntiVir 프로그램이 기본 설정으로 설치됩니다. 구성 마법사를 사용하여 사용자 지정 설정을 정의할 수 있습니다.

#### 사용자 정의

- 개별 프로그램 구성 요소를 설치하도록 선택할 수 있습니다(설치 및 제거::설치 모듈 장 참조).
- 프로그램 파일이 설치된 대상 폴더를 선택할 수 있습니다.

- 바탕 화면 아이콘 및 시작 메뉴 프로그램 그룹 만들기 옵션의 선택을 취소할 수 있습니다.
- 구성 마법사를 사용하여 AntiVir 프로그램에 대한 사용자 지정 설정을 정의하고 설치 후 자동으로 수행되는 간단한 시스템 검사를 시작할 수 있습니다.

### 설치를 시작하기 전에

- ▶ 전자 메일 프로그램을 닫습니다. 실행 중인 응용 프로그램을 모두 종료하는 것이 좋습니다.
- ▶ 다른 어떤 바이러스 백신 솔루션도 설치되지 않았어야 합니다. 여러 보안 솔루션의 자동 보호 기능이 서로 충돌할 수 있습니다.
- ▶ 인터넷 연결을 설정합니다. 다음 설치 단계를 수행하려면 인터넷 연결이 필요합니다.
- ▶ 설치 프로그램을 통해 최신 프로그램 파일, 검사 엔진 및 최신 바이러스 정의 파일 다운로드(인터넷 기반 설치)
- ▶ 해당하는 경우, 설치 완료 후 업데이트 수행
- ▶ AntiVir 프로그램의 정품 인증을 받으려면 라이선스 파일인 hbedv.key를 컴퓨터 시스템에 저장합니다.

### 참고

인터넷 기반 설치:

Avira GmbH 웹 서버에서는 인터넷 기반의 프로그램 설치를 위해 설치에 앞서 최신 프로그램 파일을 로드하는 설치 프로그램을 제공합니다. 그러면 AntiVir 프로그램이 최신 바이러스 정의 파일과 함께 설치됩니다.

설치 패키지로 설치:

설치 패키지에는 설치 프로그램 및 필요한 모든 프로그램 파일이 모두 포함되어 있습니다. 설치 패키지로 설치할 때는 AntiVir 프로그램의 언어를 선택할 수 없습니다. 설치 후에 바이러스 정의 파일을 업데이트하는 것이 좋습니다.

### 설치

설치 프로그램은 설명이 따로 필요 없는 대화 상자 모드로 실행됩니다. 모든 창에는 설치 프로세스를 제어하는 특정 단추들이 포함되어 있습니다.

대표적인 단추는 다음과 같습니다.

- **확인:** 작업을 확인합니다.
- **중단:** 작업을 중단합니다.
- **다음:** 다음 단계로 이동합니다.
- **뒤로:** 이전 단계로 이동합니다.

AntiVir 프로그램 설치:

### 참고

Windows 방화벽을 사용하지 않도록 설정하는 다음 작업은 Windows XP 운영 체제에만 적용됩니다.

- ▶ 인터넷에서 다운로드한 설치 파일을 두 번 클릭하여 설치 프로그램을 시작하거나 프로그램 CD를 넣습니다.

### 인터넷 기반 설치

시작... 대화 상자가 나타납니다.

- ▶ 다음을 클릭하여 설치를 계속합니다.

언어 선택 대화 상자가 나타납니다.

- ▶ AntiVir 프로그램 설치에 사용할 언어를 선택하고 다음을 클릭하여 선택한 언어를 확인합니다.

다운로드 대화 상자가 나타납니다. Avira GmbH 웹 서버에서 설치에 필요한 모든 파일을 다운로드합니다. 다운로드가 끝나면 다운로드 창이 닫힙니다.

### 설치 패키지로 설치

Avira AntiVir Professional 대화 상자와 함께 설치 마법사가 열립니다.

- ▶ 설치를 시작하려면 동의를 클릭합니다.

설치 파일이 추출됩니다. 설치 루틴이 시작합니다.

시작... 대화 상자가 나타납니다.

- ▶ 다음을 클릭합니다.

### 인터넷 기반 설치 및 설치 패키지를 사용한 설치 계속

라이선스 계약 대화 상자가 나타납니다.

- ▶ 라이선스 계약에 동의함을 확인하고 다음을 클릭합니다.

일련 번호 생성 대화 상자가 나타납니다.

- ▶ 필요한 경우 업그레이드 과정에서 임의의 일련 번호가 생성되어 전송되었는지 확인하고 다음을 클릭합니다.

설치 유형 선택 대화 상자가 나타납니다.

- ▶ 빠른 설치 또는 사용자 정의 옵션을 사용하도록 설정합니다. 복원 지점을 만들려면 시스템 복원 지점 만들기 옵션을 사용하도록 설정합니다. 다음을 클릭하여 설정을 확인합니다.

### 사용자 정의 설치

대상 디렉터리 선택 대화 상자가 나타납니다.

- ▶ 다음을 클릭하여 지정된 대상 디렉터리를 확인합니다.

또는

찾아보기 단추를 사용하여 다른 디렉터리를 선택하고 다음을 클릭하여 확인합니다.

구성 요소 설치 대화 상자가 나타납니다.

- ▶ 필요한 구성 요소를 사용 또는 사용 안 함으로 설정하고 다음을 클릭하여 확인합니다.

ProActiv 구성 요소를 설치하도록 선택한 경우 *AntiVir ProActiv 커뮤니티* 창이 나타납니다. Avira AntiVir ProActiv 커뮤니티 참여를 확인하는 옵션이 있습니다. 이 옵션을 사용하도록 설정하는 경우, Avira AntiVir ProActiv는 ProActiv 구성 요소에 의해 발견된 의심스러운 프로그램에 대한 데이터를 Avira 맬웨어 연구 센터로 보냅니다. 이 데이터는 고급 온라인 검사 및 검색 기술의 확장과 정련에만 사용됩니다. 추가 정보 링크를 사용하여 고급 온라인 검사에 대해 자세히 알아볼 수 있습니다.

- ▶ AntiVir ProActiv 커뮤니티 참여를 사용 또는 사용 안 함으로 설정하고 다음을 클릭하여 확인합니다.

다음 대화 상자에서는 바탕 화면 바로 가기 및/또는 시작 메뉴의 프로그램 그룹을 만들 것인지 선택할 수 있습니다.

- ▶ 다음을 클릭합니다.

**다시 시작: 빠른 설치 및 사용자 정의 설치를 계속합니다.**

라이선스 설치대화 상자가 나타납니다.

- ▶ 라이선스 파일을 저장한 디렉터리로 이동한 후 대화 상자의 메시지를 읽고 다음을 클릭하여 확인합니다.

라이선스 파일이 복사되며 구성 요소가 설치되고 시작됩니다.

다음 대화 상자에서는 설치가 완료된 후 추가 정보 파일을 열 것인지, 그리고 컴퓨터를 다시 시작할 것인지를 선택할 수 있습니다.

- ▶ 필요한 경우 동의한 다음 *마침*을 클릭하여 설치를 완료합니다.

설치 마법사가 닫힙니다.

**다시 시작: 사용자 정의 설치 구성 마법사**

사용자 정의 설치를 선택한 경우 다음 단계에서 구성 마법사가 열립니다. 구성 마법사에서는 AntiVir 프로그램의 사용자 지정 설정을 정의할 수 있습니다.

- ▶ 구성 마법사의 시작 창에서 다음을 클릭하여 프로그램 구성을 시작합니다.

AHeAD 구성대화 상자에서는 AHeAD 기술의 검색 수준을 선택할 수 있습니다. 선택한 검색 수준은 검사 프로그램(온 디맨드 검사) 및 Guard(온 액세스 검사) AHeAD 기술 설정에 사용됩니다.

- ▶ 검색 수준을 선택하고 다음을 클릭하여 설치를 계속합니다.

이어지는 *확장된 위협 범주 선택* 대화 상자에서는 지정된 위협 범주에 맞게 AntiVir 프로그램의 보호 기능을 변경할 수 있습니다.

- ▶ 추가 위협 범주를 활성화하고 다음을 클릭하여 설치를 계속합니다.

AntiVir FireWall 설치 모듈을 선택한 경우 *FireWall 보안 수준* 대화 상자가 나타납니다. Avira FireWall에서 활성화된 리소스에 대한 외부 액세스 및 신뢰할 수 있는 기업의 응용 프로그램에 의한 네트워크 액세스를 허용할 것인지 정의할 수 있습니다.

- ▶ 필요한 옵션을 사용하도록 설정하고 다음을 클릭하여 구성을 계속합니다.

AntiVir Guard 설치 모듈을 선택한 경우 *Guard 시작 모드* 대화 상자가 나타납니다. Guard 시작 시간을 지정할 수 있습니다. 그러면 컴퓨터가 다시 부팅될 때마다 Guard가 지정된 시작 모드로 시작합니다.

## 참고

지정된 Guard 시작 모드는 레지스트리에 저장되며 구성을 통해 변경할 수 없습니다.

- ▶ 필요한 옵션을 사용하도록 설정하고 다음을 클릭하여 구성을 계속합니다.

이어지는 *전자 메일 설정 선택* 대화 상자에서는 전자 메일을 보내기 위한 서버 설정을 정의할 수 있습니다. AntiVir 프로그램은 SMTP를 사용하여 전자 메일을 보내고, 전자 메일 알람을 보냅니다.

- ▶ 필요에 따라 서버 설정을 조정하고 다음을 클릭하여 구성을 계속합니다.

이어지는 *시스템 검사* 대화 상자에서는 기본 시스템 검사를 사용 또는 사용 안

함으로 설정할 수 있습니다. 기본 시스템 검사는 구성이 완료된 후 및 컴퓨터가 다시 부팅되기 전에 실행되며, 실행 중인 프로그램 및 가장 중요한 시스템 파일을 대상으로 바이러스와 맬웨어를 검사합니다.

- ▶ **기본 시스템 검사** 옵션을 사용하거나 사용 안 함으로 설정하고 다음을 클릭하여 구성을 계속합니다.

다음 대화 상자에서는 **마침**을 클릭하여 구성을 완료할 수 있습니다.

- ▶ **마침**을 클릭하여 구성을 완료합니다.

지정하고 선택한 설정이 적용됩니다.

**기본 시스템 검사** 옵션을 사용하도록 설정한 경우 **Luke Filewalker** 창이 표시됩니다. 검사 프로그램에서 기본 시스템 검사를 수행합니다.

**다시 시작: 빠른 설치 및 사용자 정의 설치를 계속합니다.**

마지막 설치 마법사에서 **컴퓨터 다시 시작** 옵션을 선택한 경우 컴퓨터가 다시 부팅됩니다.

설치 마법사에서 **Readme.txt 표시** 옵션을 선택한 경우, 컴퓨터가 다시 시작된 후 **Readme** 파일이 표시됩니다.

설치가 완료되었으면 제어 센터의 **개요::상태**에서 최신 프로그램인지 확인하는 것이 좋습니다.

- ▶ 필요한 경우 바이러스 정의 파일을 최신 버전으로 업데이트합니다.
- ▶ 그런 다음 전체 시스템 검사를 수행합니다.

## 4.2 설치 변경

현재 설치된 **AntiVir** 프로그램의 개별 구성 요소를 추가하거나 제거할 수 있습니다. 설치 및 제거::설치 모듈 장을 참조하십시오.

현재 설치된 모듈을 추가하거나 제거하려는 경우 **Windows 제어판의 프로그램 추가/제거** 옵션을 사용하여 프로그램을 **변경/제거**할 수 있습니다.

**AntiVir** 프로그램을 선택하고 **변경**을 클릭합니다. 프로그램의 시작 대화 상자에서 **수정** 옵션을 선택합니다. 설치 변경 지침이 표시됩니다.

## 4.3 설치 모듈

사용자 정의 설치 또는 변경 설치에서는 다음 설치 모듈을 선택, 추가하거나 제거할 수 있습니다.

- **AntiVir Professional**

이 모듈에는 **AntiVir** 프로그램을 성공적으로 설치하는 데 필요한 모든 구성 요소가 들어 있습니다.

– **AntiVir Guard**

AntiVir Guard 는 백그라운드에서 실행됩니다. 이 프로그램은 온 액세스 모드에서 열기, 쓰기 및 복사와 같은 작업을 수행하는 동안 파일을 모니터링하고 복구합니다. 사용자가 파일 작업(예: 문서 로드, 실행, 복사)을 수행할 때마다 AntiVir 프로그램은 해당 파일을 자동으로 검사합니다. 파일 이름을 바꾸면 AntiVir Guard 에서 검사를 시작하지 않습니다.

– **AntiVir ProActiv**

ProActiv 구성 요소는 응용 프로그램 작업을 모니터링하며 의심스러운 응용 프로그램 동작을 사용자에게 알립니다. 이러한 동작 기반 인식을 통해 알 수 없는 맬웨어로부터 보호할 수 있습니다. ProActiv 구성 요소는 AntiVir Guard 에 통합되어 있습니다.

– **AntiVir MailGuard**

MailGuard 는 사용자의 컴퓨터와 해당 전자 메일 프로그램(메일 클라이언트)에서 전자 메일을 다운로드하는 전자 메일 서버 간의 인터페이스입니다. MailGuard 는 전자 메일 프로그램과 전자 메일 서버 간의 프록시 역할로 연결됩니다. 받는 전자 메일은 모두 이 프록시를 통해 라우팅되고 바이러스 및 사용자 동의 없이 설치된 프로그램 검사를 받은 다음 전자 메일 프로그램으로 전달됩니다. 구성에 따라 이 프로그램은 해당 전자 메일을 자동으로 처리하거나 사용자에게 어떤 작업을 수행할 것인지 묻습니다.

– **AntiVir WebGuard**

인터넷을 서핑할 때 사용자는 웹 브라우저를 사용하여 웹 서버로부터 데이터를 요청하게 됩니다. 일반적으로 웹 서버로부터 전송된 데이터(HTML 파일, 스크립트 및 이미지 파일, Flash 파일, 비디오 및 음악 스트림 등)는 브라우저 캐시로 이동한 다음 웹 브라우저에 표시됩니다. 따라서 AntiVir Guard 에서 수행하는 것과 같은 온 액세스 검사가 가능하지 않습니다. 그러면 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. WebGuard 는 데이터 전송에 사용되는 포트(80, 8080, 3128)를 모니터링하고 전송된 데이터에서 바이러스 및 사용자 동의 없이 설치된 프로그램을 검사하는 HTTP 프록시입니다. 구성에 따라 이 프로그램은 해당 파일을 자동으로 처리하거나 사용자에게 어떤 작업을 수행할 것인지 묻습니다.

– **Avira FireWall:**

Avira FireWall 은 컴퓨터와의 통신을 제어합니다. 보안 정책에 따라 통신을 허용하거나 거부합니다.

– **루트킷 검색**

루트킷 검색에서는 컴퓨터 시스템에 침투하면 기존의 맬웨어 차단 방법으로는 더 이상 찾아낼 수 없는 소프트웨어가 컴퓨터에 설치되었는지 여부를 확인합니다.

– **셸 확장**

셸 확장은 Windows 탐색기의 상황에 맞는 메뉴(마우스 오른쪽 단추 클릭)에 'AntiVir 를 사용하여 선택한 파일 검사' 항목을 생성합니다. 항목이 있으면 사용자가 파일 또는 디렉터리를 직접 검사할 수 있습니다.



## 4.4 제거

컴퓨터에서 AntiVir 프로그램을 제거하려는 경우 Windows 제어판에서 **프로그램 추가/제거** 옵션을 사용하여 프로그램을 **변경/제거**할 수 있습니다.

AntiVir 프로그램 제거(예: Windows XP 및 Windows Vista 에서):

- ▶ Windows 시작 메뉴에서 **제어판**을 엽니다.
- ▶ **프로그램**(Windows XP: **소프트웨어**)을 두 번 클릭합니다.
- ▶ 목록에서 AntiVir 프로그램을 선택하고 **제거**를 클릭합니다.  
프로그램을 제거할 것인지 확인하는 메시지가 표시됩니다.
- ▶ **예**를 클릭하여 확인합니다.  
Windows 방화벽을 다시 사용하도록 설정할 것인지 묻는 메시지가 나타납니다.  
Avira FireWall은 비활성 상태입니다.

- ▶ **예**를 클릭하여 확인합니다.  
프로그램의 모든 구성 요소가 제거됩니다.
- ▶ **마침**을 클릭하여 제거를 완료합니다.  
컴퓨터를 다시 시작하라는 대화 상자가 나타납니다.
- ▶ **예**를 클릭하여 확인합니다.

컴퓨터가 다시 시작되면 AntiVir 프로그램이 제거되고 해당 프로그램의 모든 디렉터리, 파일 및 레지스트리 항목이 삭제됩니다.

## 4.5 네트워크에서 설치 및 제거

여러 클라이언트 컴퓨터로 구성된 네트워크에서 시스템 관리자가 AntiVir 프로그램을 간편하게 설치할 수 있도록 하기 위해 AntiVir 프로그램에는 초기 설치 및 변경 설치를 위한 특별한 절차가 준비되어 있습니다.

자동으로 설치할 경우 설치 프로그램은 **setup.inf** 제어 파일을 사용합니다. 설치 프로그램(**presetup.exe**)은 프로그램의 설치 패키지에 들어 있습니다. 설치 스크립트 또는 배치 파일을 통해 시작되며, 필요한 모든 정보를 제어 파일에서 가져옵니다. 즉, 스크립트 명령은 설치 과정에서 일반 수동 입력을 대체합니다.

**참고**  
네트워크에서의 초기 설치에서는 라이선스 파일이 반드시 필요합니다.

**참고**  
네트워크를 통한 설치에는 AntiVir 프로그램의 설치 패키지가 필요합니다. 인터넷 기반 설치용 설치 파일은 사용할 수 없습니다.

AntiVir 프로그램은 네트워크에서 서버 로그인 스크립트 또는 SMS 를 통해 손쉽게 공유할 수 있습니다.

네트워크에서 설치 및 제거에 대한 자세한 내용은 다음 장을 참조하십시오.

- 참조: 설치 프로그램용 명령줄 매개 변수
- 참조: Setup.inf 파일의 매개 변수

- 참조: 네트워크에서 설치
- 참조: 네트워크에서 제거

**참고**

AntiVir Security Management Center에서는 네트워크에서 손쉽게 AntiVir 프로그램을 설치하고 제거할 수 있도록 또 다른 옵션을 제공합니다. AntiVir Security Management Center를 사용하면 네트워크에서 AntiVir 제품을 원격으로 설치하고 유지 관리할 수 있습니다. 자세한 내용은 웹 사이트에서 확인하십시오.

<http://www.avira.kr>

#### 4.5.1 네트워크에서 설치

이 설치의 배치 모드에서 스크립트로 제어할 수 있습니다.

이 방법은 다음과 같은 설치에 적합합니다.

- 네트워크를 통한 초기 설치(무인 설치)
- 단일 사용자 컴퓨터에서 설치

▶ 변경 설치 및 업데이트

**참고**

네트워크에서 설치 루틴을 구현하기 전에 자동 설치를 테스트하는 것이 좋습니다.

네트워크에 AntiVir 프로그램을 자동으로 설치:

관리자 권한이 있어야 합니다(배치 모드에서도 필요함).

- ▶ *setup.inf* 파일의 매개 변수를 구성하고 파일을 저장합니다.
- ▶ */inf* 매개 변수로 설치를 시작하거나 서버의 로그인 스크립트에 이 매개 변수를 통합합니다.
  - 예: `presetup.exe /inf="c:\temp\setup.inf"`  
설치를 자동으로 시작합니다.

#### 4.5.2 네트워크에서 제거

네트워크에서 AntiVir 프로그램을 자동으로 제거:

관리자 권한이 있어야 합니다(배치 모드에서도 필요함).

- ▶ */remsilent* 또는 */remsilentaskreboot* 매개 변수를 지정하여 제거를 시작하거나 서버의 로그인 스크립트에 이 매개 변수를 통합합니다.

또한 제거 로그의 매개 변수를 지정할 수도 있습니다.

- 예: `preetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`  
설치 제거를 자동으로 시작합니다.

**참고**

설치 프로그램 제거는 AntiVir 프로그램을 제거할 PC 에서 시작해야 합니다. 따라서 네트워크 드라이브에서 설치 프로그램을 시작하지 마십시오.

### 4.5.3 설치 프로그램용 명령줄 매개 변수

모든 경로 또는 파일 데이터가 "...에 위치해야 합니다.

다음 매개 변수를 설치에 사용할 수 있습니다.

- /inf

설치 프로그램이 지정된 스크립트와 함께 시작하고 필요한 모든 매개 변수를 검색합니다.

예: `presetup.exe /inf="c:\temp\setup.inf"`

다음 매개 변수를 제거에 사용할 수 있습니다.

- /remove

설치 프로그램이 AntiVir 프로그램을 제거합니다.

예: `presetup.exe /remove`

- /remsilent

설치 프로그램에서 대화 상자를 표시하지 않고 AntiVir 프로그램을 제거합니다. 제거 후 컴퓨터가 다시 시작됩니다.

예: `presetup.exe /remsilent`

- /remsilentaskreboot

설치 프로그램에서 대화 상자를 표시하지 않고 AntiVir 프로그램을 제거하며, 제거 후 컴퓨터를 다시 시작하라는 메시지를 표시합니다.

예: `presetup.exe /remsilentaskreboot`

다음 매개 변수는 제거 로그용 옵션으로 사용할 수 있습니다.

- /unsetuplog

제거 과정의 모든 작업이 기록됩니다.

예: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

#### 4.5.4 Setup.inf 파일의 매개 변수

setup.inf 제어 파일의 [DATA] 필드에 AntiVir 프로그램 자동 설치를 위해 다음 매개 변수를 설정할 수 있습니다. 매개 변수의 순서는 중요하지 않습니다. 매개 변수 설정이 누락되었거나 잘못된 경우 설치 루틴이 중단되고 오류 메시지가 표시됩니다.

##### - DestinationPath

프로그램을 설치할 대상 경로입니다. 스크립트에 포함되어야 합니다. 설치에 회사 이름 및 제품 이름이 자동으로 포함됩니다. 환경 변수를 사용할 수 있습니다.

예: DestinationPath=%PROGRAMFILES%

설치 경로 C:\Programme\Avira\AntiVir Desktop 을 생성합니다.

##### - ProgramGroup

컴퓨터의 모든 사용자를 위한 프로그램 그룹을 Windows 시작 메뉴에 만듭니다.

1: 프로그램 그룹을 만듭니다.

0: 프로그램 그룹을 만들지 않습니다.

예: ProgramGroup=1

##### - DesktopIcon

컴퓨터의 모든 사용자를 위한 바로 가기 아이콘을 바탕 화면에 만듭니다.

1: 바탕 화면 아이콘 만들기

0: 바탕 화면 아이콘을 만들지 않습니다.

예: DesktopIcon=1

##### - ShellExtension

셸 확장을 레지스트리에 등록합니다. 셸 확장을 사용하면 마우스 오른쪽 단추의 상황에 맞는 메뉴에서 파일 및 디렉터리를 대상으로 바이러스 및 맬웨어를 검사할 수 있습니다.

1: 셸 확장을 등록합니다.

0: 셸 확장을 등록하지 않습니다.

예: ShellExtension=1

##### - Guard

AntiVir Guard(온 액세스 검사 프로그램)를 설치합니다.

1: AntiVir Guard 를 설치합니다.

0: AntiVir Guard 를 설치하지 않습니다.

예: Guard=1

##### - MailScanner

AntiVir MailGuard 를 설치합니다.

1: AntiVir MailGuard 를 설치합니다.

0: MailGuard 를 설치하지 않습니다.

예: MailScanner=1

- KeyFile

설치 과정에서 복사되는 라이선스 파일의 경로를 지정합니다. 초기 설치의 경우 필수 항목입니다. 파일 이름은 완전히 지정해야 합니다(정규화된 이름). (변경 설치의 경우 선택 항목입니다.)

예: KeyFile=D:\inst\license\hbedv.key

- ShowReadMe

설치 후 readme.txt 파일을 표시합니다.

1: 파일을 표시합니다.

0: 파일을 표시하지 않습니다.

예: ShowReadMe=1

- RestartWindows

설치 후 컴퓨터를 다시 시작합니다. 이 항목은 ShowRestartMessage 보다 우선 순위가 더 높습니다.

1: 컴퓨터를 다시 시작합니다.

0: 컴퓨터를 다시 시작하지 않습니다.

예: RestartWindows=1

- ShowRestartMessage

설치 과정에서 자동으로 다시 시작하기 전에 정보를 표시합니다.

0: 정보를 표시하지 않습니다.

1: 정보를 표시합니다.

예: ShowRestartMessage=1

- SetupMode

초기 설치에는 필요하지 않습니다. 설치 프로그램에서는 초기 설치가 수행된 적이 있는지 확인합니다. 설치 유형을 지정합니다. 이미 설치된 프로그램이 있는 경우 이 설치가 업그레이드 전용인지, 변경 설치(다시 구성)인지 아니면 제거인지 여부를 SetupMode 에 지정해야 합니다.

Update: 기존 설치를 업데이트합니다. 이 경우 Guard 와 같은 구성 매개 변수는 무시됩니다.

Modify: 기존 설치를 수정(다시 구성)합니다. 그 과정에서 대상 경로에 복사되는 파일은 없습니다.

Remove: 시스템에서 AntiVir 프로그램을 제거합니다.

예: SetupMode=Update

#### - AVWinIni(옵션)

설치 과정에서 복사할 수 있는 구성 파일의 대상 경로를 지정합니다. 파일 이름은 완전히 지정해야 합니다(정규화된 이름).

예: AVWinIni=d:\inst\config\avwin.ini

#### - Password

이 옵션은 (수정) 설치 및 제거를 위해 설정된 암호를 설치 루틴에 지정합니다. 이 항목은 암호가 설정된 경우에만 설치 루틴을 통해 검사합니다. 암호가 설정되었지만 암호 매개 변수가 누락되었거나 잘못된 경우에는 설치 루틴이 중단됩니다.

예: Password=Password123

#### - WebGuard

AntiVir WebGuard 를 설치합니다.

1: AntiVir WebGuard 를 설치합니다.

0: AntiVir WebGuard 를 설치하지 않습니다.

예: WebGuard=1

#### - RootKit

루트킷 검색 모듈을 설치합니다. 루트킷 검색 기능이 없으면 검사 프로그램에서 시스템의 루트킷을 검사할 수 없습니다.

1: 루트킷 검색을 설치합니다.

0: 루트킷 검색을 설치하지 않습니다.

예: RootKit=1

#### - HIPS

AntiVir ProActiv 구성 요소를 설치합니다. AntiVir ProActiv 는 아직 알려지지 않은 맬웨어를 검색할 수 있는 패턴 기반 검색 기술입니다.

1: ProActiv 를 설치합니다.

0: ProActiv 를 설치하지 않습니다.

예: HIPS=1

### - FireWall

Avira FireWall 구성 요소를 설치합니다. Avira FireWall 은 컴퓨터 시스템에서 들어오고 나가는 데이터 트래픽을 모니터링 및 제어하고 인터넷이나 기타 네트워크 환경의 다양한 위협으로부터 컴퓨터를 보호합니다.

1: 방화벽을 설치합니다.

0: 방화벽을 설치하지 않습니다.

예: FireWall=1

## 5 AntiVir Professional 개요

이 장에서는 AntiVir 프로그램의 기능과 작동 방식을 간단히 설명합니다.

- 참조: 인터페이스 및 작업
- 참조: 방법

### 5.1 사용자 인터페이스 및 작업

AntiVir 프로그램은 세 가지 프로그램 인터페이스 요소를 통해 사용할 수 있습니다.

- 제어 센터 AntiVir 프로그램의 모니터링 및 제어
- 구성: AntiVir 프로그램 구성
- 작업 표시줄 시스템 트레이의 트레이 아이콘: 제어 센터 및 기타 기능 열기

#### 5.1.1 제어 센터

제어 센터는 컴퓨터 시스템의 보호 상태를 모니터링하고 AntiVir 프로그램의 보호 구성 요소 및 기능을 제어하고 작동하는 용도로 설계되었습니다.



제어 센터 창은 메뉴 모음, 탐색 모음 및 세부 정보 창 보기의 세 영역으로 나뉩니다.

- **메뉴 모음:** 제어 센터 메뉴 모음에서 일반 프로그램 기능 및 프로그램에 대한 정보에 액세스할 수 있습니다.
- **탐색 영역:** 탐색 영역에서 제어 센터의 개별 섹션 간에 손쉽게 전환할 수 있습니다. 개별 섹션에는 프로그램 구성 요소에 대한 정보와 기능이 작업별로 탐색 모음에 정리되어 있습니다. 예: 작업 개요 - 섹션 상태.



- **보기:** 이 창에는 탐색 영역에서 선택한 섹션이 표시됩니다. 섹션에 따라 세부 정보 창의 위쪽 막대에 기능과 작업을 실행하는 단추가 표시됩니다. 데이터 또는 데이터 개체는 개별 섹션의 목록에 표시됩니다. 목록을 정렬하는 방법을 정의한 상자를 클릭하여 목록을 정렬할 수 있습니다.

### 제어 센터 시작 및 종료

제어 센터를 시작하는 데 다음 옵션을 사용할 수 있습니다.

- 바탕 화면의 프로그램 아이콘 두 번 클릭
- 시작 | 프로그램 메뉴의 프로그램 항목 사용
- AntiVir 프로그램의 트레이 아이콘 사용

**파일** 메뉴의 **닫기** 메뉴 명령을 사용하거나 제어 센터의 닫기 탭을 클릭하여 제어 센터를 닫습니다.

### 제어 센터 작업

제어 센터를 탐색하려면

- ▶ 탐색 모음에서 작업을 선택합니다.  
작업이 열리고 다른 섹션이 표시됩니다. 작업의 첫 번째 섹션이 선택되고 보기에 표시됩니다.
- ▶ 필요한 경우 다른 섹션을 클릭하여 세부 정보 보기 창에 표시합니다.  
- 또는 -
- ▶ **보기** 메뉴를 사용하여 섹션을 선택합니다.

### 참고

[Alt] 키를 사용하여 메뉴 모음에서 키보드 탐색을 활성화할 수 있습니다. 탐색이 활성화되면 화살표 키를 사용하여 메뉴 내에서 이동할 수 있습니다. 활성 메뉴 항목을 실행하려면 Return 키를 누릅니다.

제어 센터에서 메뉴를 열거나 닫을 때 또는 메뉴 내에서 탐색할 때 [Alt]+메뉴 또는 메뉴 명령 뒤의 괄호 안에 있는 밑줄 처진 문자를 사용해도 됩니다. 메뉴, 메뉴 명령 또는 하위 메뉴에 액세스하려면 [Alt] 키를 누릅니다.

세부 정보 창에 표시된 데이터 또는 개체를 처리하려면 다음을 수행하십시오.

- ▶ 편집할 데이터나 개체를 강조 표시합니다.  
여러 요소(열의 요소)를 강조 표시하려면 Ctrl 키 또는 Shift 키를 누른 채 요소를 선택합니다.
- ▶ 세부 정보 창의 위쪽 막대에 있는 해당 단추를 클릭하여 개체를 편집합니다.

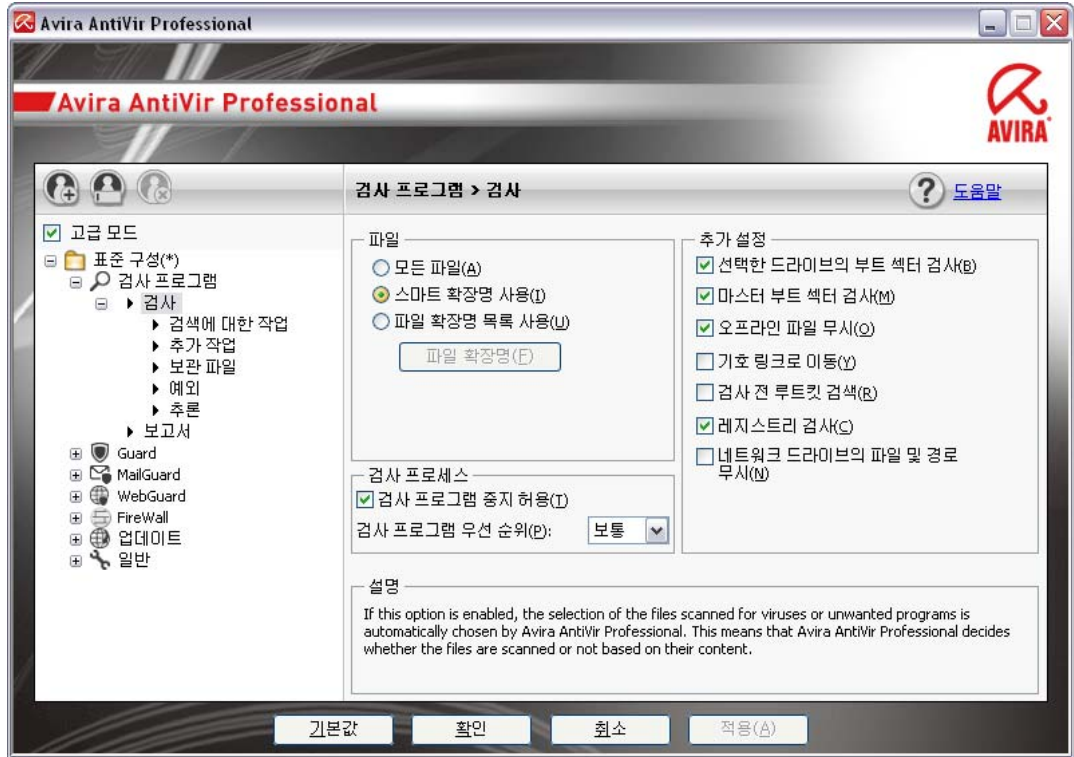
### 제어 센터 개요

- **개요:** 개요에는 AntiVir 프로그램의 기능을 모니터링할 수 있는 섹션이 모두 표시됩니다.
- **상태** 섹션에서는 활성 상태인 프로그램 모듈을 한번에 볼 수 있고 수행된 최신 업데이트에 대한 정보가 제공됩니다. 또한 소유하고 있는 라이선스가 유효한지 확인할 수 있습니다.
- **이벤트** 섹션에서는 특정 프로그램 모듈에서 생성한 이벤트를 볼 수 있습니다.

- 보고서 섹션에서는 실행한 작업의 결과를 볼 수 있습니다.
- 로컬 보호: 로컬 보호에는 컴퓨터 시스템의 파일에서 바이러스 및 맬웨어에 대해 검사하는 구성 요소가 제공됩니다.
- 검사 섹션에서는 온 디맨드 검사를 손쉽게 구성하고 시작할 수 있습니다. 미리 정의된 프로필을 사용하면 이미 적용한 표준 옵션으로 검사할 수 있습니다. 같은 방법으로 수동 선택(저장되지 않음)을 사용하거나 사용자 정의 프로필을 만들어 바이러스나 사용자 동의 없이 설치된 프로그램에 대한 검사를 개인 요구 사항에 맞게 적용할 수 있습니다.
- Guard 섹션에는 검사한 파일에 대한 정보와 기타 통계 데이터가 표시되며 이러한 데이터는 언제든지 다시 설정할 수 있고 이를 통해 보고서 파일에 액세스할 수 있습니다. 검색된 최신 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대한 세부 정보를 보려면 "단추를 누릅니다".
- 온라인 보호: 온라인 보호에는 인터넷의 바이러스 및 맬웨어와 권한이 없는 네트워크 액세스로부터 컴퓨터 시스템을 보호하는 구성 요소가 제공됩니다.
- MailGuard 섹션에는 MailGuard 에서 검사한 모든 전자 메일, 해당 속성 및 기타 통계 데이터가 표시됩니다.
- WebGuard 섹션에는 검사한 URL 및 검색된 바이러스에 대한 정보와 기타 통계 데이터가 표시되며, 이러한 정보는 언제든지 다시 설정할 수 있고 이를 통해 보고서 파일에 액세스할 수 있습니다. 검색된 최신 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대한 세부 정보를 보려면 "단추를 누릅니다".
- FireWall 섹션에서는 Avira FireWall 의 기본 설정을 구성할 수 있습니다. 또한, 네트워크 연결을 사용하는 현재 데이터 전송 속도 및 모든 활성 응용 프로그램이 표시됩니다.
- 관리: 관리에는 의심스럽거나 감염된 파일을 격리 및 관리하고 반복 작업을 계획하는 도구가 있습니다.
- 격리 섹션에는 격리 관리자가 들어 있습니다. 이 관리자는 격리 저장소에 넣은 파일 또는 격리 저장소에 넣을 의심스러운 파일에 대한 중앙 통제소입니다. 또한 선택한 파일을 전자 메일로 Avira 맬웨어 연구 센터에 보낼 수 있습니다.
- 스케줄러 섹션에서는 예약된 검사 및 업데이트 작업과 을 구성하고 기존 작업을 적용 또는 삭제할 수 있습니다.

### 5.1.2 구성

구성에서 AntiVir 프로그램의 설정을 정의할 수 있습니다. 설치 후 AntiVir 프로그램은 표준 설정으로 구성되어 컴퓨터 시스템을 최적으로 보호해 줍니다. 하지만 컴퓨터 시스템이나 AntiVir 프로그램에 대한 특정 요구 사항에 맞게 프로그램의 보호 구성 요소를 적용해야 할 수 있습니다.



구성을 실행하면 대화 상자가 열리며 이 대화 상자에서 확인이나 적용 단추를 사용하여 구성 설정을 저장하거나, 취소 단추를 클릭하여 설정을 삭제하거나, 기본값 단추를 사용하여 기본 구성 설정을 복원할 수 있습니다. 왼쪽의 탐색 모음에서는 개별 구성 섹션을 선택할 수 있습니다.

### 구성 액세스

다음과 같은 방법을 사용하여 구성에 액세스할 수 있습니다.

- Windows 제어판 사용
- Windows XP 서비스 팩 2 의 Windows 보안 센터 사용
- AntiVir 프로그램의 트레이 아이콘 사용
- 제어 센터에서 기타 | 구성 메뉴 항목 사용
- 제어 센터에서 구성 단추 사용

### 참고

제어 센터의 구성 단추를 통해 구성에 액세스하는 경우 제어 센터에서 활성화된 섹션의 구성 레지스터로 이동합니다. 고급 모드가 활성화되어야 개별 구성 레지스터를 선택할 수 있습니다. 이 경우 고급 모드를 활성화할 것인지 묻는 대화 상자가 나타납니다.

### 구성 작업

Windows 탐색기에서처럼 구성 창에서 탐색합니다.

- ▶ 트리 구조의 항목을 클릭하면 세부 정보 창에 이 구성 섹션이 표시됩니다.
- ▶ 항목 앞에 있는 더하기 기호를 클릭하면 구성 섹션이 확장되고 트리 구조에 구성 하위 섹션이 표시됩니다.

- ▶ 구성 하위 섹션을 숨기려면 확장한 구성 섹션 앞에 있는 빼기 기호를 클릭합니다.

**참고**

구성 옵션을 활성화 또는 비활성화하고 단추를 사용하기 위해 [Alt]+옵션 이름 또는 단추 설명 뒤의 괄호 안에 밑줄이 쳐진 문자를 눌러도 됩니다.

**참고**

모든 구성 섹션은 고급 모드에서만 표시됩니다. 모든 구성 섹션을 표시하려면 고급 모드를 활성화합니다. 고급 모드는 활성화 시 정의해야 하는 암호로 보호할 수 있습니다.

구성 설정을 확인하려면 다음을 수행합니다.

- ▶ **확인**을 클릭합니다.  
구성 창이 닫히고 설정이 적용됩니다.  
또는

- ▶ **적용**을 클릭합니다.  
설정이 적용됩니다. 구성 창이 열린 채로 유지됩니다.

설정을 확인하지 않고 구성을 마치려면 다음과 같이 합니다.

- ▶ **취소**를 클릭합니다.  
구성 창이 닫히고 설정이 취소됩니다.

모든 구성 설정을 기본값으로 복원하려면 다음과 같이 합니다.

- ▶ **기본값 복원**을 클릭합니다.  
구성의 모든 설정을 기본값으로 복원합니다. 기본 설정으로 복원하면 모든 수정 사항과 사용자 지정 항목이 손실됩니다.

**구성 프로필**

구성 설정을 구성 프로필로 저장할 수 있습니다. 구성 프로필에서 모든 구성 옵션은 그룹에 저장됩니다. 구성은 탐색 모음에서 노드로 표시됩니다. 기본 구성에 다른 구성을 추가할 수 있습니다. 또한 특정 구성으로 전환하는 규칙을 정의할 수도 있습니다.

규칙 기반 절차를 사용하여 구성을 전환할 때 LAN 또는 인터넷 연결을 사용하여 구성을 연결할 수 있습니다(기본 게이트웨이를 통해 확인). 따라서 서로 다른 랩톱 사용 시나리오에 맞는 구성 프로필을 만들 수 있습니다.

- 회사 네트워크에서 사용: 인트라넷 서버를 통해 업데이트, WebGuard 비활성화
- 집에서 사용: 기본 Avira GmbH web 서버를 통해 업데이트, WebGuard 활성화

전환 규칙을 정의하지 않은 경우 트레이 아이콘의 상황에 맞는 메뉴에서 수동으로 구성을 전환할 수 있습니다. 구성을 추가하고 이름을 바꾸거나 삭제, 복사 또는 복원할 수 있으며, 탐색 모음의 단추를 사용하거나 구성 섹션의 상황에 맞는 메뉴의 명령을 사용하여 구성을 전환하는 규칙을 정의할 수 있습니다.

**참고**

다른 구성으로 자동 전환 기능은 Windows 2000 에서 지원되지 않습니다. Windows 2000에서는 구성 전환에 대한 규칙을 정의할 수 없습니다.

### 구성 옵션 개요

다음 구성 옵션을 사용할 수 있습니다.

– **검사 프로그램:** 온 디맨드 검사 구성

검사 옵션

검색에 대한 작업

파일 검사 옵션

온 디맨드 검사 예외

온 디맨드 검사 추론

보고서 기능 설정

– **Guard:** 온 액세스 검사 구성

검사 옵션

검색에 대한 작업

온 액세스 검사 예외

온 액세스 검사 추론

보고서 기능 설정

– **MailGuard:** MailGuard 구성

검사 옵션: POP3 계정, IMAP 계정, 보내는 전자 메일(SMTP) 모니터링 사용

맬웨어에 대한 작업

MailGuard 검사 추론

MailGuard 검사 예외

캐시 구성, 캐시 비우기

보낸 전자 메일의 바닥글 구성

보고서 기능 설정

– **WebGuard:** WebGuard 구성

검사 옵션, WebGuard 사용/사용 안 함

검색에 대한 작업

차단된 액세스: 원치 않는 파일 형식 및 MIME 형식, 알려진 원치 않는 URL(맬웨어, 피싱 등)에 대한 웹 필터

WebGuard 검사 예외: URL, 파일 형식, MIME 형식

WebGuard 추론

보고서 기능 설정

– **FireWall:** FireWall 구성

어댑터 규칙 설정

사용자 정의 응용 프로그램 규칙 설정

신뢰할 수 있는 공급자 목록(응용 프로그램의 네트워크 액세스 예외)

확장 설정: 규칙 시간 초과, Windows 호스트 파일 잠금, Windows 방화벽 중지, 알람

팝업 설정(응용 프로그램의 네트워크 액세스 관련 알람)

- 일반:

SMTP 를 사용하는 전자 메일 구성

온 액세스 및 온 디맨드 검사에 대한 확장된 위험 범주

제어 센터로 이동하여 로컬 보호 및 구성

보안: 상태 표시 업데이트, 전체 시스템 검사 상태 표시, 제품 보호

WMI: WMI 지원 사용

이벤트 로그 구성

보고서 기능 구성

사용된 디렉터리 설정

업데이트: 다운로드 서버와의 연결 구성, 다운로드 방법(웹 서버 또는 파일 서버 사용), 제품 업데이트 설정

알람: 구성 요소에 대한 전자 메일 알람 구성:

검사 프로그램

Guard



업데이트 프로그램

검사 프로그램, Guard 구성 요소에 대한 네트워크 알람 구성

맬웨어 검색 시 음향 알람 구성

### 5.1.3 트레이 아이콘

설치하면 AntiVir 프로그램의 트레이 아이콘이 작업 표시줄의 시스템 트레이에 표시됩니다.

아이콘	설명
	AntiVir Guard 와 FireWall 을 둘 다 사용합니다.
	AntiVir Guard 와 FireWall 을 둘 다 사용하지 않습니다.

트레이 아이콘은 Guard 및 FireWall 의 서비스 상태를 표시합니다.

트레이 아이콘의 상황에 맞는 메뉴를 통해 AntiVir 프로그램의 핵심 기능에 빠르게 액세스할 수 있습니다. 상황에 맞는 메뉴를 열려면 마우스 오른쪽 단추로 트레이 아이콘을 클릭합니다.

#### 상황에 맞는 메뉴의 항목

- **AntiVir Guard 활성화:** AntiVir Guard 를 활성화하거나 비활성화합니다.
- **AntiVir MailGuard 사용:** AntiVir MailGuard 를 활성화하거나 비활성화합니다.

- **AntiVir WebGuard 사용:** AntiVir WebGuard 를 활성화하거나 비활성화합니다.
- **FireWall:**
  - FireWall 사용: FireWall 을 활성화하거나 비활성화합니다.
  - 모든 트래픽 차단: 사용: 호스트 컴퓨터 시스템(로컬 호스트/IP 127.0.0.1)으로의 전송을 제외한 모든 데이터 전송을 차단합니다.
  - 게임 모드 사용: 모드를 활성화하거나 비활성화합니다.  
사용: 활성화된 경우 정의된 모든 어댑터 및 응용 프로그램 규칙이 적용됩니다. 규칙이 정의되지 않은 응용 프로그램은 네트워크 액세스가 허용되며 팝업 창이 열리지 않습니다.
- **AntiVir 시작:** 제어 센터를 엽니다.
- **AntiVir 구성:** 구성을 엽니다.
- **업데이트 시작** 업데이트를 시작합니다.
- **구성 선택:** 사용 가능한 구성 프로파일의 하위 메뉴를 엽니다. 구성을 클릭하여 활성화합니다. 구성으로 자동 전환하기 위한 규칙을 아직 정의하지 않은 경우 메뉴 명령을 사용할 수 없습니다.
- **도움말:** 온라인 도움말을 엽니다.
- **AntiVir Professional 정보:** AntiVir 프로그램에 대한 정보가 있는 대화 상자가 표시됩니다. 제품 정보, 버전 정보, 라이선스 정보 등이 표시됩니다.
- **Avira 인터넷 주소:** 인터넷에서 Avira 의 웹 포털을 엽니다. 조건은 인터넷에 대한 활성 연결을 사용해야 합니다.

## 5.2 방법

### 5.2.1 라이선스 활성화

#### AntiVir 프로그램의 라이선스 활성화:

hbedv.key 라이선스 파일을 사용하여 Avira 제품의 라이선스를 활성화하십시오. 라이선스 파일은 Avira GmbH 에서 전자 메일을 통해 제공합니다. 라이선스 파일에는 하나의 주문 프로세스에서 주문한 모든 제품의 라이선스가 포함되어 있습니다.

AntiVir 프로그램을 아직 설치하지 않은 경우:

- ▶ 해당 컴퓨터의 로컬 디렉터리에 라이선스 파일을 저장합니다.
- ▶ AntiVir 프로그램을 설치합니다.
- ▶ 설치 중에 라이선스 파일의 저장 위치를 입력합니다.

AntiVir 프로그램을 이미 설치한 경우:

- ▶ 파일 관리자 또는 활성화 전자 메일에서 라이선스 파일을 두 번 클릭한 다음 라이선스 관리자가 열리면 화면의 지침대로 수행합니다.

또는

- ▶ AntiVir 프로그램의 제어 센터에서 도움말/라이선스 파일 로드 메뉴 항목에 액세스합니다....


**참고**

Windows Vista에서는 사용자 계정 컨트롤 대화 상자가 나타납니다. 관리자로 로그인합니다. **계속**을 클릭합니다.

- ▶ 라이선스 파일을 강조 표시하고 **열기**를 클릭합니다.  
메시지가 나타납니다.
- ▶ **확인**을 클릭하여 확인합니다.  
라이선스가 활성화되었습니다.
- ▶ 필요한 경우 시스템을 다시 시작합니다.

## 5.2.2 자동 업데이트 수행

AntiVir 스케줄러에서 AntiVir 프로그램을 자동 업데이트하는 작업 만들기:

- ▶ 제어 센터에서 **관리 :: 스케줄러** 섹션의 홈 페이지에 새로 만든 순서가 활성화된 상태(확인 표시)로 나타납니다.
- ▶  **마법사로 새 작업 만들기** 아이콘을 클릭합니다.  
작업의 이름 및 설명 대화 상자가 나타납니다.
- ▶ 작업 이름과 설명을 입력합니다.
- ▶ **다음**을 클릭합니다.  
작업 유형 대화 상자가 나타납니다.
- ▶ 목록에서 **업데이트** 작업을 선택합니다.
- ▶ **다음**을 클릭합니다.  
작업 시간 대화 상자가 나타납니다.
- ▶ 업데이트 시간을 선택합니다.
  - 즉시
  - 매일
  - 매주
  - 간격
  - 단일
  - 로그인






**참고**

자동 업데이트를 정기적으로, 자주 수행하는 것이 좋습니다. 권장되는 업데이트 간격은 60 분.

- ▶ 선택 항목에 따라 날짜를 지정합니다.
- ▶ 다음 추가 옵션을 선택합니다. 선택 가능 여부는 작업 유형에 따라 다릅니다.
  - **인터넷에 연결할 때도 작업 시작**  
정의된 빈도 외에도 인터넷 연결이 설정되어 있으면 작업을 수행합니다.
  - **시간이 만료된 경우 작업 반복**  
컴퓨터 전원이 꺼지는 등 기타 이유로 인해 필요한 시각에 수행할 수 없었던 지난 작업을 수행합니다.



- ▶ 다음을 클릭합니다.  
디스플레이 모드 선택 대화 상자가 나타납니다.
- ▶ 작업 창의 디스플레이 모드를 선택합니다.
  - 최소화: 진행률 표시줄만
  - 최대화: 전체 작업 창
  - 숨기기: 작업 없음 창
- ▶ 마침을 클릭합니다.  
새로 만든 작업이 관리자 :: 검사 섹션의 시작 페이지에 활성화된 상태(확인 표시)로 나타납니다.
- ▶ 수행하지 않을 작업은 비활성화합니다.  
작업을 더 자세히 정의하려면 다음 아이콘을 사용합니다.

-  작업의 속성 보기
-  작업 수정
-  작업 삭제
-  작업 시작
-  작업 중지

### 5.2.3 수동 업데이트 시작

다양한 옵션으로 업데이트를 수동으로 시작할 수 있습니다. 업데이트를 수동으로 시작하면 항상 바이러스 정의 파일 및 검사 엔진이 업데이트됩니다. 제품 업데이트를 수행하려면 자동으로 제품 업데이트 다운로드 및 설치(구성 섹션 일반 :: 업데이트) 옵션을 활성화해야 합니다.

AntiVir 프로그램 업데이트를 수동으로 시작:

- ▶ 작업 표시줄에서 AntiVir 트레이 아이콘을 마우스 오른쪽 단추로 클릭합니다.  
상황에 맞는 메뉴가 나타납니다.
- ▶ 업데이트 시작을 선택합니다.  
업데이트 프로그램 대화 상자가 나타납니다.  
또는
- ▶ 제어 센터에서 개요 :: 상태 섹션을 선택합니다.
- ▶ 최신 업데이트 필드에서 업데이트 시작 링크를 클릭합니다.  
업데이트 프로그램 대화 상자가 나타납니다.  
또는
- ▶ 제어 센터의 업데이트 메뉴에서 업데이트 시작 메뉴 명령을 선택합니다.  
업데이트 프로그램 대화 상자가 나타납니다.

**참고**

자동 업데이트를 정기적으로 수행하는 것이 좋습니다. 권장되는 업데이트 간격은 60 분.

**참고**

또한 Windows 보안 센터에서 곧바로 수동 업데이트를 수행할 수도 있습니다.

## 5.2.4 온 디맨드 검사: 검사 프로필을 사용한 바이러스 및 맬웨어 검사

검사 프로필은 검사할 드라이브 및 디렉터리의 집합입니다.

검사 프로필을 사용하는 검사에 다음 옵션을 사용할 수 있습니다.

- 미리 정의된 검사 프로필 사용
  - 미리 정의된 검사 프로필이 요구 사항과 일치하는 경우
- 검사 프로필을 사용자 지정하고 적용합니다(수동 선택).
  - 사용자 지정된 검사 프로필로 검사하려는 경우
- 새 검사 프로필을 만들어 적용합니다.
  - 직접 검사 프로필을 만들려는 경우

운영 체제에 따라 다양한 아이콘을 사용하여 검사 프로필을 시작할 수 있습니다.

- Windows XP 및 2000:



이 아이콘은 검사 프로필을 통해 검사를 시작합니다.

- Windows Vista:

Microsoft Windows Vista 의 경우, 현재로서는 제어 센터의 권한이 제한적입니다(예: 디렉터리 및 파일에 대한 액세스). 일부 작업 및 파일 액세스는 확장된 관리자 권한이 있어야만 제어 센터에서 수행할 수 있습니다. 이 확장된 관리자 권한은 검사를 시작할 때마다 검사 프로필을 통해 부여해야 합니다.





이 아이콘은 검사 프로필을 통해 제한적인 검사를 시작합니다. Windows Vista 에서 액세스 권한을 부여한 디렉터리 및 파일만 검사합니다.



이 아이콘은 확장된 관리 권한으로 검사를 시작합니다. 확인하면 선택한 검사 프로필의 모든 디렉터리 및 파일을 검사합니다.

검사 프로필을 사용하여 바이러스 및 맬웨어를 검사하려면

- ▶ 제어 센터로 이동하여 **로컬 보호::검사** 섹션을 선택합니다.
  - 미리 정의된 검사 프로필이 나타납니다.
- ▶ 미리 정의된 검사 프로필 중 하나를 선택합니다.
  - 또는
- ▶ 검사 프로필 수동 선택을 변경합니다.
  - 또는
- ▶ 새 검사 프로필 만들기

- ▶ 아이콘을 클릭합니다(Windows XP:  또는 Windows Vista: ).
- ▶ *Luke Filewalker* 창이 나타나고 온 디맨드 검사가 시작됩니다.  
검사가 끝나면 그 결과가 표시됩니다.



검사 프로필을 변경하려는 경우

- ▶ 검사 프로필에서 **수동 선택** 파일 트리를 확장하여 검사하려는 모든 드라이브 및 디렉터리가 열리게 합니다.
  - + 아이콘을 클릭합니다. 다음 디렉터리 수준이 표시됩니다.
  - - 아이콘을 클릭합니다. 다음 디렉터리 수준이 숨겨집니다.
- ▶ 검사하려는 노드 및 디렉터를 강조 표시합니다. 원하는 디렉터리 수준에서 해당 상자를 클릭하면 됩니다.

디렉터를 선택할 때 다음 옵션을 사용할 수 있습니다.

- 하위 디렉터를 포함하여 디렉터리 선택(검정색 확인 표시)
- 하위 디렉터를 제외하고 디렉터리 선택(녹색 확인 표시)
- 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
- 디렉터리 선택 안 함(확인 표시 없음)

새 검사 프로필을 만들려는 경우

- ▶  **새 프로필 만들기** 아이콘을 클릭합니다.  
이전에 만든 프로필 아래에 **새 프로필**이 나타납니다.
- ▶ 필요하다면  아이콘을 클릭하여 검사 프로필의 이름을 바꿉니다.
- ▶ 각 디렉터리 수준의 확인란을 클릭하여 저장할 노드 및 디렉터를 강조 표시합니다.

디렉터를 선택할 때 다음 옵션을 사용할 수 있습니다.

- 하위 디렉터를 포함하여 디렉터리 선택(검정색 확인 표시)
- 하위 디렉터를 제외하고 디렉터리 선택(녹색 확인 표시)
- 한 디렉터리의 하위 디렉터리만 선택(회색 확인 표시, 하위 디렉터리는 검정색 확인 표시)
- 디렉터리 선택 안 함(확인 표시 없음)

### 5.2.5 온 디맨드 검사: 끌어서 놓기를 사용한 바이러스 및 맬웨어 검사

끌어서 놓기를 사용하여 바이러스 및 맬웨어를 체계적으로 검사하려면

*AntiVir* 프로그램의 제어 센터가 열려 있습니다.

- ▶ 검사하려는 파일 또는 디렉터를 강조 표시합니다.
- ▶ 마우스 왼쪽 단추를 사용하여 강조 표시된 파일 또는 디렉터를 **제어 센터**로 끌어옵니다.

*Luke Filewalker* 창이 나타나고 온 디맨드 검사가 시작됩니다.

검사가 끝나면 그 결과가 표시됩니다.

## 5.2.6 온 디맨드 검사: 상황에 맞는 메뉴를 사용한 바이러스 및 맬웨어 검사

상황에 맞는 메뉴를 사용하여 바이러스 및 맬웨어를 체계적으로 검사하려면


- ▶ 검사하려는 파일 또는 디렉터리를 Windows 탐색기, 바탕 화면 또는 열려 있는 Windows 디렉터리에서처럼 마우스 오른쪽 단추로 클릭합니다.  
Windows 탐색기의 상황에 맞는 메뉴가 나타납니다.
- ▶ 상황에 맞는 메뉴에서 **AntiVir**를 사용하여 선택한 파일 검사를 선택합니다.  
*Luke Filewalker* 창이 나타나고 온 디맨드 검사가 시작됩니다.  
검사가 끝나면 그 결과가 표시됩니다.

## 5.2.7 온 디맨드 검사: 바이러스 및 맬웨어 자동 검사

### 참고

설치 후 전체 시스템 검사 작업이 스케줄러에 만들어집니다. 전체 시스템 검사는 권장된 간격으로 자동으로 수행됩니다.

바이러스 및 맬웨어를 자동 검사하는 작업을 만들려면

- ▶ 제어 센터에서 **관리:: 스케줄러** 섹션을 선택합니다.
- ▶  아이콘을 클릭합니다.  
작업의 이름 및 설명 대화 상자가 나타납니다.
- ▶ 작업 이름과 설명을 입력합니다.
- ▶ 다음을 클릭합니다.  
작업 유형 대화 상자가 나타납니다.
- ▶ 검사 작업을 선택합니다.
- ▶ 다음을 클릭합니다.  
프로필 선택 대화 상자가 나타납니다.
- ▶ 검사할 프로필을 선택합니다.
- ▶ 다음을 클릭합니다.  
작업 시간 대화 상자가 나타납니다.
- ▶ 검사 시간을 선택합니다.
  - 즉시
  - 매일
  - 매주
  - 간격
  - 단일
  - 로그인
- ▶ 선택 항목에 따라 날짜를 지정합니다.
- ▶ 다음 추가 옵션을 선택합니다. 선택 가능 여부는 작업 유형에 따라 다릅니다.
  - 시간이 만료된 경우 작업 반복

컴퓨터 전원이 꺼지는 등 기타 이유로 인해 필요한 시각에 수행할 수 없었던  
지난 작업을 수행합니다.

- ▶ 다음을 클릭합니다.

*디스플레이 모드 선택* 대화 상자가 나타납니다.

- ▶ 작업 창의 디스플레이 모드를 선택합니다.

- **최소화**: 진행률 표시줄만
- **최대화**: 전체 작업 창
- **숨기기**: 작업 없음 창

- ▶ 검사가 완료된 경우 컴퓨터를 자동으로 종료하려면 *컴퓨터 종료* 옵션을  
선택합니다. 이 옵션은 디스플레이 모드가 최소화 또는 최대화로 설정된  
경우에만 사용할 수 있습니다.

- ▶ **마침**을 클릭합니다.

새로 만든 작업이 *관리자:: 스케줄러* 섹션의 시작 페이지에 활성화된 상태(확인  
표시)로 나타납니다.

- ▶ 수행하지 않을 작업은 비활성화합니다.

작업을 더 자세히 정의하려면 다음 아이콘을 사용합니다.



작업의 속성 보기



작업 수정



작업 삭제



작업 시작



작업 중지

## 5.2.8 온 디맨드 검사: 루트킷 및 활성 맬웨어에 대한 대상 지정 검사

활성 루트킷을 검사하려면 미리 정의된 검사 프로파일인 *루트킷 및 활성 맬웨어 검사*를  
사용합니다.

활성 루트킷을 체계적으로 검사하려면

- ▶ 제어 센터로 이동하여 **로컬 보호:: 검사 프로그램** 섹션을 선택합니다.

미리 정의된 검사 프로파일 나타납니다.

- ▶ 미리 정의된 검사 프로파일인 **루트킷 및 활성 맬웨어 검사**를 선택합니다.

- ▶ 각 디렉터리 수준의 확인란을 클릭하여 검사할 다른 노드 및 디렉터리를 강조  
표시합니다.

- ▶ 아이콘을 클릭합니다(Windows XP:  또는 Windows Vista: ).

*Luke Filewalker* 창이 나타나고 온 디맨드 검사가 시작됩니다.

검사가 끝나면 그 결과가 표시됩니다.

## 5.2.9 검색한 바이러스 및 맬웨어에 대응

검색에 대한 작업 섹션에서 AntiVir 프로그램의 보호 구성 요소별로 검색된 바이러스 또는 사용자 동의 없이 설치된 프로그램에 대한 AntiVir 프로그램의 대응 방법을 정의할 수 있습니다.

Guard 의 ProActiv 구성 요소에 사용할 수 있는 구성 가능한 작업 옵션은 없습니다. 검색 알림은 항상 *Guard: 의심스러운 응용 프로그램 동작* 창에 표시됩니다.

검사 프로그램에 대한 작업 옵션:

### - 대화형

대화형 작업 모드에서 검사 프로그램의 검사 결과가 대화 상자에 표시됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**검사 프로그램 검사**의 경우 검사가 완료되면 영향받는 파일 목록과 함께 알림이 제공됩니다. 콘텐츠별 메뉴를 사용하여 감염된 여러 파일에 대해 실행할 작업을 선택할 수 있습니다. 감염된 모든 파일에 대해 표준 작업을 실행하거나 검사 프로그램을 취소할 수 있습니다.

### - 자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다. *알림 표시* 옵션을 사용하면 바이러스가 검색될 때마다 수행한 작업을 알리는 알림이 표시됩니다.

Guard 에 대한 작업 옵션:

### - 대화형

대화형 작업 모드에서는 데이터 액세스가 거부되고 데스크톱 알림이 표시됩니다. 데스크톱 알림에서는 검색된 맬웨어를 제거하거나 자세히 단추를 사용하여 추가 바이러스 관리를 위해 검사 프로그램 구성 요소로 맬웨어를 전송할 수 있습니다. 검사 프로그램은 검색 알림과 함께 상황에 맞는 메뉴를 통해 영향받는 파일을 관리할 수 있는 다양한 옵션이 포함된 창을 표시합니다.

검색::검사 프로그램을 참조하십시오.

### - 자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다. *알림 표시* 옵션을 사용하면 바이러스가 검색될 때마다 데스크톱 알림이 표시됩니다.

MailGuard 및 WebGuard 에 대한 작업 옵션:

### - 대화형

대화형 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 감염된 개체에 대해 수행할 작업을 선택할 수 있는 대화 상자가 나타납니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

### - 자동

자동 작업 모드에서는 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되면 여기서 선택한 작업이 자동으로 실행됩니다. *알림 표시* 옵션을 사용하면 바이러스가 검색될 때마다 알림이 제공됩니다. 이 알림에서 수행할 작업을 확인할 수 있습니다.

대화형 작업 모드에서는 알림에 표시된 감염된 개체에 대한 작업을 선택하고 확인을 클릭하여 그 작업을 실행하는 방법으로, 감염된 바이러스 및 사용자 동의 없이 설치된 프로그램에 대응할 수 있습니다.

감염된 개체 처리를 위한 다음 작업을 선택할 수 있습니다.

#### 참고

선택 가능한 작업은 운영 체제, 검색 사실을 보고하는 보호 구성 요소(AntiVir Guard, AntiVir 검사 프로그램, AntiVir MailGuard, AntiVir WebGuard) 및 검색된 맬웨어 유형에 따라 달라집니다.

#### 검사 프로그램 및 Guard 에 대한 작업(ProActiv 검색 제외):

##### - 복구

파일이 복구됩니다.

이 옵션은 감염된 파일이 복구 가능한 경우에만 사용할 수 있습니다.

##### - 격리 저장소로 이동

파일이 특수한 형식(\*.qua)으로 패키징되어 하드 디스크에 있는 격리 저장소 디렉터리 *INFECTED* 로 이동합니다. 따라서 더 이상 직접 액세스할 수 없습니다. 이 디렉터리의 파일은 나중에 격리 저장소에서 복구하거나 필요할 경우 Avira GmbH 로 보낼 수 있습니다.

##### - 삭제

파일이 삭제됩니다. 이 프로세스는 *덮어쓰기 및 삭제*보다 훨씬 빠릅니다. 부트 섹터 바이러스가 검색된 경우 부트 섹터를 삭제하는 방법으로 이를 삭제할 수 있습니다. 새 부트 섹터가 작성됩니다.

##### - 덮어쓰기 및 삭제

파일을 기본 템플릿으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

##### - 이름 바꾸기

파일 이름의 확장명이 \*.vir 로 바뀝니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

##### - 무시

별도의 조치는 필요 없습니다. 감염된 파일은 해당 컴퓨터에서 활성 상태를 유지합니다.

#### 경고

이 경우 데이터가 손실되고 운영 체제가 손상될 수 있습니다! 부득이한 경우에만 무시 옵션을 선택하십시오.

##### - 항상 무시

Guard 검색에 대한 작업 옵션: Guard는 별도의 조치를 취하지 않습니다. 파일에 대한 액세스가 허용됩니다. 컴퓨터를 다시 시작하거나 바이러스 정의 파일을 업데이트할 때까지 이 파일에 대한 추가 액세스는 모두 허용되고 더 이상 알림은 제공되지 않습니다.

##### - 격리 저장소로 복사

루트킷 검색에 대한 작업 옵션: 검색 항목이 격리 저장소에 복사됩니다.

- 부트 섹터 복구 | 복구 도구 다운로드

감염된 부트 섹터가 발견된 경우의 작업 옵션: 감염된 디스켓 드라이브를 여러 가지 옵션으로 복구할 수 있습니다. AntiVir 프로그램에서 복구를 수행할 수 없는 경우 부트 섹터 바이러스를 검색 및 제거하는 특수 도구를 다운로드할 수 있습니다.

**참고**

실행 중인 프로세스에 대해 작업을 수행하면 작업이 수행되기 전에 해당 프로세스가 종료됩니다.

**ProActiv 구성 요소의 검색에 대한 Guard 작업(수상한 응용 프로그램 작업 알림):**

- 신뢰할 수 있는 프로그램

응용 프로그램이 계속 실행되며, 허용된 응용 프로그램 목록에 추가되고 ProActiv 구성 요소의 모니터링 대상에서 제외됩니다. 허용된 응용 프로그램 목록에 추가되면 모니터링 유형이 콘텐츠로 설정됩니다. 즉, 콘텐츠가 변경되지 않은 상태로 유지되는 경우에만 ProActiv 구성 요소의 모니터링 대상에서 해당 응용 프로그램이 제외됩니다. 구성::Guard::ProActiv::응용 프로그램 필터: 허용된 응용 프로그램을 참조하십시오.

- 프로그램 한 번 차단

응용 프로그램 차단(종료)되고 ProActiv 구성 요소에서 응용 프로그램 작업을 계속 모니터링합니다.

- 이 프로그램 항상 차단

응용 프로그램 차단(종료)되고 차단된 응용 프로그램 목록에 추가되며 더 이상 실행할 수 없습니다. 구성::Guard::ProActiv::응용 프로그램 필터: 차단할 응용 프로그램을 참조하십시오.

- 무시

응용 프로그램이 계속 실행되며, ProActiv 구성 요소에서 응용 프로그램 작업을 계속 모니터링합니다.

**MailGuard 작업: 받는 전자 메일**

- 격리 저장소로 이동

전자 메일과 모든 첨부 파일을 격리 저장소로 이동합니다. 영향받는 전자 메일이 삭제되고 전자 메일의 텍스트 본문 및 모든 첨부 파일은 기본 텍스트로 바꿉니다.

- 삭제

영향받는 전자 메일이 삭제되고 전자 메일의 텍스트 본문 및 모든 첨부 파일은 기본 텍스트로 바꿉니다.

- 첨부 파일 삭제

감염된 첨부 파일이 기본 텍스트로 바꿉니다. 전자 메일 본문도 감염된 경우 이 역시 삭제되고 기본 텍스트로 바꿉니다. 전자 메일 자체는 배달됩니다.

- 첨부 파일을 격리 저장소로 이동

감염된 첨부 파일을 격리 저장소로 이동하고 삭제합니다(기본 텍스트로 바꿨). 전자 메일 본문이 배달되며 영향받는 첨부 파일은 나중에 격리 관리자를 통해 전달할 수 있습니다.

- 무시



해당 전자 메일이 전달됩니다.

**경고**

그러면 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. 예외적인 경우에만 **무시** 옵션을 선택하십시오. 메일 클라이언트의 미리 보기를 사용하지 않도록 설정하고 절대 첨부 파일을 두 번 클릭하여 열지 마십시오!

**MailGuard 작업: 보내는 전자 메일**

- **메일을 격리 저장소로 이동(보내지 않음)**

전자 메일과 모든 첨부 파일을 격리 저장소로 복사하며 보내지는 않습니다. 전자 메일은 전자 메일 클라이언트의 보낸 편지함에 남아 있으며 전자 메일 프로그램에 오류 메시지가 표시됩니다. 사용자의 전자 메일 계정에서 보낸 다른 모든 전자 메일을 대상으로 맬웨어를 검사합니다.

- **메일 보내기 차단(보내지 않음)**

전자 메일이 전송되지 않고 전자 메일 클라이언트의 보낸 편지함에 유지됩니다. 전자 메일 프로그램에 오류 메시지가 표시됩니다. 사용자의 전자 메일 계정에서 보낸 다른 모든 전자 메일을 대상으로 맬웨어를 검사합니다.

- **무시**

해당 전자 메일을 보냅니다.

**경고**

바이러스 및 사용자 동의 없이 설치된 프로그램이 이러한 방법으로 전자 메일을 받는 사람의 컴퓨터 시스템에 침입할 수 있습니다.

**WebGuard 작업:**

- **액세스 거부**

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일이 사용자의 웹 브라우저로 전송되지 않습니다. 액세스가 거부되었음을 알리는 오류 메시지가 웹 브라우저에 표시됩니다.

- **격리 저장소로 이동**

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일을 격리 저장소로 옮깁니다. 영향받는 파일이 정보가 포함된 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

- **무시**

웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일을 WebGuard 에서 사용자의 웹 브라우저로 전달합니다.

**경고**

그러면 바이러스 및 사용자 동의 없이 설치된 프로그램이 사용자의 컴퓨터 시스템에 액세스할 수 있습니다. 예외적인 경우에만 **무시** 옵션을 선택하십시오.

**참고**

복구할 수 없는 의심스러운 파일은 모두 격리 저장소로 이동하는 것이 좋습니다.

**참고**

또한 추론에서 보고한 파일을 Avira에 보내 분석할 수도 있습니다.

예를 들어, 이 파일을 Avira 웹 사이트(<http://www.avira.it/file-upload>)에 업로드할 수 있습니다.


파일 이름에 *HEUR/* 또는 *HEURISTIC/* 접두사가 있으면 추론에서 보고한 파일입니다(예: *HEUR/testfile.\**).

### 5.2.10 격리: 격리된 파일(\*.qua) 처리

격리된 파일을 처리하려면

- ▶ 제어 센터에서 **관리 :: 격리 저장소** 섹션을 선택합니다.
- ▶ 필요한 경우 원래의 파일을 다른 위치에서 해당 컴퓨터로 다시 로드할 수 있도록 해당 파일을 선택합니다.


파일에 대한 자세한 정보를 보려는 경우

- ▶ 파일을 강조 표시하고  을 클릭합니다.

파일에 대한 자세한 정보가 표시되는 속성대화 상자가 나타납니다.

파일을 다시 검사하려는 경우


AntiVir 프로그램의 바이러스 정의 파일이 업데이트되었고 가양성 보고가 의심될 경우 파일을 검사하는 것이 좋습니다. 그러면 다시 검사하여 가양성을 확인하고 파일을 복원할 수 있습니다.

- ▶ 파일을 강조 표시하고  을 클릭합니다.

온 디맨드 검사 설정을 사용하여 파일에서 바이러스 및 맬웨어를 검사합니다.


검사가 끝나면 **검사 통계** 대화 상자가 나타나 다시 검사하기 전과 후의 파일 상태에 대한 통계 정보를 표시합니다.

파일을 삭제하려면

- ▶ 파일을 강조 표시하고  을 클릭합니다.

분석을 위해 Avira 맬웨어 연구 센터 웹 서버로 파일을 업로드하려는 경우

- ▶ 업로드할 파일을 강조 표시합니다.

- ▶  을 클릭합니다.

대화 상자가 열리고 연락처 데이터를 입력하는 양식이 표시됩니다.

- ▶ 필요한 데이터를 모두 입력합니다.
- ▶ 유형으로 **의심스러운 파일** 또는 **가양성**을 선택합니다.
- ▶ **확인**을 클릭합니다.

파일이 압축된 형식으로 Avira 맬웨어 연구 센터 웹 서버에 업로드됩니다.

**참고**

다음과 같은 경우 Avira 맬웨어 연구 센터에서 분석하는 것이 좋습니다.

**추론 검색(의심스러운 파일):** 검사 과정에서 AntiVir 프로그램에 의해 의심스러운 파일로 분류되어 격리 저장소로 이동된 경우. 바이러스 검색 대화 상자에서 또는 검색에서 생성된 보고서 파일에서 Avira 맬웨어 연구 센터의 파일 검사가 권장되었습니다.

**의심스러운 파일:** 사용자가 의심스러운 파일로 간주하고 이를 격리 저장소로 이동했으나 파일의 바이러스 및 맬웨어 검사 결과가 음성인 경우.

**가양성:** 사용자가 바이러스 검색이 가양성(오진)이라고 판단할 경우. AntiVir 프로그램은 파일에서 검색된 항목이 있음을 보고하지만, 맬웨어 감염일 가능성은 매우 낮습니다.


**참고**

업로드하는 파일의 크기는 압축하지 않은 경우 20MB, 압축한 경우 8MB 로 제한됩니다.

**참고**

업로드할 파일을 모두 선택한 다음 **개체 보내기** 단추를 클릭하여 한 번에 여러 개의 파일을 업로드할 수 있습니다.


격리된 개체를 격리 저장소에서 다른 디렉터리로 복사하려는 경우

- ▶ 격리된 개체를 강조 표시하고  을 클릭합니다.  
디렉터리를 선택할 수 있는 검사 대화 상자가 열립니다.
- ▶ 격리된 개체의 복사본을 저장할 디렉터리를 선택하고 선택 항목을 확인합니다.  
선택한 격리된 개체가 선택한 디렉터리에 저장됩니다.

**참고**

격리된 개체는 복원된 파일과 다릅니다. 격리된 개체는 암호화되며 원본 형식으로 실행하거나 읽을 수 없습니다.

격리된 개체의 속성을 텍스트 파일로 내보내려는 경우

- ▶ 격리된 개체를 강조 표시하고  을 클릭합니다.  
선택한 격리된 개체의 데이터가 포함된 텍스트 파일이 열립니다.
- ▶ 텍스트 파일을 저장합니다.


격리 저장소에서 파일을 복원할 수도 있습니다.


- 자세한 내용은 격리: 격리 저장소의 파일 복원 장을 참조하십시오.

### 5.2.11 격리: 격리 저장소의 파일 복원

복원 절차를 제어하는 아이콘은 운영 체제에 따라 다릅니다.


- Windows XP 및 2000:


 이 아이콘은 파일을 원래의 디렉터리로 복원합니다.

 이 아이콘은 파일을 사용자가 선택한 디렉터리로 복원합니다.

- Windows Vista:

Microsoft Windows Vista 의 경우, 현재로서는 제어 센터의 권한이 제한적입니다(예: 디렉터리 및 파일에 대한 액세스). 일부 작업 및 파일 액세스는 확장된 관리자 권한이 있어야만 제어 센터에서 수행할 수 있습니다. 이 확장된 관리자 권한은 검사를 시작할 때마다 검사 프로필을 통해 부여해야 합니다.

 이 아이콘은 파일을 사용자가 선택한 디렉터리로 복원합니다.

 이 아이콘은 파일을 원래의 디렉터리로 복원합니다. 이 디렉터리에 액세스하는 데 확장된 관리자 권한이 필요한 경우 이를 요청하는 메시지가 나타납니다.

격리 저장소의 파일을 복원하려면


**경고**

이 경우 컴퓨터의 데이터가 손실되고 운영 체제가 손상될 수 있습니다! 부득이한 경우에만 **선택한 개체 복원** 기능을 사용하십시오. 새 검사로 복구할 수 있는 파일만 복원합니다.



파일을 다시 검사하고 복구합니다.

- ▶ 제어 센터에서 **관리 :: 격리 저장소** 섹션을 선택합니다.


**참고**

파일 확장명이 \*.eml 인 경우 오로지  옵션을 사용하여 전자 메일 및 전자 메일 첨부 파일을 복원할 수 있습니다.

원래의 위치로 파일을 복원하려면

- ▶ 파일을 강조 표시하고 아이콘을 클릭합니다(Windows 2000/XP의 경우 , Windows Vista의 경우 ).
- 전자 메일에 대해서는 이 옵션을 사용할 수 없습니다.


**참고**

파일 확장명이 \*.eml 인 경우 오로지  옵션을 사용하여 전자 메일 및 전자 메일 첨부 파일을 복원할 수 있습니다.

파일을 복원할 것인지 묻는 메시지가 나타납니다.

- ▶ **예**를 클릭합니다.  
파일이 격리 저장소로 이동하기 전에 있던 디렉터리로 복원됩니다.


지정한 위치로 파일을 복원하려면

- ▶ 파일을 강조 표시하고  을 클릭합니다.  
파일을 복원할 것인지 묻는 메시지가 나타납니다.
- ▶ **예**를 클릭합니다.  
Windows의 디렉터리 선택 기본 창이 나타납니다.
- ▶ 파일을 복원할 디렉터리를 선택하고 확인합니다.  
선택한 디렉터리로 파일이 복원됩니다.

### 5.2.12 격리: 의심스러운 파일을 격리 저장소로 이동

의심스러운 파일을 격리 저장소로 직접 이동하려면

- ▶ 제어 센터에서 **관리 :: 격리 저장소** 섹션을 선택합니다.

- ▶  을 클릭합니다.

Windows의 파일 선택 기본 창이 나타납니다.

- ▶ 파일을 선택하고 확인합니다.  
파일이 격리 저장소로 이동합니다.

격리 저장소의 파일을 AntiVir 검사 프로그램으로 검사할 수 있습니다.

- 자세한 내용은 격리: 격리된 파일(\*.qua) 처리 장을 참조하십시오.

### 5.2.13 검사 프로필 검사 프로필의 파일 형식 수정 또는 삭제

검사 프로필에서 검사할 파일 형식을 추가로 지정하거나 특정 파일 형식을 검사 대상에서 제외하려면(수동 선택 및 사용자 지정 검사 프로필에 대해서만 가능)

제어 센터에서 **로컬 보호 :: 검사** 섹션으로 이동합니다.

- ▶ 편집할 검사 프로필을 마우스 오른쪽 단추로 클릭합니다.

상황에 맞는 메뉴가 나타납니다.

- ▶ **파일 필터**를 선택합니다.
- ▶ 상황에 맞는 메뉴의 오른쪽에 있는 작은 삼각형을 클릭하여 더 확장합니다.

기본, 모든 파일 검사 및 사용자 정의 항목이 나타납니다.

- ▶ **사용자 정의**를 선택합니다.

파일 확장명 대화 상자가 나타나면서 검사 프로필로 검사할 모든 파일 형식의 목록이 표시됩니다.

검사에서 파일 형식을 제외하려는 경우

- ▶ 파일 형식을 강조 표시하고 **삭제**를 클릭합니다.

검사에 파일 형식을 추가하려는 경우

- ▶ 파일 형식을 강조 표시합니다.
- ▶ **추가**를 클릭하고 파일 형식의 확장명을 입력란에 입력합니다.

최대 10자까지 입력 가능하며, 선행 점을 입력하지 않습니다. 와일드카드(\* 및 ? )를 대신 입력할 수 있습니다.


### 5.2.14 검사 프로필 검사 프로필의 바탕 화면 바로 가기 만들기

검사 프로필에 대한 바탕 화면 바로 가기를 이용하면 AntiVir 프로그램의 제어 센터에 액세스하지 않고 바탕 화면에서 곧바로 온 디맨드 검사를 시작할 수 있습니다.

검사 프로필에 대한 바탕 화면 바로 가기를 만들려면

제어 센터에서 **로컬 보호 :: 검사** 섹션으로 이동합니다.

- ▶ 바로 가기를 만들 검사 프로필을 선택합니다.

- ▶  아이콘을 클릭합니다.  
바탕 화면 바로 가기가 만들어집니다.

### 5.2.15 이벤트: 이벤트 필터링

AntiVir 프로그램의 프로그램 구성 요소에서 생성한 이벤트는 제어 센터의 **개요::이벤트**에 표시됩니다(Windows 운영 체제의 이벤트 표시와 유사). 프로그램 구성 요소는 다음과 같습니다.

- 업데이트 프로그램
- 스케줄러
- Guard
- MailGuard
- 검사 프로그램
- FireWall
- WebGuard
- 도우미 서비스
- ProActiv

다음 이벤트 유형이 표시됩니다.

- 정보
- 경고
- 오류
- 검색

표시된 이벤트를 필터링하려면

- ▶ 제어 센터에서 **개요 :: 이벤트** 섹션을 선택합니다.
- ▶ 활성화된 프로그램 구성 요소의 이벤트를 표시하려면 해당 구성 요소의 확인란을 선택합니다.

또는

비활성화된 프로그램 구성 요소의 이벤트를 숨기려면 해당 구성 요소의 확인란을 선택 취소합니다.

- ▶ 이벤트를 표시하려면 해당 이벤트 유형 확인란을 선택합니다.  
또는  
이벤트를 숨기려면 해당 이벤트 유형 확인란을 선택 취소합니다.

### 5.2.16 MailGuard: 검사에서 전자 메일 주소 제외

MailGuard 검사에서 제외할 전자 메일 주소(보낸 사람) 정의(허용 목록 작성):

- ▶ 제어 센터로 이동하여 **온라인 보호 :: MailGuard** 섹션을 선택합니다.  
받는 전자 메일의 목록이 표시됩니다.
- ▶ MailGuard 검사에서 제외할 전자 메일을 강조 표시합니다.

- ▶ 해당 아이콘을 클릭하여 MailGuard 검사에서 전자 메일을 제외합니다.



선택된 전자 메일 주소에 대해서는 앞으로 바이러스 및 사용자 동의 없이 설치되는 프로그램을 더 이상 검사하지 않습니다.

전자 메일 보낸 사람 주소를 제외 목록에 포함하여 더 이상 바이러스, 맬웨어 .

**경고**  
보낸 사람을 신뢰할 수 있는 경우에만 MailGuard 검사에서 전자 메일 주소를 제외하십시오.

**참고**  
구성의 MailGuard :: 일반 :: 예외에서 다른 전자 메일 주소를 제외 목록에 추가하거나 제외 목록의 전자 메일 주소를 제거할 수 있습니다.

### 5.2.17 FireWall: FireWall의 보안 수준 선택

다양한 보안 수준 중에 선택할 수 있습니다. 선택 항목에 따라 다른 어댑터 규칙 구성 옵션이 제공됩니다.

다음 보안 수준을 사용할 수 있습니다.

- 낮음
  - 플로딩 및 포트 검사를 검색합니다.
- 보통
  - 의심스러운 TCP 및 UDP 패키지를 삭제합니다.
  - 플로딩 및 포트 검사를 차단합니다.
- 높음
  - 네트워크에 컴퓨터를 표시하지 않습니다.
  - 외부로부터의 연결을 차단합니다.
  - 플로딩 및 포트 검사를 차단합니다.
- 사용자
  - 사용자 정의 규칙: 이 보안 수준을 선택하면 프로그램에서 어댑터 규칙이 수정되었음을 자동으로 인식합니다.

**참고**  
Avira FireWall 의 미리 정의된 모든 규칙에 대한 기본 보안 수준 설정은 **높음**입니다.

FireWall 의 보안 수준 정의:

- ▶ 제어 센터로 이동하여 온라인 **보호 :: FireWall** 섹션을 선택합니다.
- ▶ 슬라이더를 원하는 보안 수준으로 이동합니다.  
선택한 보안 수준이 즉시 적용됩니다.





## 6 검사 프로그램

검사 프로그램 구성 요소를 사용하면 바이러스 및 사용자 동의 없이 설치된 프로그램에 대해 대상 지정 검사(온 디맨드 검사)를 실시할 수 있습니다. 감염된 파일을 검사할 때 다음 옵션을 사용할 수 있습니다.

- **상황에 맞는 메뉴를 사용한 온 디맨드 검사**

이러한 개별 파일 및 디렉터리를 검사하려는 경우 상황에 맞는 메뉴의 온 디맨드 검사(마우스 오른쪽 단추 클릭 - **AntiVir** 로 선택한 파일 검사 항목)를 실시하는 것이 좋습니다. 상황에 맞는 메뉴를 통해 온 디맨드 검사를 실시할 경우 제어 센터를 먼저 시작할 필요가 없다는 장점도 있습니다.

- **끌어서 놓기를 사용한 온 디맨드 검사**

파일 또는 디렉터리를 제어 센터의 프로그램 창으로 끌면 검사 프로그램에서 해당 파일 또는 디렉터리와 모든 하위 디렉터리를 검사합니다. 예를 들어, 데스크톱에 저장한 개별 파일 및 디렉터리를 검사하려는 경우 이 절차를 이용하는 것이 좋습니다.

- **프로필을 사용한 온 디맨드 검사**

특정 디렉터리 및 드라이브(예: 정기적으로 새 파일을 저장하는 작업 디렉터리 또는 드라이브)를 정기적으로 검사하려는 경우 이 절차를 이용하는 것이 좋습니다. 그러면 새로 검사할 때마다 디렉터리 및 드라이브를 선택할 필요 없이 해당 프로필을 사용하여 선택하면 됩니다.

- **스케줄러를 사용한 온 디맨드 검사**

스케줄러에서는 시간 제약이 있는 검사를 실시할 수 있습니다.

루트킷 또는 부트 섹터 바이러스를 검사하거나 활성 프로세스를 대상으로 검사할 때 특별한 프로세스가 필요합니다. 다음 옵션을 사용할 수 있습니다.

- 검사 프로필인 **루트킷 및 활성 맬웨어 검사**를 통해 루트킷 검사

- 검사 프로필 **활성 프로세스**를 사용한 활성 프로세스 검사

- 추가 메뉴의 메뉴 명령인 **부트 섹터 바이러스 검사**를 사용한 부트 섹터 바이러스 검사

## 7 업데이트

바이러스 백신 소프트웨어의 효과는 해당 프로그램, 특히 바이러스 정의 파일 및 검사 엔진이 얼마나 최신 버전인가에 따라 달라집니다. AntiVir에는 정기 업데이트를 수행하기 위한 업데이트 프로그램 구성 요소가 포함되어 있습니다. AntiVir 프로그램을 항상 최신 상태로 유지하는 이 업데이트 프로그램은 매일 나타나는 새로운 바이러스를 처리할 수 있습니다. 업데이트 프로그램에서는 다음 구성 요소를 업데이트합니다.

- 바이러스 정의 파일:

바이러스 정의 파일에는 유해한 프로그램의 바이러스 패턴이 있으며, AntiVir 프로그램은 이를 사용하여 바이러스 및 맬웨어를 검사하고 감염된 개체를 복구합니다.

- 검사 엔진:

검사 엔진에는 AntiVir 프로그램이 바이러스 및 맬웨어 검사에 사용하는 메서드가 들어 있습니다.

- 프로그램 파일(제품 업데이트):

제품 업데이트용 업데이트 패키지에서는 개별 프로그램 구성 요소에서 사용할 수 있는 추가 기능을 제공합니다.

업데이트 프로그램에서는 바이러스 정의 파일 및 검사 엔진이 최신 버전인지 확인하고 필요하면 업데이트를 구현합니다. 설정된 구성에 따라 업데이트 프로그램에서는 제품 업데이트도 실시하거나 사용자에게 제품 업데이트를 이용할 수 있음을 알립니다. 제품 업데이트 후에는 컴퓨터 시스템을 다시 시작해야 할 수도 있습니다. 바이러스 정의 파일 및 검사 엔진만 업데이트된 경우에는 컴퓨터를 다시 시작할 필요가 없습니다.

### 참고

업데이트 프로그램에서는 보안을 위해 해당 컴퓨터의 Windows 호스트 파일이 수정되었는지, 이를테면 업데이트 URL 이 맬웨어에 의해 수정되어 업데이트 프로그램이 원치 않는 다운로드 사이트로 전환되는지 여부를 확인합니다. Windows 호스트 파일이 수정된 경우 이는 업데이트 프로그램 보고서 파일에 표시됩니다.

업데이트는 다음 간격으로 자동 수행됩니다. 60 분. 구성(구성::업데이트)에서 자동 업데이트를 편집하거나 해제할 수 있습니다.

제어 센터의 스케줄러에서 지정된 간격마다 업데이트 프로그램이 수행할 추가 업데이트 작업을 만들 수 있습니다. 또한 업데이트를 수동으로 시작하는 옵션도 있습니다.

- 제어 센터: 업데이트 메뉴 및 상태 섹션에서
- 트레이 아이콘의 상황에 맞는 메뉴에서

인터넷에서 전용 웹 서버를 통해 또는 인트라넷의 웹 서버 또는 파일 서버를 통해 업데이트를 얻을 수 있습니다. 인트라넷 서버는 인터넷에서 업데이트 파일을 다운로드한 다음 네트워크의 다른 컴퓨터에 제공합니다. 이 기능은 네트워크에 있는 둘 이상의 컴퓨터에서 AntiVir 프로그램을 업데이트할 때 유용합니다. 인트라넷의 다운로드 서버를 통해 최소한의 리소스를 사용하여 보호 대상 컴퓨터의 AntiVir 프로그램을 최신 버전으로 유지할 수 있습니다. 인트라넷에서 정상 작동하는 다운로드 서버를 설정하려면 AntiVir 프로그램의 업데이트 구조와 호환되는 서버가 필요합니다.

### 참고

AntiVir Internet Update Manager(Windows의 파일 서버 또는 웹 서버)를 인트라넷의 웹 서버 또는 파일 서버로 사용할 수 있습니다. Avira AntiVir 제품의 다운로드 서버를 미리링하는 AntiVir Internet Update Manager는 인터넷의 Avira 웹 사이트에서 얻을 수 있습니다.

<http://www.avira.kr>

웹 서버를 사용하여 다운로드할 경우에는 HTTP 프로토콜이 사용됩니다. 파일 서버를 사용할 경우 업데이트 파일에 대한 액세스 권한이 네트워크를 통해 제공됩니다. 웹 서버 또는 파일 서버와의 연결은 일반 :: 업데이트 구성에서 설정할 수 있습니다. 기존의 인터넷 연결을 사용하여 Avira GmbH 웹 서버와 연결하는 것이 기본 구성입니다.

## 8 Avira FireWall :: 개요

Avira FireWall 은 컴퓨터 시스템에서 들어오고 나가는 데이터 트래픽을 모니터링 및 조정하고 인터넷의 다양한 공격 및 위협으로부터 사용자를 보호합니다. 보안 지침에 따라 들어오거나 나가는 데이터 트래픽 또는 포트 수신이 허용되거나 거부됩니다. Avira FireWall 에서 네트워크 작업을 거부하여 네트워크 연결을 차단하면 데스크톱 알림을 받게 됩니다. 다음과 같은 방법을 사용하여 Avira FireWall 을 설정할 수 있습니다.

### - 제어 센터에서 보안 수준 설정

제어 센터에서 보안 수준을 정의할 수 있습니다. 낮음, 보통 및 높음 보안 수준에는 각각 패킷 필터를 기반으로 한 여러 가지 보완적인 보안 규칙이 포함되어 있습니다. 이러한 보안 규칙은 구성 섹션 FireWall::어댑터 규칙에 미리 정의된 어댑터 규칙으로 저장됩니다.

### - 네트워크 이벤트 창에서 작업 저장

응용 프로그램에서 처음으로 네트워크 또는 인터넷 연결을 설정하려고 하면 *네트워크 이벤트* 팝업 창이 나타납니다. *네트워크 이벤트* 창에서 응용 프로그램의 네트워크 작업을 허용하거나 거부하도록 선택할 수 있습니다. **이 응용 프로그램에 대한 작업 저장** 옵션을 사용하면 작업이 응용 프로그램 규칙으로 만들어지고 FireWall::응용 프로그램 규칙의 구성 섹션에 저장됩니다. 네트워크 이벤트 창에서 작업을 저장하면 응용 프로그램의 네트워크 작업에 대한 규칙 집합이 제공됩니다.

### 참고

신뢰할 수 있는 공급자의 응용 프로그램에 대해 어댑터 규칙이 네트워크 액세스를 차단하지 않으면 기본적으로 네트워크 액세스가 허용됩니다. 신뢰할 수 있는 공급자 목록에서 공급자를 제거하는 옵션이 제공됩니다.

### - 구성에서 어댑터 및 응용 프로그램 규칙 만들기

미리 정의된 어댑터 규칙을 변경하거나 구성에서 새 어댑터 규칙을 만들 수 있습니다. 어댑터 규칙을 추가하거나 변경하면 FireWall 의 보안 수준이 자동으로 *사용자값*으로 설정됩니다.

응용 프로그램 규칙을 사용하여 응용 프로그램에 대해 지정한 모니터링 규칙을 정의할 수 있습니다.

간단한 응용 프로그램 규칙을 사용하여 소프트웨어 응용 프로그램의 모든 네트워크 작업을 거부하거나 허용할 것인지 여부 또는 그러한 네트워크 작업을 *네트워크 이벤트* 팝업 창을 사용하여 처리할 것인지 여부를 정의할 수 있습니다.

*응용 프로그램 규칙 설정*의 고급 구성에서는 응용 프로그램에 대해 지정한 응용 프로그램 규칙으로 실행되는 다른 패킷 필터를 정의할 수 있습니다.

**참고**

응용 프로그램 규칙에는 *권한*모드와 *필터링*모드가 있습니다. *필터링*모드의 응용 프로그램 규칙의 경우 관련 어댑터 규칙에 우선 순위가 부여됩니다. 예를 들어 관련 어댑터 규칙이 응용 프로그램 규칙 다음에 실행됩니다. 따라서 높은 보안 수준이나 해당 어댑터 규칙으로 인해 네트워크 액세스가 거부될 수 있습니다. *권한*모드의 응용 프로그램 규칙에서는 어댑터 규칙이 무시됩니다. 응용 프로그램이 *권한* 모드에서 허용되면 응용 프로그램에 항상 네트워크 액세스 권한이 부여됩니다.

## 9 FAQ, 팁

이 장에서는 AntiVir 프로그램의 사용에 대한 팁과 중요한 문제 해결 정보를 설명합니다.

참조: 문제 해결

참조 키보드 명령

참조: Windows 보안 센터

### 9.1 문제 발생 시 도움말

여기에는 가능한 문제 원인 및 해결 방법에 대한 정보가 제공됩니다.

- 라이선스 파일을 열 수 없습니다라는 오류 메시지가 표시됩니다.
- AntiVir MailGuard가 작동하지 않습니다.
- Avira FireWall을 호스트 컴퓨터에 설치하고 Avira FireWall의 보안 수준을 보통 또는 높음으로 설정한 경우, 가상 컴퓨터(예: VMWare, Virtual PC 등)에서 네트워크에 연결할 수 없습니다.
- Avira FireWall의 보안 수준을 보통 또는 높음으로 설정한 경우 VPN(가상 사설망) 연결이 차단됩니다.
- TSL 연결을 통해 보낸 전자 메일이 MailGuard에 의해 차단되었습니다.
- Webchat이 작동하지 않습니다. 채팅 메시지가 표시되지 않습니다.

**라이선스 파일을 열 수 없습니다**라는 오류 메시지가 표시됩니다.

이유: 파일이 암호화되었습니다.

▶ 라이선스를 활성화하기 위해 파일을 열 필요는 없습니다. 프로그램 디렉터리에 저장하십시오. 라이선스 관리자 장도 참조하십시오.

**업데이트하려고 할 때 파일을 다운로드하는 중 연결이 실패했습니다**라는 오류 메시지가 표시됩니다.

이유: 인터넷 연결이 비활성 상태입니다. 따라서 인터넷의 웹 서버에 연결할 수 없습니다.

▶ WWW 또는 전자 메일과 같은 다른 인터넷 서비스가 작동하는지 테스트하십시오. 작동하지 않으면 인터넷 연결을 다시 설정하십시오.

이유: 프록시 서버에 연결할 수 없습니다.

▶ 프록시 서버에 대한 로그인이 변경되었는지 확인하고 필요한 경우 구성에 적용하십시오.

이유: 사용자의 개인 방화벽에서 update.exe 파일을 완전히 승인하지 않았습니다.

▶ 사용자의 개인 방화벽에서 update.exe 파일을 완전히 승인했는지 확인합니다.

그렇지 않은 경우 다음을 수행합니다.

- ▶ 일반::설정 업데이트 구성(고급 모드)에서 설정을 확인하십시오.

**바이러스 및 맬웨어를 이동하거나 삭제할 수 없습니다.**

이유: 파일이 Windows 를 통해 로드되어 활성화 상태입니다.

- ▶ AntiVir 제품을 업데이트하십시오.
- ▶ Windows XP 운영 체제를 사용하는 경우 시스템 복원을 비활성화합니다.
- ▶ 안전 모드로 컴퓨터를 시작합니다.
- ▶ AntiVir 프로그램을 시작하고 구성(고급 모드)을 엽니다.
- ▶ 검사 프로그램::검사::파일::모든 파일을 선택하고 창에서 **확인**을 눌러 확인합니다.
- ▶ 모든 로컬 드라이브의 검색을 시작합니다.
- ▶ 표준 모드로 컴퓨터를 시작합니다.
- ▶ 표준 모드에서 검사를 수행합니다.
- ▶ 다른 바이러스나 맬웨어가 발견되지 않으면 가능한 한 시스템 복원을 활성화하고 사용합니다.

**트레이 아이콘의 상태가 비활성화되었습니다.**

이유: AntiVir Guard 가 사용하지 않도록 설정되어 있습니다.

- ▶ 제어 센터의 AntiVir Guard 영역에 있는 개요::상태 섹션에서 **사용** 링크를 클릭합니다.

이유: AntiVir Guard 가 방화벽에 의해 차단되었습니다.

- ▶ 방화벽 구성에서 AntiVir Guard 에 대한 일반 승인을 정의합니다. AntiVir Guard 는 127.0.0.1(localhost) 주소에서만 작동합니다. 인터넷 연결이 설정되지 않았습니니다. 이는 AntiVir MailGuard 에도 동일하게 적용됩니다.

그렇지 않은 경우 다음을 수행합니다.

- ▶ AntiVir Guard 서비스 시작 유형을 확인합니다 필요한 경우 서비스를 활성화합니다. 작업 표시줄에서 "시작 | 설정 | 제어판"을 선택합니다. 두 번 클릭하여 구성 패널 "서비스"를 시작합니다(Windows 2000 및 Windows XP 에서 서비스 애플릿은 하위 디렉터리 "관리 도구"에 있음). *Avira AntiVir Guard* 항목을 찾습니다. 시작 유형이 "자동"이어야 하고 상태가 "시작"이어야 합니다. 필요한 경우 관련 줄을 선택하고 "시작" 단추를 클릭하여 서비스를 수동으로 시작합니다. 오류 메시지가 표시되면 이벤트 표시를 확인하십시오.

**데이터 백업을 수행하면 컴퓨터 속도가 너무 느립니다.**

이유: AntiVir Guard 는 백업하는 동안 백업 과정에 이용되는 모든 파일을 검사합니다.

- ▶ 구성(고급 모드)에서 Guard::검사::예외를 선택하고 백업 소프트웨어의 프로세스 이름을 입력합니다.

**방화벽이 활성화되는 즉시 AntiVir Guard 및 AntiVir MailGuard 에 보고를 합니다.**

이유: AntiVir Guard 와 AntiVir MailGuard 는 TCP/IP 인터넷 프로토콜을 통해 통신합니다. 방화벽은 이 프로토콜을 통해 모든 연결을 모니터링합니다.

▶ AntiVir Guard 및 AntiVir MailGuard 에 대한 일반 승인을 정의합니다. AntiVir Guard 는 127.0.0.1(localhost) 주소에서만 작동합니다. 인터넷 연결이 설정되지 않았습니까. 이는 AntiVir MailGuard 에도 동일하게 적용됩니다.

### AntiVir MailGuard 가 작동하지 않습니다.

AntiVir MailGuard 에 문제가 발생한 경우 다음 검사 목록을 사용하여 AntiVir MailGuard 가 제대로 작동하는지 확인하십시오.

#### 검사 목록

▶ 메일 클라이언트가 Kerberos, APOP 또는 RPA를 통해 서버에 로그인했는지 확인하십시오. 이러한 확인 방법은 현재 지원되지 않습니다.

▶ 메일 클라이언트가 SSL(TSL - Transport Layer Security이라고도 함)을 통해 서버에 보고하는지 확인합니다. AntiVir MailGuard는 SSL을 지원하지 않으므로 암호화된 SSL 연결을 종료합니다. MailGuard로 보호되지 않은 상태에서 암호화된 SSL 연결을 사용하려면 MailGuard에서 연결을 모니터링하지 않는 포트를 사용해야 합니다. MailGuard에서 모니터링하는 포트는 구성 섹션 MailGuard::검사에서 구성할 수 있습니다.

▶ AntiVir MailGuard 서비스가 활성화 상태입니까 필요한 경우 서비스를 활성화합니다. 작업 표시줄에서 "시작 | 설정 | 제어판"을 선택합니다. 두 번 클릭하여 구성 패널 "서비스"를 시작합니다(Windows 2000 및 Windows XP 에서 서비스 애플릿은 하위 디렉터리 "관리 도구"에 있음). Avira AntiVir MailGuard 항목을 찾습니다. 시작 유형이 "자동"이어야 하고 상태가 "시작"이어야 합니다. 필요한 경우 관련 줄을 선택하고 "시작" 단추를 클릭하여 서비스를 수동으로 시작합니다. 오류 메시지가 표시되면 이벤트 표시를 확인하십시오. 이 작업이 성공적으로 수행되지 않으면 "시작 | 설정 | 제어판 | 프로그램 추가/제거"에서 AntiVir 프로그램을 완전히 제거하고 컴퓨터를 다시 시작한 후 AntiVir 프로그램을 다시 설치해야 합니다.

#### 일반

▶ TLS(전송 계층 보안)라고도 하는 SSL(Secure Sockets Layer)을 통해 암호화된 POP3 연결은 현재 보호할 수 없으며 무시됩니다.

▶ 메일 서버에 대한 확인은 현재 "암호"를 통해서만 지원됩니다. "Kerberos" 및 "RPA"는 현재 지원되지 않습니다.

▶ AntiVir 프로그램은 보내는 전자 메일에 바이러스 및 사용자 동의 없이 설치된 프로그램이 있는지 검사하지 않습니다.

#### 참고

보안에 허점이 생기지 않도록 Microsoft 업데이트를 정기적으로 설치하는 것이 좋습니다.

Avira FireWall 을 호스트 컴퓨터에 설치하고 Avira FireWall 의 보안 수준을 보통 또는 높음으로 설정한 경우, 가상 컴퓨터(예: VMWare, Virtual PC 등)에서 네트워크에 연결할 수 없습니다.



가상 시스템(예: VMWare, Virtual PC 등)을 실행 중인 컴퓨터에 Avira FireWall 을 설치하고 Avira FireWall 의 보안 수준을 보통 또는 높음으로 설정한 경우, 방화벽은 가상 시스템에 대한 모든 네트워크 연결을 차단합니다. 보안 수준이 낮음으로 설정된 경우에는 FireWall 이 정상적으로 작동합니다.

이유: 가상 시스템은 소프트웨어를 사용하여 네트워크 카드를 에뮬레이션합니다. 이 에뮬레이션은 게스트 시스템의 데이터 패킷을 특수한 패킷(UDP 패킷)로 캡슐화하고 외부 게이트웨이를 통해 호스트 시스템에 라우팅합니다. Avira FireWall 은 보안 수준 보통부터 외부에서 들어오는 이러한 패킷을 차단합니다.

이러한 동작이 발생하지 않도록 하려면 다음을 수행하십시오.

- ▶ 제어 센터로 이동하여 **온라인 보호 :: FireWall** 섹션을 선택합니다.
- ▶ 구성 링크를 클릭합니다.
- ▶ 구성대화 상자가 나타납니다. 구성 섹션 **응용 프로그램 규칙**이 표시됩니다.
- ▶ **고급 모드** 옵션을 활성화합니다.
- ▶ 구성 섹션 **어댑터 규칙**을 선택합니다.
- ▶ **규칙 추가**를 클릭합니다.
- ▶ **들어오는 규칙** 섹션에서 **UDP** 를 선택합니다.
- ▶ 규칙 이름 섹션에 규칙 이름을 입력합니다.
- ▶ **확인**을 클릭합니다.
- ▶ 규칙이 **모든 IP 패킷 거부** 규칙 바로 위에 있는지 확인합니다.

#### 경고

이 규칙은 UDP 패킷을 필터링하지 않고 허용하므로 위험 가능성이 있습니다. 가상 시스템 작업 후에 이전 보안 수준으로 변경하십시오.

#### Avira FireWall 의 보안 수준을 보통 또는 높음으로 설정한 경우 VPN(가상 사설망) 연결이 차단됩니다.

이유: 이 문제는 마지막 규칙인 **모든 IP 패킷 거부** 규칙이 그 위에 있는 규칙을 따르지 않는 모든 패킷을 무시하기 때문에 발생합니다. VPN 소프트웨어(GRE 패킷이라고도 함)에서 발송한 패킷 유형은 다른 범주에 맞지 않기 때문에 이 규칙에 의해 필터링됩니다.

**모든 IP 패킷 거부** 규칙을 TCP 및 UPD 패킷을 거부하는 두 개의 새 규칙으로 바꿉니다. 이 방법은 다른 프로토콜의 패킷을 허용할 가능성이 있습니다.

#### TSL 연결을 통해 보낸 전자 메일이 MailGuard 에 의해 차단되었습니다.

이유: TLS(전송 계층 보안: 인터넷에서 데이터 전송을 위한 암호화 프로토콜)는 현재 MailGuard 에서 지원하지 않습니다. 전자 메일을 보내는 데 사용할 수 있는 옵션은 다음과 같습니다.

- ▶ 25 번 포트는 SMTP 에 사용되므로 다른 포트를 사용하십시오. 이렇게 하면 MailGuard 에 의한 모니터링이 무시됩니다.
- ▶ TSL 암호화된 연결을 해제하고 전자 메일 클라이언트에서 TSL 지원을 비활성화하십시오.

- ▶ MailGuard::Scan 구성에서 보내는 전자 메일에 대한 MailGuard 모니터링을 임시로 비활성화합니다.

### Webchat 이 작동하지 않습니다. 채팅 메시지가 표시되지 않고 데이터가 브라우저에 로드 중입니다.

이 현상은 'transfer-encoding= chunked' 로 설정된 HTTP 프로토콜을 기반으로 한 채팅 중에 발생할 수 있습니다.

이유: WebGuard 는 전송된 데이터가 웹 브라우저에 로드되기 전에 해당 데이터에 대해 바이러스 및 사용자 동의 없이 설치된 프로그램을 먼저 검사합니다.

WebGuard 는 'transfer-encoding= chunked'로 설정된 데이터 전송 시 메시지 길이나 데이터 볼륨을 확인하지 못합니다.

- ▶ 웹 채팅 URL의 구성을 예외로 입력합니다(구성: WebGuard::예외 참조).

## 9.2 바로 가기

키보드 명령은 바로 가기라고도 하며, 이를 통해 신속하게 프로그램을 탐색하고 개별 모듈을 검색하고 작업을 시작할 수 있습니다.

다음은 사용 가능한 키보드 명령에 대한 개요입니다. 도움말의 해당 장에서 기능에 대한 세부 지침을 찾아 볼 수 있습니다.

### 9.2.1 대화 상자에서

바로 가기	설명
Ctrl+Tab Ctrl+Page Down	제어 센터 탐색 다음 섹션으로 이동합니다.
Ctrl+Shift+Tab Ctrl+Page Up	제어 센터 탐색 이전 섹션으로 이동합니다.
← ↑ → ↓	구성 섹션 탐색 먼저 마우스를 사용하여 구성 섹션에 포커스를 둡니다.
Tab	다음 옵션 또는 옵션 그룹으로 변경합니다.
Shift+Tab	이전 옵션 또는 옵션 그룹으로 변경합니다.
← ↑ → ↓	표시된 드롭다운 목록의 옵션 간에 또는 옵션 그룹의 여러 옵션 간에 변경합니다.
공백	활성 옵션이 확인란일 경우 확인란을 활성화하거나 비활성화합니다.
Alt+밑줄 문자	옵션을 선택하거나 명령을 시작합니다.

Alt+ ↓ F4	선택한 드롭다운 목록을 엽니다.
Esc	선택한 드롭다운 목록을 닫습니다. 명령을 취소하고 대화 상자를 닫습니다.
Enter	활성 옵션이나 단추에 대한 명령을 시작합니다.

### 9.2.2 도움말에서

바로 가기	설명
Alt+스페이스바	시스템 메뉴를 표시합니다.
Alt+Tab	도움말과 열려 있는 다른 창 간에 전환합니다.
Alt+F4	도움말을 닫습니다.
Shift + F10	상황에 맞는 도움말 메뉴를 표시합니다.
Ctrl+Tab	탐색 창의 다음 섹션으로 이동합니다.
Ctrl+Shift+Tab	탐색 창의 이전 섹션으로 이동합니다.
페이지 위로	목차, 색인 또는 검색 결과 목록에서 위에 표시된 제목으로 변경합니다.
페이지 아래로	목차, 색인 또는 검색 결과 목록에서 현재 제목 아래에 표시된 제목으로 변경합니다.
페이지 위로 페이지 아래로	제목을 검색합니다.

### 9.2.3 제어 센터에서

#### 일반

바로 가기	설명
F1	도움말 표시
Alt+F4	제어 센터 닫기
F5	새로 고침
F8	구성 열기
F9	업데이트 시작

#### 검사 섹션

바로 가기	설명
F2	선택한 프로필 이름 바꾸기

F3	선택한 프로필을 사용하여 검사 시작
F4	선택한 프로필에 대한 마당 화면 링크 만들기
Ins	새 프로필 만들기
Del	선택한 프로필 삭제

### FireWall 섹션

바로 가기	설명
Return	속성

### 격리 섹션

바로 가기	설명
F2	개체 다시 검사
F3	개체 복원
F4	개체 보내기
F6	개체를 다음으로 복원...
Return	속성
Ins	파일 추가
Del	개체 삭제

### 스케줄러 섹션

바로 가기	설명
F2	작업 편집
Return	속성
Ins	새 작업 삽입
Del	작업 삭제

### 보고서 섹션

바로 가기	설명
F3	보고서 파일 표시
F4	보고서 파일 인쇄
Return	보고서 표시
Del	보고서 삭제

이벤트 섹션

바로 가기	설명
F3	이벤트 내보내기
Return	이벤트 표시
Del	이벤트 삭제

### 9.3 Windows 보안 센터

- Windows XP 서비스 팩 2 이상 -

#### 9.3.1 일반

Windows 보안 센터에서는 컴퓨터 상태를 확인하여 중요한 보안 측면을 검사합니다. 이러한 중요한 측면 중 하나에서 문제가 발견되면(예: 오래된 바이러스 백신 프로그램), 보안 센터는 알림을 표시하고 컴퓨터 보호를 향상시키는 방법에 대한 권장 사항을 제공합니다.

#### 9.3.2 Windows 보안 센터 및 AntiVir 프로그램

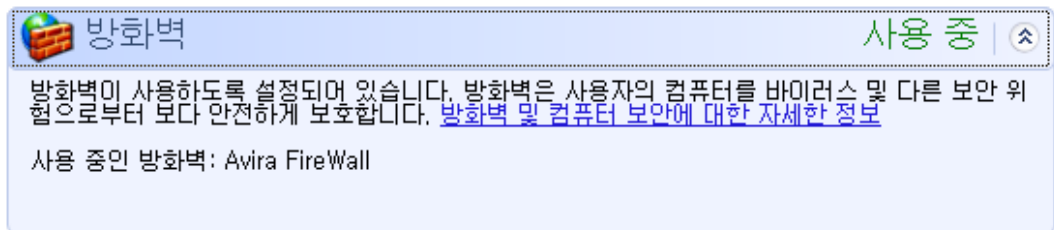
##### FireWall

보안 센터에서 방화벽에 대한 다음 정보를 받을 수 있습니다.

- FireWall 활성화/FireWall 켜짐
- FireWall 비활성화/FireWall 꺼짐



##### FireWall 활성화/FireWall 켜짐

AntiVir 프로그램을 설치하고 Windows 방화벽을 해제하면 다음 메시지가 표시됩니다.



##### FireWall 비활성화/FireWall 꺼짐

Avira FireWall 을 비활성화하는 즉시 다음 메시지가 표시됩니다.

 방화벽
사용 안 함 | 

방화벽이 사용하지 않도록 설정되어 있습니다. 방화벽은 사용자의 컴퓨터에 손상을 줄 수 있는 인터넷 콘텐츠로부터 사용자의 컴퓨터를 안전하게 보호하도록 돕습니다. 이 문제를 해결하는 방법을 보려면 [권장 사항]을 클릭하십시오. [방화벽 및 컴퓨터 보안에 대한 자세한 정보](#)

사용 중이 아닌 방화벽: Avira FireWall

**참고**

제어 센터의 상태 탭을 통해 Avira FireWall 을 활성화하거나 비활성화할 수 있습니다.

**경고**

Avira FireWall 을 해제하면 권한이 없는 사용자가 네트워크나 인터넷을 통해 컴퓨터에 액세스하는 것을 차단할 수 없습니다.



**바이러스 방지 소프트웨어/악의적인 소프트웨어로부터 보호**

Windows 보안 센터에서 바이러스 방지에 대한 다음 정보를 받을 수 있습니다.

- 바이러스 방지 기능을 찾을 수 없음
- 바이러스 방지 기능이 오래됨
- 바이러스 방지 기능 설정
- 바이러스 방지 기능 해제
- 바이러스 방지 기능이 모니터링되지 않음

**바이러스 방지 기능을 찾을 수 없음**

Windows 보안 센터에서 사용자의 컴퓨터를 확인하여 바이러스 방지 소프트웨어를 찾을 수 없으면 다음과 같은 Windows 보안 센터 정보가 나타납니다.

 바이러스 백신
찾을 수 없음 | 

Windows가 이 컴퓨터에서 바이러스 백신 소프트웨어를 찾지 못했습니다. 바이러스 백신 소프트웨어는 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 보다 안전하게 보호합니다. 사용자가 수행할 수 있는 작업을 보려면 [권장 사항]을 클릭하십시오. [바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

참고: Windows에서 모든 바이러스 백신 프로그램을 감지하지는 못합니다.

**참고**

바이러스 및 기타 사용자 동의 없이 설치된 프로그램으로부터 보호하려면 컴퓨터에 AntiVir 프로그램을 설치하십시오.

**바이러스 방지 기능이 오래됨**

Windows XP 서비스 팩 2 또는 Windows Vista 를 설치하고 AntiVir 프로그램을 설치하거나, AntiVir 프로그램이 이미 설치된 시스템에 Windows XP 서비스 팩 2 또는 Windows Vista 를 설치하는 경우 다음 메시지가 표시됩니다.

바이러스 백신
최신 버전 아님

바이러스 백신 소프트웨어가 최신으로 유지되어 있지 않습니다. 사용자가 수행할 수 있는 작업을 보려면 [권장 사항]을 클릭하십시오.  
[바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

참고: Windows에서 모든 바이러스 백신 프로그램을 검색하지는 못합니다.  
 최신으로 유지해야 하는 바이러스 백신 소프트웨어: AntiVir Desktop

권장 사항(E)...

**참고**  
 Windows 보안 센터에서 AntiVir 프로그램을 최신 상태로 인식하게 하려면 설치 후 업데이트를 수행해야 합니다. 업데이트를 수행하여 시스템을 업데이트합니다.

바이러스 방지 설정

AntiVir 프로그램을 설치하고 업데이트를 설치하면 다음 메시지가 표시됩니다.

바이러스 백신
사용 중

바이러스 백신 소프트웨어가 최신으로 유지되어 있으며 바이러스 검사 기능이 사용되고 있음이 검색되었습니다. 바이러스 백신 소프트웨어는 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 보다 안전하게 보호합니다. [바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

사용 중인 바이러스 백신 소프트웨어: AntiVir Desktop

AntiVir 프로그램이 현재 최신 상태이며 AntiVir Guard 가 활성화 상태입니다.

바이러스 방지 끄기

AntiVir Guard 를 비활성화하거나 Guard 서비스를 중지하면 다음 메시지가 표시됩니다.

바이러스 백신
사용 안 함

바이러스 프로그램이 사용되고 있지 않습니다. 바이러스 백신 소프트웨어는 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 보다 안전하게 보호합니다. 사용자가 수행할 수 있는 작업을 보려면 [권장 사항]을 클릭하십시오.  
[바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

참고: Windows에서 모든 바이러스 백신 프로그램을 검색하지는 못합니다.  
 검색된 바이러스 백신 프로그램: AntiVir Desktop



권장 사항(E)...

**참고**  
 제어 센터의 개요::상태 섹션에서 AntiVir Guard 를 사용하거나 사용하지 않도록 설정할 수 있습니다. 작업 표시줄에 빨간색 우산이 켜져 있으면 AntiVir Guard 를 사용 중인 것입니다.

바이러스 방지 기능이 모니터링되지 않음

Windows 보안 센터에서 다음 메시지를 받을 경우 바이러스 방지 소프트웨어를 직접 모니터링하도록 설정한 것입니다.

**참고**  
 Windows Vista 에서는 이 기능을 지원하지 않습니다.

 바이러스 백신
모니터링하지 않음 

사용자가 직접 관리하는 바이러스 백신 소프트웨어를 사용하고 있다고 선택했습니다. 사용자의 컴퓨터를 바이러스 및 다른 보안 위협으로부터 안전하게 보호하기 위해 바이러스 백신 소프트웨어를 사용하고 최신으로 유지하고 있는지 확인하십시오.  
[바이러스 백신 소프트웨어 및 컴퓨터 보안에 대한 자세한 정보](#)

**참고**

AntiVir 프로그램은 Windows 보안 센터를 지원합니다. "권장 사항..." 단추를 사용하여 언제든지 이 옵션을 사용하도록 설정할 수 있습니다.

**참고**

Windows XP 서비스 팩 2 또는 Windows Vista 를 설치한 경우에도 바이러스 방지 솔루션이 필요합니다. Windows XP 서비스 팩 2 는 바이러스 방지 소프트웨어를 모니터링하지만 바이러스 방지 기능 자체가 포함되어 있지는 않습니다. 따라서 추가 바이러스 방지 솔루션이 없으면 바이러스 및 기타 맬웨어로부터 보호되지 않습니다.



# 10 바이러스 및 기타

## 10.1 확장된 위협 범주

### 다이얼러(다이얼러)

인터넷에서 제공하는 일부 서비스는 유료입니다. 독일의 경우 0190/0900 번호의 다이얼러에서 요금이 부과됩니다. 오스트리아 및 스위스에서는 09x0 이고 독일에서는 중반기에 09x0 으로 바뀔 예정입니다. 이러한 프로그램이 컴퓨터에 설치되면 해당 프리미엄 요금제 번호를 통한 연결이 보장되는데, 요금에 큰 차이가 있을 수 있습니다.

전화 요금 고지서를 통한 온라인 콘텐츠 마케팅은 합법적이며 사용자에게 유익할 수 있습니다. 정품 다이얼러는 사용자가 목적에 따라 의도적으로 사용하므로 위험할 여지가 없습니다. 이러한 다이얼러는 명확하고 확실히 표시되는 레이블 또는 요청을 통해 사용자가 동의한 경우에만 사용자의 컴퓨터에 설치됩니다. 정품 다이얼러의 전화 접속 프로세스는 명확하게 표시됩니다. 게다가 정품 다이얼러에서는 발생한 요금을 착오 없이 정확하게 알려 줍니다.

그러나 의심스러운 수단을 통해 또는 속이려는 의도로 사용자 모르게 컴퓨터에 설치되는 다이얼러도 있습니다. 예를 들어, 인터넷 사용자의 기본 ISP(Internet Service Provider) 데이터 통신 링크를 바꿔 놓고 연결이 설정될 때마다 유료 번호, 종종 엄청나게 비싼 0190/0900 번호로 전화를 걸게 합니다. 사용자는 전화요금 고지서를 받아볼 때까지는 자신의 컴퓨터에 설치된 0190/0900 다이얼러 프로그램이 연결할 때마다 프리미엄 요금제 번호로 전화를 걸어 통신 요금이 크게 늘어났다는 사실을 알아채기가 어렵습니다.

전화 서비스 공급자에게 직접 연락해 그 번호 범위를 차단하도록 요청함으로써 사용자 동의 없이 설치되는 다이얼러(0190/0900 다이얼러)를 즉시 차단하는 것이 좋습니다.

AntiVir 프로그램은 대표적인 다이얼러를 기본적으로 감지할 수 있습니다.

확장된 위협 범주 구성에서 **다이얼러** 옵션이 사용되도록 설정된 경우(확인 표시 있음), 다이얼러가 검색되면 알림이 표시됩니다. 이제 사용자 동의 없이 설치되었을 0190/0900 다이얼러를 간단하게 삭제할 수 있습니다. 그러나 사용자가 동의하여 설치된 전화 접속 프로그램인 경우 이를 예외 파일로 선언하면 앞으로 더 이상 검사하지 않습니다.

### 게임(GAMES)

컴퓨터 게임을 즐겨도 괜찮은 곳이 있습니다. 그러나 (아마도 점심 시간을 제외하고) 직장은 해당되지 않을 것입니다. 그럼에도 불구하고 회사 직원 및 공무원들이 인터넷에서 다운로드할 수 있는 수많은 게임, 지뢰찾기, **Patience** 등을 즐기곤 합니다. 인터넷에서 온갖 종류의 게임을 다운로드할 수 있습니다. 전자 메일 게임 또한 갈수록 인기를 얻는 중입니다. 간단한 체스부터 "해전"(어뢰 전투 등)까지 수많은 종류의 게임들이 배포되고 있습니다. 이러한 게임이 전자 메일 프로그램을 통해 파트너에게 전해지기도 합니다.

조사에 따르면, 업무 중에 컴퓨터 게임에 보내는 시간이 미치는 경제적 영향은 이미 오래 전부터 상당한 수준에 이르렀습니다. 따라서 점점 더 많은 기업들이 업무용 컴퓨터에서 컴퓨터 게임을 금지하는 방법을 모색하고 있습니다.

**AntiVir** 프로그램은 컴퓨터 게임을 인식합니다. 위협 범주 구성에서 **게임** 옵션에 확인 표시를 하여 사용하도록 설정한 경우, **AntiVir** 프로그램에 게임이 감지되면 해당하는 알림을 받게 됩니다. 이제 간단하게 삭제할 수 있으므로, 진정한 의미로 게임은 끝난 것입니다.

### 장난 프로그램(JOKES)

장난 프로그램은 피해를 주거나 복제되는 일 없이 누군가를 놀라게 하거나 재미를 선사하는 데 목적이 있습니다. 장난 프로그램이 로드된 컴퓨터는 특정 시점에 어떤 멜로디를 재생하거나 이상한 화면을 표시합니다. 예를 들면, 디스크 드라이브의 세탁기(DRAIN.COM) 또는 화면을 차지하는 프로그램(BUGSRES.COM)이 있습니다.

그러나 조심하십시오. 장난 프로그램의 모든 증상이 바이러스 또는 트로이 목마에서 비롯되었을 수도 있습니다. 적어도 사용자가 너무 놀라거나 당황한 나머지 화를 자초할 수도 있습니다.

**AntiVir** 프로그램은 광범위한 검사 및 식별 루틴을 통해 장난 프로그램을 감지하고, 필요하면 이를 사용자 동의 없이 설치된 프로그램으로 간주하여 제거할 수 있습니다. 위협 범주 구성에서 **장난 프로그램** 옵션에 확인 표시를 하여 사용하도록 설정한 경우, 장난 프로그램이 감지되면 알림이 표시됩니다.

### SPR(Security Privacy Risk)

시스템의 보안을 손상시킬 소지가 있는 소프트웨어는 사용자 동의 없이 설치된 프로그램의 활동을 개시하거나 개인 정보를 유출하거나 사용자의 동작을 염탐하므로 이 역시 사용자 동의 없이 설치되는 것으로 간주할 수 있습니다.

**AntiVir** 프로그램은 "SPR(Security Privacy Risk)" 소프트웨어를 감지합니다. 확장된 위협 범주 구성에서 **SPR(Security Privacy Risk)**에 확인 표시를 하여 사용하도록 설정한 경우, **AntiVir** 프로그램에 그러한 소프트웨어가 감지되면 해당하는 알림을 받게 됩니다.

### 백도어 클라이언트(BDC)

사용자 몰래 컴퓨터에 설치되어 데이터를 유출하거나 컴퓨터를 조작하는 프로그램을 백도어 서버 프로그램이라고 합니다. 이 프로그램은 제 3 자가 인터넷이나 네트워크를 통해 백도어 제어 소프트웨어(클라이언트)를 사용하여 제어할 수 있습니다.

AntiVir 프로그램은 "백도어 제어 소프트웨어"를 인식합니다. 확장된 위협 범주 구성에서 **백도어 제어 소프트웨어(BDC)** 옵션에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 그러한 소프트웨어가 감지되면 해당하는 알람을 받게 됩니다.

#### **애드웨어/스파이웨어(ADSPY)**

"광고를 표시하거나 사용자의 개인 데이터를 당사자 모르게 또는 당사자의 동의 없이 제 3 자에게 보내는 소프트웨어이며, 따라서 사용자 동의 없이 설치되는 소프트웨어로 간주할 수 있습니다."

AntiVir 프로그램은 "애드웨어/스파이웨어"를 인식합니다. 확장된 위협 범주 구성에서 **애드웨어/스파이웨어(ADSPY)**에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 애드웨어나 스파이웨어가 감지되면 해당하는 알람을 받게 됩니다.

#### **비정상적인 런타임 압축 프로그램(PCK)**

비정상적인 런타임 압축 프로그램으로 압축된 파일은 잠재적 의심 파일로 분류할 수 있습니다.

AntiVir 프로그램은 "비정상적인 런타임 압축 프로그램"을 인식합니다. 확장된 위협 범주 구성에서 **비정상적인 런타임 압축 프로그램**에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 그러한 압축 프로그램이 감지되면 해당하는 알람을 받게 됩니다.

#### **이중 확장명 파일(HEUR-DBLEXT)**

실제 파일 확장명을 의심스럽게 숨긴 실행 파일입니다. 이러한 위장 방법은 맬웨어에서 종종 사용합니다.

AntiVir 프로그램은 "이중 확장명 파일"을 인식합니다. 확장된 위협 범주 구성에서 **이중 확장명 파일(HEUR-DBLEXT)**에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 그러한 파일이 감지되면 해당하는 알람을 받게 됩니다.

#### **피싱**

*브랜드 스푸핑*이라고도 하는 피싱은 인터넷 서비스 공급자, 은행, 온라인 बैं킹 서비스, 등록 기관 등의 고객 또는 잠재 고객을 겨냥하는, 지능적인 데이터 도용 수법입니다.

인터넷에서 전자 메일 주소를 보내거나 온라인 양식을 작성하거나 뉴스 그룹 또는 웹 사이트에 액세스할 경우 "인터넷 크롤링 스파이더"에서 데이터를 훔쳐내 본인의 동의 없이 사기 또는 기타 범죄 행위에 이용할 수 있습니다.

AntiVir 프로그램은 "피싱"을 인식합니다. 확장된 위협 범주 구성에서 **피싱**에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 그러한 동작이 감지되면 해당하는 알람을 받게 됩니다.

#### **응용 프로그램(APPL)**

APPL 은 사용할 경우 위험을 초래할 수 있거나 출처가 의심스러운 응용 프로그램을 가리킵니다.

AntiVir 프로그램은 "응용 프로그램(APPL)"을 인식합니다. 확장된 위협 범주 구성에서 **응용 프로그램(APPL)**에 확인 표시를 하여 사용하도록 설정한 경우, AntiVir 프로그램에 그러한 동작이 감지되면 해당하는 알림을 받게 됩니다.

## 10.2 바이러스 및 기타 맬웨어

### 애드웨어

애드웨어는 컴퓨터 화면에 나타나는 표시줄을 통해 배너 또는 팝업 창을 표시하는 소프트웨어입니다. 일반적으로 이러한 광고는 제거할 수 없어 항상 표시되곤 합니다. 연결 데이터를 통해 사용 동작에 관한 많은 정보를 얻을 수 있어 데이터 보안 측면에서 문제가 됩니다.

### 백도어

백도어는 컴퓨터 액세스 보안 메커니즘을 우회하여 컴퓨터에 액세스할 수 있습니다. 백그라운드에서 실행 중인 프로그램은 사이버 범죄자에게 거의 무제한의 권한을 부여할 수 있습니다. 백도어를 통해 사용자의 개인 정보를 엿볼 수 있습니다. 그러나 백도어는 주로 다른 컴퓨터 바이러스나 웜을 관련된 시스템에 설치하는 데 이용됩니다.

### 부트 바이러스

하드 디스크의 부트 또는 마스터 부트 섹터는 주로 부트 섹터 바이러스에 감염됩니다. 부트 섹터 바이러스는 시스템을 실행하는 데 필요한 중요 정보를 덮어씁니다. 심각한 결과 중 하나로 컴퓨터 시스템을 더 이상 로드할 수 없게 됩니다....

### 봇넷

인터넷에 있는 원격 PC 네트워크라고 정의되는 봇넷은 서로 통신하는 봇들로 구성됩니다. 봇넷은 일반 명령 및 제어 인프라를 통해 프로그램(일반적으로 웜, 트로이 목마라고 함)을 실행하는 일련의 감염된 시스템으로 구성될 수 있습니다. 봇넷은 DoS(Denial-of-Service)를 비롯한 다양한 목적으로 이용되며, 감염된 PC 사용자는 대개 공격을 인식하지 못합니다. 봇넷의 가장 큰 위험성은 이 네트워크가 컴퓨터 수천 대의 규모로 커지면서 총 대역폭이 일반적인 인터넷 액세스 대부분을 불능 상태로 만들 수 있다는 것입니다.

### 익스플로잇

익스플로잇(보안 허점)은 버그, 결함 또는 취약점을 이용하여 컴퓨터 시스템에 대한 권한 상승 또는 DoS 를 유발하는 컴퓨터 프로그램 또는 스크립트입니다. 익스플로잇 형식의 예로는 조작된 데이터 패키지를 활용한 인터넷 공격이 있습니다. 더 높은 액세스 권한을 얻기 위해 프로그램을 침투시킬 수 있습니다.

### 혹스(Hoax)

몇 년 전부터 인터넷 및 기타 네트워크 사용자들에게 전자 메일을 통해 유포되었다는 바이러스에 관한 알람 메시지가 전달되곤 했습니다. 전자 메일을 통해 받게 되는 이러한 알람에서는 가급적 많은 동료 및 사용자들에게 그 메시지를 전달하여 모든 사람들에게 "위험"을 경고해야 한다고 주장합니다.

### 허니팟

허니팟은 네트워크에 설치된 서비스(프로그램 또는 서버)입니다. 네트워크를 모니터링하고 공격을 기록하는 기능을 합니다. 이 서비스는 합법적인 사용자에게 알려지지 않으며, 따라서 사용자의 주소가 지정되지 않습니다. 공격자가 네트워크의 취약점을 찾고 허니팟에서 제공하는 서비스를 이용할 경우, 로그에 기록되고 알람이 발효됩니다.

### 매크로 바이러스

매크로 바이러스는 응용 프로그램의 매크로 언어(예: WinWord 6.0 의 WordBasic)로 작성되어 이 응용 프로그램 문서에서만 확산될 수 있는 작은 프로그램입니다. 따라서 문서 바이러스라고도 합니다. 매크로 바이러스가 활성화하려면 해당 응용 프로그램이 활성화되고 감염된 매크로 중 하나가 실행되어야 합니다. "일반적인" 바이러스와 달리 매크로 바이러스는 실행 파일이 아니라 해당 호스트 응용 프로그램의 문서를 공격 대상으로 삼습니다.

### 파밍

파밍은 웹 브라우저의 호스트 파일을 수정하여 쿼리가 스푸핑된 웹 사이트로 전달되게 합니다. 이는 고전적인 피싱 수법에서 발전된 형태입니다. 파밍 수법을 구사하는 자들은 가짜 웹 사이트가 저장된 대규모 서버 팜을 자체적으로 운영합니다. 파밍은 다양한 DNS 공격 유형을 아우르는 용어로 쓰이고 있습니다. 호스트 파일을 수정하는 경우, 트로이 목마 또는 바이러스를 이용하여 시스템을 수정하곤 합니다. 그로 인해 올바른 웹 주소를 입력하더라도 해당 시스템은 가짜 웹 사이트에만 액세스하게 됩니다.

### 피싱

피싱은 인터넷 사용자의 개인 정보를 얻어내는 것입니다. 일반적으로 피싱 수법에서는 공식 서한처럼 보이는 전자 메일 등을 피해자들에게 보내 그들이 좋은 의도로 기밀 정보(특히 온라인 बैं킹 계정의 사용자 이름, 암호, PIN, TAN 등)를 공개하게끔 유도합니다. 이렇게 훔쳐낸 액세스 정보를 이용하여 그 피해자의 신분을 가장하고 거래를 수행합니다. 분명한 것은 은행 및 보험사에서는 절대로 전자 메일, SMS 또는 전화를 통해 신용카드 번호, PIN, TAN 또는 기타 액세스 정보를 요청하지 않는다는 점입니다.

### 다형성 바이러스

폴리모프 바이러스는 위장의 귀재입니다. 자체 프로그래밍 코드를 바꾸므로 찾아내기가 매우 어렵습니다.

### 프로그램 바이러스

컴퓨터 바이러스는 실행된 후 다른 프로그램에 첨부되어 감염시킬 수 있는 프로그램입니다. 바이러스는 논리 폭탄(지발형 바이러스)이나 트로이 목마와 달리 스스로 증식됩니다. 웜과는 대조적으로 바이러스는 악성 코드를 실행할 호스트 프로그램이 반드시 필요합니다. 호스트 프로그램 자체가 실행된다는 규칙은 바뀌지 않습니다.

### 루트킷

루트킷은 컴퓨터 시스템이 침입을 받은 후 설치되는 소프트웨어 도구의 모음으로서 침입자의 로그인을 은폐하고 프로세스를 숨기며 데이터를 기록합니다. 요컨대 침입자가 드러나지 않게 합니다. 이미 설치된 스파이 프로그램을 업데이트하고 삭제된 스파이웨어를 다시 설치하려고 시도합니다.

### 스크립트 바이러스 및 웜

이러한 바이러스는 매우 쉽게 프로그래밍할 수 있으므로, 필요한 기술만 있다면 전자 메일을 통해 불과 몇 시간 만에 전 세계에 확산될 수 있습니다.

스크립트 바이러스 및 웜은 Javascript, VBScript 와 같은 스크립트 언어를 이용하여 다른 새로운 스크립트에 침투하거나 운영 체제 기능을 호출하여 유포됩니다. 주로 전자 메일 또는 파일(문서)을 주고 받는 과정에서 종종 발생합니다.

웜은 자체적으로 증식되지만 호스트를 감염시키지는 않는 프로그램입니다. 따라서 웜은 다른 프로그램 시퀀스에 포함될 수 없습니다. 주로 웜은 보안 수단이 제한된 시스템에 유해 프로그램을 침투시키는 역할만 담당합니다.

### 스파이웨어

스파이웨어는 사용자의 명시적인 동의 없이 컴퓨터 작업을 가로채거나 부분적으로 제어하는 스파이 프로그램입니다. 스파이웨어는 감염된 컴퓨터를 이용해 금전적 이익을 얻기 위해 만들어집니다.

### 트로이 목마

현재 트로이는 매우 일반적인 바이러스입니다. 특정 기능이 있는 것처럼 가장하지만, 실행된 후에 본색을 드러내면서 대개의 경우 파괴적인 다른 기능을 수행하는 프로그램이 트로이 목마에 해당합니다. 트로이 목마는 자가 증식할 수 없다는 특징으로 바이러스 및 웜과 구별됩니다. 대부분의 트로이 목마는 사용자가 트로이 목마를 실행하도록 하기 위해 흥미를 끄는 이름(SEX.EXE 또는 STARTME.EXE)이 붙어 있습니다. 실행 직후 활성화되어 하드 디스크를 포맷하는 등의 작업을 수행할 수 있습니다. 드로퍼(dropper)는 특수한 형태의 트로이 목마로서 바이러스를 '투하'합니다. 즉 바이러스가 컴퓨터 시스템에 내장되게 합니다.

### 좀비

좀비 PC는 맬웨어 프로그램에 감염된 컴퓨터이며 해커가 해당 컴퓨터를 원격으로 제어하여 범죄에 이용할 수 있습니다. 감염된 PC는 해커의 명령에 따라 DoS 공격을 개시하거나 스팸 및 피싱 전자 메일을 보냅니다.

# 11 정보 및 서비스

이 장은 Avira 에 문의하는 방법을 안내합니다.

참조: 연락처 주소

참조: 기술 지원

참조: 의심스러운 파일

참조: 가양성 보고

참조: 보안 강화를 위한 사용자 의견 보내기

## 11.1 연락처 주소

AntiVir 제품군에 대해 궁금한 사항이나 요청 사항이 있을 경우 언제든지 문의해 주십시오. 연락처 정보는 제어 센터의 도움말 :: Avira AntiVir Professional 정보를 참조하십시오.

## 11.2 기술 지원

Avira 지원 부서에서는 고객의 질문 또는 기술적 문제를 해결할 수 있도록 믿음직한 서비스를 제공합니다.

Avira 의 종합적인 지원 서비스에 대한 모든 정보는 웹 사이트에서 확인하실 수 있습니다.

<http://www.avira.kr/support>

신속하고 확실한 지원이 이루어질 수 있도록 다음 정보를 함께 제공해 주십시오.

- **라이선스 정보.** 프로그램 인터페이스는 도움말 :: Avira AntiVir Professional 정보 :: 라이선스 정보
- **버전 정보.** 프로그램 인터페이스는 도움말 :: Avira AntiVir Professional 정보:: 버전 정보 메뉴 항목에서 확인하실 수 있습니다.
- 설치된 **운영 체제 버전** 및 모든 서비스 팩
- 설치된 **소프트웨어 패키지**(예: 다른 공급업체의 바이러스 백신 소프트웨어)
- 프로그램 또는 보고서 파일의 **정확한 메시지**

## 11.3 의심스러운 파일

Avira 제품에서 검색하거나 제거할 수 없는 바이러스 또는 의심스러운 파일은 Avira 에 보내 주십시오. 몇 가지 방법을 통해 보내실 수 있습니다.

- AntiVir Server 콘솔 제어 센터의 격리 관리자에서 파일을 확인하고 상황에 맞는 메뉴 또는 해당 단추를 사용하여
  - 필요한 파일을 압축(WinZIP, PKZip, Arj 등)하고 전자 메일에 첨부하여 주소로 보내 주십시오.  
virus@avira.kr
- 일부 전자 메일 게이트웨이에서는 바이러스 백신 소프트웨어와 연동하므로 파일과 함께 암호도 제공해야 합니다. 반드시 암호를 알려 주십시오.

또는 Avira 웹 사이트를 통해 의심스러운 파일을 보낼 수도 있습니다. <http://www.avira.it/file-upload>

## 11.4 가양성 보고

AntiVir 프로그램에서 검색된 항목이 있다고 보고한 파일이 "깨끗한" 파일일 가능성이 매우 크다고 생각되는 경우, 해당 파일을 압축(WinZIP, PKZip, Arj 등)하고 전자 메일에 첨부하여 다음 주소로 보내 주십시오.

- virus@avira.kr

일부 전자 메일 게이트웨이에서는 바이러스 백신 소프트웨어와 연동하므로 파일과 함께 암호도 제공해야 합니다. 반드시 암호를 알려 주십시오.

## 11.5 보안 강화를 위한 사용자 의견 보내기

Avira 는 고객 여러분의 보안을 무엇보다 중요하게 생각합니다. 따라서 Avira 는 사내 전문가 팀을 통해 제품 출시에 앞서 모든 Avira GmbH 솔루션의 품질과 보안을 테스트할 뿐 아니라 만일에 발생할 수 있는 보안 관련 허점의 징후도 중요하게 간주하며, 이 문제를 진지하게 취급하고 있습니다.

Avira 제품에서 보안 허점을 발견하신 경우 다음 주소로 전자 메일을 보내 주십시오.  
vulnerabilkries@avira.kr



## 12 참조: 구성 옵션

구성 참조는 사용할 수 있는 모든 구성 옵션을 문서화합니다.

### 12.1 검사 프로그램

구성의 검사 프로그램 섹션에서는 온 디맨드 검사를 구성합니다.

#### 12.1.1 검사

여기에서는 온 디맨드 검사에 대한 검사 루틴의 기본 동작을 정의합니다. 온 디맨드 검사에서 검사할 특정 디렉터리를 선택하는 경우 구성에 따라 검사 프로그램에서 다음과 같이 검사합니다.

- 특정 우선 순위를 적용하여 검사
- 부트 섹터와 주 메모리 검사
- 특정 또는 모든 부트 섹터 및 주 메모리 검사
- 디렉터리의 모든 파일 또는 선택한 파일 검사

#### 파일

검사 프로그램에서는 필터를 사용하여 특정 확장명(형식)이 지정된 파일만 검사할 수 있습니다.

#### 모든 파일

이 옵션을 선택하면 파일 내용과 파일 확장명에 관계없이 모든 파일을 대상으로 바이러스 및 사용자 동의 없이 설치되는 프로그램을 검사하며, 필터는 사용되지 않습니다.

#### 참고

모든 파일 옵션을 사용하는 경우 **파일 확장명** 단추를 선택할 수 없습니다.

#### 스마트 확장명

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 있는지 검사할 파일을 프로그램에서 자동으로 선택합니다. 즉, 파일을 검사할지 여부를 AntiVir 프로그램이 파일 내용에 따라 결정합니다. 이 절차는 파일 확장명 목록 사용보다는 다소 느리지만 파일 확장명만을 기준으로 검사하지 않으므로 더 정확합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

#### 참고

스마트 확장명 옵션을 사용하는 경우 **파일 확장명** 단추를 선택할 수 없습니다.

#### 파일 확장명 목록 사용

이 옵션을 사용하면 지정된 확장명의 파일만 검사합니다. 바이러스와 사용자 동의 없이 설치된 프로그램을 포함할 수 있는 모든 파일 형식이 미리 설정되어 있습니다. 이 목록은 "**파일 확장명**" 단추를 통해 수동으로 편집할 수 있습니다.

**참고**

이 옵션을 사용하고 파일 확장명 목록에서 모든 항목을 삭제한 경우 **파일 확장명** 단추 아래에 "파일 확장명 없음"이라는 텍스트가 표시됩니다.

**파일 확장명**

이 단추를 누르면 "**파일 확장명 목록 사용**" 모드에서 검사할 모든 파일 확장명이 표시된 대화 상자가 열립니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

**참고**

기본 목록은 버전마다 다를 수 있습니다.

**추가 설정****선택한 드라이브의 부트 섹터 검사(B)**

이 옵션을 사용하면 검사 프로그램에서 온 디맨드 검사용으로 선택된 드라이브의 부트 섹터만 검사합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**마스터 부트 섹터 검사**

이 옵션을 사용하면 검사 프로그램에서 시스템에 사용된 하드 디스크의 마스터 부트 섹터를 검사합니다.

**오프라인 파일 무시**

이 옵션을 사용하면 직접 검사에서 검사 시 오프라인 파일을 완전히 무시합니다. 다시 말해서 이러한 파일에 대해 바이러스 및 사용자 동의 없이 설치된 프로그램의 포함 여부를 검사하지 않습니다. 오프라인 파일은 HSMS(계층적 저장소 관리 시스템)를 통해 예컨대 하드 디스크에서 테이프 물리적으로 이동된 파일입니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**시스템 파일에 대한 무결성 확인**

이 옵션을 사용하면 온 디맨드 검사에서 가장 중요한 Windows 시스템 파일에 대해 맬웨어에 의한 변경 여부를 확인하는 특수 보안 검사가 실시됩니다. 수정된 파일이 발견되면 의심스러운 항목으로 보고됩니다. 이 기능에는 컴퓨터 용량을 많이 사용되므로 이 옵션은 기본적으로 사용되지 않습니다.

**중요**

이 옵션은 Windows Vista 이상에서만 사용할 수 있습니다. SMC 에서 AntiVir 프로그램을 관리하는 경우에는 이 옵션을 사용할 수 없습니다.

**참고**

시스템 파일을 수정하고 부팅 또는 시작 화면을 사용자 고유의 요구 사항에 맞게 조정하는 타사 도구(예: skinpacks, TuneUp utilities 또는 Vista Customization)를 사용하는 경우에는 이 옵션을 사용하지 마십시오.

**최적화된 검사**

이 옵션을 사용하면 검사 프로그램 검사 시 프로세서 용량 활용이 최적화됩니다. 성능상의 이유로 최적화된 검사는 표준 수준에서만 기록됩니다.

**참고**

이 옵션은 다중 프로세서 시스템에서만 사용할 수 있습니다. SMC 에서 AntiVir 프로그램을 관리하는 경우 이 옵션이 항상 표시되며 사용하도록 설정할 수 있습니다. 관리되는 시스템에 프로세서가 한 개뿐인 경우에는 검사 프로그램 옵션이 사용되지 않습니다.

**기호 링크로 이동**

이 옵션을 사용하면 검사 프로그램에서 검사 프로파일 또는 선택한 디렉터리의 모든 기호 링크를 따라가 연결된 파일에 대해 바이러스 및 맬웨어 포함 여부를 검사하는 방식으로 검사를 수행합니다. 이 옵션은 Windows 2000 에서 지원되지 않으며 비활성화되어 있습니다.

**중요**

이 옵션에는 바로 가기가 포함되지 않지만, 파일 시스템에서 보이지 않는 기호 링크(mklink.exe 로 생성됨) 또는 연결 지점(junction.exe 를 통해 생성됨)만을 참조합니다.

**검사 전 루트킷 검색**

이 옵션을 사용하는 상태에서 검사를 시작하면 검사 프로그램에서 Windows 시스템 디렉터리에 대해 바로 가기에 활성 루트킷이 있는지 검사합니다. 이 프로세스는 "루트킷 검사" 검사 프로파일만큼 포괄적으로 컴퓨터에 대해 활성 루트킷을 검사하지 않지만, 수행 속도가 상당히 빠릅니다.

**중요**

Windows XP 64 비트에는 루트킷 검사를 사용할 수 없습니다.

**레지스트리 검사**

이 옵션을 사용하면 레지스트리에서 맬웨어 참조를 검사합니다.

**네트워크 드라이브의 파일 및 경로 검사 안 함**

이 옵션을 사용하면 컴퓨터에 연결된 네트워크 드라이브가 온 디맨드 검사에서 제외됩니다. 서버 또는 다른 워크스테이션 자체를 바이러스 백신 소프트웨어로 보호하는 경우에는 이 옵션을 사용하는 것이 좋습니다. 이 옵션은 기본적으로 사용되지 않습니다.

**검사 프로세스**

**검사 프로그램 중지 허용**

이 옵션을 사용하면 "Luke Filewalker" 창에서 "중지" 단추를 사용하여 바이러스나 사용자 동의 없이 설치된 프로그램에 대한 검사를 언제든지 종료할 수 있습니다. 이 설정을 사용하지 않는 경우에는 "Luke Filewalker" 창에 "중지" 단추가 회색으로 표시됩니다. 따라서 검사 프로세스를 조기에 종료할 수 없습니다! 이 옵션은 기본적으로 사용하도록 설정됩니다.

**검사 프로그램 우선 순위**

온 디맨드 검사 시 검사 프로그램에서는 우선 순위를 구분합니다. 몇 개 프로세스가 워크스테이션에서 동시에 실행 중인 경우에만 적용됩니다. 선택에 따라 검사 속도가 달라집니다.

**낮음**

다른 프로세스에서 계산 시간을 필요로 하지 않는 경우에만 운영 체제에서 검사 프로그램에 프로세서 시간을 할당합니다. 따라서 검사 프로그램이 최저 속도로 실행됩니다. 대체로 다른 프로그램과의 작업이 최적화됩니다. 즉, 검사 프로그램을 백그라운드에서 계속 실행하는 동안 다른 프로그램이 계산 시간을 필요로 할 경우 컴퓨터가 더 빨리 응답합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

**보통**

검사 프로그램이 보통의 우선 순위로 실행됩니다. 운영 체제에서 모든 프로세스에 동일한 양의 프로세서 시간을 할당합니다. 특수한 경우 다른 응용 프로그램과의 작업에 영향이 미칠 수도 있습니다.

#### 높음

검사 프로그램에 최고 우선 순위가 부여됩니다. 다른 응용 프로그램과의 동시 작업이 거의 불가능합니다. 하지만 검사 프로그램이 최고 속도로 검사를 수행합니다.

### 12.1.1.1. 검색에 대한 작업

#### **검색에 대한 작업**

바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견했을 때 검사 프로그램에서 수행할 작업을 정의할 수 있습니다.

#### 대화형

이 옵션을 사용하면 검사 프로그램의 검사 결과가 대화 상자에 표시됩니다. 검사 프로그램을 사용하여 검사를 수행할 경우 검사가 완료되면 영향받는 파일 목록과 함께 알림이 제공됩니다. 콘텐츠별 메뉴를 사용하여 감염된 여러 파일에 대해 실행할 작업을 선택할 수 있습니다. 감염된 모든 파일에 대해 표준 작업을 실행하거나 검사 프로그램을 취소할 수 있습니다.

#### 참고

검사 프로그램 대화 상자에는 '격리 저장소로 이동' 작업이 기본 작업으로 표시됩니다.

#### 허용되는 작업

이 상자에서 작업을 지정하면 바이러스가 검색되었을 때 개별 알림 또는 고급 알림 모드에서 해당 작업을 선택할 수 있습니다. 작업을 지정하려면 해당 옵션을 활성화해야 합니다.

#### 복구

가능한 경우 검사 프로그램에서 감염된 파일을 복구합니다.

#### 이름 바꾸기

검사 프로그램에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 나중에 파일을 복구한 후 이름을 원래 상태로 되돌릴 수 있습니다.

#### 격리

검사 프로그램에서 파일을 격리 저장소로 옮깁니다. 해당 파일이 정보가 포함된 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다. 파일에 따라 격리 관리자에서 선택할 수 있는 옵션이 늘어납니다.

#### 삭제

파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

#### 무시

파일을 무시합니다.

#### 덮어쓰기 및 삭제

검사 프로그램에서 파일을 기본 패턴으로 덮어쓴 후 파일을 삭제합니다. 이 파일은 복원할 수 없습니다.

### 기본값

이 단추는 검사 프로그램에서 감염된 파일을 처리하기 위한 기본 작업을 정의하는데 사용됩니다. 작업을 강조 표시하고 "기본값" 단추를 클릭합니다. 통합 알림 모드에서 관련 파일에 대해 선택한 기본 작업만 실행할 수 있습니다. 개별 알림 및 고급 알림 모드에서는 관련 파일에 대해 선택된 기본 작업이 미리 선택되어 있습니다.

#### 참고

복구 작업은 기본 작업으로 선택할 수 없습니다.

#### 참고

삭제 또는 덮어쓰기 및 삭제를 기본 작업으로 선택했으며 알림 모드를 통합 알림 모드로 설정하려는 경우, 추론 적중 시 영향받는 파일이 삭제되지 않으며 대신 격리 저장소로 이동됩니다.

자세한 내용을 보려면 여기를 클릭하십시오.

### 자동

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. 검사 프로그램은 이 섹션에서 미리 정의한 기본 및 보조 작업 설정에 따라 대응합니다.

### 격리 저장소에 백업

이 옵션을 사용하면 검사 프로그램에서 요청한 기본 작업 또는 보조 작업을 수행하기 전에 백업 복사본을 만듭니다. 백업 복사본은 격리 저장소에 저장되며, 정보 값이 있는 파일은 격리 저장소에서 복원할 수 있습니다. 또한 추가 조사를 위해 백업 복사본을 Avira 맬웨어 연구 센터로 보낼 수도 있습니다.

### 검색 알림 표시

이 옵션을 활성화하면 바이러스 또는 사용자 동의 없이 설치된 프로그램이 검색될 때마다 실행할 작업을 표시하는 알림이 나타납니다.

### 기본 작업

기본 작업은 검사 프로그램이 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우에 수행할 작업입니다. "복구" 옵션을 선택했지만 해당 파일을 복구할 수 없으면 "보조 작업"에서 선택한 작업이 수행됩니다.

#### 참고

기본 작업 아래에서 복구 설정을 선택한 경우에만 보조 작업 옵션을 선택할 수 있습니다.

### 복구

이 옵션을 사용하면 검사 프로그램에서 영향받는 파일을 자동으로 복구합니다. 영향받는 파일을 복구할 수 없는 경우 검사 프로그램에서는 보조 작업에 선택된 작업을 수행합니다.

#### 참고

자동 복구를 사용하는 것이 좋지만, 이 경우 검사 프로그램에서 워크스테이션의 파일을 수정하게 됩니다.

### 삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

### 덮어쓰기 및 삭제

이 옵션을 사용하면 검사 프로그램에서 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

#### 이름 바꾸기

이 옵션을 사용하면 검사 프로그램에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

#### 무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

#### **경고**

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

#### 격리

이 옵션을 사용하면 검사 프로그램에서 파일을 격리 저장소로 옮깁니다. 이러한 파일은 나중에 복구하거나 필요할 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

#### 보조 작업

"기본 작업" 아래에서 복구 설정을 선택한 경우에만 "보조 작업" 옵션을 선택할 수 있습니다. 이 옵션을 사용하면 영향받는 파일을 복구할 수 없는 경우 해당 파일에 대해 수행할 작업을 결정할 수 있습니다.

#### 삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

#### 덮어쓰기 및 삭제

이 옵션을 사용하면 검사 프로그램에서 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

#### 이름 바꾸기

이 옵션을 사용하면 검사 프로그램에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

#### 무시

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

#### **경고**

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

#### 격리

이 옵션을 사용하면 검사 프로그램에서 파일을 격리 저장소로 옮깁니다. 이러한 파일은 나중에 복구하거나 필요할 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

#### **참고**

기본 또는 보조 작업으로 삭제 또는 덮어쓰기 및 삭제를 선택한 경우, 추론 적중 시 영향받는 파일이 삭제되지 않으며 대신 격리 저장소로 이동됩니다.



### 12.1.1.2. 추가 작업

#### 검색 후 프로그램 실행

온 디맨드 검사 후 검사 프로그램에서는 하나 이상의 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견된 경우 사용자가 선택한 파일(예: 전자 메일 프로그램)을 열어서 다른 사용자나 관리자에게 알릴 수 있습니다.

#### 참고

보안상의 이유로 사용자가 컴퓨터에 로그인한 경우에만 검색 후 프로그램을 시작할 수 있습니다. 그러면 로그인한 사용자에게 적용되는 권한을 사용하여 해당 파일이 열립니다. 로그인한 사용자가 없으면 이 옵션이 수행되지 않습니다.

#### 프로그램 이름

이 입력란에는 검사 프로그램에서 검색 후 시작할 프로그램의 이름 및 관련 경로를 입력할 수 있습니다.



이 단추는 파일 선택 대화 상자를 사용하여 원하는 프로그램을 선택할 수 있는 창을 표시합니다.

#### 인수

이 입력란에는 필요할 경우 시작할 프로그램에 대한 명령줄 매개 변수를 입력할 수 있습니다.

#### 이벤트 로그

##### 이벤트 로그 사용

이 옵션을 사용하면 검사 프로그램의 검사가 완료된 후 검사 결과와 함께 이벤트 보고서가 Windows 이벤트 로그로 전송됩니다. Windows 이벤트 뷰어에서 이벤트를 불러올 수 있습니다. 이 옵션은 기본적으로 사용되지 않습니다.

보관 파일을 검사하는 경우 검사 프로그램에서는 재귀적 검사를 수행하므로, 보관 파일 안에 포함된 보관 파일도 압축을 풀어서 바이러스와 사용자 동의 없이 설치된 프로그램의 포함 여부를 검사하게 됩니다. 파일을 검사하고 나서 압축을 풀어서 파일을 다시 검사합니다.

##### 보관 파일 검사

이 옵션을 사용하면 보관 목록에서 선택한 보관 파일을 검사합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

##### 모든 보관 파일 형식

이 옵션을 사용하면 보관 목록의 모든 보관 파일 형식을 선택하여 검사합니다.

##### 스마트 확장명

이 옵션을 사용하면 검사 프로그램에서 파일 확장명이 일반적인 확장명과 다르더라도 파일이 압축된 파일 형식(보관 파일)인지 여부를 확인하여 보관 파일을 검사합니다. 하지만 이 경우 모든 파일을 열어야 하므로 검사 속도가 느려집니다. 예: \*.zip 보관 파일의 확장명이 \*.xyz 인 경우 검사 프로그램에서는 이 보관 파일의 압축을 풀어서 검사합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**참고**

보관 목록에 표시된 보관 파일 형식만 지원됩니다.

**재귀 수준**

재귀적 보관 파일의 압축을 풀어서 검사하려면 컴퓨터 시간과 리소스가 많이 필요할 수 있습니다. 이 옵션을 사용하면 여러 번 압축된 보관 파일의 검사 수준을 특정 압축 수준 수(최대 재귀 수준)로 제한할 수 있습니다. 따라서 시간과 컴퓨터 리소스가 절약됩니다.

**참고**

보관 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램을 찾으려면 검사 프로그램에서 바이러스나 사용자 동의 없이 설치된 프로그램이 있는 재귀 수준까지 검사해야 합니다.

**최대 재귀 수준**

최대 재귀 수준을 입력하려면 재귀 수준 제한 옵션을 사용해야 합니다. 원하는 재귀 수준을 직접 입력하거나 입력 필드에 있는 오른쪽 화살표 키를 사용할 수 있습니다. 허용되는 값은 1 ~ 99 입니다. 표준 값 20 을 그대로 사용하는 것이 좋습니다.

**기본값**

이 단추는 보관 파일 검사에 대해 미리 정의된 값을 복원합니다.

**보관 파일**

이 표시 영역에서는 검사 프로그램에서 검사해야 할 보관 파일을 설정할 수 있습니다. 이 경우 관련 항목을 선택해야 합니다.

**12.1.1.3. 예외****검사 프로그램에서 생략할 파일 개체**

이 창의 목록에는 바이러스나 사용자 동의 없이 설치된 프로그램 검사 시 검사 프로그램에서 포함하면 안 되는 특정 파일 및 경로가 포함되어 있습니다.

여기에는 어떤 이유로든 일반 검사에 포함하면 안 되는 파일 등과 같이 반드시 필요한 예외 항목만 입력하십시오. 이 목록에 포함되기 전에 이러한 파일에 대해 바이러스나 사용자 동의 없이 설치된 프로그램의 포함 여부를 항상 검사하는 것이 좋습니다!

**참고**

이 목록의 항목에 사용되는 글자 수는 총 6000 자를 넘지 않아야 합니다.

**경고**

이러한 파일은 검사에 포함되지 않습니다!

**참고**

이 목록에 포함된 파일은 보고서 파일에 기록됩니다. 여기서 파일을 제외한 이유가 더 이상 존재하지 않을 수도 있으므로 가끔씩 보고서 파일에서 검사되지 않는 파일을 확인하십시오. 이 경우 이 목록에서 해당 파일의 이름을 다시 제거해야 합니다.

**입력란**



이 입력란에는 온 디맨드 검사에 포함되지 않는 파일 개체의 이름을 입력할 수 있습니다. 기본적으로 파일 개체가 입력되어 있지 않습니다.



이 단추를 사용하여 표시되는 창에서 필요한 파일이나 필요한 경로를 선택할 수 있습니다.

전체 경로와 함께 파일 이름을 입력한 경우 이 파일에 대해서만 감염 여부가 검사되지 않습니다. 경로 없이 파일 이름만 입력하면 경로나 드라이브와 상관없이 이 이름을 사용하는 모든 파일이 검사되지 않습니다.

**추가**

이 단추를 사용하면 입력란에 입력한 파일 개체를 표시 창에 추가할 수 있습니다.

**삭제**

이 단추는 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 단추가 비활성화됩니다.

**참고**

파일 개체 목록에 전체 파티션을 추가할 경우 해당 파티션의 루트에 저장되는 파일만 검사에서 제외되며, 해당 파티션의 하위 디렉터리에 있는 파일에는 이 사항이 적용되지 않습니다.

예: 생략할 파일 개체: D:\ = D:\file.txt 는 검사 프로그램의 검사에서 제외되지만, D:\폴더\file.txt 는 검사에서 제외되지 않습니다.

**참고**

SMC 에서 AntiVir 프로그램을 관리하는 경우, 파일 예외에 대한 경로 정보에 변수를 사용할 수 있습니다. 사용 가능한 변수 목록은 변수: Guard 및 검사 프로그램 예외에 있습니다.

**12.1.1.4. 추론**

이 구성 섹션에는 검사 엔진의 추론 설정이 들어 있습니다.

AntiVir 제품에는 알려지지 않은 맬웨어를 사전에, 즉 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 확인할 수 있는 매우 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 가양성(오진) 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

**매크로 바이러스 추론**

**매크로 바이러스 추론**

AntiVir 제품에는 매우 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

**AHeAD(고급 추론 분석 및 검색)****AHeAD 사용**

AntiVir 프로그램은 일종의 AntiVir AHeAD 기술로 매우 강력한 추론 기능을 제공하므로 알려지지 않은 신종 맬웨어를 감지할 수 있습니다. 이 옵션을 사용하면 이 추론의 "공격성" 수준을 정의할 수 있습니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**낮은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 줄어들기 때문에 가양성 문제가 발생할 위험이 낮습니다.

**보통 검색 수준**

이 추론을 사용하도록 선택한 경우 이 옵션은 기본 설정으로 사용됩니다.

**높은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 현저히 늘어나지만 가양성일 확률도 높아집니다.

**12.1.2 신고**

검사 프로그램에서는 포괄적인 보고 기능을 제공합니다. 따라서 온 디맨드 검사 결과에 대한 정확한 정보를 얻을 수 있습니다. 보고서 파일에는 시스템의 모든 항목은 물론 온 디맨드 검사에 대한 알림과 메시지도 포함됩니다.

**참고**

바이러스나 사용자 동의 없이 설치된 프로그램이 검색되었을 때 검사 프로그램에서 수행한 작업을 확인하려면 반드시 보고서 파일을 만들어야 합니다.

**보고****해제**

이 옵션을 사용하면 검사 프로그램에서 온 디맨드 검사에 대한 작업 및 결과를 보고하지 않습니다.

**기본값**

이 옵션을 활성화하면 검사 프로그램에서 경로와 관련된 파일의 이름을 기록합니다. 또한 현재 검사의 구성, 버전 정보 및 라이선스 보유자에 대한 정보도 보고서 파일에 기록됩니다.

**고급**

이 옵션을 활성화하면 검사 프로그램에서 기본 정보와 함께 알림 및 팁을 기록합니다.

**완료**

이 옵션을 활성화하면 검사 프로그램에서 검사한 모든 파일을 기록합니다. 또한 알림 및 팁은 물론 관련된 모든 파일이 보고서 파일에 포함됩니다.

**참고**

문제 해결을 위해 지원 센터로 보고서 파일을 보내야 하는 경우 이 모드에서 이 보고서 파일을 만드십시오.

## 12.2 Guard

구성의 Guard 섹션에서는 온 액세스 검사를 구성할 수 있습니다.

### 12.2.1 검사

일반적으로는 시스템을 지속적으로 모니터링하게 됩니다. 이 경우에는 Guard(= 온 액세스 검사 프로그램)를 사용합니다. 그러면 컴퓨터에 열려 있거나 복사되는 모든 파일을 대상으로 바이러스와 사용자 동의 없이 설치된 프로그램을 "즉시" 검사할 수 있습니다.

#### 검사 모드

여기에는 파일의 검사 시간이 정의됩니다.

#### 읽을 때 검사

이 옵션을 사용하면 파일을 응용 프로그램 또는 운영 체제에서 읽거나 실행하기 전에 Guard 에서 먼저 검사합니다.

#### 쓸 때 검사

이 옵션을 사용하면 Guard 에서 파일에 쓸 때 파일을 검사합니다. 이 프로세스를 완료한 후에만 파일에 다시 액세스할 수 있습니다.

#### 읽거나 쓸 때 검사

이 옵션을 사용하면 파일을 열거나 읽거나 실행하기 전에, 그리고 파일에 쓰기 전에 Guard 에서 파일을 검사합니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

#### 파일

Guard에서는 필터를 사용하여 특정 확장명(형식)이 지정된 파일만 검사할 수 있습니다.

#### 모든 파일

이 옵션을 선택하면 파일 콘텐츠와 파일 확장명에 관계없이 모든 파일을 대상으로 바이러스 또는 사용자 동의 없이 설치된 프로그램을 검사합니다.

#### 참고

모든 파일 옵션을 사용하는 경우 **파일 확장명** 단추를 선택할 수 없습니다.

#### 스마트 확장명

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 있는지 검사할 파일을 프로그램에서 자동으로 선택합니다. 즉, 파일을 검사할지 또는 콘텐츠에 따라 검사할지 여부를 프로그램이 결정합니다. 이 절차는 파일 확장명 목록 사용보다는 다소 느리지만 파일 확장명만을 기준으로 검사하지 않으므로 더 정확합니다.

#### 참고

스마트 확장명 옵션을 사용하면 **파일 확장명** 단추를 선택할 수 없습니다.

**파일 확장명 목록 사용**

이 옵션을 사용하면 지정된 확장명의 파일만 검사합니다. 바이러스와 사용자 동의 없이 설치된 프로그램을 포함할 수 있는 모든 파일 형식이 미리 설정되어 있습니다. "**파일 확장명**" 단추를 누르고 이 목록을 수동으로 편집할 수 있습니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

**참고**

이 옵션을 사용하고 파일 확장명 목록에서 모든 항목을 삭제한 경우, **파일 확장명** 단추 아래에 "파일 확장명 없음"이라는 텍스트가 표시됩니다.

**파일 확장명**

이 단추를 누르면 "**파일 확장명 목록 사용**" 모드에서 검사할 모든 파일 확장명이 표시된 대화 상자가 열립니다. 확장명에 대한 기본 항목이 설정되어 있지만 항목을 추가하거나 삭제할 수 있습니다.

**참고**

파일 확장명 목록은 버전마다 다를 수 있습니다.

**보관 파일****보관 파일 검사**

이 옵션을 사용할 경우 보관 파일을 검사합니다. 압축된 파일을 검사하고 나서 압축이 풀린 파일을 다시 검사합니다. 이 옵션은 기본적으로 비활성화됩니다. 보관 파일 검사는 재귀 수준, 검사할 파일 수 및 보관 파일 크기를 사용하여 제한할 수 있습니다. 최대 재귀 수준, 검사할 파일 수 및 최대 보관 파일 크기를 설정할 수 있습니다.

**참고**

이 옵션은 컴퓨터 처리 성능이 많이 요구되므로 기본적으로 비활성화됩니다. 일반적으로 보관 파일은 온 디맨드 검사를 사용하여 검사하는 것이 좋습니다.

**최대 재귀 수준**

보관 파일을 검사하는 경우 Guard에서는 재귀적 검사를 수행하므로, 보관 파일 안에 포함된 보관 파일도 압축을 풀어서 바이러스와 사용자 동의 없이 설치된 프로그램의 포함 여부를 검사하게 됩니다. 이 경우 재귀 수준을 정의할 수 있습니다. 재귀 수준의 기본값은 1이며 이 값을 그대로 사용하는 것이 좋습니다. 그러면 주 보관 파일 바로 아래에 위치한 모든 보관 파일을 검사합니다.

**최대 파일 수**

보관 파일을 검사할 때 보관 파일에서 최대 파일 수를 지정하여 검사를 제한할 수 있습니다. 검사할 최대 파일 수에 대한 기본값은 10이며 이 값을 그대로 사용하는 것이 좋습니다.

**최대 크기(KB)**

보관 파일을 검사할 때 압축을 풀 최대 보관 파일의 크기를 지정하여 검사를 제한할 수 있습니다. 표준 값인 1000KB를 사용하는 것이 좋습니다.

**드라이브****네트워크 드라이브**

이 옵션을 사용하면 서버 볼륨, 피어 드라이브 등 네트워크 드라이브(매핑된 드라이브)의 파일을 검사합니다.

**참고**

컴퓨터의 성능이 크게 저하되지 않도록 하려면 **네트워크 드라이브** 옵션은 예외적인 경우에만 사용해야 합니다.

**경고**

이 옵션을 사용하지 않으면 네트워크 드라이브가 모니터링되지 **않습니다**. 따라서 바이러스나 사용자 동의 없이 설치된 프로그램으로부터 더 이상 보호되지 않습니다.

**참고**

네트워크 드라이브에서 파일을 실행하는 경우 **네트워크 드라이브** 옵션에 대한 설정과 관계없이 Guard에서 해당 파일을 검사합니다. 경우에 따라 **네트워크 드라이브** 옵션이 사용되지 않더라도 네트워크 드라이브의 파일을 여는 동안 파일이 검사될 수도 있습니다. 이유: 이러한 파일이 '파일 실행' 권한으로 액세스되기 때문입니다. 이러한 파일이나 네트워크 드라이브에서 실행된 파일을 Guard의 검사 대상에서 제외하려면 제외할 파일 개체 목록에 파일을 입력합니다. Guard::검사::예외를 참조하십시오.

**캐싱 사용**

이 옵션을 사용하면 네트워크 드라이브에서 모니터링된 파일을 Guard의 캐시에서 사용할 수 있습니다. 캐시 기능을 사용하지 않고 네트워크 드라이브를 모니터링하는 것이 보다 안전하지만 캐시를 사용할 경우에 비해 모니터링이 제대로 수행되지 않습니다.

### 12.2.1.1. 검색에 대한 작업

**검색에 대한 작업**

바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견했을 때 Guard에서 수행할 작업을 정의할 수 있습니다.

**대화형**

이 옵션을 사용하면 Guard에서 바이러스나 사용자 동의 없이 설치된 프로그램을 발견한 경우 데스크톱 알림이 나타납니다. 검색된 맬웨어를 제거하거나 '자세히' 단추를 사용하여 가능한 다른 바이러스 위협에 액세스할 수 있습니다. 작업은 대화 상자에 표시됩니다. 작업은 대화 상자에 표시됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**허용되는 작업**

대화 상자에 추가 작업으로 제공되는 바이러스 관리 작업을 이 표시란에서 지정할 수 있습니다. 작업을 지정하려면 해당 옵션을 활성화해야 합니다.

**복구**

가능한 경우 Guard에서 감염된 파일을 복구합니다.

**이름 바꾸기**

Guard에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 나중에 파일을 복구한 후 이름을 원래 상태로 되돌릴 수 있습니다.

**격리**

Guard 는 파일을 격리 저장소로 옮깁니다. 해당 파일이 정보가 포함된 중요한 파일인 경우 격리 관리자를 통해 복구하거나 필요한 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다. 파일에 따라 격리 관리자에서 선택할 수 있는 옵션이 더 늘어납니다.

#### 삭제

파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

#### 무시

파일에 대한 액세스가 허용되고 파일을 무시합니다.

#### 덮어쓰기 및 삭제

Guard 에서 파일을 삭제하기 전에 파일을 기본 패턴으로 덮어씁니다. 이 파일은 복원할 수 없습니다.

#### 기본값

이 단추를 사용하면 바이러스가 발견될 때 대화 상자에서 기본적으로 활성화되는 작업을 선택할 수 있습니다. 기본적으로 활성화할 작업을 선택하고 "기본값" 단추를 클릭합니다.

#### 참고

복구 작업은 기본 작업으로 선택할 수 없습니다.

자세한 내용을 보려면 여기를 클릭하십시오.

#### 자동

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. Guard 는 이 섹션에서 미리 정의한 기본 및 보조 작업 설정에 따라 대응합니다.

#### 격리 저장소에 백업

이 옵션을 사용하면 Guard 에서 요청한 기본 작업 또는 보조 작업을 수행하기 전에 백업 복사본을 만듭니다. 백업 복사본은 격리 저장소에 저장됩니다. 파일에 정보 값이 있는 경우 격리 관리자를 통해 파일을 복원할 수 있습니다. 또한 추가 조사를 위해 백업 복사본을 Avira 맬웨어 연구 센터로 보낼 수 있습니다. 개체에 따라 격리 관리자에서 선택할 수 있는 옵션이 더 늘어납니다.

#### 검색 알림 표시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때마다 알림 메시지가 나타납니다.

#### 기본 작업

기본 작업은 Guard 가 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우에 수행하는 작업입니다. "복구" 옵션을 선택했지만 해당 파일을 복구할 수 없으면 "보조 작업"에서 선택한 작업이 수행됩니다.

#### 참고

기본 작업에서 복구 설정을 선택한 경우에만 보조 작업 옵션을 선택할 수 있습니다.

#### 복구

이 옵션을 사용하면 Guard에서 영향받는 파일을 자동으로 복구합니다. 해당 파일을 복구할 수 없는 경우 Guard는 보조 작업에서 선택한 작업을 수행합니다.

#### 참고

자동 복구를 사용하는 것이 좋지만, 이 경우 Guard 에서 워크스테이션의 파일을 수정하게 됩니다.

#### 삭제

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

**덮어쓰기 및 삭제**

이 옵션을 사용하면 Guard 에서 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

**이름 바꾸기**

이 옵션을 사용하면 Guard 에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

**무시**

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

**경고**

영향받는 파일은 워크스테이션에서 활성화 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

**액세스 거부**

보고서 기능이 활성화되어 있는 경우 이 옵션을 사용하면 Guard에서 보고서 파일에 검색 정보만 입력합니다. 또한 이 옵션을 사용하면 Guard는 이벤트 로그에 항목을 작성합니다.

**격리**

이 옵션을 사용하면 Guard 는 파일을 격리 저장소로 옮깁니다. 이 디렉터리의 파일은 나중에 복구하거나 필요할 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

**보조 작업**

"보조 작업" 옵션은 "기본 작업"에서 "복구" 옵션을 선택한 경우에만 선택할 수 있습니다. 이 옵션을 사용하면 영향받는 파일을 복구할 수 없는 경우 해당 파일에 대해 수행할 작업을 결정할 수 있습니다.

**삭제**

이 옵션을 사용하면 파일이 삭제됩니다. 이 프로세스는 "덮어쓰기 및 삭제"보다 훨씬 빠릅니다.

**덮어쓰기 및 삭제**

이 옵션을 사용하면 Guard 에서 파일을 기본 패턴으로 덮어쓴 다음 삭제합니다. 이 파일은 복원할 수 없습니다.

**이름 바꾸기**

이 옵션을 사용하면 Guard 에서 파일 이름을 바꿉니다. 따라서 두 번 클릭과 같은 방법으로 이러한 파일에 직접 액세스할 수 없습니다. 파일을 나중에 복구하고 원래 이름을 다시 지정할 수 있습니다.

**무시**

이 옵션을 사용하면 파일에 액세스할 수 있고 파일이 그대로 유지됩니다.

**경고**

영향받는 파일은 워크스테이션에서 활성화 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

**액세스 거부**



보고서 기능이 활성화되어 있는 경우 이 옵션을 사용하면 Guard에서 보고서 파일에 검색 정보만 입력합니다. 또한 이 옵션을 사용하면 Guard는 이벤트 로그에 항목을 작성합니다.

#### **격리**

이 옵션을 사용하면 Guard는 파일을 격리 저장소로 옮깁니다. 이러한 파일은 나중에 복구하거나 필요할 경우 Avira 맬웨어 연구 센터로 보낼 수 있습니다.

#### **참고**

기본 또는 보조 작업으로 **삭제** 또는 **덮어쓰기 및 삭제**를 선택한 경우, 추론 적중 시 영향받는 파일이 삭제되지 않으며 대신 격리 저장소로 이동됩니다.

## 12.2.1.2. 추가 작업

### **알림**

#### **이벤트 로그**

##### **이벤트 로그 사용**

이 옵션을 사용하면 검색될 때마다 Windows 이벤트 로그에 항목이 추가됩니다. Windows 이벤트 뷰어에서 이벤트를 불러올 수 있습니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### **자동 시작**

##### **자동 시작 기능 차단**

이 옵션을 사용하면 USB 스틱, CD/DVD 드라이브, 네트워크 드라이브 등 연결된 모든 드라이브에서 Windows 자동 시작 기능의 실행이 차단됩니다. Windows 자동 시작 기능을 사용하면 데이터 미디어나 네트워크 드라이브에 있는 파일을 로드 또는 연결되는 즉시 읽으므로 파일을 자동으로 시작하거나 복사할 수 있습니다. 그러나 이 기능은 사용자 동의 없이 설치되는 프로그램과 맬웨어가 자동 시작 시 설치될 수 있으므로 보안 위험이 높습니다. 특히 USB 스틱의 경우 스틱에 저장된 데이터가 언제든지 변경될 수 있으므로 주의해야 합니다.

##### **CD 및 DVD 제외**

이 옵션을 사용하면 CD 및 DVD 드라이브에서 자동 시작 기능이 허용됩니다.

#### **경고**

신뢰할 수 있는 데이터 미디어를 사용하는 경우에만 CD 및 DVD 드라이브에 대해 자동 시작 기능을 해제하십시오.



### 12.2.1.3. 예외

이러한 옵션을 사용하면 Guard(온 액세스 검사)에 대한 예외 개체를 구성할 수 있습니다. 그러면 해당 개체가 온 액세스 검사에 포함되지 않습니다. Guard에서는 생략할 프로세스의 목록을 통해 온 액세스 검사 중에 이러한 개체에 대한 파일 액세스를 무시할 수 있습니다. 이 기능은 데이터베이스 또는 백업 솔루션을 사용하는 경우 등에 유용합니다.

생략할 프로세스 및 파일 개체를 지정할 때는 다음에 주의하십시오. 목록은 맨 위에서부터 아래 순서로 처리됩니다. 목록이 길수록 프로세서에서 각 액세스에서 목록을 처리하는 데 더 많은 시간이 소요됩니다. 따라서 목록을 가능한 짧게 유지하십시오.

#### Guard에서 생략할 프로세스

이 목록에 있는 프로세스에 대한 모든 파일 액세스가 Guard를 통한 모니터링에서 제외됩니다.

#### 입력란

이 필드에 실시간 검사에서 무시할 프로세스의 이름을 입력합니다. 기본적으로 프로세스 이름이 입력되어 있지 않습니다.

#### 참고

최대 128 개의 프로세스를 입력할 수 있습니다.

#### 참고

프로세스를 입력할 때 유니코드 기호를 사용할 수 있습니다. 즉, 특수 기호가 포함된 프로세스 이름이나 디렉터리 이름을 입력할 수 있습니다.

#### 참고

완전한 경로 정보가 없는 프로세스는 Guard 모니터링 대상에서 제외할 수 있습니다. application.exe

그러나 이는 실행 파일이 하드 디스크 드라이브에 있는 프로세스에만 적용됩니다. 실행 파일이 연결 드라이브(예: 네트워크 드라이브)에 있는 프로세스는 완전한 경로 정보가 있어야 합니다. 연결된 네트워크 드라이브의 예외에 나와 있는 표기법에 대한 일반 정보에 주의하십시오.

실행 파일이 동적 드라이브에 있는 프로세스에 대해 예외를 지정하지 마십시오. 동적 드라이브는 CD, DVD 또는 USB 스틱 등 이동식 디스크에 사용됩니다.

#### 참고

다음과 같은 드라이브 정보를 입력해야 합니다. [드라이브 문자]:\

콜론 기호(:)는 드라이브를 지정하는 데만 사용됩니다.

#### 참고

프로세스를 지정할 때 와일드카드 \*(문자 수 임의) 및 ??(문자 하나)를 사용할 수 있습니다.

C:\Program Files\Application\application.exe

C:\Program Files\Application\applicatio?.exe

C:\Program Files\Application\applic\*.exe

C:\Program Files\Application\\*.exe

프로세스가 Guard의 모니터링 대상에서 전체적으로 제외되는 일이 없도록 하기 위해, \*(별표), ?(물음표), /(슬래시), \ (백슬래시), . (점), : (콜론)만 사용하여 지정하는 것은 인정되지 않습니다.

**참고**

프로세스의 경로 및 파일 이름은 255 자 이내로 지정해야 합니다. 이 목록의 항목에 사용되는 글자 수는 총 6000 자를 넘지 않아야 합니다.

**경고**

목록에 기록된 프로세스에 의한 모든 파일 액세스가 바이러스 및 사용자 동의 없이 설치된 프로그램 검사에서 제외됩니다. Windows 탐색기와 운영 체제 자체는 제외될 수 없습니다. 목록에서 해당 항목이 무시됩니다.



이 단추는 실행 파일을 선택할 수 있는 창을 엽니다.

**프로세스**

"프로세스" 단추를 누르면 실행 중인 프로세스가 표시된 "프로세스 선택" 창이 열립니다.

**추가**

이 단추를 사용하면 입력란에 입력된 프로세스를 표시 창에 추가할 수 있습니다.

**삭제**

이 단추를 사용하면 선택한 프로세스를 표시 창에서 삭제할 수 있습니다.

**Guard 에서 생략할 파일 개체**

이 목록에 있는 개체에 대한 모든 파일 액세스가 Guard 를 통한 모니터링에서 제외됩니다.

**입력란**

이 상자에 온 액세스 검사에 포함되지 않는 파일 개체의 이름을 입력할 수 있습니다. 기본적으로 파일 개체가 입력되어 있지 않습니다.

**참고**

생략할 파일 개체를 지정할 때 와일드카드 \*(문자 수 임의) 및 ?? (문자 하나)를 사용할 수 있습니다. 개별 파일 확장명을 제외할 수도 있습니다(와일드카드 포함).

C:\Directory\\*.mdb

\*.mdb

\*.md?

\*.xls\*

C:\Directory\\*.log

**참고**

디렉터리 이름은 백슬래시(\)로 끝나야 하며, 그렇지 않으면 파일 이름으로 간주됩니다.

**참고**

이 목록의 항목은 총 문자 수가 6000 자를 넘지 않아야 합니다.

**참고**

디렉터리가 제외되는 경우 모든 하위 디렉터리도 자동으로 제외됩니다.

**참고**

각 드라이브에 대해 드라이브 문자로 시작하는 전체 경로를 입력하여 최대 20 개의 예외를 지정할 수 있습니다.

예를 들면 다음과 같습니다. C:\Program Files\Application\Name.log

전체 경로를 사용하지 않을 경우 가능한 최대 예외 수는 64 개입니다.

예를 들면 다음과 같습니다. \*.log

\computer1\C\directory1

**참고**

다른 드라이브의 디렉터리로 탑재되는 동적 드라이브의 경우 예외 목록에서 통합 드라이브의 운영 체제 별칭을 사용해야 합니다.

예: \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\ C:\DynDrive 와 같이 탑재 지점 자체를 사용하는 경우에는 동적 드라이브가 검사됩니다. Guard 보고서 파일에서 사용할 운영 체제의 별칭을 결정할 수 있습니다.



이 단추는 제외할 파일 개체를 선택할 수 있는 창을 엽니다.

**추가**

이 단추를 사용하면 입력란에 입력한 파일 개체를 표시 창에 추가할 수 있습니다.

**삭제**

이 단추를 사용하면 선택한 파일 개체를 표시 창에서 삭제할 수 있습니다.

예외를 지정할 때는 추가 정보에 유의하십시오.

**참고**

짧은 DOS 파일 이름(DOS 이름 규칙 8.3)을 사용하여 액세스하는 개체도 제외하려면 해당 짧은 파일 이름도 목록에 입력해야 합니다.

**참고**

와일드카드를 포함하는 파일 이름은 백슬래시로 끝낼 수 없습니다.

예:

C:\Program Files\Application\applic\*.exe\

이 항목은 잘못되었으므로 예외로 처리되지 않습니다.

**참고**

연결된 네트워크 드라이브에 대한 예외와 관련하여, 연결된 네트워크 드라이브의 드라이브 문자를 사용하는 경우 지정한 파일 및 폴더가 Guard 검사에서 제외되지 않습니다. 예외 목록의 UNC 경로가 네트워크 드라이브에 연결하는 데 사용되는 UNC 경로와 다른 경우(예외 목록의 IP 주소 지정 - 네트워크 드라이브에 연결하기 위한 컴퓨터 이름 지정) 지정된 폴더와 파일이 Guard 검사에서 제외되지 않습니다. Guard 보고서 파일에서 해당 UNC 경로를 찾아보십시오.

\\<컴퓨터 이름>\<Enable>\ - 또는 - \\<IP 주소>\<Enable>\

**참고**

Guard에서 감염된 파일을 검사하는 데 사용하는 경로는 Guard 보고서 파일에서 찾아볼 수 있습니다. 예외 목록에 동일한 경로를 지정하십시오. 다음과 같이 진행합니다. Guard::보고서 아래의 구성 섹션에서 Guard의 프로토콜 기능을 **완료**로 설정합니다. 이제 Guard를 활성화한 상태에서 파일, 폴더, 탑재된 드라이브 또는 연결된 네트워크 드라이브에 액세스합니다. 이제 Guard 보고서 파일에서 사용되는 경로를 확인할 수 있습니다. 보고서 파일은 제어 센터의 로컬 보호::Guard에서 액세스할 수 있습니다.

**참고**

SMC에서 AntiVir 프로그램을 관리하는 경우, 프로세스 및 파일 예외에 대한 경로 정보에 변수를 사용할 수 있습니다. 사용 가능한 변수 목록은 변수: Guard 및 검사 프로그램 예외에 있습니다.

제외할 프로세스의 예:

- application.exe

application.exe 프로세스는 어떤 하드 디스크 드라이브의 어떤 디렉터리에 있는지 Guard 검사 대상에서 제외됩니다.

- C:\Program Files1\Application.exe

C:\Program Files1 경로에 있는 application.exe 파일의 프로세스는 Guard 검사 대상에서 제외됩니다.

- C:\Program Files1\\*.exe

C:\Program Files1 경로에 있는 실행 파일의 모든 프로세스는 Guard 검사 대상에서 제외됩니다.

제외할 파일의 예:

- \*.mdb

확장명이 'mdb'인 모든 파일은 Guard 검사 대상에서 제외됩니다.

- \*.xls\*

확장명이 'xls'로 시작하는 모든 파일(예: 확장명이 .xls 및 .xlsx 인 파일)은 Guard 검사 대상에서 제외됩니다.

- C:\Directory\\*.log

C:\Directory에 있고 확장명이 'log'인 모든 로그 파일은 Guard 검사 대상에서 제외됩니다.

- \\Computer name\Shared1\

'\\Computer name1\Shared1' 연결을 통해 액세스해야 하는 모든 파일은 Guard 검사 대상에서 제외됩니다. 이는 대개 컴퓨터 이름 'Computer name1' 및 공유 이름 'Shared1'을 사용하여 공유 폴더가 있는 다른 컴퓨터에 액세스하는 연결된 네트워크 드라이브입니다.

- \\1.0.0.0\Shared1\\*.mdb

'\\1.0.0.0\Shared1' 연결을 통해 액세스해야 하고 확장명이 'mdb'인 모든 파일은 Guard 검사 대상에서 제외됩니다. 이는 대개 IP 주소 '1.0.0.0' 및 공유 이름 'Shared1'을 사용하여 공유 폴더가 있는 다른 컴퓨터에 액세스하는 연결된 네트워크 드라이브입니다.

#### 12.2.1.4. 추론

이 구성 섹션에는 검사 엔진의 추론 설정이 들어 있습니다.

AntiVir 제품에는 알려지지 않은 맬웨어를 사전에, 즉 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 확인할 수 있는 매우 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 가양성(오진) 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

##### **매크로 바이러스 추론**

###### **매크로 바이러스 추론**

AntiVir 제품에는 매우 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

##### **AHeAD(고급 추론 분석 및 검색)**

###### **AHeAD 사용**

AntiVir 프로그램은 일종의 AntiVir AHeAD 기술로 매우 강력한 추론 기능을 제공하므로 알려지지 않은 신종 맬웨어를 감지할 수 있습니다. 이 옵션을 사용하면 이 추론의 "공격성" 수준을 정의할 수 있습니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

###### **낮은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 줄어들기 때문에 가양성 문제가 발생할 위험이 낮습니다.

###### **보통 검색 수준**

이 추론을 사용하도록 선택한 경우 이 옵션은 기본 설정으로 사용됩니다.

###### **높은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 현저히 늘어나지만 가양성일 확률도 높아집니다.

## 12.2.2 ProActiv

Avira AntiVir ProActiv 는 바이러스 정의나 추론이 아직 준비되지 않은 새롭고 알려지지 않은 위협으로부터 사용자를 보호합니다. Guard 구성 요소에 통합된 ProActiv 기술이 수행한 프로그램 작업을 감시하고 분석합니다. 프로그램의 동작은 일반적인 맬웨어 작업 패턴, 즉 작업 유형 및 작업 시퀀스를 기준으로 검사됩니다. 프로그램에서 맬웨어를 나타내는 일반적인 동작을 보이면 이는 바이러스 검색으로 처리됩니다( 프로그램을 차단하거나 알람을 무시하고 프로그램을 계속 사용할 수 있습니다. 프로그램을 신뢰할 수 있는 프로그램으로 분류하고 허용된 프로그램에 대한 응용 프로그램 필터에 추가할 수 있습니다. 항상 차단 명령을 사용하여 차단된 프로그램에 대한 응용 프로그램 필터에 이 프로그램을 추가할 수 있습니다.

ProActiv 구성 요소는 Avira 맬웨어 연구 센터에서 개발한 규칙 집합을 사용하여 의심스러운 동작을 식별합니다. 규칙 집합은 Avira GmbH 데이터베이스에서 제공됩니다. Avira AntiVir ProActiv 는 검색된 의심스러운 프로그램에 대한 정보를 Avira 데이터베이스로 보내 기록하도록 합니다. Avira 데이터베이스로 데이터가 전송되지 않도록 할 수 있습니다.

### 참고

현재 64 비트 시스템에서는 ProActiv 기술을 사용할 수 없습니다. Windows 2000에서는 ProActiv 구성 요소를 지원하지 않습니다.

### 일반

#### **Avira AntiVir ProActiv 사용**

이 옵션을 사용하면 컴퓨터 시스템에서 프로그램을 모니터링하고 의심스러운 작업을 검사합니다. 일반적인 맬웨어 동작이 검색되면 메시지가 제공됩니다. 프로그램을 차단하거나 "무시"를 선택하여 프로그램을 계속 사용할 수 있습니다. 기본적으로 허용된 응용 프로그램 필터에 포함된 신뢰할 수 있고 서명된 프로그램으로 분류된 프로그램과 허용된 프로그램에 대한 응용 프로그램 필터에 추가한 모든 프로그램은 모니터링 프로세스에서 제외됩니다.

#### **AntiVir ProActiv 커뮤니티에 참여하여 컴퓨터의 보안 수준을 높일 수 있습니다.**

이 옵션을 사용하면 Avira AntiVir ProActiv 가 의심스러운 프로그램에 대한 데이터는 물론 경우에 따라 의심스러운 프로그램 파일(실행 파일)까지 Avira 맬웨어 연구 센터로 보내어 고급 온라인 검사를 실시하도록 합니다. 이러한 데이터는 평가 후 ProActiv 동작 분석 규칙 집합에 추가됩니다. 이러한 방식으로 사용자는 Avira ProActiv 커뮤니티의 일원이 되어 ProActiv 보안 기술의 지속적인 향상 및 개선에 기여하게 됩니다. 이 옵션을 사용하지 않으면 아무 데이터도 전송되지 않습니다. 이는 ProActiv 의 기능에 영향을 주지 않습니다.

#### **자세한 내용을 보려면 여기를 클릭하십시오.**

이 링크를 통해 고급 온라인 검사에 대한 자세한 정보가 실려 있는 인터넷 페이지에 액세스할 수 있습니다. 이 인터넷 페이지에는 고급 온라인 검사 중 전송되는 모든 데이터가 수록되어 있습니다.

### 12.2.2.1. 응용 프로그램 필터: 차단할 응용 프로그램

**응용 프로그램 필터:** 차단할 응용 프로그램에서는 유해한 것으로 분류한 응용 프로그램과 Avira AntiVir ProActiv 에서 기본적으로 차단할 응용 프로그램을 입력할 수 있습니다. 추가된 응용 프로그램은 컴퓨터 시스템에서 실행할 수 없습니다. 또한 이 프로그램 항상 차단 옵션을 선택하여 이 프로그램을 응용 프로그램 필터에 추가하고 의심스러운 프로그램 동작에 대한 Guard 알림을 통해 프로그램을 차단하도록 할 수 있습니다.

#### 차단할 응용 프로그램

##### 응용 프로그램

이 목록에는 구성에서 입력했거나 ProActiv 구성 요소에 알림으로써 유해한 것으로 분류한 모든 응용 프로그램이 포함됩니다. 목록의 응용 프로그램은 Avira AntiVir ProActiv 에 의해 차단되며 컴퓨터 시스템에서 실행할 수 없습니다. 차단된 프로그램이 시작되면 운영 체제 메시지가 나타납니다. Avira AntiVir ProActiv 는 지정된 경로 및 파일 이름을 기반으로 차단할 응용 프로그램을 식별하고 해당 콘텐츠와 관계없이 차단합니다.

##### 입력란

차단할 응용 프로그램을 이 상자에 입력합니다. 응용 프로그램을 식별하려면 전체 경로, 파일 이름 및 파일 확장명을 지정해야 합니다. 경로는 응용 프로그램이 있는 드라이브를 표시하거나 환경 변수로 시작해야 합니다.



이 단추를 클릭하면 표시되는 창에서 차단할 응용 프로그램을 선택할 수 있습니다.

##### 추가

"추가" 단추를 사용하여 입력란에 지정된 응용 프로그램을 차단할 응용 프로그램 목록으로 보낼 수 있습니다.

##### 참고

운영 체제의 작업에 필요한 응용 프로그램은 추가할 수 없습니다.

##### 삭제

The "삭제" 단추를 사용하면 차단할 응용 프로그램 목록에서 강조 표시된 응용 프로그램을 제거할 수 있습니다.

### 12.2.2.2. 응용 프로그램 필터: 허용된 응용 프로그램

**응용 프로그램 필터:** 허용된 응용 프로그램 섹션에는 ProActiv 구성 요소의 모니터링 대상에서 제외되는 응용 프로그램, 즉 신뢰할 수 있는 것으로 분류되고 기본적으로 목록에 포함된 서명된 프로그램과 신뢰할 수 있는 것으로 분류되고 응용 프로그램 필터에 추가한 모든 응용 프로그램이 나열됩니다. 구성에서 허용된 응용 프로그램을 목록에 추가할 수 있습니다. 또한 Guard 알림에서 신뢰할 수 있는 프로그램 옵션을 사용하여 Guard 알림을 통해 의심스러운 프로그램 동작에 응용 프로그램을 추가할 수도 있습니다.



## 건너뛰려 응용 프로그램

### 응용 프로그램

이 목록에는 ProActiv 구성 요소의 모니터링 대상에서 제외되는 응용 프로그램이 포함됩니다. 기본 설치 설정에서 목록에는 신뢰할 수 있는 공급자의 서명된 응용 프로그램이 포함됩니다. 사용자가 신뢰할 수 있는 것으로 간주하는 응용 프로그램은 구성이나 Guard 알림을 통해 추가할 수 있습니다. ProActiv 구성 요소는 경로, 파일 이름 및 콘텐츠를 사용하여 응용 프로그램을 식별합니다. 업데이트와 같은 변경 사항을 통해 프로그램에 매크드가 추가될 수 있으므로 콘텐츠를 검사하는 것이 좋습니다. 지정된 유형에서 콘텐츠 검사를 수행할지 여부를 결정할 수 있습니다. 예를 들어 "콘텐츠" 유형의 경우 ProActiv 구성 요소의 모니터링 대상에서 제외하기 전에 경로 및 파일 이름으로 지정된 응용 프로그램에 대해 파일 콘텐츠 변경 내용을 검사합니다. 파일 콘텐츠가 수정된 경우에는 ProActiv 구성 요소에서 응용 프로그램을 다시 모니터링합니다. "경로" 유형의 경우 Guard의 모니터링 대상에서 응용 프로그램을 제외한 이후에 콘텐츠 검사가 수행됩니다. 제외 유형을 변경하려면 표시된 유형을 클릭하십시오.

### 경고

예외적인 경우에만 경로 유형을 사용하십시오. 업데이트를 통해 응용 프로그램에 매크드가 추가될 수 있습니다. 원래 유해한 응용 프로그램은 맬웨어로 분류됩니다.

### 참고

AntiVir 프로그램의 모든 응용 프로그램 구성 요소를 포함하여 일부 신뢰할 수 있는 응용 프로그램은 목록에 들어 있지 않더라도 기본적으로 ProActiv 구성 요소의 모니터링 대상에서 제외됩니다.

### 입력란

이 상자에 ProActiv 구성 요소의 모니터링 대상에서 제외할 응용 프로그램을 입력합니다. 응용 프로그램을 식별하려면 전체 경로, 파일 이름 및 파일 확장명을 지정해야 합니다. 경로는 응용 프로그램이 있는 드라이브를 표시하거나 환경 변수로 시작해야 합니다.



이 단추를 사용하여 표시되는 창에서 제외할 응용 프로그램을 선택할 수 있습니다.

### 추가

"추가" 단추를 사용하여 입력란에 지정된 응용 프로그램을 제외할 응용 프로그램 목록으로 보낼 수 있습니다.

### 삭제

The "삭제" 단추를 사용하면 제외할 응용 프로그램 목록에서 강조 표시된 응용 프로그램을 제거할 수 있습니다.

## 12.2.3 신고

Guard에는 사용자 또는 관리자에게 검색 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 포함됩니다.



**보고**

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

**해제**

이 옵션을 사용하면 Guard 에서 로그를 만들지 않습니다. 평가관을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을 테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

**기본값**

이 옵션을 사용하면 Guard 에서 바이러스 발견, 알람 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**고급**

이 옵션을 사용하면 Guard 에서 덜 중요한 정보도 보고서 파일에 기록합니다.

**완료**

이 옵션을 사용하면 Guard 에서 파일 크기, 파일 형식, 날짜 등 사용할 수 있는 모든 정보를 보고서 파일에 기록합니다.

**보고서 파일 제한**

**nMB 로 크기 제한**

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 가능한 값은 1~100MB 입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB 의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 (지정된 크기 - 50KB)의 크기가 될 때까지 오래된 항목이 삭제됩니다.

**줄이기 전에 보고서 파일 백업**

이 옵션을 사용하면 보고서 파일의 크기를 줄이기 전에 보고서 파일이 백업됩니다. 저장 위치는 구성 :: 일반 :: 디렉터리 :: 보고서 디렉터리를 참조하십시오.

**보고서 파일에 구성 쓰기**

이 옵션을 사용하면 온 액세스 검사의 구성이 보고서 파일에 기록됩니다.

**참고**

보고서 파일에 대해 아무런 제한을 지정하지 않은 경우, 보고서 파일이 100MB 가 되면 자동으로 새 보고서 파일이 만들어집니다. 이전 보고서 파일의 백업도 만들어집니다. 이전 보고서 파일의 백업은 세 개까지 저장되며, 가장 오래된 백업부터 삭제됩니다.

## 12.3 MailGuard

구성의 MailGuard 섹션에서는 MailGuard 를 구성합니다.

## 12.3.1 검사

MailGuard 를 사용하여 받는 전자 메일에 대해 바이러스 및 맬웨어를 검사할 수 있습니다. MailGuard 는 보내는 전자 메일에 대해 바이러스 및 맬웨어 포함 여부를 검사할 수 있습니다.

### 검사

#### **MailGuard 켜기**

이 옵션을 사용하면 MailGuard 가 전자 메일 트래픽을 모니터링합니다. MailGuard 는 사용자의 전자 메일 서버와 컴퓨터 시스템의 전자 메일 클라이언트 프로그램 간에 주고받는 데이터 트래픽을 검사하는 프록시 서버입니다. 받는 전자 메일의 맬웨어 포함 여부는 기본적으로 검사됩니다. 이 옵션을 사용하지 않는 경우에도 MailGuard 서비스는 시작되지만 MailGuard 의 모니터링은 작동하지 않습니다.

#### **받는 전자 메일 검사**

이 옵션을 사용하면 받는 전자 메일에 대해 바이러스 및 맬웨어와 . MailGuard 는 POP3 및 IMAP 프로토콜을 지원합니다. 전자 메일 클라이언트에서 전자 메일을 받는 데 사용하는 받은 편지함 계정에 대해 MailGuard 에서 모니터링할 수 있도록 설정하십시오.

#### **POP3 계정 모니터링**

이 옵션을 사용하면 지정된 포트에서 POP3 계정이 모니터링됩니다.

#### **모니터링되는 포트**

이 필드에는 POP3 프로토콜에서 받은 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트를 입력할 경우 쉼표로 구분합니다.

#### **기본값**

이 단추는 지정된 포트를 기본 POP3 포트로 다시 설정합니다.

#### **IMAP 계정 모니터링**

이 옵션을 사용하면 지정된 포트에서 IMAP 계정이 모니터링됩니다.

#### **모니터링되는 포트**

이 필드에는 IMAP 프로토콜에서 받은 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트를 입력할 경우 쉼표로 구분합니다.

#### **기본값**

이 단추는 지정된 포트를 기본 IMAP 포트로 다시 설정합니다.

#### **보내는 전자 메일 검사(SMTP)**

이 옵션을 사용하면 보내는 전자 메일에 대해 바이러스 및 맬웨어 포함 여부를 검사합니다.

#### **모니터링되는 포트**

이 필드에는 SMTP 프로토콜에서 보낸 편지함으로 사용할 포트를 입력해야 합니다. 여러 개의 포트를 입력할 경우 쉼표로 구분합니다.

#### **기본값**

이 단추는 지정된 포트를 기본 SMTP 포트로 다시 설정합니다.

### 참고

사용된 프로토콜 및 포트를 확인하려면 전자 메일 클라이언트 프로그램에서 전자 메일 계정의 속성을 확인하십시오. 대체로 기본 포트가 사용됩니다.

### 12.3.1.1. 검색에 대한 작업

이 구성 섹션에는 MailGuard 에서 전자 메일이나 첨부 파일에서 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우 수행하는 작업에 대한 기타 설정이 포함되어 있습니다.

#### 참고

이러한 작업은 받는 전자 메일에서 바이러스가 검색될 때와 보내는 전자 메일에서 바이러스가 검색될 때 모두 수행됩니다.

#### 검색에 대한 작업

##### 대화형

이 옵션을 사용하면 전자 메일이나 첨부 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때 사용자가 관련 파일에 대해 수행할 작업을 선택할 수 있는 대화 상자가 나타납니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

##### 허용되는 작업

이 상자에서 작업을 지정하면 바이러스가 검색되었을 때 해당 작업이 표시되도록 선택할 수 있습니다. 작업을 지정하려면 해당 옵션을 활성화해야 합니다.

##### 격리 저장소로 이동

이 옵션을 활성화하면 모든 첨부 파일을 포함한 전자 메일이 격리 저장소로 이동합니다. 이 전자 메일은 나중에 격리 관리자를 통해 전달할 수 있습니다. 영향받는 전자 메일이 삭제되고 전자 메일의 텍스트 본문 및 모든 첨부 파일은 기본 텍스트로 바뀝니다.

##### 삭제

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 경우 영향받는 전자 메일이 삭제되고, 전자 메일의 텍스트 본문 및 모든 첨부 파일은 기본 텍스트로 바뀝니다.

##### 첨부 파일 삭제

이 옵션이 활성화된 경우 영향받는 첨부 파일이 기본 텍스트로 대체됩니다. 전자 메일의 본문이 감염된 경우, 본문이 삭제되고 기본 텍스트로 대체됩니다. 전자 메일 자체는 배달됩니다.

##### 첨부 파일을 격리 저장소로 이동

이 옵션을 활성화하면 해당하는 첨부 파일이 격리 저장소로 이동된 다음 삭제됩니다(기본 텍스트로 대체됨). 전자 메일 본문이 배달되며 영향받는 첨부 파일은 나중에 격리 관리자를 통해 전달할 수 있습니다.

##### 무시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견되어도 영향받는 전자 메일이 배달됩니다.

##### 기본값

이 단추를 사용하면 바이러스가 발견될 때 대화 상자에서 기본적으로 활성화되는 작업을 선택할 수 있습니다. 기본적으로 활성화할 작업을 선택하고 기본값 단추를 클릭합니다.

##### 진행률 표시줄 표시

이 옵션을 사용하면 MailGuard 에서 전자 메일 다운로드 중 진행률 표시줄을 표시합니다. 이 옵션은 **대화형** 옵션을 선택한 경우에만 사용할 수 있습니다.

### 자동

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 더 이상 알림이 제공되지 않습니다. 이 섹션에서 정의한 설정에 따라 MailGuard 가 작동합니다.

### 기본 작업

기본 작업은 MailGuard 가 전자 메일에서 바이러스나 사용자 동의 없이 설치된 프로그램을 발견한 경우에 수행하는 작업입니다. "전자 메일 무시" 옵션을 선택하는 경우, 첨부 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때 수행할 작업을 "영향받는 첨부 파일"에서도 선택할 수 있습니다.

### 전자 메일 삭제

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색되면 감염된 전자 메일이 자동으로 삭제됩니다. 전자 메일의 본문은 아래 지정된 기본 텍스트로 대체됩니다. 포함된 모든 첨부 파일에도 동일하게 적용됩니다. 따라서 이러한 첨부 파일도 기본 텍스트로 대체됩니다.

### 전자 메일 격리

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 모든 첨부 파일을 포함한 전체 전자 메일이 격리 저장소에 보관됩니다. 필요할 경우 나중에 복원할 수 있습니다. 감염된 전자 메일 자체는 삭제됩니다. 전자 메일의 본문은 아래 지정된 기본 텍스트로 대체됩니다. 포함된 모든 첨부 파일에도 동일하게 적용됩니다. 따라서 이러한 첨부 파일도 기본 텍스트로 대체됩니다.

### 전자 메일 무시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색되어도 감염된 전자 메일이 무시됩니다. 하지만 감염된 첨부 파일에 대해 수행할 작업을 결정할 수 있습니다.

### 영향받는 첨부 파일

"영향받는 첨부 파일" 옵션은 "기본 작업"에서 "전자 메일 무시" 설정을 선택한 경우에만 선택할 수 있습니다. 이 옵션을 사용하면 첨부 파일에서 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 경우 수행할 작업을 결정할 수 있습니다.

### 삭제

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 발견된 경우 영향받는 첨부 파일이 삭제되고 기본 텍스트로 대체됩니다.

### 격리

이 옵션을 사용하면 영향받는 첨부 파일이 격리 저장소로 이동된 다음 삭제됩니다(기본 텍스트로 대체됨). 나중에 필요한 경우, 영향받는 첨부 파일을 복원할 수 있습니다.

### 무시

이 옵션을 사용하면 바이러스나 사용자 동의 없이 설치된 프로그램이 검색되어도 첨부 파일이 무시되고 배달됩니다.

**경고**

이 옵션을 선택하면 MailGuard 에서 바이러스나 사용자 동의 없이 설치된 프로그램으로부터 사용자를 보호하지 않습니다. 어떠한 작업을 수행해야 할 지 확실히 알고 있는 경우에만 이 항목을 선택하십시오. 전자 메일 프로그램에서 미리 보고를 사용하지 마십시오. 두 번 클릭해도 첨부 파일이 열리지 않습니다!

**12.3.1.2. 기타 작업**

이 구성 섹션에는 MailGuard 에서 전자 메일이나 첨부 파일에서 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우 수행하는 작업에 대한 기타 설정이 포함되어 있습니다.

**참고**

이러한 작업은 받는 전자 메일에서 바이러스가 검색될 때만 수행됩니다.

**삭제 및 이동된 전자 메일에 대한 기본 텍스트**

이 상자의 텍스트는 영향받는 전자 메일 대신에 전자 메일에 메시지로 삽입됩니다. 이 메시지를 편집할 수 있으며, 텍스트 길이는 최대 500 자입니다.

서식 지정 시 다음 키 조합을 사용할 수 있습니다.

**Strg + Enter** 줄 바꿈을 삽입합니다.

**기본값**

이 단추는 편집 상자에 미리 정의된 기본 텍스트를 삽입합니다.

**삭제 및 이동된 첨부 파일에 대한 기본 텍스트**

이 상자의 텍스트는 영향받는 첨부 파일 대신에 전자 메일에 메시지로 삽입됩니다. 이 메시지를 편집할 수 있으며, 텍스트 길이는 최대 500 자입니다.

서식 지정 시 다음 키 조합을 사용할 수 있습니다.

**Strg + Enter** 줄 바꿈을 삽입합니다.

**기본값**

이 단추는 편집 상자에 미리 정의된 기본 텍스트를 삽입합니다.

**12.3.1.3. 추론**

이 구성 섹션에는 검사 엔진의 추론 설정이 들어 있습니다.

AntiVir 제품에는 알려지지 않은 맬웨어를 사전에, 즉 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 확인할 수 있는 매우 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 가양성(오진) 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

## 매크로 바이러스 추론

### 매크로 바이러스 추론 활성화

AntiVir 제품에는 매우 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

## AHeAD(고급 추론 분석 및 검색)

### AHeAD 사용

AntiVir 프로그램은 일종의 AntiVir AHeAD 기술로 매우 강력한 추론 기능을 제공하므로 알려지지 않은 신종 맬웨어를 감지할 수 있습니다. 이 옵션을 사용하면 이 추론의 "공격성" 수준을 정의할 수 있습니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### 낮은 검색 수준

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 줄어들기 때문에 가양성 문제가 발생할 위험이 낮습니다.

#### 보통 검색 수준

이 추론을 사용하도록 선택한 경우 이 옵션은 기본 설정으로 사용됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

#### 높은 검색 수준

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 현저히 늘어나지만 가양성일 확률도 높아집니다.

## 12.3.2 일반

### 12.3.2.1. 예외


#### 검사 예외

이 테이블은 AntiVir MailGuard의 검사로부터 제외되는 전자 메일 주소 목록(허용 목록)을 표시합니다.

#### 참고

받는 전자 메일의 경우 MailGuard에서만 예외 목록이 사용됩니다.

#### 상태

아이콘	설명
	이 전자 메일 주소에 대해 맬웨어 포함 여부를 더 이상 검사하지 않습니다.

#### 이메일 주소

더 이상 검사하지 않을 전자 메일입니다.

#### 맬웨어

이 옵션을 사용하면 전자 메일 주소에 대해 맬웨어 포함 여부를 더 이상 검사하지 않습니다.

**위로**

이 단추를 사용하면 강조 표시된 전자 메일 주소를 목록에서 위쪽으로 이동할 수 있습니다. 목록에 강조 표시된 항목이 없거나 강조 표시된 주소가 목록의 첫 번째 항목인 경우에는 이 단추를 사용할 수 없습니다.

**아래로**

이 단추를 사용하면 강조 표시된 전자 메일 주소를 목록에서 아래쪽으로 이동할 수 있습니다. 목록에 강조 표시된 항목이 없거나 강조 표시된 주소가 목록의 마지막 항목인 경우에는 이 단추를 사용할 수 없습니다.

**입력란**

이 상자에는 검사하지 않을 전자 메일 주소 목록에 추가할 전자 메일 주소를 입력합니다. 설정에 따라 해당 전자 메일 주소에 대해 MailGuard 에서 이후에 더 이상 검사하지 않습니다.

**추가**

이 단추를 사용하면 입력란에 입력한 전자 메일 주소를 검사하지 않을 전자 메일 주소의 목록에 추가할 수 있습니다.

**삭제**

이 단추는 강조 표시된 전자 메일 주소를 목록에서 삭제합니다.

### 12.3.2.2. 캐시

**캐시**

MailGuard 캐시에는 제어 센터의 MailGuard 에 통계 데이터로 표시되는 검사한 전자 메일에 관한 데이터가 포함되어 있습니다.

**캐시의 최대 전자 메일 수**

이 필드는 MailGuard 에서 캐시에 저장하는 최대 전자 메일 수를 설정하는 데 사용됩니다. 전자 메일은 가장 오래된 것부터 삭제됩니다.

**최대 전자 메일 보관 기간(일)**

이 상자에는 최대 전자 메일 보관 기간을 일 단위로 입력합니다. 이 기간이 경과되면 전자 메일이 캐시에서 제거됩니다.

**캐시 비우기**

이 단추를 클릭하면 캐시에 저장된 전자 메일이 삭제됩니다.

### 12.3.2.3. 바닥글

*바닥글*에서는 보내는 전자 메일에 표시되는 전자 메일 바닥글을 구성할 수 있습니다. 이 기능을 사용하려면 보내는 전자 메일에 대한 MailGuard 검사를 활성화해야 합니다(구성::MailGuard::검사의 *보내는 전자 메일 검사(SMTP)* 옵션 참조). 정의된 AntiVir MailGuard 바닥글을 사용하여 바이러스 방지 프로그램이 보낸 전자 메일을 검사했음을 확인할 수 있습니다. 또한 사용자 정의 바닥글을 삽입할 수 있습니다. 두 바닥글 옵션을 모두 사용하는 경우에는 AntiVir MailGuard 바닥글이 사용자 정의 텍스트 앞에 옵니다.

### 전송할 전자 메일의 바닥글

#### **AntiVir MailGuard** 바닥글 첨부

이 옵션을 사용하면 보낸 전자 메일의 메시지 텍스트 아래에 AntiVir MailGuard 바닥글이 표시됩니다. AntiVir MailGuard 바닥글은 AntiVir MailGuard. AntiVir MailGuard 바닥글에는 "AntiVir MailGuard [제품 버전] [검색 엔진의 이니셜 및 버전 번호] [바이러스 정의 파일의 이니셜 및 버전 번호](으)로 검사됨"이라는 텍스트가 포함됩니다.

#### **이 바닥글 첨부**

이 옵션을 사용하면 입력란에 삽입한 텍스트가 보낸 전자 메일에 바닥글로 표시됩니다.

#### **입력란**

이 입력란에는 보낸 전자 메일에 바닥글로 표시할 텍스트를 삽입할 수 있습니다.

## 12.3.3 신고

MailGuard에는 사용자 또는 관리자에게 검색 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 포함됩니다.

#### **보고**

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

#### **해제**

이 옵션을 사용하면 MailGuard에서 로그를 만들지 않습니다.

평가관을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을 테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

#### **기본값**

이 옵션을 사용하면 MailGuard에서 바이러스 발견, 알람 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### **고급**

이 옵션을 사용하면 MailGuard는 덜 중요한 정보도 보고서 파일에 기록합니다.

#### **완료**

이 옵션을 사용하면 MailGuard는 모든 정보를 보고서 파일에 기록합니다.

### 보고서 파일 제한

#### **nMB 로 크기 제한**

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 가능한 값은 1~100MB입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 (지정된 크기 - 50KB)의 크기가 될 때까지 오래된 항목이 삭제됩니다.

#### **줄이기 전에 보고서 파일 백업**



이 옵션을 사용하면 보고서 파일의 크기를 줄이기 전에 보고서 파일이 백업됩니다. 저장 위치는 구성 :: 일반 :: 디렉터리 :: 보고서 디렉터리를 참조하십시오.

**보고서 파일에 구성 쓰기**

이 옵션을 사용하면 MailGuard 구성이 보고서 파일에 기록됩니다.

**참고**

보고서 파일에 대해 아무런 제한을 지정하지 않은 경우, 보고서 파일이 100MB 가 되면 자동으로 새 보고서 파일이 만들어집니다. 이전 보고서 파일의 백업도 만들어집니다. 이전 보고서 파일의 백업은 세 개까지 저장되며, 가장 오래된 백업부터 삭제됩니다.

## 12.4 방화벽

구성의 FireWall 섹션에서는 Avira FireWall 을 구성합니다.

### 12.4.1 어댑터 규칙

Avira FireWall 에서 어댑터는 소프트웨어 시뮬레이트된 하드웨어 장치(예: 미니포트, 브리지 연결 등) 또는 실제 하드웨어 장치(예: 네트워크 카드)를 나타냅니다.

Avira FireWall 에서는 컴퓨터에서 드라이버가 설치된 기존의 모든 어댑터에 대한 어댑터 규칙을 표시합니다.

미리 정의된 어댑터 규칙은 보안 수준에 따라 다릅니다. 제어 센터의 온라인 보호 :: FireWall 설정 변경 가능에서 보안 수준을 변경하거나 고유의 어댑터 규칙을 정의할 수 있습니다. 고유의 어댑터 규칙을 정의한 경우, 제어 센터의 FireWall 섹션에서 보안 수준이 사용자 지정으로 설정됩니다.

**참고**

Avira FireWall 의 모든 미리 정의된 규칙에 대한 기본 보안 수준 설정은 **보통**입니다.

#### ICMP 프로토콜

ICMP(Internet Control Message Protocol)는 네트워크에서 오류 및 정보 메시지를 교환하는 데 사용됩니다. 이 프로토콜은 ping 또는 tracert 를 이용한 상태 메시지에도 사용됩니다.

이 규칙을 사용하면 들어오고 나가는 메시지 중 차단되는 메시지 유형, 플로딩 동작 및 조각화된 ICMP 패킷의 반응을 정의할 수 있습니다. 이 규칙은 모든 패킷에 응답하므로 공격을 받은 컴퓨터의 CPU 로드를 증가시키는 ICMP 플로드 공격을 방지하는 역할을 수행합니다.

**ICMP 프로토콜에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
수신 차단된 유형: 유형 없음	낮은 수준에도 동일한 규칙이	수신 차단된 유형: 여러 유형

<p>발신 차단된 유형: <b>유형 없음</b></p> <p>패킷 간 지연이 <b>50</b> 밀리초보다 짧으면 플로딩으로 간주합니다.</p> <p><b>거부</b> - 조각화된 ICMP 패킷을 거부합니다.</p>	<p>적용됩니다.</p>	<p>발신 차단된 유형: <b>여러 유형</b></p> <p>패킷 간 지연이 <b>50</b> 밀리초보다 짧으면 플로딩으로 간주합니다.</p> <p><b>거부</b> - 조각화된 ICMP 패킷을 거부합니다.</p>
---	---------------	---

**수신 차단된 유형: 유형 없음/여러 유형**

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 수신 ICMP 메시지 유형을 지정할 수 있습니다.

**발신 차단된 유형: 유형 없음/여러 유형**

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 발신 ICMP 메시지 유형을 선택할 수 있습니다.

**플로딩**

이 링크를 클릭하면 허용되는 최대 ICMPA 지연을 입력할 수 있는 대화 상자가 나타납니다.

**조각화된 ICMP 패킷**

이 링크를 클릭하면 조각화된 ICMP 패킷을 거부할지 여부를 선택할 수 있습니다.

**TCP 포트 검사**

이 규칙을 사용하면 FireWall 에서 TCP 포트 검사로 간주하는 경우와 그 경우 취해야 할 조치를 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 TCP 포트를 감지하는 TCP 포트 검사 공격을 방지하는 역할을 수행합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

**TCP 포트 검사에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.</p>	<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가합니다.</p>	<p>중간 수준에도 동일한 규칙이 적용됩니다.</p>

**포트**

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 TCP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

**포트 검사 시간 창**

이 링크를 클릭하면 TCP 포트 검사로 간주할 특정 포트 검사 횟수에 대한 시간 범위를 입력할 수 있는 대화 상자가 나타납니다.

**보고서 파일**

이 링크를 클릭하면 공격자의 IP 주소를 기록할지 여부를 선택할 수 있습니다.

**규칙**

이 링크를 클릭하면 TCP 포트 검사 공격을 차단하는 규칙을 추가할지 여부를 선택할 수 있습니다.

**UDP 포트 검사**

이 규칙을 사용하면 FireWall 에서 UDP 포트 검사로 간주하는 경우와 이 경우에 수행해야 할 작업을 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 UDP 포트를 감지하는 UDP 포트 검사 공격을 방지합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

**UDP 포트 검사에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.</p>	<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가합니다.</p>	<p>중간 수준에도 동일한 규칙이 적용됩니다.</p>

**포트**

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 UDP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

**포트 검사 시간 창**

이 링크를 클릭하면 UDP 포트 검사로 간주할 특정 포트 검사 횟수에 대한 시간 범위를 입력할 수 있는 대화 상자가 나타납니다.

**보고서 파일**

이 링크를 클릭하면 공격자의 IP 주소를 기록할지 여부를 선택할 수 있습니다.

**규칙**

이 링크를 클릭하면 UDP 포트 검사 공격을 차단하는 규칙을 추가할지 여부를 선택할 수 있습니다.

**12.4.1.1. 들어오는 규칙**

들어오는 규칙은 들어오는 데이터 트래픽을 Avira FireWall 에서 제어하기 위해 정의합니다.

**참고**

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

**TCP 데이터 트래픽 데이터 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
들어오는 데이터 트래픽을 Avira FireWall 에서 차단하지 않습니다.	<ul style="list-style-type: none"> <li>- 135 에 대해 설정된 TCP 연결 허용</li> <li>로컬 포트가 <b>{135}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 TCP 패킷을 허용합니다. 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> <li>- 135 에 대한 TCP 패킷 거부</li> <li>로컬 포트가 <b>{135}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의</li> </ul>	<ul style="list-style-type: none"> <li>- 설정된 TCP 데이터 트래픽 모니터</li> <li>로컬 포트가 <b>{0-65535}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 TCP 패킷을 허용합니다. 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> </ul>

**TCP** 패킷을 거부합니다.  
모든 패킷에 적용됩니다.  
패킷이 규칙과 일치하는 경우 기록하지 않습니다.  
고급: 오프셋  
**0** 에서 <빈>  
마스크를 사용하는 <빈>  
마이트가 따라오는 패킷을 무시합니다.

- TCP 정상 데이터 트래픽 모니터

로컬 포트가 {**0-65535**}이고  
원격 포트가 {**0-65535**}인 경우  
**0.0.0.0**  
마스크를 사용하는  
**0.0.0.0** 주소의 TCP 패킷을 허용합니다.  
연결 시작 및 기존 연결 패킷에 적용됩니다.  
패킷이 규칙과 일치하는 경우 기록하지 않습니다.  
고급: **0** 오프셋에 <빈> 마스크를 사용하는 <빈>  
마이트가 따라오는 패킷을 무시합니다.

- 모든 TCP 패킷 거부

	<p>로컬 포트가 <b>{0-65535}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 <b>TCP</b> 패킷을 거부합니다. <b>모든 패킷</b>에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 마이트가 따라오는 패킷을 무시합니다.</p>	
--	---	--

**TCP 패킷 허용/거부**

이 링크를 클릭하면 특별하게 정의된 들어오는 TCP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**로컬 포트**

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

**원격 포트**

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

**적용 방법**

이 링크를 클릭하면 모든 패킷이 아닌 기존 연결 패킷에 대해서만 규칙을 적용하거나 연결 시작 및 기존 연결 패킷에 대해 규칙을 적용할 수 있습니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

**필터링된 콘텐츠: 데이터**

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 TCP 헤더가 끝나는 위치부터 계산됩니다.

**UDP 데이터 트래픽 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	<ul style="list-style-type: none"> <li>UDP 허용 데이터 트래픽 모니터</li> <li>로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 허용합니다. 열린 포트에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 0 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> <li>모든 UDP 패킷 거부</li> <li>로컬 포트가 {0-65535}이고 원격</li> </ul>	<p>설정된 UDP 트래픽 모니터</p> <p>로컬 포트가 {0-65535} 범위이고 원격 포트가 {53, 67, 68, 123} 범위인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 허용합니다. 열린 포트에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 0 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p>

포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 거부합니다. 모든 포트에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 0 오프셋에 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.

#### UDP 패킷 허용/거부

이 링크를 클릭하면 특별하게 정의된 들어오는 UDP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

#### IP 주소

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

#### IP 마스크

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

#### 로컬 포트

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

#### 원격 포트

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

#### 적용 방법

이 링크를 클릭하면 규칙을 모든 포트에 적용할지 아니면 열려 있는 모든 포트에만 적용할지를 선택할 수 있습니다.

#### 보고서 파일

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

#### 필터링된 콘텐츠: 데이터



이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 UDP 헤더가 끝나는 위치부터 계산됩니다.

**ICMP 데이터 트래픽 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	- IP 주소를 기반으로 ICMP 취소 안 함  <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 ICMP 패킷을 허용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 <빈> 마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.	중간 수준에도 동일한 규칙이 적용됩니다.

**ICMP 패킷 허용/거부**

이 링크를 클릭하면 특별하게 정의된 들어오는 ICMP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

고급 기능을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

**필터링된 콘텐츠: 데이터**

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 ICMP 헤더가 끝나는 위치부터 계산됩니다.

**IP 패킷에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	-	모든 IP 패킷 거부  <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 <b>IP 패킷</b> 을 거부합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다.

**IP 패킷 허용/거부**

이 링크를 클릭하면 특별히 정의된 IP 패키지를 허용할지 거부할지 여부를 결정할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**사용할 수 있는 IP 프로토콜 기반 IP 패키지 모니터링 규칙**

**IP 패키지**

이 링크를 클릭하면 특별히 정의된 IP 패키지를 허용할지 거부할지 여부를 결정할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**프로토콜**

이 링크를 클릭하면 필요한 IP 프로토콜을 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**12.4.1.2. 나가는 규칙**

나가는 규칙은 Avira FireWall 에서 나가는 데이터 트래픽을 제어하기 위해 정의합니다. IP, ICMP, UDP 및 TCP 프로토콜 중 하나에 대한 나가는 규칙을 정의할 수 있습니다.

**참고**

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

**단추**

단추	설명
추가	새 규칙을 만들 수 있습니다. 이 단추를 누르면 "새 규칙 추가 대화 상자가 열립니다". 이 대화 상자에서 새 규칙을 선택할 수 있습니다.
제거	선택한 규칙을 제거합니다.
규칙 아래로	선택한 규칙을 한 줄 아래로 이동하여 규칙 우선 순위를 낮춥니다.
규칙 위로	선택한 규칙을 한 줄 위로 이동하여 규칙 우선 순위를 높입니다.
이름 바꾸기	선택한 규칙에 다른 이름을 지정할 수 있습니다.

**참고**

컴퓨터에 있는 모든 어댑터 또는 개별 어댑터에 대해 새 규칙을 추가할 수 있습니다. 모든 어댑터에 대해 어댑터 규칙을 추가하려면 표시되는 어댑터 계층 구조에서 컴퓨터를 선택하고 **추가 단추**를 클릭합니다.

**참고**

규칙을 원하는 위치로 끌어놓음으로써 규칙의 위치를 변경할 수도 있습니다.

**12.4.2 응용 프로그램 규칙**

**사용자의 응용 프로그램 규칙**

이 목록에는 시스템의 모든 사용자가 포함됩니다. 관리자로 로그인한 경우 규칙을 적용할 사용자를 선택할 수 있습니다. 관리 권한을 가진 사용자가 아닌 경우 현재 로그인한 사용자만 볼 수 있습니다.

### 응용 프로그램 목록

이 표에는 규칙이 정의된 응용 프로그램의 목록이 표시됩니다. 응용 프로그램 목록에는 Avira FireWall 이 설치된 이후에 실행되고 규칙을 저장한 각 응용 프로그램에 대한 설정이 포함되어 있습니다.

#### 일반 보기

	설명
응용 프로그램	응용 프로그램의 이름입니다.
모드	선택한 응용 프로그램 규칙 모드를 표시합니다. <b>필터링</b> 모드에서는 응용 프로그램을 실행한 후 어댑터 규칙을 검사하고 실행합니다. <b>권한</b> 모드에서는 어댑터 규칙이 무시됩니다. 다른 모드로 전환하려면 이 링크를 클릭합니다.
작업	네트워크 사용 유형과 상관없이 응용 프로그램에서 네트워크를 사용할 때 Avira FireWall 에서 자동으로 수행할 작업을 표시합니다. 이 링크를 클릭하면 다른 작업 유형으로 전환할 수 있습니다. 작업 유형에는 <b>요청</b> , <b>허용</b> 또는 <b>거부</b> 가 있습니다. 기본 작업은 <b>요청</b> 입니다.

#### 확장 구성

응용 프로그램의 네트워크 액세스에 개별 규칙이 필요한 경우 어댑터 규칙을 만들 때와 동일한 방식으로 패킷 필터 기반의 응용 프로그램 규칙을 만들 수 있습니다. 응용 프로그램 규칙의 확장 구성으로 변경하려면 먼저 고급 모드를 활성화합니다. 그런 다음 FireWall::설정 섹션: **확장 설정** 사용 옵션에서 응용 프로그램 규칙 설정을 변경하고 **적용** 또는 **확인**을 클릭하여 설정을 저장합니다. FireWall 구성에서 **FireWall::응용 프로그램 규칙** 섹션을 선택합니다. 응용 프로그램 규칙 목록에 제목이 **필터링**이고 **기본**이라는 항목이 있는 추가 열이 표시됩니다. 이제 **필터링: 고급- 작업: 규칙** 옵션이 추가되어 확장 구성을 선택할 수 있습니다.

	설명
응용 프로그램	응용 프로그램의 이름입니다.
모드	선택한 응용 프로그램 규칙 모드를 표시합니다. <b>필터링</b> 모드에서는 응용 프로그램을 실행한 후 어댑터 규칙을 검사하고 실행합니다. <b>권한</b> 모드에서는 어댑터 규칙이 무시됩니다. 다른 모드로 전환하려면 이 링크를 클릭합니다.
작업	네트워크 사용 유형과 상관없이 응용 프로그램에서 네트워크를 사용할 때 Avira FireWall 에서 자동으로 수행할 작업을 표시합니다.

	<p><b>필터링</b>- 기본을 선택한 경우 링크를 클릭하여 다른 작업 유형을 선택할 수 있습니다. 값은 <b>요청, 허용, 거부</b> 또는 <b>확장</b>입니다.</p> <p><b>필터링</b>- 고급을 선택한 경우 <b>규칙</b>작업 유형이 표시됩니다. <b>규칙</b> 링크를 클릭하면 응용 프로그램에 대한 특정 규칙을 입력할 수 있는 <b>응용 프로그램 규칙</b> 창이 열립니다.</p>
필터링	<p>필터링 유형을 표시합니다. 링크를 클릭하여 다른 필터링 유형을 선택할 수 있습니다.</p> <p><b>기본</b>: 기본 필터링의 경우 소프트웨어 응용 프로그램에서 수행하는 모든 네트워크 작업에 대해 지정된 작업이 실행됩니다.</p> <p><b>고급</b>: 이 유형의 필터링을 사용하면 확장 구성에 추가된 규칙이 적용됩니다.</p>

응용 프로그램에 대한 특정 규칙을 만들려면 **필터링**아래에서 **고급** 항목을 선택합니다. 그러면 **작업** 열에 **규칙**항목이 표시됩니다. **규칙**을 클릭하면 특정 응용 프로그램 규칙을 만들 수 있는 창이 열립니다.

**확장 구성에 지정된 응용 프로그램 규칙**

지정된 응용 프로그램 규칙을 사용하여 응용 프로그램에 대해 지정된 데이터 트래픽을 허용 또는 거부하거나 개별 포트에 대한 수동 수신 대기기를 허용 또는 거부할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

**코드 삽입 허용 또는 거부**

코드 삽입은 다른 프로세스의 주소 공간에 작업을 실행할 코드를 삽입하여 해당 프로세스에서 DLL(동적 연결 라이브러리)을 강제로 로드하는 기술입니다. 코드 삽입은 특히 맬웨어에서 다른 프로그램 몰래 코드를 실행하는 데 사용됩니다. 이 방법을 사용하면 FireWall 보다 먼저 인터넷에 몰래 액세스할 수 있습니다. 기본 모드에서 코드 삽입은 서명된 모든 응용 프로그램에 대해 사용하도록 설정됩니다.

**응용 프로그램 포트에 대한 수동적 수신 대기 허용 또는 거부**

**데이터 트래픽 허용 또는 거부**

**들어오거나 나가는 IP 패킷 허용 또는 거부**

**들어오거나 나가는 TCP 패킷 허용 또는 거부**

**들어오거나 나가는 UDP 패킷 허용 또는 거부**

각 응용 프로그램에 대해 원하는 수만큼 응용 프로그램 규칙을 만들 수 있습니다. 응용 프로그램 규칙은 표시된 순서대로 실행됩니다. 자세한 내용은 를 참조하십시오.

**참고**

응용 프로그램 규칙의 **고급**필터링을 변경할 경우 확장 구성의 기존 응용 프로그램 규칙은 영구적으로 삭제되는 것이 아니라 비활성화 상태가 됩니다. **고급**필터링을 다시 선택하면 기존 응용 프로그램 규칙이 다시 활성화되어 응용 프로그램 규칙에 대한 확장 구성 창에 표시됩니다.

**응용 프로그램 정보**

이 상자에서는 응용 프로그램 목록 상자에서 선택한 응용 프로그램에 대한 자세한 정보를 볼 수 있습니다.

	설명
이름	응용 프로그램의 이름입니다.
경로	실행 파일의 전체 경로입니다.

### 단추

단추	설명
응용 프로그램 추가	새 응용 프로그램 규칙을 만들 수 있습니다. 이 단추를 누르면 대화 상자가 열립니다. 여기에서 새 규칙을 만드는 데 필요한 응용 프로그램을 선택할 수 있습니다.
규칙 제거	선택한 응용 프로그램 규칙을 제거합니다.
다시 로드	응용 프로그램 목록을 다시 로드하고 방금 변경한 응용 프로그램 규칙의 변경 내용을 취소합니다.

## 12.4.3 신뢰할 수 있는 공급자

신뢰할 수 있는 소프트웨어 공급자 목록은 **신뢰할 수 있는 공급자** 아래에 표시됩니다. **네트워크 이벤트** 팝업 창의 **이 공급자를 항상 신뢰** 옵션을 사용하여 목록에 공급자를 추가하거나 목록에서 공급자를 제거할 수 있습니다. **신뢰할 수 있는 공급자의 응용 프로그램을 자동으로 허용** 옵션을 사용하여 기본적으로 나열된 공급자가 서명한 응용 프로그램의 네트워크 액세스를 허용할 수 있습니다.

### 사용자의 신뢰할 수 있는 공급업체

이 목록에는 시스템의 모든 사용자가 포함됩니다. 관리자로 로그인한 경우 신뢰할 수 있는 공급자 목록을 보거나 업데이트하려는 사용자를 선택할 수 있습니다. 관리 권한을 가진 사용자가 아닌 경우 현재 로그인한 사용자만 볼 수 있습니다.

### **신뢰할 수 있는 공급업체가 만든 응용 프로그램을 자동으로 허용**

이 옵션을 사용하면 신뢰할 수 있으며 확인된 공급업체의 서명과 함께 제공된 응용 프로그램에 대해 네트워크 액세스가 자동으로 허용됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

### 공급업체

이 목록에는 신뢰할 수 있는 공급자로 분류된 공급자가 모두 표시됩니다.

### 단추

단추	설명
----	----

제거	강조 표시된 항목을 신뢰할 수 있는 공급자 목록에서 제거합니다. 목록에서 선택한 공급자를 영구적으로 제거하려면 구성 창에서 <b>적용</b> 또는 <b>확인</b> 을 클릭합니다.
다시 로드	변경을 취소합니다. 마지막으로 저장되었던 목록이 로드됩니다.

**참고**  
 목록에서 공급자를 제거한 후 **적용**을 선택하면 공급자가 목록에서 영구적으로 제거됩니다. **다시 로드**를 사용해도 변경 사항을 취소할 수 없습니다. 그러나 **네트워크 이벤트** 팝업 창의 **이 공급자를 항상 신뢰** 옵션을 사용하여 신뢰할 수 있는 공급자 목록에 공급자를 다시 추가할 수 있습니다.

**참고**  
 FireWall 에서는 신뢰할 수 있는 공급자 목록에 항목을 추가하기 전에 응용 프로그램 규칙에 우선 순위를 부여합니다. 응용 프로그램 규칙을 만들었으며 응용 프로그램 공급자가 신뢰할 수 있는 공급자 목록에 나열된 경우 응용 프로그램 규칙이 실행됩니다.

#### 12.4.4 설정

##### 고급 옵션

##### **FireWall** 사용

이 옵션을 활성화하면 Avira FireWall 이 사용하도록 설정되어 인터넷 및 기타 네트워크에서 비롯되는 위협으로부터 컴퓨터를 보호합니다.

##### **시작 시 Windows 방화벽 중지**

이 옵션을 사용하면 컴퓨터를 다시 부팅할 때 Windows 방화벽이 비활성화됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

##### **Windows 호스트 파일이 잠겨 있지 않음/잠겨 있음**

이 옵션을 잠김으로 설정한 경우 Windows 호스트 파일에 대한 쓰기가 금지되고 더 이상 수정할 수 없습니다. 예를 들어 맬웨어가 사용자를 원치 않는 웹 사이트로 리디렉션할 수 없습니다. 이 옵션의 상태는 기본적으로 잠겨 있지 않음입니다.

##### 자동 규칙 시간 초과

##### **영구 차단**

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등과 같이 자동으로 생성된 규칙이 유지됩니다.

##### **다음 이후 규칙 제거(초)**

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등 자동으로 생성된 규칙이 사용자가 정의한 시간이 지나면 제거됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**알림**

알림은 FireWall 의 데스크톱 알림을 받고자 하는 이벤트를 정의합니다.

**포트 검사**

이 옵션을 활성화하면 FireWall 에서 포트 검사가 감지될 경우 사용자에게 데스크톱 알림이 전달됩니다.

**플로딩**

이 옵션을 활성화하면 FireWall 에서 플로딩 공격이 감지될 경우 사용자에게 데스크톱 알림이 전달됩니다.

**차단된 응용 프로그램**

이 옵션을 활성화하면 FireWall 에서 응용 프로그램의 네트워크 작업을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

**차단된 IP**

이 옵션을 활성화하면 FireWall 에서 한 IP 주소의 데이터 트래픽을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

**응용 프로그램 규칙**

응용 프로그램 규칙 옵션은 FireWall::응용 프로그램 규칙 섹션에서 응용 프로그램 규칙에 대한 구성 옵션을 설정하는 데 사용됩니다.

**고급 옵션**

이 옵션을 사용하면 응용 프로그램의 다양한 네트워크 액세스를 개별적으로 조정할 수 있습니다.

**기본 설정**

이 옵션을 사용하면 응용 프로그램의 다양한 네트워크 액세스에 대해 한 가지 작업만 설정할 수 있습니다.

## 12.4.5 팝업 설정

**팝업 설정****프로세스 시작 스택 검사**

이 옵션을 사용하면 프로세스 스택 검사에서 보다 정확하게 제어할 수 있습니다. FireWall 에서는 스택의 프로세스 중 신뢰할 수 없는 프로세스가 실제로 하위 프로세스를 통해 네트워크에 액세스하는 프로세스가 될 수 있다고 가정합니다. 따라서 프로세스 스택의 프로세스 중 신뢰할 수 없는 프로세스마다 다른 팝업 창이 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

**프로세스당 여러 팝업 허용**

이 옵션을 사용하면 응용 프로그램이 네트워크에 연결하려고 할 때마다 팝업이 나타납니다. 또는 첫 번째 연결 시도에 대한 정보만 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

**게임 모드인 경우 팝업 알림 자동으로 표시 안 함**



이 옵션을 사용하도록 설정하면 컴퓨터 시스템에서 응용 프로그램을 전체 화면 모드로 실행할 경우 Avira FireWall 게임 모드가 자동으로 활성화됩니다. 게임 모드에서는 정의된 모든 어댑터 및 응용 프로그램 규칙이 적용됩니다. "허용" 또는 "거부" 작업을 통해 정의된 규칙이 없는 응용 프로그램에 대한 네트워크 액세스가 일시적으로 허용되며 이에 따라 네트워크 이벤트에 대해 묻는 팝업 창이 나타나지 않습니다.

### **이 응용 프로그램에 대한 작업 기억**

#### **항상 사용**

이 옵션을 사용하도록 설정하면 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### **항상 사용 안 함**

이 옵션을 사용할 경우 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용되지 않습니다.

#### **서명된 응용 프로그램 허용**

이 옵션을 사용하면 서명된 응용 프로그램에서 네트워크에 액세스할 때 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 자동으로 사용됩니다. 제조업체에는 Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia 가 있습니다.

#### **마지막으로 사용된 상태 기억**

이 옵션을 사용할 경우 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 마지막 네트워크 이벤트와 동일한 방식으로 사용됩니다. "이 응용 프로그램에 대한 작업 기억" 옵션을 사용하도록 설정하면 다음과 같은 네트워크 이벤트에도 이 옵션이 사용됩니다. 마지막 네트워크 이벤트에 대해 "이 응용 프로그램에 대한 작업 기억" 옵션이 사용 안 함으로 설정되어 있었다면 다음 네트워크 이벤트에 이 옵션이 사용되지 않습니다.

### **세부 정보 표시**

이 구성 옵션 그룹에서는 **네트워크 이벤트** 창의 세부 정보 표시를 설정할 수 있습니다.

#### **요구 시 세부 정보 표시**

이 옵션을 사용하면 요청 시에만 세부 정보가 "네트워크 이벤트" 창에 표시됩니다. 예를 들어 "네트워크 이벤트" 창에서 "세부 정보 표시" 단추를 클릭하면 세부 정보가 표시됩니다.

#### **항상 세부 정보 표시**

이 옵션을 사용하면 세부 정보가 "네트워크 이벤트" 창에 항상 표시됩니다.

#### **마지막으로 사용된 상태 기억**

이 옵션을 사용하면 세부 정보 표시가 이전 네트워크 이벤트에서와 같은 방식으로 관리됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 표시되었거나 액세스된 경우 다음 네트워크 이벤트에 대해 세부 정보가 표시됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 숨겨졌거나 표시되지 않은 경우에는 다음 네트워크 이벤트에 대해 세부 정보가 표시되지 않습니다.

**권한 허용**

이 구성 옵션 그룹에서는 **네트워크 이벤트** 창의 **권한 허용** 옵션에 대한 상태를 정의할 수 있습니다.

**항상 사용**

이 옵션을 사용하면 "**권한 허용**" 옵션이 "**네트워크 이벤트**" 창에서 기본적으로 사용됩니다.

**항상 사용 안 함**

이 옵션을 사용하면 "**권한 허용**" 옵션이 "**네트워크 이벤트**" 창에서 기본적으로 사용되지 않습니다.

**마지막으로 사용된 상태 기억**

이 옵션을 사용하면 "**권한 허용**" 옵션의 상태가 "**네트워크 이벤트**" 창에서 이전 네트워크 이벤트의 경우와 동일한 방식으로 처리됩니다. 마지막 네트워크 이벤트 실행에 대해 "**권한 허용**" 옵션을 사용하면 다음 네트워크 이벤트에 대해 이 옵션이 기본적으로 사용됩니다. 마지막 네트워크 이벤트 실행에 대해 "**권한 허용**" 옵션을 사용하지 않았다면 다음 네트워크 이벤트에 대해 이 옵션이 기본 설정으로 사용되지 않습니다.

## 12.5 SMC 아래 방화벽

이 FireWall 은 Avira Security Management Center 를 통해 특정 관리 요구 사항을 충족하도록 구성되어 있습니다. 개별 구성 옵션에는 다음과 같은 확장 옵션 및 제한이 있습니다.

- FireWall 설정은 클라이언트 컴퓨터의 모든 사용자에게 적용됩니다.
- 어댑터 규칙: 상황에 맞는 메뉴를 사용하여 개별 어댑터에 대한 보안 수준을 설정할 수 있습니다.
- 응용 프로그램 규칙: 응용 프로그램의 네트워크 액세스를 허용하거나 거부할 수 있습니다. 특정 응용 프로그램 규칙을 만들 수는 없습니다.

Avira Security Management Center 에서 AntiVir 프로그램을 관리하는 경우 클라이언트 컴퓨터의 제어 센터에서 다음 FireWall 설정 옵션이 비활성화됩니다.

- FireWall 보안 수준 설정
- 어댑터 및 응용 프로그램 규칙 설정

### 12.5.1 일반 설정

**고급 옵션****Windows 호스트 파일 잠금**

이 옵션을 사용하면 Windows 호스트 파일에 대한 쓰기가 금지되고 더 이상 수정할 수 없습니다. 예를 들어 맬웨어가 사용자를 원치 않는 웹 사이트로 리디렉션할 수 없습니다.

**게임 모드 사용**

이 옵션을 사용하도록 설정하면 컴퓨터 시스템에서 응용 프로그램을 전체 화면 모드로 실행할 경우 Avira FireWall 게임 모드가 자동으로 활성화됩니다. 게임 모드에서는 정의된 모든 어댑터 및 응용 프로그램 규칙이 적용됩니다. "허용" 또는 "거부" 작업을 통해 정의된 규칙이 없는 응용 프로그램에 대한 네트워크 액세스가 일시적으로 허용되며 이에 따라 네트워크 이벤트에 대해 묻는 팝업 창이 나타나지 않습니다.

#### **시작 시 Windows 방화벽 중지**

이 옵션을 사용하면 컴퓨터를 다시 부팅할 때 Windows 방화벽이 비활성화됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### **FireWall 사용**

이 옵션을 활성화하면 Avira FireWall 이 사용하도록 설정되어 인터넷 및 기타 네트워크에서 비롯되는 위협으로부터 컴퓨터를 보호합니다.

#### **자동 규칙 시간 초과**

##### **영구 차단**

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등과 같이 자동으로 생성된 규칙이 유지됩니다.

##### **다음 이후 규칙 제거(초)**

이 옵션을 사용하면 포트 검사 중에 생성된 규칙 등 자동으로 생성된 규칙이 사용자가 정의한 시간이 지나면 제거됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

## 12.5.2 일반 어댑터 규칙

설정된 네트워크 연결이 지정된 어댑터입니다. 어댑터 규칙은 다음 클라이언트 네트워크 연결에 적용될 수 있습니다.

- 기본 어댑터: LAN 또는 고속 인터넷
- 무선
- 전화 접속 연결

어댑터의 상황에 맞는 메뉴에서 사용 가능한 모든 어댑터에 대해 미리 정의된 어댑터 규칙을 지정할 수 있습니다.

- 보안 수준 - 높음
- 보안 수준 - 보통
- 보안 수준 - 낮음

또한 특정 요구 사항에 맞게 개별 어댑터 규칙을 수정할 수도 있습니다.

#### **참고**

Avira FireWall 의 모든 미리 정의된 규칙에 대한 기본 보안 수준 설정은 **보통**입니다.

#### **ICMP 프로토콜**

ICMP(Internet Control Message Protocol)는 네트워크에서 오류 및 정보 메시지를 교환하는 데 사용됩니다. 이 프로토콜은 ping 또는 tracert 를 이용한 상태 메시지에도 사용됩니다.

이 규칙을 사용하면 들어오고 나가는 메시지 중 차단되는 메시지 유형, 플로딩 동작 및 조각화된 ICMP 패킷의 반응을 정의할 수 있습니다. 이 규칙은 모든 패킷에 응답하므로 공격을 받은 컴퓨터의 CPU 로드를 증가시키는 ICMP 플로드 공격을 방지하는 역할을 수행합니다.

**ICMP 프로토콜에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
수신 차단된 유형: <b>유형 없음</b>	낮은 수준에도 동일한 규칙이 적용됩니다.	수신 차단된 유형: <b>여러 유형</b>
발신 차단된 유형: <b>유형 없음</b>		발신 차단된 유형: <b>여러 유형</b>
패킷 간 지연이 <b>50</b> 밀리초보다 짧으면 플로딩으로 간주합니다.		패킷 간 지연이 <b>50</b> 밀리초보다 짧으면 플로딩으로 간주합니다.
<b>거부</b> - 조각화된 ICMP 패킷을 거부합니다.		<b>거부</b> - 조각화된 ICMP 패킷을 거부합니다.

**수신 차단된 유형: 유형 없음/여러 유형**

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 수신 ICMP 메시지 유형을 지정할 수 있습니다.

**발신 차단된 유형: 유형 없음/여러 유형**

이 링크를 클릭하면 ICMP 패킷 유형 목록이 표시됩니다. 이 목록에서 차단할 발신 ICMP 메시지 유형을 선택할 수 있습니다.

**플로딩**

이 링크를 클릭하면 허용되는 최대 ICMPPA 지연을 입력할 수 있는 대화 상자가 나타납니다.

**조각화된 ICMP 패킷**

이 링크를 클릭하면 조각화된 ICMP 패킷을 거부할지 여부를 선택할 수 있습니다.

**TCP 포트 검사**

이 규칙을 사용하면 FireWall 에서 TCP 포트 검사로 간주하는 경우와 이 경우에 수행해야 할 작업을 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 TCP 포트를 감지하는 TCP 포트 검사 공격을 방지하는 역할을 수행합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

**TCP 포트 검사에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
--------	--------	--------

<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.</p>	<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 TCP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가합니다.</p>	<p>중간 수준에도 동일한 규칙이 적용됩니다.</p>
---	---	-------------------------------

**포트**

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 TCP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

**포트 검사 시간 창**

이 링크를 클릭하면 TCP 포트 검사로 간주할 특정 포트 검사 횟수에 대한 시간 범위를 입력할 수 있는 대화 상자가 나타납니다.

**보고서 파일**

이 링크를 클릭하면 공격자의 IP 주소를 기록할지 여부를 선택할 수 있습니다.

**규칙**

이 링크를 클릭하면 TCP 포트 검사 공격을 차단하는 규칙을 추가할지 여부를 선택할 수 있습니다.

**UDP 포트 검사**

이 규칙을 사용하면 FireWall 에서 UDP 포트 검사로 간주하는 경우와 그 경우에 취해야 할 조치를 정의할 수 있습니다. 이 규칙은 컴퓨터에 열려 있는 UDP 포트를 감지하는 UDP 포트 검사 공격을 방지합니다. 이러한 종류의 공격은 컴퓨터에서 취약점을 검색하는 데 사용되며 보다 위험한 공격 유형으로 이어지는 경우가 많습니다.

**UDP 포트 검사에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가하지 않습니다.</p>	<p><b>50</b> 개 이상의 포트가 <b>5,000</b> 밀리초 안에 검사된 경우 UDP 포트 검사로 간주합니다. 발견되면 공격자의 IP 를 기록하고 공격을 차단하는 규칙을 추가합니다.</p>	<p>중간 수준에도 동일한 규칙이 적용됩니다.</p>

**포트**

이 링크를 클릭하면 몇 개의 포트가 검사될 경우 UDP 포트 검사로 간주할지를 입력할 수 있는 대화 상자가 나타납니다.

**포트 검사 시간 창**

이 링크를 클릭하면 UDP 포트 검사로 간주할 특정 포트 검사 횟수에 대한 시간 범위를 입력할 수 있는 대화 상자가 나타납니다.

**보고서 파일**

이 링크를 클릭하면 공격자의 IP 주소를 기록할지 여부를 선택할 수 있습니다.

**규칙**

이 링크를 클릭하면 UDP 포트 검사 공격을 차단하는 규칙을 추가할지 여부를 선택할 수 있습니다.

**12.5.2.1. 들어오는 규칙**

들어오는 규칙은 들어오는 데이터 트래픽을 Avira FireWall 에서 제어하기 위해 정의합니다.

**참고**

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

**TCP 데이터 트래픽 데이터 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
<p>들어오는 데이터 트래픽을 Avira FireWall 에서 차단하지 않습니다.</p>	<ul style="list-style-type: none"> <li>- 135 에 대해 설정된 TCP 연결 허용</li> <li>로컬 포트가 <b>{135}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 TCP 패킷을 허용합니다. 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> </ul>	<ul style="list-style-type: none"> <li>- 설정된 TCP 데이터 트래픽 모니터</li> <li>로컬 포트가 <b>{0-65535}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 TCP 패킷을 허용합니다. 기존 연결 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> </ul>

- 135 에 대한 TCP 패킷 거부

로컬 포트가 **{135}**이고 원격 포트가 **{0-65535}**인 경우 **0.0.0.0**

마스크를 사용하는 **0.0.0.0** 주소의 **TCP** 패킷을 거부합니다.

모든 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다.

고급: 오프셋 **0** 에서 <빈>

마스크를 사용하는 <빈> 바이트가 따라오는 패킷을 무시합니다.

- TCP 정상 데이터 트래픽 모니터

로컬 포트가 **{0-65535}**이고 원격 포트가 **{0-65535}**인 경우 **0.0.0.0**

마스크를 사용하는 **0.0.0.0** 주소의 TCP 패킷을 허용합니다.

연결 시작 및 기존 연결 패킷에 적용됩니다.

패킷이 규칙과 일치하는 경우

	<p>기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p> <p>- 모든 TCP 패킷 거부</p> <p>로컬 포트가 <b>{0-65535}</b>이고 원격 포트가 <b>{0-65535}</b>인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 <b>TCP</b> 패킷을 거부합니다. 모든 패킷에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p>	
--	---	--

**TCP 패킷 허용/거부**

이 링크를 클릭하면 특별하게 정의된 들어오는 TCP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**로컬 포트**

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.



**원격 포트**

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

**적용 방법**

이 링크를 클릭하면 모든 패킷이 아닌 기존 연결 패킷에 대해서만 규칙을 적용하거나 연결 시작 및 기존 연결 패킷에 대해 규칙을 적용할 수 있습니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**고급 기능**을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

**필터링된 콘텐츠: 데이터**

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 TCP 헤더가 끝나는 위치부터 계산됩니다.

**UDP 트래픽 데이터 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	<ul style="list-style-type: none"> <li>UDP 허용 데이터 트래픽 모니터</li> <li>로컬 포트가 {<b>0-65535</b>}이고 원격 포트가 {<b>0-65535</b>}인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 UDP 패킷을 허용합니다. <b>열린 포트</b>에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를</li> </ul>	<ul style="list-style-type: none"> <li>설정된 UDP 트래픽 모니터</li> <li>로컬 포트가 {<b>0-65535</b>} 범위이고 원격 포트가 {<b>53, 67, 68, 123</b>} 범위인 경우 <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 <b>UDP</b> 패킷을 허용합니다. <b>열린 포트</b>에 규칙을 적용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</li> </ul>

	<p>사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p> <ul style="list-style-type: none"> <li>- 모든 UDP 패킷 거부</li> </ul> <p>로컬 포트가 {0-65535}이고 원격 포트가 {0-65535}인 경우 0.0.0.0 마스크를 사용하는 0.0.0.0 주소의 UDP 패킷을 거부합니다. 모든 포트에 적용됩니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: 0 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p>	
--	--	--

**UDP 패킷 허용/거부**

이 링크를 클릭하면 특별하게 정의된 들어오는 UDP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**로컬 포트**

이 링크를 클릭하면 로컬 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

**원격 포트**

이 링크를 클릭하면 원격 포트 번호 또는 전체 포트 범위를 정의할 수 있는 대화 상자가 나타납니다.

**적용 방법**

이 링크를 클릭하면 규칙을 모든 포트에 적용할지 아니면 열려 있는 모든 포트에만 적용할지를 선택할 수 있습니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**고급 기능**을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

**필터링된 콘텐츠: 데이터**

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 UDP 헤더가 끝나는 위치부터 계산됩니다.

**ICMP 트래픽 데이터 모니터에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	<ul style="list-style-type: none"> <li>- IP 주소를 기반으로 ICMP 취소 안 함</li> </ul> <p><b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 ICMP 패킷을 허용합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다. 고급: <b>0</b> 오프셋에 &lt;빈&gt; 마스크를 사용하는 &lt;빈&gt; 바이트가 따라오는 패킷을 무시합니다.</p>	중간 수준에도 동일한 규칙이 적용됩니다.

**ICMP 패킷 허용/거부**

이 링크를 클릭하면 특별하게 정의된 들어오는 ICMP 패킷을 허용할지 거부할지 여부를 선택할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**고급 기능**을 사용하면 콘텐츠를 필터링할 수 있습니다. 예를 들어 특정 오프셋에 특정 데이터를 포함하는 패킷을 거부할 수 있습니다. 이 옵션을 사용하지 않으려면 파일을 선택하지 않거나 빈 파일을 선택하십시오.

**필터링된 콘텐츠: 데이터**

이 링크를 클릭하면 특정 버퍼를 포함하는 파일을 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 마스크**

이 링크를 클릭하면 특정 마스크를 선택할 수 있는 대화 상자가 나타납니다.

**필터링된 콘텐츠: 오프셋**

이 링크를 클릭하면 필터링된 콘텐츠 오프셋을 정의할 수 있는 대화 상자가 나타납니다. 오프셋은 ICMP 헤더가 끝나는 위치부터 계산됩니다.

**IP 패킷에 대해 미리 정의된 규칙**

설정: 낮음	설정: 보통	설정: 높음
-	-	모든 IP 패킷 거부  <b>0.0.0.0</b> 마스크를 사용하는 <b>0.0.0.0</b> 주소의 <b>IP 패킷</b> 을 거부합니다. 패킷이 규칙과 일치하는 경우 기록하지 않습니다.

**IP 패킷 허용/거부**

이 링크를 클릭하면 특별히 정의된 IP 패키지를 허용할지 거부할지 여부를 결정할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**사용할 수 있는 IP 프로토콜 기반 IP 패키지 모니터링 규칙**

**IP 패키지**

이 링크를 클릭하면 특별히 정의된 IP 패키지를 허용할지 거부할지 여부를 결정할 수 있습니다.

**IP 주소**

이 링크를 클릭하면 필요한 IP 주소를 입력할 수 있는 대화 상자가 열립니다.

**IP 마스크**

이 링크를 클릭하면 필요한 IP 마스크를 입력할 수 있는 대화 상자가 열립니다.

**프로토콜**

이 링크를 클릭하면 필요한 IP 프로토콜을 입력할 수 있는 대화 상자가 열립니다.

**보고서 파일**

이 링크를 클릭하면 보고서 파일에 쓸지 여부 또는 패키지가 규칙을 준수하는지 여부를 결정할 수 있습니다.

**12.5.2.2. 나가는 규칙**

나가는 규칙은 Avira FireWall 에서 나가는 데이터 트래픽을 제어하기 위해 정의합니다. IP, ICMP, UDP 및 TCP 프로토콜 중 하나에 대한 나가는 규칙을 정의할 수 있습니다.

**참고**

패킷이 필터링될 경우 해당 규칙이 차례차례 적용되므로 규칙 순서가 매우 중요합니다. 수행하는 작업에 대해 잘 알고 있는 경우에만 규칙 순서를 변경하십시오.

**단추**

단추	설명
추가	새 규칙을 만들 수 있습니다. 이 단추를 누르면 "새 규칙 추가 대화 상자가 열립니다". 이 대화 상자에서 새 규칙을 선택할 수 있습니다.
제거	선택한 규칙을 제거합니다.
규칙 아래로	선택한 규칙을 한 줄 아래로 이동하여 규칙 우선 순위를 낮춥니다.
규칙 위로	선택한 규칙을 한 줄 위로 이동하여 규칙 우선 순위를 높입니다.
이름 바꾸기	선택한 규칙에 다른 이름을 지정할 수 있습니다.

**참고**

컴퓨터에 있는 모든 어댑터 또는 개별 어댑터에 대해 새 규칙을 추가할 수 있습니다. 모든 어댑터에 대해 어댑터 규칙을 추가하려면 표시되는 어댑터 계층 구조에서 컴퓨터를 선택하고 추가 단추를 클릭합니다.

**참고**

규칙을 원하는 위치로 끌어놓음으로써 규칙의 위치를 변경할 수도 있습니다.

### 12.5.3 응용 프로그램 목록

응용 프로그램 목록을 사용하여 응용 프로그램에서 네트워크에 액세스하는 방법을 지정하는 규칙을 만들 수 있습니다. 목록에 응용 프로그램을 추가하고 상황에 맞는 메뉴를 사용하여 선택한 응용 프로그램에 대해 **허용** 및 **차단** 규칙을 설정할 수 있습니다.

- **허용** 규칙이 설정된 응용 프로그램에서는 네트워크에 액세스할 수 있습니다.
- **차단** 규칙이 설정된 응용 프로그램에서는 네트워크에 액세스할 수 없습니다.

응용 프로그램을 추가하면 **허용** 규칙이 설정됩니다.

#### 응용 프로그램 목록

이 표에는 규칙이 정의된 응용 프로그램의 목록이 표시됩니다. 기호는 응용 프로그램의 네트워크 액세스가 허용되는지 또는 거부되었는지를 나타냅니다. 응용 프로그램에 대한 규칙은 상황에 맞는 메뉴를 사용하여 변경할 수 있습니다.

#### 단추

단추	설명
경로를 사용하여 추가	이 단추는 응용 프로그램을 선택할 수 있는 대화 상자를 표시합니다. 응용 프로그램은 " <b>네트워크 액세스 허용</b> " 규칙이 설정된 상태로 응용 프로그램 목록에 추가됩니다. " <b>경로를 사용하여 추가</b> " 옵션을 선택하면 추가된 FireWall 응용 프로그램이 경로 및 파일 이름으로 식별됩니다. 업데이트 등으로 인해 추가한 실행 파일의 내용이 달라지더라도 응용 프로그램의 규칙은 효력이 유지되며 FireWall 에서 그 규칙을 사용합니다.
MD5 를 사용하여 추가	이 단추는 응용 프로그램을 선택할 수 있는 대화 상자를 표시합니다. 응용 프로그램은 " <b>네트워크 액세스 허용</b> " 규칙이 설정된 상태로 응용 프로그램 목록에 추가됩니다. " <b>MD5 를 사용하여 추가</b> " 옵션을 선택하면 추가된 모든 응용 프로그램이 MD5 체크섬을 사용하여 고유하게 식별됩니다. 이로써 FireWall 은 파일 내용의 변경 내용을 식별할 수 있게 됩니다. 업데이트 후에 응용 프로그램이 변경된 경우, 예를 들어 응용 프로그램에 해당 규칙이 설정된 경우 이 응용 프로그램은 응용 프로그램 목록에서 자동으로 제거됩니다. 따라서 변경 내용을 적용한 후에는 응용 프로그램을 목록에 다시 추가하고 원하는 규칙을 다시 적용해야 합니다.
그룹 추가	이 단추는 디렉토리를 선택할 수 있는 대화 상자를 표시합니다. 선택한 경로에 있는 모든 응용 프로그램은 " <b>네트워크 액세스 허용</b> " 규칙이 설정된 상태로 응용 프로그램 목록에 추가됩니다.
제거	선택한 응용 프로그램 규칙이 제거됩니다.

모두 제거    모든 응용 프로그램 규칙이 제거됩니다.

### 12.5.4 신뢰할 수 있는 공급자

신뢰할 수 있는 소프트웨어 공급자 목록은 **신뢰할 수 있는 공급자** 아래에 표시됩니다. 나열된 소프트웨어 제조업체의 응용 프로그램에는 네트워크에 대한 액세스 권한이 부여됩니다. 목록에서 제조업체를 추가하거나 제거할 수 있습니다.

#### 공급업체

이 목록에는 신뢰할 수 있는 공급자로 분류된 공급자가 모두 표시됩니다.

#### 단추

단추	설명
추가	이 단추는 응용 프로그램을 선택할 수 있는 대화 상자를 표시합니다. 응용 프로그램의 제조업체가 설정되고 신뢰할 수 있는 공급자 목록에 추가됩니다.
그룹 추가	이 단추는 디렉토리를 선택할 수 있는 대화 상자를 표시합니다. 선택한 경로에 있는 모든 응용 프로그램의 제조업체가 설정되고 신뢰할 수 있는 공급자 목록에 추가됩니다.
제거	강조 표시된 항목을 신뢰할 수 있는 공급자 목록에서 제거합니다. 목록에서 선택한 공급자를 영구적으로 제거하려면 구성 창에서 " <b>적용</b> " 또는 " <b>확인</b> "을 클릭합니다.
모두 제거	신뢰할 수 있는 공급자 목록에서 모든 항목이 제거됩니다.
다시 로드	변경을 취소합니다. 마지막으로 저장되었던 목록이 로드됩니다.

**참고**  
 목록에서 공급자를 제거한 후 **적용**을 선택하면 공급자가 목록에서 영구적으로 제거됩니다. **다시 로드**를 사용해도 변경 사항을 취소할 수 없습니다.

**참고**  
 FireWall에서는 신뢰할 수 있는 공급자 목록에 항목을 추가하기 전에 응용 프로그램 규칙에 우선 순위를 부여합니다. 응용 프로그램 규칙을 만들었으며 응용 프로그램 공급자가 신뢰할 수 있는 공급자 목록에 나열된 경우 응용 프로그램 규칙이 실행됩니다.

### 12.5.5 추가 설정

#### 알림

알림은 FireWall 의 데스크톱 알림을 받고자 하는 이벤트를 정의합니다.

#### 포트 검사

이 옵션을 활성화하면 FireWall 에서 포트 검사가 감지될 경우 사용자에게 데스크톱 알림이 전달됩니다.

#### 플로딩

이 옵션을 활성화하면 FireWall 에서 플로딩 공격이 감지될 경우 사용자에게 데스크톱 알림이 전달됩니다.

#### 차단된 응용 프로그램

이 옵션을 활성화하면 FireWall 에서 응용 프로그램의 네트워크 작업을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

#### 차단된 IP

이 옵션을 활성화하면 FireWall 에서 한 IP 주소의 데이터 트래픽을 거부(차단)한 경우 사용자에게 데스크톱 알림이 전달됩니다.

### **팝업 설정**

#### 프로세스 시작 스택 검사

이 옵션을 사용하면 프로세스 스택 검사에서 보다 정확하게 제어할 수 있습니다. FireWall 에서는 스택의 프로세스 중 신뢰할 수 없는 프로세스가 실제로 하위 프로세스를 통해 네트워크에 액세스하는 프로세스가 될 수 있다고 가정합니다. 따라서 프로세스 스택의 프로세스 중 신뢰할 수 없는 프로세스마다 다른 팝업 창이 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

#### 프로세스당 여러 팝업 허용

이 옵션을 사용하면 응용 프로그램이 네트워크에 연결하려고 할 때마다 팝업이 나타납니다. 또는 첫 번째 연결 시도에 대한 정보만 표시됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

#### 게임 모드인 경우 팝업 알림 자동으로 표시 안 함

이 옵션을 사용하도록 설정하면 컴퓨터 시스템에서 응용 프로그램을 전체 화면 모드로 실행할 경우 Avira FireWall 게임 모드가 자동으로 활성화됩니다. 게임 모드에서는 정의된 모든 어댑터 및 응용 프로그램 규칙이 적용됩니다. "허용" 또는 "거부" 작업을 통해 정의된 규칙이 없는 응용 프로그램에 대한 네트워크 액세스가 일시적으로 허용되며 이에 따라 네트워크 이벤트에 대해 묻는 팝업 창이 나타나지 않습니다.

## 12.5.6 표시 설정

### **이 응용 프로그램에 대한 작업 기억**

#### 항상 사용

이 옵션을 사용하도록 설정하면 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### 항상 사용 안 함



이 옵션을 사용할 경우 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 기본 설정으로 사용되지 않습니다.

**서명된 응용 프로그램 허용**

이 옵션을 사용하면 서명된 응용 프로그램에서 네트워크에 액세스할 때 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 자동으로 사용됩니다. 제조업체에는 Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia 가 있습니다.

**마지막으로 사용된 상태 기억**

이 옵션을 사용할 경우 "네트워크 이벤트" 대화 상자의 "이 응용 프로그램에 대한 작업 기억" 옵션이 마지막 네트워크 이벤트와 동일한 방식으로 사용됩니다. "이 응용 프로그램에 대한 작업 기억" 옵션을 사용하도록 설정하면 다음과 같은 네트워크 이벤트에도 이 옵션이 사용됩니다. 마지막 네트워크 이벤트에 대해 "이 응용 프로그램에 대한 작업 기억" 옵션이 사용 안 함으로 설정되어 있었다면 다음 네트워크 이벤트에 이 옵션이 사용되지 않습니다.

**세부 정보 표시**

이 구성 옵션 그룹에서는 **네트워크 이벤트** 창의 세부 정보 표시를 설정할 수 있습니다.

**요구 시 세부 정보 표시**

이 옵션을 사용하면 요청 시에만 세부 정보가 "네트워크 이벤트" 창에 표시됩니다. 예를 들어 "네트워크 이벤트" 창에서 "세부 정보 표시" 단추를 클릭하면 세부 정보가 표시됩니다.

**항상 세부 정보 표시**

이 옵션을 사용하면 세부 정보가 "네트워크 이벤트" 창에 항상 표시됩니다.

**마지막으로 사용된 상태 기억**

이 옵션을 사용하면 세부 정보 표시가 이전 네트워크 이벤트에서와 같은 방식으로 관리됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 표시되었거나 액세스된 경우 다음 네트워크 이벤트에 대해 세부 정보가 표시됩니다. 세부 정보가 마지막 네트워크 이벤트 중에 숨겨졌거나 표시되지 않은 경우에는 다음 네트워크 이벤트에 대해 세부 정보가 표시되지 않습니다.

**권한 허용**

이 구성 옵션 그룹에서는 **네트워크 이벤트** 창의 **권한 허용** 옵션에 대한 상태를 정의할 수 있습니다.

**항상 사용**

이 옵션을 사용하면 "권한 허용" 옵션이 "네트워크 이벤트" 창에서 기본적으로 사용됩니다.

**항상 사용 안 함**

이 옵션을 사용하면 "권한 허용" 옵션이 "네트워크 이벤트" 창에서 기본적으로 사용되지 않습니다.

**마지막으로 사용된 상태 기억**

이 옵션을 사용하면 "권한 허용" 옵션의 상태가 "네트워크 이벤트" 창에서 이전 네트워크 이벤트의 경우와 동일한 방식으로 처리됩니다. 마지막 네트워크 이벤트 실행에 대해 권한 허용 옵션을 사용하면 다음 네트워크 이벤트에 대해 이 옵션이 기본적으로 사용됩니다. 마지막 네트워크 이벤트 실행에 대해 권한 허용 옵션을 사용하지 않았다면 다음 네트워크 이벤트에 대해 이 옵션이 기본 설정으로 사용되지 않습니다.

## 12.6 WebGuard

구성의 WebGuard 섹션에서는 WebGuard 를 구성합니다.

### 12.6.1 검사

WebGuard 는 인터넷에서 웹 브라우저에 로드되는 웹 페이지로부터 바이러스나 맬웨어가 사용자의 컴퓨터로 옮겨지지 않도록 차단합니다. 검사 항목을 사용하여 WebGuard 구성 요소의 동작을 설정할 수 있습니다.

#### 검사

##### **WebGuard 사용(W)**

이 옵션을 사용하면 인터넷 브라우저를 통해 요청하는 웹 페이지에 대해 바이러스 및 맬웨어를 검사합니다. WebGuard 에서는 포트 80, 8080, 3128 에서 HTTP 프로토콜을 사용하여 인터넷에서 전송되는 데이터를 모니터링합니다. 감염된 웹 페이지가 발견될 경우 해당 웹 페이지의 로드가 차단됩니다. 이 옵션을 사용하지 않는 경우 WebGuard 서비스는 시작된 상태로 유지되지만 바이러스 및 맬웨어 포함 여부를 검사하지 않습니다.

#### Drive-by 보호

Drive-by 보호 기능을 사용하면 인라인 프레임이라고 하는 I-Frame 을 차단하도록 설정할 수 있습니다. I-Frame 은 HTML 요소로 웹 페이지 영역을 구분하는 인터넷 페이지 요소입니다. I-Frame 을 사용하면 서로 다른 웹 콘텐츠(일반적으로 서로 다른 URL)를 브라우저의 하위 창에서 개별 문서로 로드하여 표시할 수 있습니다. I-Frame 은 대부분 배너 광고용으로 사용됩니다. 경우에 따라 I-Frame 은 맬웨어를 감추는 데 사용되기도 합니다. 이 경우 I-Frame 의 영역은 브라우저에서 대부분 보이지 않거나 거의 보이지 않습니다. *의심스러운 I-Frame 차단* 옵션을 사용하면 I-Frame 의 로드를 확인하여 차단할 수 있습니다.

##### **의심스러운 I-frames 차단**

이 옵션을 사용하면 사용자가 요청하는 웹 페이지의 I-Frame 을 특정 기준에 따라 검사합니다. 요청한 웹 페이지에 의심스러운 I-Frame 이 있는 경우 해당 I-Frame 이 차단됩니다. I-Frame 창에는 오류 메시지가 표시됩니다.

##### **기본값**

이 옵션을 사용하는 경우 의심스러운 콘텐츠가 포함된 I-Frame 이 차단됩니다.

##### **고급**

이 옵션을 사용하면 의심스러운 콘텐츠가 포함된 I-Frame 과 의심스러운 방식으로 사용되는 I-Frame 이 차단됩니다. I-Frame 이 매우 작아서 보이지 않거나 I-Frame 이 웹 페이지의 비정상적인 위치에 있어서 브라우저에서 거의 보이지 않는 경우 해당 I-Frame 의 사용을 의심스러운 것으로 간주합니다.

### 12.6.1.1. 검색에 대한 작업

#### 검색에 대한 작업

바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견했을 때 WebGuard 에서 수행할 작업을 정의할 수 있습니다.

#### 대화형

이 옵션을 사용하면 온 디맨드 검사 시 바이러스나 사용자 동의 없이 설치된 프로그램이 검색될 때 사용자가 해당 파일에 대해 수행할 작업을 선택할 수 있는 대화 상자가 나타납니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

#### 허용되는 작업

이 상자에서 작업을 지정하면 바이러스가 검색되었을 때 해당 작업이 표시되도록 선택할 수 있습니다. 작업을 지정하려면 해당 옵션을 활성화해야 합니다.

#### 액세스 거부

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일이 사용자의 웹 브라우저로 전송되지 않습니다. 액세스가 거부되었음을 알리는 오류 메시지가 웹 브라우저에 표시됩니다. 보고서 기능이 활성화된 경우 WebGuard에서 보고서 파일에 검색 정보를 기록합니다.

#### 격리

바이러스 또는 맬웨어가 검색되는 경우 웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일이 격리 저장소로 이동됩니다. 영향받는 파일에 정보 값이 있으면 격리 관리자에서 파일을 복원하거나 Avira 맬웨어 연구 센터로 보낼 수 있습니다(필요한 경우).

#### 무시

웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일을 WebGuard 에서 사용자의 웹 브라우저로 전달합니다.

#### 기본값

이 단추를 사용하면 바이러스가 발견될 때 대화 상자에서 기본적으로 활성화되는 작업을 선택할 수 있습니다. 기본적으로 활성화할 작업을 선택하고 "기본값" 단추를 클릭합니다.

자세한 내용을 보려면 여기를 클릭하십시오.

#### 진행률 표시줄 표시

이 옵션을 사용하면 웹 사이트 콘텐츠를 다운로드할 때 20 초의 시간 제한이 초과되면 다운로드 진행률 표시줄에 데스크톱 알림이 표시됩니다. 이 데스크톱 알림은 특별히 대량의 데이터가 포함된 웹 사이트를 다운로드할 경우를 위한 것입니다. WebGuard 를 사용하여 서핑할 경우 웹 콘텐츠가 인터넷 브라우저에 표시되기 전에 해당 콘텐츠에 바이러스 및 맬웨어가 있는지 검사하므로 웹 콘텐츠가 인터넷 브라우저에서 점진적으로 다운로드되지 않습니다. 이 옵션은 기본적으로 사용되지 않습니다.

#### **자동**

이 옵션을 사용하면 바이러스가 검색되어도 대화 상자가 표시되지 않습니다. WebGuard 는 이 섹션에서 미리 정의한 기본 및 보조 작업 설정에 따라 대응합니다.

#### **검색 알림 표시**

이 옵션을 활성화하면 바이러스 또는 사용자 동의 없이 설치된 프로그램이 검색될 때마다 실행할 작업을 표시하는 알림이 나타납니다.

#### **기본 작업**

기본 작업은 WebGuard 가 바이러스 또는 사용자 동의 없이 설치된 프로그램을 발견한 경우에 수행하는 작업입니다.

#### **액세스 거부**

웹 서버에서 요청한 웹 사이트 및/또는 전송된 모든 데이터나 파일이 사용자의 웹 브라우저로 전송되지 않습니다. 액세스가 거부되었음을 알리는 오류 메시지가 웹 브라우저에 표시됩니다. 보고서 기능이 활성화된 경우 WebGuard에서 보고서 파일에 검색 정보를 기록합니다.

#### **격리**

바이러스 또는 맬웨어가 검색되는 경우 웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일이 격리 저장소로 이동됩니다. 영향받는 파일에 정보 값이 있으면 격리 관리자에서 파일을 복원하거나 Avira 맬웨어 연구 센터로 보낼 수 있습니다(필요한 경우).

#### **무시**

웹 서버에서 요청한 웹 사이트 및/또는 전송된 데이터와 파일을 WebGuard 에서 사용자의 웹 브라우저로 전달합니다. 파일에 대한 액세스가 허용되고 파일을 무시합니다.

#### **경고**

영향받는 파일은 워크스테이션에서 활성 상태로 유지됩니다. 이로 인해 워크스테이션에 심각한 손상이 발생할 수 있습니다.

### 12.6.1.2. 잠긴 요청

잠긴 요청에서는 WebGuard 에서 차단할 파일 형식 및 MIME 형식(전송되는 데이터의 콘텐츠 형식)을 지정할 수 있습니다. 웹 필터를 사용하면 알려진 피싱 및 맬웨어 URL 을 차단할 수 있습니다. WebGuard 는 인터넷에서 사용자의 컴퓨터 시스템으로 데이터가 전송되는 것을 방지합니다.

#### **WebGuard 에서 차단할 파일 형식/MIME 형식(사용자 정의)**

이 목록에 있는 모든 파일 형식 및 MIME 형식(전송되는 데이터의 콘텐츠 형식)이 WebGuard 에 의해 차단됩니다.

#### **입력란**

이 입력란에는 WebGuard 에서 차단할 MIME 형식 및 파일 형식의 이름을 입력합니다. 파일 형식의 경우 **.htm** 과 같은 파일 확장명을 입력합니다. MIME 형식의 경우 미디어 형식과 해당되는 경우 하위 형식을 지정합니다. 두 문을 슬래시로 구분합니다(예: **video/mpeg** 또는 **audio/x-wav**).

**참고**

WebGuard 에 의해 차단되었지만 임시 인터넷 파일로 컴퓨터 시스템에 이미 저장되어 있는 파일은 컴퓨터의 인터넷 브라우저를 통해 인터넷에서 로컬로 다운로드할 수 있습니다. 임시 인터넷 파일은 인터넷 브라우저에서 웹 사이트에 더 빨리 액세스할 수 있도록 하기 위해 컴퓨터에 저장되는 파일입니다.

**참고**

차단된 파일 및 MIME 형식 목록은 WebGuard::검사::예외에서 제외된 파일 및 MIME 형식 목록에 입력한 경우 무시됩니다.

**참고**

파일 형식과 MIME 형식을 입력할 때 와일드카드(임의 개수의 문자를 나타내는 \* 또는 한 문자를 나타내는 ?)를 사용할 수 없습니다.

MIME 형식: 미디어 형식의 예:

- text = 텍스트 파일
- image = 그래픽 파일
- video = 비디오 파일
- audio = 사운드 파일
- application = 특정 프로그램에 연결된 파일

예: 제외된 파일 및 MIME 형식

- application/octet-stream = application/octet-stream MIME 형식 파일(실행 파일 \*.bin, \*.exe, \*.com, \*.dll, \*.class)이 WebGuard 에 의해 차단됩니다.
- application/olescript = application/olescript MIME 형식 파일(ActiveX 스크립트 파일 \*.axs)이 WebGuard 에 의해 차단됩니다.
- .exe = .exe(실행 파일) 확장명이 붙은 모든 파일이 WebGuard 에 의해 차단됩니다.
- .msi = .msi(Windows Installer 파일) 확장명이 붙은 모든 파일이 WebGuard 에 의해 차단됩니다.

**추가**

이 단추를 사용하면 입력 필드에서 표시 창으로 MIME 및 파일 형식을 복사할 수 있습니다.

**삭제**

이 단추는 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 단추가 비활성화됩니다.

**웹 필터**

웹 필터는 내부 데이터베이스를 기반으로 하며 매일 업데이트되고 콘텐츠에 따라 URL 을 분류합니다.

**웹 필터 활성화**

이 옵션을 사용하면 웹 필터 목록에서 선택한 범주와 일치하는 모든 URL 이 차단됩니다.

**웹 필터 목록**

웹 필터 목록에서는 WebGuard 에서 차단할 URL 이 포함된 콘텐츠 범주를 선택할 수 있습니다.

**참고**

WebGuard::검사::예외에서 제외된 URL 목록에 포함된 항목의 경우에는 웹 필터가 무시됩니다.

**참고**

스팸 URL 은 스팸 전자 메일로 함께 전송되는 URL 입니다. 부정/사기 범주에는 “가입 만료(Subscription Expires)”가 표시된 웹 페이지 또는 공급자의 비용 안내가 없는 서비스 제공이 포함됩니다.

**12.6.1.3. 예외**

이 옵션을 사용하면 URL(인터넷 주소)의 파일 형식과 MIME 형식(전송되는 데이터의 콘텐츠 형식)에 따라 WebGuard 검사에서 제외되는 예외 항목을 설정할 수 있습니다. 지정된 MIME 형식과 URL 은 WebGuard 에서 무시됩니다. 따라서 데이터가 컴퓨터 시스템으로 전송될 때 해당 데이터에 대해 바이러스 및 맬웨어 포함 여부를 검사하지 않습니다.

**WebGuard 에서 건너뛰는 MIME 형식**

이 필드에서는 검사 중에 WebGuard 에서 무시할 MIME 형식(전송되는 데이터의 콘텐츠 형식)을 선택할 수 있습니다.

**WebGuard 에서 건너뛰는 파일 형식/MIME 형식(사용자 정의)**

이 목록의 모든 MIME 형식(전송되는 데이터의 콘텐츠 형식)은 검사 중에 WebGuard 에서 무시됩니다.

**입력란**

이 입력란에는 검사 중에 WebGuard 에서 무시할 MIME 형식 및 파일 형식의 이름을 입력할 수 있습니다. 파일 형식의 경우 **.htm** 과 같은 파일 확장명을 입력합니다. MIME 형식의 경우 미디어 형식과 해당되는 경우 하위 형식을 지정합니다. 두 문을 슬래시로 구분합니다(예: **video/mpeg** 또는 **audio/x-wav**).

**참고**

파일 형식과 MIME 형식을 입력할 때 와일드카드(임의 개수의 문자를 나타내는 \* 또는 한 문자를 나타내는 ?)를 사용할 수 없습니다.

### 경고

제외 목록의 모든 파일 형식과 콘텐츠 형식은 차단된 액세스(WebGuard::검사::차단된 액세스의 차단될 파일 형식 및 MIME 형식 목록)에 대한 추가 검사 또는 WebGuard를 통한 추가 검사 없이 인터넷 브라우저로 다운로드됩니다. 제외 목록의 모든 항목의 경우 차단될 파일 및 MIME 형식 목록에 있는 항목이 무시됩니다. 바이러스 및 맬웨어 포함 여부를 검사하지 않습니다.

### MIME 형식: 미디어 형식의 예:

- text = 텍스트 파일
- image = 그래픽 파일
- video = 비디오 파일
- audio = 사운드 파일
- application = 특정 프로그램에 연결된 파일

### 예: 제외된 파일 및 MIME 형식

- audio/ = 모든 오디오 미디어 형식 파일이 WebGuard 검사에서 제외됩니다.
- video/quicktime = 모든 Quicktime 하위 형식 비디오 파일(\*.qt, \*.mov)이 WebGuard 검사에서 제외됩니다.
- .pdf = 모든 Adobe PDF 파일이 WebGuard 검사에서 제외됩니다.

### 추가

이 단추를 사용하면 입력 필드에서 표시 창으로 MIME 및 파일 형식을 복사할 수 있습니다.

### 삭제

이 단추는 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 단추가 비활성화됩니다.

### WebGuard 에서 건너편 URL

이 목록의 모든 URL 은 WebGuard 검사에서 제외됩니다.

### 입력란

이 입력란에는 **www.domainname.com** 과 같이 WebGuard 검사에서 제외할 URL(인터넷 주소)을 입력할 수 있습니다. URL 의 일부분에 선행 또는 후행 점을 넣어 도메인 수준을 나타낼 수 있습니다. 예를 들어 .domainname.com 은 이 도메인의 모든 페이지와 모든 하위 도메인을 나타냅니다. 후행 점을 사용하면 최상위 도메인(.com 또는 .net)의 웹사이트를 지정할 수 있습니다(domainname.). 선행 또는 후행 점 없이 문자열을 지정할 경우 문자열이 최상위 도메인으로 해석됩니다. 예를 들어 **net** 은 모든 NET 도메인(www.domain.net)을 나타냅니다.

**참고**

또한 URL 을 지정할 때 임의 개수의 문자를 나타내는 와일드카드 \*도 사용할 수 있습니다. 와일드카드와 함께 선행 또는 후행 점을 사용하여 도메인 수준을 나타낼 수도 있습니다.

.domainname.\*

\*.domainname.com

.\*name\*.com(사용할 수는 있지만 권장되지 않음)

\*name\*과 같이 점 없이 지정하면 최상위 도메인의 일부로 해석되므로 바람직하지 않습니다.

**경고**

제외된 URL 목록에 있는 모든 웹 사이트는 웹 필터 또는 WebGuard에서 추가로 검사하지 않고 인터넷 브라우저로 다운로드됩니다. 제외된 URL 목록에 있는 모든 항목에 대해 웹 필터의 항목(WebGuard::검사::차단된 액세스)이 무시됩니다. 바이러스 및 맬웨어 포함 여부를 검사하지 않습니다. 그러므로 신뢰할 수 있는 URL만 WebGuard 검사에서 제외해야 합니다.

**추가**

이 단추를 사용하면 입력 필드에 입력한 URL(인터넷 주소)을 뷰어 창으로 복사할 수 있습니다.

**삭제**

이 단추는 목록에서 선택한 항목을 삭제합니다. 항목을 선택하지 않으면 이 단추가 비활성화됩니다.

**예: 건너뛴 URL**

- www.avira.com -또는- www.avira.com/\*

= 도메인이 'www.avira.com'인 모든 URL 이 WebGuard 검사에서 제외됩니다.

www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html,

www.avira.com/en/download/index.html 등이 있습니다.

도메인이 'www.avira.de'인 모든 URL 이 WebGuard 검사에서 제외되지 않습니다.

- avira.com -또는- \*.avira.com

= 2 수준 및 최상위 도메인이 'avira.com'인 모든 URL 이 WebGuard 검사에서

제외됩니다. 여기에는 '.avira.com'에 대한 기존의 모든 하위 도메인이 포함됩니다.

www.avira.com, forum.avira.com 등이 있습니다.

- avira. -또는- \*.avira.\*

= 2 수준 도메인이 'avira'인 모든 URL 이 WebGuard 검사에서 제외됩니다.

'avira'에 대한 기존의 모든 최상위 도메인 또는 하위 도메인이 포함됩니다.

www.avira.com, www.avira.de, forum.avira.com 등이 있습니다.

- \*.domain\*.\*

2 수준 도메인에 'domain' 문자열이 포함된 모든 URL 이 WebGuard 검사에서

제외됩니다. www.domain.com, www.new-domain.de, www.sample-domain1.de

등이 있습니다.

- net -또는- \*.net

= 최상위 도메인이 'net'인 모든 URL 이 WebGuard 검사에서 제외됩니다.

www.name1.net, www.name2.net 등이 있습니다.



**경고**

WebGuard 에서 제외할 URL 을 가능한 한 정확하게 입력합니다. 맬웨어 및 사용자 동의 없이 설치된 프로그램을 배포하는 인터넷 페이지가 제외의 전역 지정을 통해 WebGuard 검사에서 제외될 위험이 있으므로 전체 최상위 도메인 또는 2 수준 도메인의 일부는 가급적 지정하지 않는 것이 좋습니다. 최소한 전체 2 수준 도메인과 최상위 도메인을 지정하는 것이 좋습니다(예: domainname.com)

**12.6.1.4. 추론**

이 구성 섹션에는 검사 엔진의 추론 설정이 들어 있습니다.

AntiVir 제품에는 알려지지 않은 맬웨어를 사전에, 즉 손상 요소에 대응할 특수한 바이러스 서명을 생성하고 바이러스 방지 업데이트가 전달되기 전에 확인할 수 있는 매우 강력한 추론 기능이 포함되어 있습니다. 바이러스를 검색하려면 감염된 코드를 광범위하게 분석하고 조사하여 맬웨어의 특징적인 기능을 찾아야 합니다. 검사 대상 코드가 이러한 특징을 나타내는 경우 해당 코드가 의심스러운 코드로 보고됩니다. 의심스러운 코드가 반드시 실제 맬웨어의 코드를 의미하지는 않습니다. 때로는 가양성(오진) 문제가 발생할 수도 있습니다. 감염된 코드를 처리하는 방법은 코드의 출처를 신뢰할 수 있는지 여부에 따라 사용자가 결정해야 합니다.

**매크로 바이러스 추론**

**매크로 바이러스 추론**

AntiVir 제품에는 매우 강력한 매크로 바이러스 추론이 포함되어 있습니다. 이 옵션을 사용하면 관련 문서의 모든 매크로가 복구 시 삭제되거나 의심스러운 문서만 보고됩니다. 즉 사용자에게 경고가 표시됩니다. 이 옵션은 기본적으로 사용되며 가급적이면 사용하는 것이 좋습니다.

**AHeAD(고급 추론 분석 및 검색)**

**AHeAD 사용**

AntiVir 프로그램은 일종의 AntiVir AHeAD 기술로 매우 강력한 추론 기능을 제공하므로 알려지지 않은 신종 맬웨어를 감지할 수 있습니다. 이 옵션을 사용하면 이 추론의 "공격성" 수준을 정의할 수 있습니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

**낮은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 줄어들기 때문에 가양성 문제가 발생할 위험이 낮습니다.

**보통 검색 수준**

이 추론을 사용하도록 선택한 경우 이 옵션은 기본 설정으로 사용됩니다.

**높은 검색 수준**

이 옵션을 사용하면 알려지지 않은 맬웨어가 감지되는 횟수가 현저히 늘어나지만 가양성일 확률도 높아집니다.

## 12.6.2 신고

WebGuard에는 사용자 또는 관리자에게 검색 유형 및 방식에 대한 정확한 정보를 제공하기 위한 광범위한 로깅 기능이 포함됩니다.

### 보고

이 그룹에서는 보고서 파일의 콘텐츠를 결정할 수 있습니다.

### 해제

이 옵션을 사용하면 WebGuard에서 로그를 만들지 않습니다.

평가판을 실행하여 여러 바이러스나 사용자 동의 없이 설치된 프로그램을 테스트하려는 경우처럼 예외적인 상황이 아니면 로깅 기능을 해제하지 않는 것이 좋습니다.

### 기본값

이 옵션을 사용하면 WebGuard에서 바이러스 발견, 알람 및 오류 관련 중요 정보를 보고서 파일에 기록하고 중요 항목의 보다 확실한 전달을 위해 중요도가 낮은 정보는 무시합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

### 고급

이 옵션을 사용하면 WebGuard에서 덜 중요한 정보도 보고서 파일에 기록합니다.

### 완료

이 옵션을 사용하면 WebGuard에서 파일 크기, 파일 형식, 날짜 등 사용할 수 있는 모든 정보를 보고서 파일에 기록합니다.

## 보고서 파일 제한

### nMB 로 크기 제한

이 옵션을 사용하면 보고서 파일을 특정 크기로 제한할 수 있습니다. 가능한 값은 1~100MB입니다. 보고서 파일의 크기를 제한하여 시스템 리소스 사용을 최소화하면 약 50KB의 추가 공간이 확보됩니다. 로그 파일의 크기가 지정된 크기를 50KB 이상 초과하는 경우에는 지정된 크기가 20% 줄어들 때까지 오래된 항목이 삭제됩니다.

### 줄이기 전에 보고서 파일 백업

이 옵션을 사용하면 보고서 파일의 크기를 줄이기 전에 보고서 파일이 백업됩니다. 저장 위치는 구성 :: 일반 :: 디렉터리 :: 보고서 디렉터리를 참조하십시오.

### 보고서 파일에 구성 쓰기

이 옵션을 사용하면 온 액세스 감사의 구성이 보고서 파일에 기록됩니다.

### 참고

보고서 파일에 대해 아무런 제한을 지정하지 않은 경우, 보고서 파일이 100MB가 되면 오래된 항목이 자동으로 삭제됩니다. 보고서 파일의 크기가 80MB가 될 때까지 항목이 계속 삭제됩니다.

## 12.7 업데이트

업데이트 섹션에서는 업데이트 자동 받기 및 다운로드 서버 연결을 구성할 수 있습니다. 여러 가지 업데이트 간격을 지정하고 자동 업데이트를 활성화하거나 비활성화할 수 있습니다.

### 참고

AntiVir Security Management Center 에서 AntiVir 프로그램을 구성하는 경우, 자동 업데이트를 사용할 수 없습니다.

### 자동 업데이트

#### 활성화

이 옵션을 사용하면 설정된 이벤트에 대해 지정된 간격으로 자동 업데이트가 수행됩니다.

#### n 일/시간/분마다 자동 업데이트

이 상자에서 자동 업데이트의 수행 간격을 지정할 수 있습니다. 업데이트 간격을 변경하려면 상자에서 시간 옵션 중 하나를 강조 표시하고 입력 상자의 오른쪽에 있는 화살표 키를 사용하여 해당 옵션을 변경합니다.

#### 인터넷에 연결(전화 접속)하는 동안 작업 시작

이 옵션을 사용하면 지정된 업데이트 간격 외에도 인터넷에 연결할 때마다 업데이트 작업이 수행됩니다.

#### 시간이 만료된 경우 작업 반복

이 옵션을 사용하면 컴퓨터 전원이 꺼지는 등의 이유로 인해 지정된 시간에 수행하지 못한 지난 업데이트 작업이 수행됩니다.

### 다운로드

#### 웹 서버를 통해

웹 서버를 통해 HTTP 연결로 업데이트가 수행됩니다. 인터넷의 전용 웹 서버를 사용하거나 인터넷의 전용 다운로드 서버에서 업데이트 파일을 가져오는 인트라넷의 웹 서버를 사용할 수 있습니다.

### 참고

웹 서버를 통해 업데이트하는 작업에 대한 추가 설정에 액세스하려면 구성 :: 일반 :: 업데이트 :: 웹 서버로 이동합니다.

#### 파일 서버/공유 폴더를 통해

인터넷의 전용 다운로드 서버에서 업데이트 파일을 가져오는 인트라넷 파일 서버를 통해 업데이트가 수행됩니다.

### 참고

파일 서버를 통해 업데이트하는 작업에 대한 추가 설정에 액세스하려면 구성 :: 일반 :: 업데이트 :: 파일 서버로 이동합니다.

## 12.7.1 제품 업데이트 시작

제품 업데이트에서는 제품의 업데이트 방법 또는 사용 가능한 제품 업데이트에 대한 알림 처리 방법을 구성합니다.

### 제품 업데이트

#### 자동으로 제품 업데이트 다운로드 및 설치

이 옵션을 사용하면 제품 업데이트가 제공되는 즉시 업데이트 구성 요소에서 제품 업데이트를 자동으로 다운로드하여 설치합니다. 바이러스 정의 파일 및 검사 엔진에 대한 업데이트는 이 설정과는 별도로 수행됩니다. 이 옵션을 사용하려면 업데이트 구성을 완료하고 다운로드 서버에 연결되어 있어야 합니다.

#### 제품 업데이트 다운로드. 다시 시작해야 하는 경우 시스템을 다시 시작한 후 업데이트를 설치하십시오. 그렇지 않으면 바로 설치됩니다.

이 옵션을 사용하면 제품 업데이트가 제공되는 즉시 다운로드됩니다. 다시 시작할 필요가 없는 경우에는 업데이트 파일이 다운로드된 후 업데이트가 자동으로 설치되지만, 제품 업데이트를 위해 컴퓨터를 다시 시작해야 하는 경우에는 업데이트 파일이 다운로드된 직후가 아니라 다음에 사용자가 시스템을 다시 부팅할 때 제품 업데이트가 실행됩니다. 따라서 사용자가 컴퓨터에서 작업 중인 동안에는 다시 시작되지 않으므로 안심하고 작업을 계속할 수 있습니다. 바이러스 정의 파일 및 검사 엔진에 대한 업데이트는 이 설정과는 별도로 수행됩니다. 이 옵션을 사용하려면 업데이트 구성을 완료하고 다운로드 서버에 연결되어 있어야 합니다.

#### 사용 가능한 새 제품 업데이트가 있을 때 알림

이 옵션을 사용하면 새 제품 업데이트를 사용할 수 있을 때 전자 메일을 통해 알림이 제공됩니다. 바이러스 정의 파일 및 검사 엔진에 대한 업데이트는 이 설정과는 별도로 수행됩니다. 이 옵션을 사용하려면 업데이트 구성을 완료하고 다운로드 서버에 연결되어 있어야 합니다. 제어 센터의 개요::이벤트에 표시되는 업데이트 프로그램의 알림 및 데스크톱 팝업 창을 통해 알림이 수신됩니다.

#### n일 후에 다시 알림

초기 알림 후에 제품 업데이트가 설치되지 않은 경우 특정 기간(일)이 경과된 후에 제품 업데이트를 사용할 수 있음을 다시 알리도록 해당 기간(일)을 이 상자에 입력합니다.

#### 제품 업데이트 다운로드 안 함

이 옵션을 사용하면 업데이트 프로그램을 통한 제품 업데이트 알림 또는 자동 제품 업데이트가 수행되지 않습니다. 바이러스 정의 파일 및 검색 엔진에 대한 업데이트는 이 설정과는 별도로 수행됩니다.

#### **중요**

바이러스 정의 파일 및 검색 엔진에 대한 업데이트가 제품 업데이트의 설정과 별도로 모든 업데이트 프로세스 중에 수행됩니다(업데이트 장 참조).

#### **참고**

자동 제품 업데이트 옵션을 사용하도록 설정한 경우 다시 시작 설정에서 다시 시작 알림 및 취소 옵션을 추가로 구성할 수 있습니다.

## 12.7.2 다시 시작 설정

AntiVir 프로그램의 제품 업데이트를 수행한 경우 컴퓨터 시스템을 다시 시작해야 할 수 있습니다. 일반::업데이트::제품 업데이트에서 자동 제품 업데이트를 선택한 경우에는 **다시 시작 설정**에서 다른 다시 시작 알림 및 다시 시작 취소 옵션을 선택할 수 있습니다.

### 참고

다시 시작 설정을 사용하면 구성 섹션 일반::업데이트::제품 업데이트에서 컴퓨터를 다시 시작해야 하는 제품 업데이트 실행에 대한 두 가지 옵션 중 하나를 선택할 수 있습니다.

업데이트를 사용할 수 있는 경우 컴퓨터를 다시 시작해야 하는 제품 업데이트 자동 실행: 업데이트 및 다시 시작은 사용자가 컴퓨터에서 작업하는 동안 수행됩니다. 이 옵션을 사용하면 취소 옵션 또는 미리 알림 기능을 통해 다시 시작 루틴을 쉽게 선택할 수 있습니다.

다음에 시스템이 다시 부팅된 후 컴퓨터를 다시 시작해야 하는 제품 업데이트 실행: 사용자가 컴퓨터를 시작하고 로그인한 후에 업데이트 및 다시 시작이 수행됩니다. 이 옵션에는 자동 다시 시작 루틴을 사용하는 것이 좋습니다.

### 다시 시작 설정

#### n초 후 컴퓨터 다시 시작

이 옵션을 사용하면 제품 업데이트가 실행된 후 해야 하는 다시 시작이 지정된 간격으로 **자동** 수행됩니다. 컴퓨터 다시 시작을 취소할 수 있는 옵션이 없는 카운터다운 메시지가 나타납니다.

#### n초마다 다시 시작 메시지 알림

이 옵션을 사용하면 제품 업데이트가 실행된 후 해야 하는 다시 시작이 자동 수행되지 **않습니다**. 지정된 간격이 되면, 취소 옵션이 없는 다시 시작 알림을 받게 됩니다. 이러한 알림에서 컴퓨터 다시 시작을 확인하거나 "**다시 알림**" 옵션을 선택할 수 있습니다.

#### 컴퓨터 다시 시작 여부 쿼리

이 옵션을 사용하면 제품 업데이트가 실행된 후 해야 하는 다시 시작이 자동 수행되지 **않습니다**. 다시 시작을 직접 수행하거나 다시 시작 루틴을 취소할 수 있는 옵션이 포함된 메시지 한 통만 받게 됩니다.

#### 쿼리하지 않고 컴퓨터 다시 시작

이 옵션을 사용하면 제품 업데이트가 실행된 후 해야 하는 다시 시작이 **자동으로** 수행됩니다. 알림은 제공되지 **않습니다**.

### 12.7.3 파일 서버

네트워크에 두 대 이상의 워크스테이션이 있는 경우, AntiVir 프로그램은 인트라넷의 파일 서버에서 업데이트를 다운로드할 수 있습니다. 인트라넷의 이 서버는 다시 인터넷의 전용 다운로드 서버에서 업데이트 파일을 가져옵니다. 따라서 모든 워크스테이션에서 AntiVir 프로그램이 최신 상태로 유지됩니다.

#### 참고

구성 섹션은 구성 :: 일반 :: 제품 업데이트 에서 **파일 서버/공유 폴더를 통해** 옵션을 선택한 경우에만 사용할 수 있습니다.

#### 다운로드

AntiVir 프로그램의 업데이트 파일 및 필요한 디렉터리 '/release/update/'가 있는 파일 서버의 이름을 입력합니다. 이 경우 file:// <파일 서버의 IP 주소>/release/update/를 지정해야 합니다. 'release' 디렉터리는 모든 사용자가 액세스할 수 있는 디렉터리여야 합니다.



이 단추는 필요한 다운로드 디렉터리를 선택할 수 있는 창을 엽니다.

#### 서버 로그인

##### 로그인 이름

서버에 로그인할 사용자 이름을 입력합니다. 해당 서버에서 사용할 공유 폴더에 대한 액세스 권한이 있는 사용자 계정을 사용하십시오.

##### 로그인 암호

사용자 계정의 암호를 입력합니다. 입력한 문자는 \*로 마스크됩니다.

#### 참고

서버 로그인 섹션에서 데이터를 지정하지 않으면 파일 서버에 액세스할 때 인증이 수행되지 않습니다. 이 경우 해당 사용자에게 파일 서버에 대한 충분한 권한이 있어야 합니다.

인터넷 또는 인트라넷의 웹 서버를 통해 업데이트를 직접 수행할 수 있습니다.

#### 웹 서버 연결

##### 기존 연결(네트워크) 사용

이 설정은 연결이 네트워크를 통해 사용되는 경우에 표시됩니다.

##### 다음 연결 사용

이 설정은 연결을 개별적으로 정의하는 경우에 표시됩니다.

업데이트 프로그램에서 사용할 수 있는 연결 옵션을 자동으로 검색합니다. 사용할 수 없는 연결 옵션은 회색으로 표시되고 활성화할 수 없습니다. 예를 들면 Windows의 전화 번호부 항목을 통해 전화 접속 연결을 수동으로 설정할 수 있습니다.

- **사용자:** 선택한 계정의 사용자 이름을 입력합니다.

- **암호:** 이 계정에 대한 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다.

**참고**  
기존 인터넷 계정 이름이나 암호를 잊은 경우 인터넷 서비스 공급자에게 문의하십시오.

**참고**  
전화 접속 도구(예: SmartSurfer, Oleco 등)를 통한 업데이트 프로그램의 자동 전화 접속은 아직 사용할 수 없는 상태입니다.

**업데이트를 위해 설정된 전화 접속 연결 종료**  
이 옵션을 사용하면 다운로드가 완료되는 즉시 업데이트를 위한 RDT 연결이 자동으로 다시 중단됩니다.

**참고**  
이 옵션은 Vista 에서 사용할 수 없습니다. Vista 에서는 다운로드가 완료되는 즉시 업데이트를 위한 전화 접속 연결이 항상 종료됩니다.

**다운로드**

**표준 서버**

업데이트 및 필요한 업데이트 디렉터리 'update'를 로드할 웹 서버의 주소(URL)를 입력합니다. 웹 서버의 주소 형식은 http://<웹 서버 주소>[:Port]/update 입니다. 포트를 지정하지 않은 경우에는 포트 80 이 사용됩니다. 업데이트에는 기본적으로 액세스 가능한 Avira GmbH 웹 서버가 지정됩니다. 그러나 회사 인트라넷의 고유 웹 서버를 사용할 수 있습니다. 여러 웹 서버를 지정할 경우에는 각 웹 서버를 쉼표로 구분합니다.

**기본값**

이 단추는 미리 정의된 주소를 복원합니다.

**우선 순위 서버**

이 필드에는 가장 먼저 업데이트를 제공하도록 요청할 웹 서버의 URL 및 업데이트 디렉터리를 입력합니다. 이 서버에 연결할 수 없으면 지정된 표준 서버가 사용됩니다. 웹 서버의 주소 형식은 http://<웹 서버 주소>[:포트]/update 입니다. 포트를 지정하지 않은 경우에는 포트 80 이 사용됩니다.

## 12.8 일반

### 12.8.1 이메일

AntiVir 프로그램은 경우에 따라 한 명 이상의 받는 사람에게 알림 및 메시지를 전자 메일로 보낼 수 있습니다. 이 작업은 SMTP(Simple Message Transfer Protocol)를 통해 수행됩니다.

메시지는 다양한 이벤트에 의해 트리거될 수 있습니다. 전자 메일 보내기를 지원하는 구성 요소는 다음과 같습니다.

- Guard: 알림 보내기



- 검사 프로그램: 알림 보내기
- 업데이트 프로그램: 알림 보내기

**참고**

ESMTP 는 지원되지 않습니다. 또한 TLS(Transport Layer Security)나 SSL(Secure Sockets Layer)을 통한 암호화된 전송도 현재 지원되지 않습니다.

**전자 메일 메시지****SMTP 서버**

여기에 사용할 호스트의 이름(IP 주소 또는 직접 호스트 이름)을 입력합니다. 호스트 이름의 최대 허용 길이는 127 자입니다.

예:

192.168.1.100 또는 mail.samplecompany.com

**보낸 사람 주소**

이 입력란에는 보낸 사람의 전자 메일 주소를 입력합니다. 보낸 사람 주소의 최대 허용 길이는 127 자입니다.

**인증**

일부 메일 서버의 경우 전자 메일을 보내기 전에 프로그램에서 자체적으로 서버(로그인)에 대해 인증을 받아야 합니다. 인증과 알림을 전자 메일로 SMTP 서버로 전송할 수 있습니다.

**인증 사용**

이 옵션을 사용하면 로그인(인증) 관련 상자에 사용자 이름 및 암호를 입력할 수 있습니다.

- **사용자 이름:** 여기에 사용자 이름을 입력합니다.
- **암호:** 여기에 관련 암호를 입력합니다. 이 암호는 암호화된 형태로 저장됩니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다.

**테스트 전자 메일 보내기**

이 단추를 클릭하면 프로그램은 입력된 데이터를 확인하기 위해 보낸 사람 주소로 테스트 전자 메일을 보냅니다.

## 12.8.2 위협 범주

**위협 범주 선택**

AntiVir 제품은 컴퓨터 바이러스로부터 사용자를 보호해 줍니다.

또한 다음과 같은 확장된 위협 범주에 따라 시스템을 검사할 수 있습니다.

- 백도어 클라이언트(BDC)
- 다이얼러(DIALER)



- 게임(GAMES)
- 장난 프로그램(JOKES)
- SPR(Security Privacy Risk)
- 애드웨어/스파이웨어(ADSPY)
- 비정상적인 런타임 압축 프로그램(PCK)
- 이중 확장명 파일(HEUR-DBLEXT)
- 피싱
- 응용 프로그램(APPL)

관련 상자를 클릭하면 선택한 유형이 사용되거나(확인 표시가 있는 경우) 또는 사용되지 않습니다(확인 표시가 없는 경우).

**모두 선택**

이 옵션을 사용하면 모든 유형이 사용됩니다.

**기본값**

이 단추는 미리 정의된 기본값을 복원합니다.

**참고**  
 유형 중 하나를 사용하지 않으면 관련 프로그램 유형으로 인식되는 파일이 더 이상 표시되지 않습니다. 보고서 파일에 항목이 작성되지 않습니다.

### 12.8.3 암호

암호를 사용하여 다양한 영역에서 AntiVir 프로그램을 보호할 수 있습니다. 암호가 지정된 경우 보호된 영역을 열려고 할 때마다 이 암호를 묻는 메시지가 표시됩니다.

**암호**

**암호 입력**

여기에 필요한 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다. 암호의 최대 길이는 20 자입니다. 암호를 지정한 경우 정확하지 않은 암호를 입력하면 프로그램에서 액세스가 거부됩니다. 이 상자를 비워 두면 "암호가 지정되지 않습니다".

**암호 확인**

위에서 입력한 암호를 여기에 다시 한 번 입력하여 확인합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다.

**참고**  
 암호는 대/소문자를 구분합니다.

**암호로 보호된 영역**

AntiVir 프로그램은 개별 영역을 암호로 보호할 수 있습니다. 필요에 따라 해당 상자를 클릭하여 개별 영역에 대한 암호 요청을 사용하거나 사용하지 않도록 설정할 수 있습니다.

암호로 보호된 영역	기능
------------	----

제어 센터	이 옵션을 사용하면 제어 센터를 시작할 때 미리 정의된 암호를 입력해야 합니다.
Guard 활성화/비활성화	이 옵션을 사용하면 AntiVir Guard 를 사용하거나 사용하지 않으려는 경우 미리 정의된 암호를 입력해야 합니다.
MailGuard 활성화/비활성화	이 옵션을 사용하면 MailGuard 를 사용하거나 사용하지 않으려는 경우 미리 정의된 암호를 입력해야 합니다.
FireWall 활성화/비활성화	이 옵션을 사용하면 FireWall 을 사용하거나 사용하지 않도록 설정할 때 미리 정의된 암호를 입력해야 합니다.
WebGuard 활성화/비활성화	이 옵션을 사용하면 WebGuard 를 사용하거나 사용하지 않으려는 경우 미리 정의된 암호를 입력해야 합니다.
인터넷에서 복구 CD 다운로드	이 옵션을 사용하면 Avira 복구 CD 다운로드를 시작할 때 미리 정의된 암호를 입력해야 합니다.
격리	이 옵션을 사용하면 암호로 보호되는 격리 관리자의 모든 영역을 사용할 수 있게 됩니다. 관련 상자를 클릭하여 필요에 따라 개별 영역에 대해 암호 조회를 비활성화하거나 다시 활성화할 수 있습니다.
영향받는 개체 복원	이 옵션을 사용하면 개체를 복원할 때 미리 정의된 암호를 입력해야 합니다.
감염된 개체 다시 검사	이 옵션을 사용하면 개체를 다시 검사할 때 미리 정의된 암호를 입력해야 합니다.
영향받는 개체 속성	이 옵션을 사용하면 개체의 속성을 표시할 때 미리 정의된 암호를 입력해야 합니다.
영향받는 개체 삭제	이 옵션을 사용하면 개체를 삭제할 때 미리 정의된 암호를 입력해야 합니다.
Avira 로 전자 메일 보내기	이 옵션을 사용하면 검사를 위해 Avira 맬웨어 연구 센터로 개체를 보낼 때 미리 정의된 암호를 입력해야 합니다.
영향받는 개체 복사	이 옵션을 사용하면 영향 받는 개체를 복사할 때 미리 정의된 암호를 입력해야 합니다.
작업 추가 및 수정	이 옵션을 사용하면 스케줄러에서 작업을 추가 및 변경할 때 미리 정의된

	암호를 입력해야 합니다.
제품 업데이트 시작	이 옵션을 사용하면 업데이트 메뉴에서 제품 업데이트를 시작할 때 미리 정의된 암호를 입력해야 합니다.
구성	이 옵션을 사용하면 미리 정의된 암호를 입력해야만 프로그램을 구성할 수 있습니다.
구성 수동 전환	이 옵션을 사용하면 다른 구성 프로파일로 수동 전환할 때 미리 정의된 암호를 입력해야 합니다.
고급 모드 사용	이 옵션을 사용하면 고급 모드를 사용할 때 미리 정의된 암호를 입력해야 합니다.
설치/제거	이 옵션을 사용하면 프로그램을 설치하거나 제거할 때 미리 정의된 암호를 입력해야 합니다.

### 12.8.4 보안

#### 업데이트(U)

##### 최신 업데이트가 n 일보다 이전인 경우 알림

이 상자에 마지막 업데이트 이후에 허용할 최대 경과 기간(일)을 입력할 수 있습니다. 이 기간이 지나면 제어 센터의 상태 아래에 있는 업데이트 상태에 빨간색 아이콘이 표시됩니다.

##### 바이러스 정의 파일이 만료된 경우 알림 표시

이 옵션을 사용하면 바이러스 정의 파일이 최신 버전이 아닌 경우 알림을 받게 됩니다. 이 알림 옵션을 사용하면 마지막 업데이트 후 n 일이 지났을 때 알림을 표시하는 임시 알림 간격을 구성할 수 있습니다.

#### 제품 보호

##### 참고

Guard 를 사용자 정의 설치 옵션으로 설치하지 않은 경우 제품 보호 옵션을 사용할 수 없습니다.

##### 원치 않게 종료되지 않도록 프로세스 보호

이 옵션을 사용하면 프로그램이 바이러스 및 맬웨어에 의해 사용자 동의 없이 종료되거나 사용자가 작업 관리자 등을 사용하여 '제어되지 않은 상태'로 종료할 수 없도록 모든 프로그램 프로세스가 보호됩니다. 이 옵션은 기본적으로 사용하도록 설정됩니다.

##### 고급 프로세스 보호

이 옵션을 사용하면 프로그램이 사용자 동의 없이 종료되지 않도록 모든 프로그램 프로세스가 고급 옵션으로 보호됩니다. 고급 프로세스 보호에는 단순 보호보다 상당히 많은 컴퓨터 리소스가 필요합니다. 이 옵션은 기본적으로 사용하도록 설정됩니다. 이 옵션을 사용하지 않으려면 컴퓨터를 다시 시작해야 합니다.

**중요**

Windows XP 64 비트에는 암호 보호를 사용할 수 없습니다.

**경고**

프로세스 보호 기능을 사용하는 경우 다른 소프트웨어 제품과의 상호 작용에 문제가 발생할 수 있습니다. 이러한 경우 프로세스 보호를 해제하십시오.

**파일 및 레지스트리 항목을 수정할 수 없도록 보호**

이 옵션을 사용하면 프로그램의 모든 레지스트리 항목과 모든 프로그램 파일(이진 파일 및 구성 파일)이 수정할 수 없도록 보호됩니다. 수정할 수 없도록 보호하는 데는 쓰기 및 삭제 보호는 물론 경우에 따라 사용자나 외부 프로그램에 의한 레지스트리 항목 또는 프로그램에 대한 읽기 액세스 보호도 포함됩니다. 이 옵션을 사용하려면 컴퓨터를 다시 시작해야 합니다.

**경고**

이 옵션을 사용하지 않으면 특정 유형의 맬웨어에 감염된 컴퓨터를 복구하지 못하게 될 수 있습니다.

**참고**

이 옵션이 활성화되면 사용자 인터페이스에서 검사 또는 업데이트 요청의 변경 등 구성만 변경할 수 있습니다.

**중요**

Windows XP 64 비트에는 파일 및 레지스트리 항목 보호를 사용할 수 없습니다.

## 12.8.5 WMI

### WMI(Windows Management Instrumentation)에 대한 지원

WMI(Windows Management Instrumentation)는 스크립트와 프로그래밍 언어를 사용하여 Windows 시스템 설정에 대한 로컬 및 원격 읽기/쓰기 액세스를 허용하는 기본적인 Windows 관리 기법입니다. AntiVir 프로그램은 WMI 를 지원하며 데이터(상태 정보, 통계 데이터, 보고서, 계획된 요청 등)는 물론 이벤트 및 메서드(프로세스 중지 및 시작)까지 인터페이스를 통해 제공합니다. WMI 를 사용하면 프로그램에서 작업 데이터를 다운로드하고 프로그램을 제어할 수 있습니다. WMI 인터페이스에 대한 전체 참조 설명서를 제조업체에 요청할 수 있습니다. 기밀 유지 계약에 서명하는 경우 PDF 형식의 참조 파일을 사용할 수 있습니다.

#### WMI 지원 사용

이 옵션을 사용하면 WMI 를 통해 프로그램에서 작업 데이터를 다운로드할 수 있습니다.

#### 서비스 사용/사용 안 함 허용

이 옵션을 사용하면 WMI 를 통해 프로그램 서비스를 사용하거나 사용하지 않도록 설정할 수 있습니다.

## 12.8.6 디렉터리

### 임시 경로

이 입력란에 프로그램의 임시 파일을 저장할 경로를 입력합니다.

### 기본 시스템 설정 사용

이 옵션을 사용하면 시스템의 설정이 임시 파일을 처리하는 데 사용됩니다.

### 참고

시스템에서 임시 파일을 저장하는 위치를 확인할 수 있습니다. 예를 들어 Windows XP의 경우 시작/설정/제어판/시스템/"고급" 탭/"환경 변수" 단추를 누르면 됩니다. 시스템 변수(TEMP, TMP)와 현재 등록된 사용자에게 대한 임시 변수(TEMP, TMP)가 관련 값과 함께 여기에 표시됩니다.

### 다음 디렉터리 사용

이 옵션을 사용하면 입력란에 표시된 경로가 사용됩니다.



이 단추는 필요한 임시 경로를 선택할 수 있는 창을 엽니다.

### 기본값

이 단추는 임시 경로에 대해 미리 정의된 디렉터리를 복원합니다.

### 보고서 디렉터리

이 입력란에는 보고서 디렉터리에 대한 경로가 들어 있습니다.



이 단추는 필요한 디렉터리를 선택할 수 있는 창을 엽니다.

### 기본값

이 단추는 보고서 디렉터리에 대해 미리 정의된 경로를 복원합니다.

### 격리 디렉터리

이 상자에는 격리 디렉터리에 대한 경로가 들어 있습니다.



이 단추는 필요한 디렉터리를 선택할 수 있는 창을 엽니다.

### 기본값

이 단추는 격리 디렉터리에 대해 미리 정의된 경로를 복원합니다.

## 12.8.7 프록시

### 프록시 서버

#### 프록시 서버 사용 안 함

이 옵션을 사용하면 웹 서버에 연결할 때 프록시 서버를 경유하지 않습니다.

#### Windows 시스템 설정 사용

이 옵션을 사용하면 프록시 서버를 통해 웹 서버에 연결할 때 현재의 Windows 시스템 설정이 사용됩니다. **제어판::인터넷 옵션::연결::LAN 설정**에서 프록시 서버를 사용하도록 Windows 시스템 설정을 구성하십시오. Internet Explorer의 Extras 메뉴에서도 인터넷 옵션에 액세스할 수 있습니다.

#### **경고**

인증이 필요한 프록시 서버를 사용하는 경우, *이 프록시 서버 사용* 옵션 아래에 필요한 모든 데이터를 입력하십시오. *Windows 시스템 설정 사용* 옵션은 인증이 필요 없는 프록시 서버에만 사용할 수 있습니다.

#### 이 프록시 서버 사용(U)

웹 서버 연결이 프록시 서버를 통해 설정되는 경우 여기에 관련 정보를 입력할 수 있습니다.

#### 주소

웹 서버에 연결할 때 사용할 프록시 서버의 컴퓨터 이름 또는 IP 주소를 입력합니다.

#### 포트

웹 서버에 연결할 때 사용할 프록시 서버의 포트 번호를 입력합니다.

#### 로그인 이름

프록시 서버에 로그인할 사용자 이름을 입력합니다.

#### 로그인 암호

여기에 프록시 서버에 로그인하기 위한 해당 암호를 입력합니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다.

예:

주소: proxy.domain.com    포트: 8080

주소: 192.168.1.100    포트: 3128

## 12.8.8 경고

### 12.8.8.1. 네트워크

검사 프로그램 또는 Guard에서 네트워크의 모든 워크스테이션으로 개별 구성 가능한 알림을 보낼 수 있습니다.

#### **참고**

"메시지 서비스"가 시작되었는지 여부를 확인하십시오. Windows XP의 경우 "시작/설정/시스템 제어/관리/서비스"에서 이 서비스를 찾을 수 있습니다.

**참고**

알림은 항상 특정 사용자가 아니라 컴퓨터로 전송됩니다.

**경고**

다음 운영 체제에서는 이 기능이 더 이상 지원되지 않습니다.

Windows Server 2008 이상

Windows Vista 이상

**다음으로 메시지 보내기**

이 창의 목록에는 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 때 메시지를 받는 컴퓨터의 이름이 표시됩니다.

**참고**

항상 각 컴퓨터를 이 목록에 한 번만 입력할 수 있습니다.

**삽입**

이 단추를 누르면 다른 컴퓨터를 추가할 수 있습니다. 새 컴퓨터의 이름을 입력하여 다른 컴퓨터를 추가할 수 있습니다. 컴퓨터 이름의 길이는 최대 15 자입니다.



이 단추를 누르면 표시되는 창에서 사용자 컴퓨터 환경에 있는 컴퓨터를 직접 선택할 수 있습니다.

**삭제**

이 단추를 누르면 현재 선택된 항목을 목록에서 삭제할 수 있습니다.

**Guard**

**네트워크 알림**

이 옵션을 사용하면 네트워크 알림이 전송됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

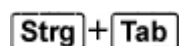
**참고**

이 옵션을 활성화하려면 일반 :: 알림 :: 네트워크에서 한 명 이상의 받는 사람을 입력해야 합니다.

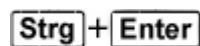
**보낼 메시지**

이 창에는 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 때 선택한 워크스테이션으로 전송되는 메시지가 표시됩니다. 이 메시지를 편집할 수 있으며, 텍스트 길이는 최대 500 자입니다.

메시지 서식 지정 시 다음 키 조합을 사용할 수 있습니다.



탭을 삽입합니다. 현재 줄을 오른쪽으로 몇 자 들여 씁니다.



줄 바꿈을 삽입합니다.

검색 도중 발견된 정보를 넣기 위한 와일드카드를 메시지에 포함할 수 있습니다. 이러한 와일드카드는 보낼 때 실제 텍스트로 대체됩니다.

다음 와일드카드를 사용할 수 있습니다.

%VIRUS%	발견된 바이러스 또는 사용자 동의 없이 설치된 프로그램의 이름을 포함합니다.
%FILE%	영향을 받는 파일의 경로 및 파일 이름을 포함합니다.
%COMPUTER%	Guard 를 실행 중인 컴퓨터의 이름을 포함합니다.
%NAME%	영향을 받는 파일에 액세스한 사용자의 이름을 포함합니다.
%ACTION%	바이러스 발견 후 수행된 작업을 포함합니다.
%MACADDR%	Guard 를 실행 중인 컴퓨터의 MAC 주소를 포함합니다.

### 기본값

이 단추는 미리 정의된 알림 기본 텍스트를 복원합니다.

### 검사 프로그램

#### 네트워크 알림 사용

이 옵션을 사용하면 네트워크 알림이 전송됩니다. 이 옵션은 기본적으로 사용되지 않습니다.

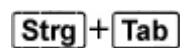
### 참고

이 옵션을 활성화하려면 일반 :: 알림 :: 네트워크에서 한 명 이상의 받는 사람을 입력해야 합니다.

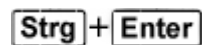
### 보낼 메시지

이 창에는 바이러스나 사용자 동의 없이 설치된 프로그램이 발견될 때 선택한 워크스테이션으로 전송되는 메시지가 표시됩니다. 이 메시지를 편집할 수 있으며, 텍스트 길이는 최대 500 자입니다.

메시지 서식 지정 시 다음 키 조합을 사용할 수 있습니다.



탭을 삽입합니다. 현재 줄을 오른쪽으로 몇 자 들여 씁니다.



줄 바꿈을 삽입합니다.

검색 도중 발견된 정보를 넣기 위한 와일드카드를 메시지에 포함할 수 있습니다. 이러한 와일드카드는 보낼 때 실제 텍스트로 대체됩니다.

다음 와일드카드를 사용할 수 있습니다.

%VIRUS%	발견된 바이러스 또는 사용자 동의 없이 설치된 프로그램의 이름을 포함합니다.
%NAME%	검사 프로그램을 사용하는 로그인한 사용자의 이름을 포함합니다.

### 기본값

이 단추는 미리 정의된 알림 기본 텍스트를 복원합니다.



## 12.8.8.2. 전자 메일

### 이메일

AntiVir 프로그램은 경우에 따라 한 명 이상의 받는 사람에게 알림 및 메시지를 전자 메일로 보낼 수 있습니다. 이 작업은 SMTP(Simple Message Transfer Protocol)를 통해 수행됩니다.

메시지는 다양한 이벤트에 의해 트리거될 수 있습니다. 전자 메일 보내기를 지원하는 구성 요소는 다음과 같습니다.

- Guard: 알림 보내기
- 검사 프로그램: 알림 보내기
- 업데이트 프로그램: 알림 보내기

### 참고

ESMTP 는 지원되지 않습니다. 또한 TLS(Transport Layer Security)나 SSL(Secure Sockets Layer)을 통한 암호화된 전송도 현재 지원되지 않습니다.

### 전자 메일 메시지

#### **SMTP 서버**

여기에 사용할 호스트의 이름(IP 주소 또는 직접 호스트 이름)을 입력합니다. 호스트 이름의 최대 허용 길이는 127 자입니다.

예:

192.168.1.100 또는 mail.samplecompany.com

#### **보낸 사람 주소**

이 입력란에는 보낸 사람의 전자 메일 주소를 입력합니다. 보낸 사람 주소의 최대 허용 길이는 127 자입니다.

### 인증

일부 메일 서버의 경우 전자 메일을 보내기 전에 프로그램에서 자체적으로 서버(로그인)에 대해 인증을 받아야 합니다. 인증과 알림을 전자 메일로 SMTP 서버로 전송할 수 있습니다.

#### **인증 사용**

이 옵션을 사용하면 로그인(인증) 관련 상자에 사용자 이름 및 암호를 입력할 수 있습니다.

- **사용자 이름:** 여기에 사용자 이름을 입력합니다.
- **암호:** 여기에 관련 암호를 입력합니다. 이 암호는 암호화된 형태로 저장됩니다. 보안을 유지하기 위해 이 공간에 입력하는 실제 문자는 별표(\*)로 대체됩니다.

### 테스트 전자 메일 보내기

이 단추를 클릭하면 프로그램은 입력된 데이터를 확인하기 위해 보낸 사람 주소로 테스트 전자 메일을 보냅니다.

## Guard

AntiVir Guard에서는 특정 이벤트에 대해 전자 메일을 통해 한 명 이상의 받는 사람에게 알림을 보낼 수 있습니다.

## Guard

### 전자 메일 알림

이 옵션을 사용하면 특정 이벤트가 발생할 때 AntiVir Guard에서 가장 중요한 정보가 포함된 전자 메일 메시지를 보냅니다. 이 옵션은 기본적으로 사용되지 않습니다.

### 다음 이벤트에 대한 전자 메일 메시지

**온 액세스 검사에서 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되었습니다.**

이 옵션을 사용하면 온 액세스 검사에서 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견될 때마다 영향을 받는 파일과 바이러스 또는 사용자 동의 없이 설치된 프로그램의 이름이 포함된 전자 메일을 받게 됩니다.

### 수정

"*편집*" 단추를 누르면 "온 액세스 발견" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

### Guard에서 오류가 발생했습니다.

이 옵션을 사용하도록 설정하면 내부 오류가 발견될 때마다 전자 메일을 받게 됩니다.

## 참고

이 경우에는 전자 메일에 제공된 데이터를 포함하여 기술 지원에 알려 주십시오. 검사할 수 있도록 지정된 파일도 보내 주셔야 합니다.

### 수정

"*편집*" 단추를 누르면 "Guard 오류" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

### 받는 사람

이 상자에 받는 사람의 전자 메일 주소를 입력합니다. 각 주소를 쉼표로 구분합니다. 모든 주소의 전체 최대 길이(총 문자열)는 260 자입니다.

## 검사 프로그램

온 디펜드 검사에서는 전자 메일을 통해 특정 이벤트 발생 시 한 명 이상의 받는 사람에게 알림과 메시지를 보낼 수 있습니다.

## 검사 프로그램

### 전자 메일 알림 사용

이 옵션을 사용하면 특정 이벤트가 발생할 때 프로그램에서 가장 중요한 정보가 포함된 전자 메일 메시지를 보냅니다. 이 옵션은 기본적으로 사용되지 않습니다.

### 다음 이벤트에 대한 전자 메일 메시지

**온 디맨드 검사에서 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견되었습니다.**

이 옵션을 사용하면 온 디맨드 검사에서 바이러스 또는 사용자 동의 없이 설치된 프로그램이 발견될 때마다 영향을 받는 파일과 바이러스 또는 사용자 동의 없이 설치된 프로그램의 이름이 포함된 전자 메일을 받게 됩니다.

### 수정

"편집" 단추를 누르면 "검사 발견" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

### 예약된 검사의 끝입니다.

이 옵션을 활성화하면 검사 작업이 수행될 때 전자 메일을 보내 줍니다. 이 전자 메일에는 검사 작업 시점 및 검사 소요 시간, 검사한 폴더 및 파일, 발견된 바이러스 및 경고에 대한 데이터가 포함됩니다.

### 수정

"편집" 단추를 누르면 "검사 종료" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

### 보고서 파일을 첨부 파일로 추가

이 옵션을 사용하면 검사 프로그램에서 알림을 보낼 때 검사 프로그램 구성 요소의 현재 보고서 파일이 전자 메일에 첨부 파일로 추가됩니다.

### 받는 사람 주소

이 상자에 받는 사람의 전자 메일 주소를 입력합니다. 각 주소를 쉼표로 구분합니다. 모든 주소의 전체 최대 길이(총 문자열)는 260 자입니다.

## 업데이트 프로그램

업데이트 프로그램 구성 요소에서는 전자 메일을 통해 특정 이벤트 발생 시 한 명 이상의 받는 사람에게 알림을 보낼 수 있습니다.

## 업데이트 프로그램

### 전자 메일 알림

이 옵션을 사용하면 특정 이벤트가 발생할 때 업데이트 구성 요소에서 가장 중요한 정보 데이터가 포함된 전자 메일 메시지를 보냅니다. 이 옵션은 기본적으로 사용되지 않습니다.

### 다음 이벤트에 대한 전자 메일 메시지

**업데이트가 필요하지 않습니다. 프로그램이 최신 상태입니다.**

이 옵션을 사용하면 업데이트 프로그램에서 다운로드 서버에 연결했지만 서버에 사용할 수 있는 새 파일이 없는 경우 전자 메일을 보냅니다. 즉, AntiVir 프로그램이 최신 상태입니다.

#### 수정

"편집" 단추를 누르면 "업데이트가 필요하지 않습니다" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

#### 업데이트가 완료되었습니다. 새 파일이 설치되었습니다.

이 옵션을 사용하면 수행된 모든 업데이트에 대해 전자 메일이 전송됩니다. 이 업데이트는 제품 업데이트나 바이러스 정의 파일 또는 검사 엔진의 업데이트일 수 있습니다.

#### 수정

"편집" 단추를 누르면 "업데이트 완료 - 새 파일이 설치되었습니다" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

#### 업데이트가 완료되었습니다. 새 제품 업데이트를 사용할 수 있습니다.

이 옵션을 사용하면 제품 업데이트가 있는데도 제품 업데이트를 제외하고 검사 엔진 또는 바이러스 정의 파일이 업데이트된 경우에만 전자 메일이 전송됩니다.

#### 수정

"편집" 단추를 누르면 "업데이트 완료 - 제품 업데이트를 사용할 수 있습니다" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

#### 업데이트하지 못했습니다.

이 옵션을 사용하면 오류로 인해 업데이트에 실패한 경우 전자 메일이 전송됩니다.

#### 수정

"편집" 단추를 누르면 "업데이트 실패" 이벤트에 대한 알림을 구성할 수 있는 "전자 메일 템플릿" 창이 열립니다. 전자 메일의 제목 줄과 본문에 텍스트를 삽입할 수 있으며, 이러한 용도의 변수를 사용할 수 있습니다. 구성::일반::전자 메일::알림::전자 메일 템플릿을 참조하십시오.

#### 보고서 파일을 첨부 파일로 추가

이 옵션을 사용하면 업데이트 프로그램에서 알림을 보낼 때 업데이트 프로그램의 현재 보고서 파일이 전자 메일에 첨부 파일로 추가됩니다.

#### 받는 사람

이 상자에 받는 사람의 전자 메일 주소를 입력합니다. 각 주소를 쉼표로 구분합니다. 모든 주소의 전체 최대 길이(총 문자열)는 260 자입니다.

**참고**

업데이트 프로그램 알림을 위한 SMTP 서버 및 받는 사람 주소가 구성된 경우, 다음 이벤트에 대해 항상 전자 메일 알림이 전송됩니다.

프로그램의 모든 후속 업데이트에 제품 업데이트가 필요합니다.

제품 업데이트가 필요하므로 검사 엔진 또는 바이러스 정의 파일의 업데이트를 수행할 수 없습니다.

이러한 알림 메시지는 업데이트 구성 요소의 전자 메일 경고에 대한 설정과 관계없이 전송됩니다.

**전자 메일 템플릿**

전자 메일 템플릿 창에서는 설정된 이벤트에 대해 개별 구성 요소의 전자 메일 알림을 구성할 수 있습니다. 제목 줄에는 최대 128 자, 메시지 필드에는 최대 1024 자의 텍스트를 삽입할 수 있습니다.

전자 메일 제목 및 전자 메일 메시지에 다음과 같은 변수를 사용할 수 있습니다.

**전역적으로 허용되는 변수**

변수	값
Windows 환경 변수	전자 메일 알림 구성 요소는 모든 Windows 환경 변수를 지원합니다.
%SYSTEM_IP%	컴퓨터의 IP 주소
%FQDN%	정규화된 도메인 이름
%TIMESTAMP%	이벤트 타임스탬프: 운영 체제의 언어 설정에 따른 날짜 및 시간 형식
%COMPUTERNAME%	NetBIOS 컴퓨터 이름
%USERNAME%	구성 요소에 액세스하는 사용자의 이름
%PRODUCTVER%	제품 버전
%PRODUCTNAME%	제품 이름
%MODULENAME%	전자 메일을 보내는 구성 요소의 이름
%MODULEVER%	전자 메일을 보내는 구성 요소의 버전

**특정 구성 요소 변수**

변수	값	구성 요소 전자 메일
%ENGINEVER%	사용한 검사 엔진의 버전	Guard 검사 프로그램
%VDFVER%	사용되는 바이러스 정의 파일의 버전	Guard 검사 프로그램

%SOURCE%	정규화된 파일 이름	Guard
%VIRUSNAME%	바이러스 또는 사용자 동의 없이 설치된 프로그램의 이름	Guard
%ACTION%	검색 후 수행한 작업	Guard
%MACADDR%	등록된 첫 번째 네트워크 카드의 MAC 주소	Guard
%UPDFILESLIST%	업데이트된 파일 목록	업데이트 프로그램
%UPDATETYPE%	업데이트 유형: 검사 엔진 및 바이러스 정의 파일의 업데이트 또는 검사 엔진 및 바이러스 정의 파일의 업데이트가 포함된 제품 업데이트	업데이트 프로그램
%UPDATEURL%	업데이트에 사용되는 다운로드 서버의 URL	업데이트 프로그램
%UPDATE_ERROR%	업데이트 오류 설명	업데이트 프로그램
%DIRCOUNT%	검사한 디렉터리 수입니다.	검사 프로그램
%FILECOUNT%	검사한 파일 수	검사 프로그램
%MALWARECOUNT%	검색된 바이러스 및 사용자 동의 없이 설치된 프로그램 수	검사 프로그램
%REPAIREDCOUNT%	복구한 감염된 파일 수	검사 프로그램
%RENAMEDCOUNT%	이름을 바꾼 감염된 파일 수	검사 프로그램
%DELETEDCOUNT%	삭제한 감염된 파일 수	검사 프로그램
%WIPECOUNT%	덜어쓰기 및 삭제한 감염된 파일 수	검사 프로그램
%MOVEDCOUNT%	격리로 이동한 감염된 파일 수	검사 프로그램
%WARNINGCOUNT%	경고 수	검사 프로그램
%ENDTYPE%	검사 상태: 종료됨/성공적으로 완료됨	검사 프로그램
%START_TIME%	검사 시작 시간: 업데이트 시작 시간	검사 프로그램 업데이트 프로그램
%END_TIME%	검사 종료	검사 프로그램

	업데이트 종료	업데이트 프로그램
%TIME_TAKEN%	검사 기간(분) 업데이트 기간(분)	검사 프로그램 업데이트 프로그램
%LOGFILEPATH%	보고서 파일의 경로 및 파일 이름	검사 프로그램 업데이트 프로그램

### 12.8.8.3. 음향 알림

#### 음향 알림

검사 프로그램 또는 Guard 에서 바이러스나 맬웨어를 발견하면 대화형 작업 모드에서 음향 알림이 울립니다. 음향 알림을 활성화하거나 비활성화하도록 선택하고 알림용으로 웨이브 파일을 선택할 수 있습니다.

#### 참고

검사 프로그램의 작업 모드는 구성 섹션 검사 프로그램::검사::검색에 대한 작업에서 설정됩니다. Guard의 작업 모드는 구성 섹션 Guard::검사::검색에 대한 작업에서 설정됩니다.

#### 경고 없음

이 옵션을 사용하도록 설정하면 검사 프로그램 또는 Guard 에서 바이러스가 발견될 때 음향 알림이 울리지 않습니다.

#### PC 스피커 사용(대화형 모드에서만)

이 옵션을 사용하면 검사 프로그램 또는 Guard 에서 바이러스가 발견될 때 기본 신호를 사용하는 음향 알림이 울립니다. 즉, 음향 알림이 PC 의 내부 스피커에서 울립니다.

#### 다음 웨이브 파일 사용(대화형 모드에서만)

이 옵션을 사용하면 검사 프로그램 또는 Guard 에서 바이러스가 발견될 때 선택한 웨이브 파일을 사용하는 음향 알림이 울립니다. 선택한 웨이브 파일은 연결된 외부 스피커에서 재생됩니다.

#### 웨이브 파일

이 입력란에 선택한 오디오 파일의 이름과 관련 경로를 입력할 수 있습니다. 프로그램의 기본 음향 신호가 표준으로 입력됩니다.



이 단추는 파일 탐색기를 사용하여 필요한 파일을 선택할 수 있는 창을 엽니다.

#### 테스트

이 단추는 선택한 웨이브 파일을 테스트하는 데 사용됩니다.

### 12.8.8.4. 경고

AntiVir 프로그램에서는 특정 이벤트에 대해 슬라이드 창 형식의 데스크톱 알림을 생성하여 프로그램 시퀀스(예: 업데이트)의 성공 또는 실패 사실을 알려 줍니다.

경고에서는 특정 이벤트에 대한 알림을 설정하거나 해제할 수 있습니다.

데스크톱 알림을 사용하면 슬라이드 창에서 직접 알림을 해제할 수 있습니다. 또한 경고에서 알림 해제를 되돌릴 수 있습니다.

**경고****전화 접속 연결을 사용한 경우**

이 옵션을 사용하면 컴퓨터에서 다이얼러가 전화 또는 ISDN 네트워크를 통해 전화 접속 연결을 생성하는 경우 데스크톱 알림이 제공됩니다. 사용자 동의 없이 설치되는 알 수 없는 다이얼러에 의해 연결이 생성되고 이러한 연결에 대해 요금이 부과될 수 있는 위험이 있습니다. (바이러스 및 기타::위협 범주: 다이얼러를 참조하십시오.)

**업데이트한 파일의 경우**

이 옵션을 사용하면 업데이트가 성공적으로 수행되고 파일이 업데이트될 때마다 데스크톱 알림이 제공됩니다.

**업데이트가 실패한 경우**

이 옵션을 사용하면 업데이트가 실패할 때마다 데스크톱 알림이 제공됩니다. 즉, 다운로드 서버에 대한 연결을 만들 수 없거나 업데이트 파일을 설치할 수 없는 경우가 여기에 해당됩니다.

**업데이트가 필요하지 않은 경우**

이 옵션을 사용하면 업데이트가 시작되었지만 프로그램이 최신 상태여서 파일을 설치할 필요가 없는 경우 데스크톱 알림이 제공됩니다.

**12.8.9 이벤트****이벤트 데이터베이스 크기 제한****최대 이벤트 수를 n 개 항목으로 제한**

이 옵션을 사용하면 이벤트 데이터베이스에 나열된 최대 이벤트 수를 특정 크기(예: 100 개 또는 10000 개 항목)로 제한할 수 있습니다. 입력된 항목 수를 초과하면 가장 오래된 항목이 삭제됩니다.

**n 일보다 이전인 이벤트 삭제**

이 옵션을 사용하면 특정 기간이 경과된 후 이벤트 데이터베이스에 나열된 이벤트가 삭제됩니다. 가능한 값은 1 ~ 90 일입니다. 이 옵션은 기본적으로 사용되며 기본값은 30 일입니다.

**이벤트 데이터베이스 크기 제한 안 함(이벤트 수동으로 삭제)**

이 옵션을 활성화하면 이벤트 데이터베이스 크기에 대한 제한이 없습니다. 하지만 프로그램 인터페이스의 이벤트 아래에는 최대 20,000 개 항목이 표시됩니다.

**12.8.10 보고서 제한****보고서 수 제한****개수를 n 개로 제한**

이 옵션을 사용하면 최대 보고서 수를 특정 개수로 제한할 수 있습니다. 1 ~ 300 의 값을 사용할 수 있습니다. 지정한 개수를 초과하면 해당 시점에 가장 오래된 보고서가 삭제됩니다.



**n 일보다 이전인 보고서 모두 삭제**

이 옵션을 사용하면 특정 기간(일)이 경과된 경우 보고서가 자동으로 삭제됩니다. 사용할 수 있는 값은 1 ~ 90 일입니다. 이 옵션은 기본적으로 사용되며 기본값은 30 일입니다.

**보고서 수 제한 안 함(보고서 수동으로 삭제)**

이 옵션을 사용하면 보고서 수에 제한이 없습니다.

이 매뉴얼은 상당한 주의를 기울여 작성되었지만 디자인 및 내용상 오류가 있을 수 있습니다.  
Avira GmbH의 사전 서면 동의 없이 본 문서나 본 문서의 일부를 어떤 형식으로든 복제해서는 안됩니다.

오류 및 기술적 사항이 변경될 수 있습니다.

2011년 2분기 발행

AntiVir®는 Avira Operations GmbH & Co. KG 의 등록 상표입니다. 다른 모든 브랜드 및 제품명은 해당 소유자의 상표 또는 등록상표입니다.  
이 설명서에서는 보호되는 상표를 따로 표시하지 않습니다. 하지만 그렇다고 해서 그러한 상표를 마음대로 사용할 수 있는 것은 아닙니다.



live free.™