



AVG 9 Internet Security

사용자 설명서

문서 개정 90.21 (3.2.2010)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
다른 모든 상표는 해당 소유자의 재산입니다 .

이 제품은 RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991을 사용합니다 .

이 제품은 C-SaCzech 라이브러리 코드 , Copyright (c) 1996-2001 Jaromir Dolecek(dolecek@ics.muni.cz)을 사용합니다 .

이 제품은 압축 라이브러리 zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler를 사용합니다 .

이 제품은 압축 라이브러리 libbzip2, Copyright (c) 1996-2002 Julian R. Seward를 사용합니다 .

목차

1. 소개	8
2. AVG 설치 요구 사항	9
2.1 지원되는 운영 체제	9
2.2 최소 / 권장 하드웨어 요구 사항	9
3. AVG 설치 옵션	11
4. AVG 다운로드 관리 프로그램	12
4.1 언어 선택	12
4.2 연결성 확인	13
4.3 프록시 설정	14
4.4 설치할 파일 다운로드	15
5. AVG 설치 프로세스	16
5.1 설치 시작	16
5.2 라이선스 계약	17
5.3 시스템 상태 확인	17
5.4 설치 유형 선택	18
5.5 AVG 라이선스 활성화	18
5.6 사용자 지정 설치 - 대상 폴더	19
5.7 사용자 지정 설치 - 구성 요소 선택	20
5.8 AVG DataCenter	21
5.9 AVG Security Toolbar	22
5.10 열려 있는 응용 프로그램 닫기	23
5.11 AVG 설치	24
5.12 정기적 스캔 및 업데이트 예약	25
5.13 컴퓨터 사용법 선택	25
5.14 컴퓨터의 인터넷 연결 :	26
5.15 AVG 보호 구성이 완료되었습니다	27
6. 설치 후 작업	28
6.1 스캔 최적화	28
6.2 제품 등록	28
6.3 사용자 인터페이스 액세스	28
6.4 전체 컴퓨터 스캔	29

6.5	티CAR 테스트	29
6.6	AVG 기본 구성	30
7.	AVG 사용자 인터페이스	31
7.1	시스템 메뉴	32
7.1.1	파일	32
7.1.2	구성 요소	32
7.1.3	기록	32
7.1.4	도구	32
7.1.5	도움말	32
7.2	보안 상태 정보	35
7.3	빠른 링크	36
7.4	구성 요소 개요	36
7.5	통계	38
7.6	시스템 트레이 아이콘	38
8.	AVG 구성 요소	40
8.1	Anti-Virus	40
8.1.1	Anti-Virus 원리	40
8.1.2	Anti-Virus 인터페이스	40
8.2	Anti-Spyware	42
8.2.1	Anti-Spyware 원리	42
8.2.2	Anti-Spyware 인터페이스	42
8.3	Anti-Spam	44
8.3.1	Anti-Spam 원리	44
8.3.2	Anti-Spam 인터페이스	44
8.4	Anti-Rootkit	46
8.4.1	Anti-Rootkit 원리	46
8.4.2	Anti-Rootkit 인터페이스	46
8.5	시스템 도구	48
8.5.1	프로세스	48
8.5.2	네트워크 연결	48
8.5.3	자동 시작	48
8.5.4	브라우저 확장	48
8.5.5	LSP 뷰어	48
8.6	방화벽	55
8.6.1	방화벽 원리	55
8.6.2	방화벽 프로필	55

8.6.3 방화벽 인터페이스	55
8.7 전자 메일 스캐너	59
8.7.1 전자 메일 스캐너 원리	59
8.7.2 전자 메일 스캐너 인터페이스	59
8.7.3 전자 메일 스캐너 검색	59
8.8 ID Protection	64
8.8.1 ID Protection 원리	64
8.8.2 ID Protection 인터페이스	64
8.9 라이선스	66
8.10 Link Scanner	67
8.10.1 Link Scanner 원리	67
8.10.2 Link Scanner 인터페이스	67
8.10.3 AVG Search-Shield	67
8.10.4 AVG Active Surf-Shield	67
8.11 Online Shield	71
8.11.1 Online Shield 원리	71
8.11.2 Online Shield 인터페이스	71
8.11.3 Online Shield 탐지	71
8.12 Resident Shield	77
8.12.1 상주 보호 원리	77
8.12.2 상주 보호 인터페이스	77
8.12.3 상주 보호 검색	77
8.13 업데이트 관리자	82
8.13.1 업데이트 관리자 원리	82
8.13.2 업데이트 관리자 인터페이스	82
9. AVG Security Toolbar	85
9.1 AVG Security Toolbar 인터페이스	85
9.2 AVG Security Toolbar 옵션	87
9.2.1 탭 일반	87
9.2.2 탭 유용한 단추	87
9.2.3 탭 보안	87
9.2.4 탭 고급 옵션	87
10. AVG 고급 설정	92
10.1 모양	92
10.2 사운드	94
10.3 오류 상태 무시	96

10.4 Identity Protection	97
10.4.1 Identity Protection 설정	97
10.4.2 허용 목록	97
10.5 바이러스 저장소	101
10.6 PUP 예외	102
10.7 Anti-Spam	104
10.7.1 설정	104
10.7.2 성능	104
10.7.3 RBL	104
10.7.4 허용 목록	104
10.7.5 차단 목록	104
10.7.6 고급 설정	104
10.8 Online Shield	116
10.8.1 웹 보호	116
10.8.2 인스턴트 메시징	116
10.9 Link Scanner	120
10.10 스캔	121
10.10.1 전체 컴퓨터 스캔	121
10.10.2 셀 확장 스캔	121
10.10.3 특정 파일 또는 폴더 스캔	121
10.10.4 이동식 장치 스캔	121
10.11 예약	128
10.11.1 예약된 스캔	128
10.11.2 바이러스 데이터베이스 업데이트 일정	128
10.11.3 Anti-Spam 업데이트 일정	128
10.12 E-mail Scanner	140
10.12.1 인증	140
10.12.2 메일 필터링	140
10.12.3 로그 및 결과	140
10.12.4 서버	140
10.13 Resident Shield	149
10.13.1 고급 설정	149
10.13.2 디렉터리 제외	149
10.13.3 제외된 파일	149
10.14 캐시 서버	154
10.15 Anti-Rootkit	155
10.16 업데이트	156
10.16.1 프록시	156

10.16.2 전화 접속	156
10.16.3 URL	156
10.16.4 관리	156
10.17 원격 관리	163
11. 방화벽 설정	165
11.1 일반	165
11.2 보안	166
11.3 영역 및 어댑터 프로필	167
11.4 로그	168
11.5 프로필	170
11.5.1 프로필 정보	170
11.5.2 정의된 네트워크	170
11.5.3 응용 프로그램	170
11.5.4 시스템 서비스	170
12. AVG 스캔	183
12.1 스캔 인터페이스	183
12.2 미리 정의된 스캔	184
12.2.1 전체 컴퓨터 스캔	184
12.2.2 특정 파일 또는 폴더 스캔	184
12.2.3 Anti-Rootkit 스캔	184
12.3 Windows 탐색기에서 스캔	194
12.4 명령줄 스캔	195
12.4.1 CMD 스캔 매개 변수	195
12.5 스캔 일정	197
12.5.1 예약 설정	197
12.5.2 스캔 방법	197
12.5.3 스캔 대상	197
12.6 스캔 결과 개요	208
12.7 스캔 결과 세부 정보	209
12.7.1 결과 개요 탭	209
12.7.2 감염 탭	209
12.7.3 스파이웨어 탭	209
12.7.4 경고 탭	209
12.7.5 루트킷 탭	209
12.7.6 정보 탭	209
12.8 바이러스 저장소	218



13. AVG 업데이트	220
13.1 업데이트 수준	220
13.2 업데이트 유형	220
13.3 업데이트 프로세스	221
14. 이벤트 기록	222
15. FAQ 및 기술 지원	224



1. 소개

이 사용자 설명서에는 **AVG 9 Internet Security**에 대한 포괄적인 내용이 포함되어 있습니다 .

AVG 9 Internet Security 구매를 축하합니다 .

AVG 9 Internet Security 프로그램은 안정적인 방식으로 PC를 완벽하게 보호할 수 있도록 설계된 수상 경력에 빛나는 AVG 제품 중 하나입니다 . 모든 AVG 제품과 마찬가지로 **AVG 9 Internet Security**도 사용자에게 더욱 친숙하고 효율적인 새로운 방식으로 AVG의 뛰어난 고품질 보안 기능을 제공할 수 있도록 기초부터 완벽하게 재설계되었습니다 .

새로운 **AVG 9 Internet Security** 제품에는 보다 능동적이고 신속한 스캔 기능과 효율적인 인터페이스가 결합되어 있습니다 . 사용자 편의를 위해 많은 보안 기능이 자동화되었으며 이러한 보안 기능이 사용자의 생활 방식에 맞게 지능적 사용자 옵션이 새로 추가되었습니다 . 따라서 사용 편의성과 동시에 보안을 강화할 수 있습니다 .

AVG는 컴퓨팅 및 네트워킹 활동을 보호하도록 설계 및 개발되었습니다 . AVG가 제공하는 완전한 보호를 경험해 보십시오 .



2. AVG 설치 요구 사항

2.1. 지원되는 운영 체제

AVG 9 Internet Security 제품은 다음 운영 체제가 실행되는 워크스테이션을 보호합니다 .

- Windows 2000 Professional SP4 + 업데이트 롤업 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista(x86 및 x64, 모든 버전)
- Windows 7(x86 및 x64, 모든 버전)

특정 운영 체제의 경우에는 상위 버전의 서비스 팩이 필요할 수 있습니다 .

참고 : [ID Protection](#) 구성 요소는 Windows 2000 및 XP x64에서 지원되지 않습니다 . 이러한 운영 체제에 AVG 9 Internet Security 제품을 설치할 수 있지만 IDP 구성 요소는 사용할 수 없습니다 .

2.2. 최소/ 권장 하드웨어 요구 사항

AVG 9 Internet Security의 최소 하드웨어 요구 사항 :

- Intel Pentium CPU 1,5GHz
- 512MB 이상의 RAM 메모리
- 390MB의 사용 가능한 하드 드라이브 공간 (설치용)

AVG 9 Internet Security의 권장 하드웨어 요구 사항 :

- Intel Pentium CPU 1,8GHz
- 512MB 이상의 RAM 메모리



- 510MB의 사용 가능한 하드 드라이브 공간 (설치용)



3. AVG 설치 옵션

AVG를 설치하려면 설치 CD에 있는 설치 파일을 사용하거나 AVG 웹 사이트 (<http://www.avg.com/>)에서 최신 설치 파일을 다운로드하십시오 .

AVG를 설치하기 전에 먼저 AVG 웹 사이트 (<http://www.avg.com/>)를 방문하여 새 설치 파일이 있는지 확인하시기 바랍니다 . 이렇게 하면 AVG 9 Internet Security의 최신 버전을 설치할 수 있습니다 .

설치 파일을 필요한 언어로 설치하는 데 유용한 새로운 [AVG 다운로드 관리 프로그램](#) 도구를 사용할 것을 권장합니다 .

설치 중에 라이선스 / 판매 번호를 요구하는 메시지가 표시됩니다 . 설치를 시작하기 전에 해당 정보를 확인하시기 바랍니다 . 판매 번호는 CD 패키지에 있습니다 . AVG 제품을 온라인으로 구입한 경우 전자 메일을 통해 라이선스 번호를 제공받게 됩니다 .

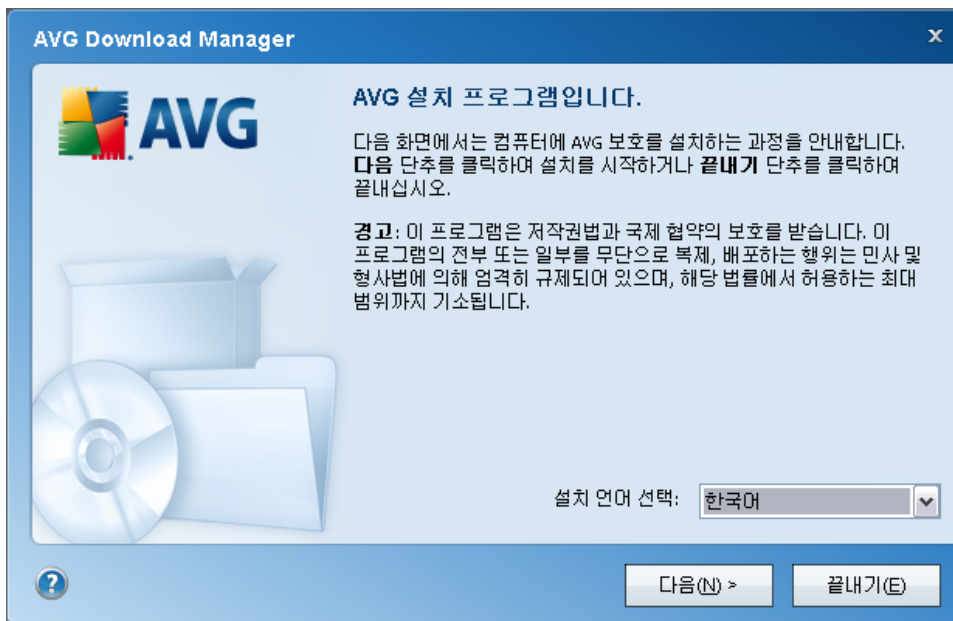
4. AVG 다운로드 관리 프로그램

AVG 다운로드 관리 프로그램 은(는) AVG 제품 평가판 버전에 적합한 설치 파일을 선택하는 데 도움이 되는 간단한 도구입니다 . 이 관리 프로그램은 사용자 입력 데이터를 기반으로 제품 , 라이선스 유형 , 적절한 구성 요소 및 언어를 선택합니다 . 그런 다음 **AVG 다운로드 관리 프로그램** 은(는) 다운로드를 진행하고 적합한 설치 프로세스 를 시작합니다 .

경고 : AVG 다운로드 관리 프로그램은 네트워크 및 SBS Edition의 다운로드에는 적합하지 않으며 Windows 2000(SP4 + SRP 롤업), Windows XP, Windows Vista 및 Windows 7 운영 체제만 지원합니다 .

AVG 다운로드 관리 프로그램 은(는) AVG 웹 사이트 (<http://www.avg.com/>)에서 다운로드할 수 있습니다 . 다음 섹션에서는 **AVG 다운로드 관리 프로그램** 에서 수행해야 하는 각 단계에 대한 간략한 설명을 확인할 수 있습니다 .

4.1. 언어 선택

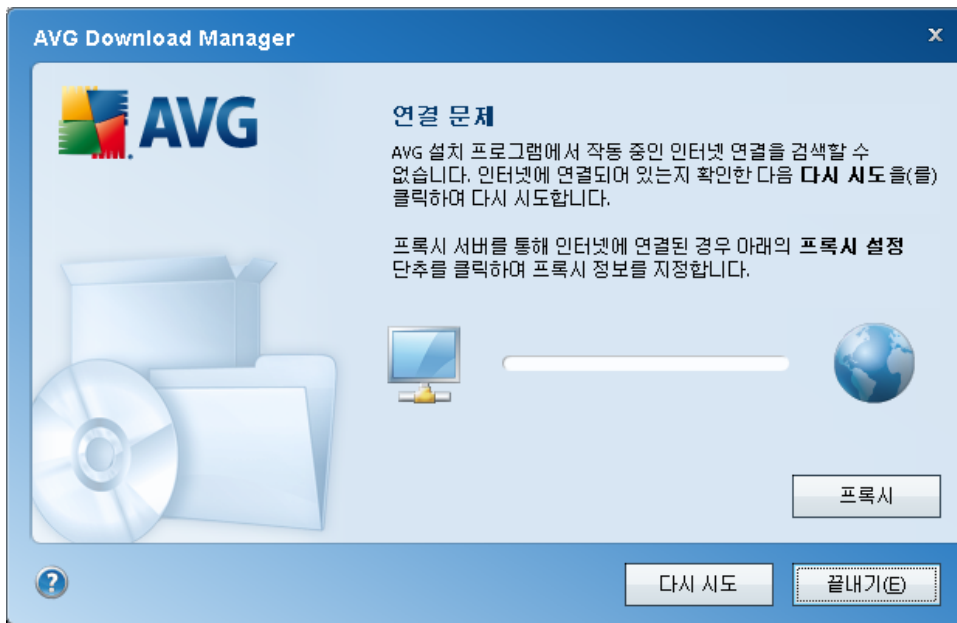


AVG 다운로드 관리 프로그램 의 첫 번째 단계에 있는 롤다운 메뉴에서 설치 언어를 선택하십시오 . 선택한 언어는 설치 프로세스에만 적용됩니다 . 설치를 마치면 프로그램 설정에서 바로 언어를 변경할 수 있습니다 . 그리고 나서 **다음** 단추를 눌러 계속 진행하십시오 .

4.2. 연결성 확인

다음 단계로 **AVG 다운로드 관리 프로그램**에서는 업데이트를 찾을 수 있도록 인터넷 연결을 시도합니다. **AVG 다운로드 관리 프로그램**에서 연결성 테스트를 완료하기 전에는 다운로드 프로세스를 진행할 수 없습니다.

- 테스트에서 연결할 수 없다는 결과가 나타나면 인터넷 연결이 잘 되어 있는지 확인해야 합니다. 그런 다음 **다시 시도** 단추를 클릭합니다.



- 인터넷에 프록시 연결을 사용하는 경우 **프록시 설정** 단추를 클릭하여 [프록시 정보](#)를 지정합니다.
- 검사가 완료되면 **다음** 단추를 눌러 계속합니다.

4.3. 프록시 설정



AVG Download Manager

프록시 설정을 지정하십시오.

AVG 설치 프로그램에서 프록시 설정을 식별할 수 없습니다.
해당 정보를 아래에서 지정하십시오.

서버:

포트:

☐ 프록시 인증 사용

인증 유형 선택:

사용자 이름:

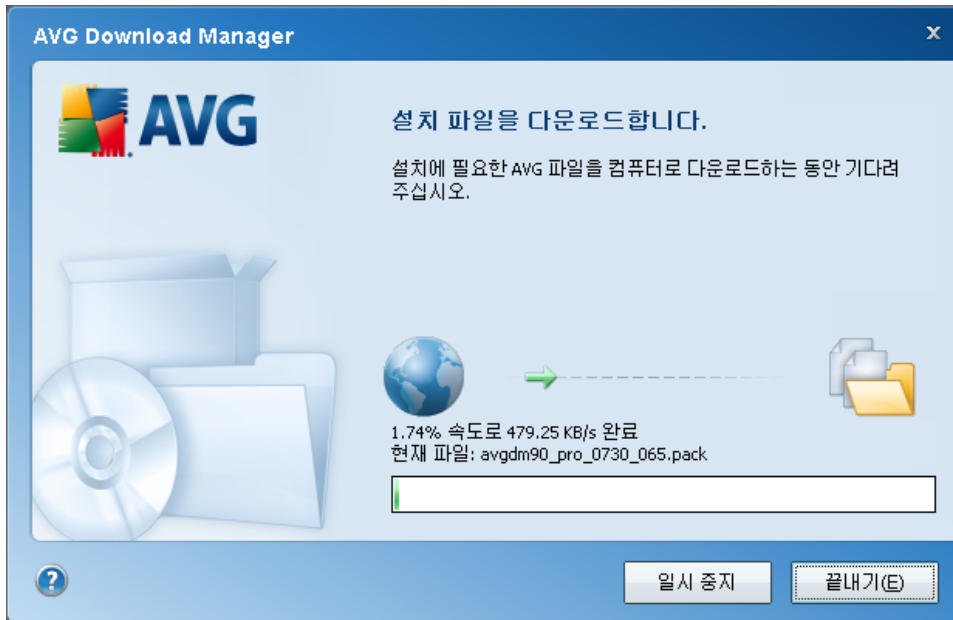
암호:

AVG 다운로드 관리 프로그램 에서 프록시 설정을 식별하지 못했으므로 수동으로 지정해야 합니다 . 다음 데이터를 입력하십시오 .

- **서버** - 유효한 프록시 서버 이름 또는 IP 주소를 입력합니다 .
- **포트** - 해당 포트 번호를 제공합니다 .
- **프록시 인증 사용** - 프록시 서버에서 인증을 필요로 하는 경우 이 확인란을 선택합니다 .
- **인증 선택** - 드롭다운 메뉴에서 인증 유형을 선택합니다 . 되도록이면 기본값을 유지하는 것이 좋습니다 . 그러면 *프록시 서버에서 자동으로 요구 사항을 전달합니다* . 그러나 숙련된 사용자의 경우에는 기본 (*일부 서버에서 사용*) 또는 NTLM(*모든 ISA 서버에서 사용*) 옵션을 선택할 수도 있습니다 . 그런 다음 올바른 **사용자 이름** 및 **암호** (선택 사항)를 입력합니다 .

적용 단추를 눌러 설정을 확인하고 **AVG 다운로드 관리 프로그램** 의 다음 단계를 진행합니다 .

4.4. 설치할 파일 다운로드



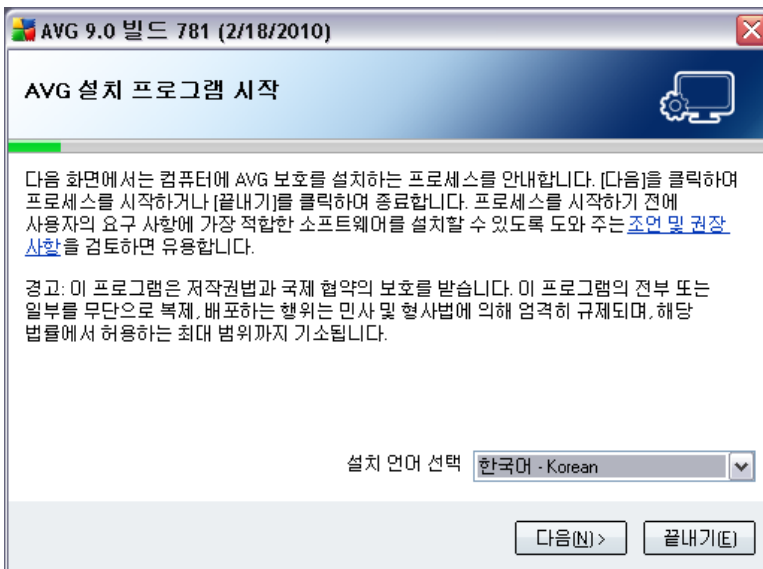
이제 **AVG 다운로드 관리 프로그램** 에서 설치 패키지를 다운로드하고 설치 프로세스를 시작하는 데 필요한 모든 정보를 알아보았습니다 . 다음으로 [AVG 설치 프로세스](#) 로 이동합니다 .

5. AVG 설치 프로세스

컴퓨터에 **AVG 9 Internet Security** 제품을 설치하려면 최신 설치 파일을 확보해야 합니다. 제품 포장 박스에 포함된 CD에 들어 있는 설치 파일을 사용할 수 있지만, 이 파일은 최신 버전이 아닐 수 있습니다. 따라서 최신 설치 파일을 온라인으로 다운로드하는 것이 좋습니다. 이 파일은 AVG 웹 사이트 (<http://www.avg.com/>)의 [지원 센터 / 다운로드](#) 섹션에서 다운로드할 수 있습니다. 또는 필요한 설치 패키지를 만들고 다운로드할 수 있도록 지원하는 새 [AVG 다운로드 관리 프로그램](#) 도구를 사용하여 설치 프로세스를 시작할 수도 있습니다.

설치는 일련의 대화 상자 창으로 진행되며 이 대화 상자에는 각 단계에서 수행할 작업에 대한 간략한 설명이 나와 있습니다. 다음 페이지에서는 각 대화 상자 창에 대해 설명합니다.

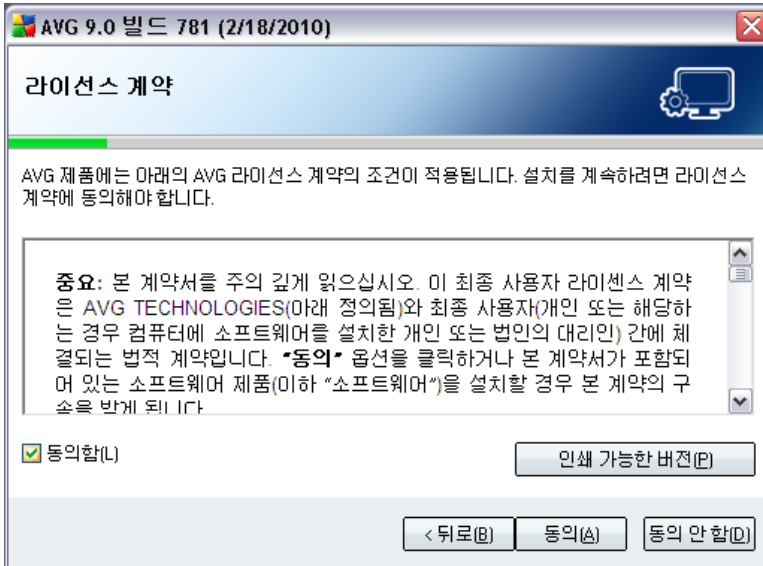
5.1. 설치 시작



설치 프로세스는 **AVG 설치 프로그램 시작** 창에서 시작합니다. 이 창에서 설치 프로세스에 사용될 언어를 선택합니다. 대화 상자 창의 아래쪽에는 **설치 언어 선택** 항목이 있으며 이 항목의 드롭다운 메뉴에서 원하는 언어를 선택합니다. 그리고 나서 **다음** 단추를 눌러 다음 대화 상자를 계속 진행합니다.

주의 : 여기서는 설치 프로세스 전용 언어를 선택합니다. AVG 응용 프로그램 언어는 선택하지 마십시오. 이 언어는 설치 과정에서 나중에 지정할 수 있습니다.

5.2. 라이선스 계약



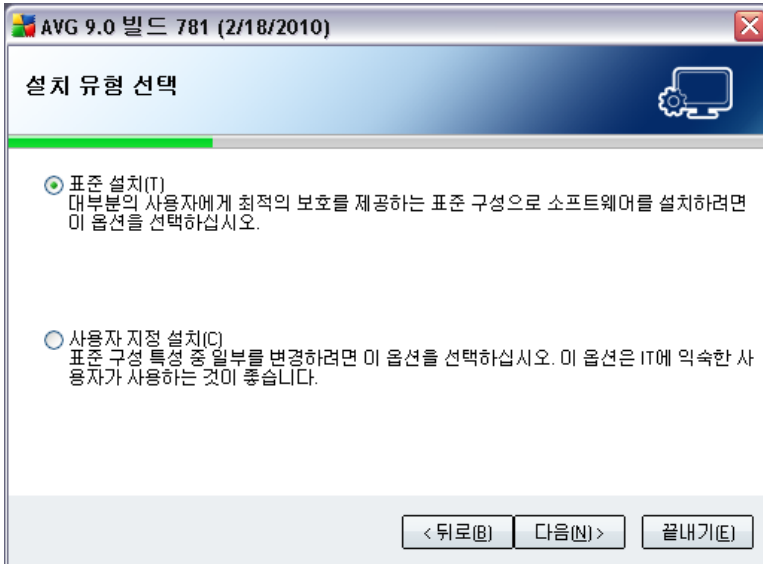
라이선스 계약 대화 상자에는 AVG 라이선스 계약의 전체 내용이 제공됩니다 . 계약 내용을 읽은 후 **동의함** 확인란을 선택하고 **동의** 단추를 눌러 계약 내용을 읽고 이해했으며 동의한다는 의사를 확인해 주십시오 .

라이선스 계약에 동의하지 않을 경우 **동의 안 함** 단추를 누르면 설치 프로세스가 즉시 종료됩니다 .

5.3. 시스템 상태 확인

라이선스 계약을 확인하면 **시스템 상태 확인 중** 대화 상자로 리디렉션됩니다 . 이 대화 상자는 AVG 설치를 시작하기 전에 시스템을 확인 중임을 보여 주는 대화 상자이므로 어떠한 사용자 개입도 필요 없습니다 . 프로세스를 마칠 때까지 기다리십시오 . 프로세스가 끝나면 다음 대화 상자로 자동으로 넘어갑니다 .

5.4. 설치 유형 선택



설치 유형 선택 대화 상자는 **표준** 및 **사용자 지정** 설치 옵션을 제공합니다 .

대부분의 사용자는 프로그램 공급업체에서 미리 정의한 설정을 사용하여 완전 자동 모드로 AVG를 설치하는 **표준 설치** 옵션을 유지하는 것이 좋습니다 . 이 구성은 최적의 리소스 사용률과 최상의 보안 수준을 제공합니다 . 나중에 구성을 변경할 필요가 있는 경우에는 언제든지 AVG 응용 프로그램에서 직접 변경할 수 있습니다 .

사용자 지정 설치 는 AVG를 비표준 설정으로 설치해야 할 타당한 이유가 있는 숙련된 사용자만 사용해야 합니다 . 예를 들면 특정한 시스템 요구 사항에 맞추기 위한 경우가 이에 해당합니다 .

5.5. AVG 라이선스 활성화

AVG 라이선스 활성화 대화 상자에서 등록 데이터를 입력해야 합니다 . 이름 (**사용자 이름** 필드) 및 조직 이름 (**회사 이름** 필드)을 입력합니다 .

그런 다음 **라이선스 번호** 텍스트 필드에 라이선스 / 판매 번호를 입력합니다 . 판매 번호는 **AVG 9 Internet Security** 상자에 들어 있는 CD 패키지에서 확인할 수 있습니다 . 라이선스 번호는 온라인에서 **AVG 9 Internet Security** 제품을 구매한 후에 받은 확인 전자 메일에 있습니다 . 번호를 정확하게 입력해야 합니다 . 라이선스 번호를 **전자 메일을 통해** 디지털 형식으로 제공받은 경우에는 직접 입력하지 말고 복사하여 붙여넣는 것이 좋습니다 .

AVG 9.0 빌드 781 (2/18/2010)

AVG 라이선스 활성화

사용자 이름(U):

회사 이름(C):

라이선스 번호(L):

예: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

온라인으로 소프트웨어를 구입한 경우 라이선스 번호가 전자 메일로 사용자에게 보내집니다. 입력 오류를 방지하려면 라이선스 번호를 전자 메일에서 잘라내어 이 화면으로 붙여 넣는 것이 좋습니다.

소매점에서 이 소프트웨어를 구입한 경우 패키지에 포함된 제품 등록 카드에 라이선스 번호가 나와 있습니다. 번호를 정확하게 복사하십시오.

< 뒤로(B) 다음(N) > 끝내기(F)

다음 단추를 눌러 설치 프로세스를 계속합니다 .

이전 단계에서 표준 설치를 선택한 경우에는 **AVG Security Toolbar 대화 상자**로 직접 **리디렉션됩니다** . 사용자 지정 설치를 선택한 경우에는 **대상 폴더** 대화 상자가 열립니다 .

5.6. 사용자 지정 설치 - 대상 폴더

AVG 9.0 빌드 781 (2/18/2010)

대상 폴더

기본 대상 폴더가 아래에 나와 있습니다. 찾아보기 단추를 클릭하여 다른 폴더를 선택할 수 있지만 기본 설정을 사용하는 것이 좋습니다.

대상 폴더(D):

찾아보기(F)

< 뒤로(B) 다음(N) > 끝내기(F)

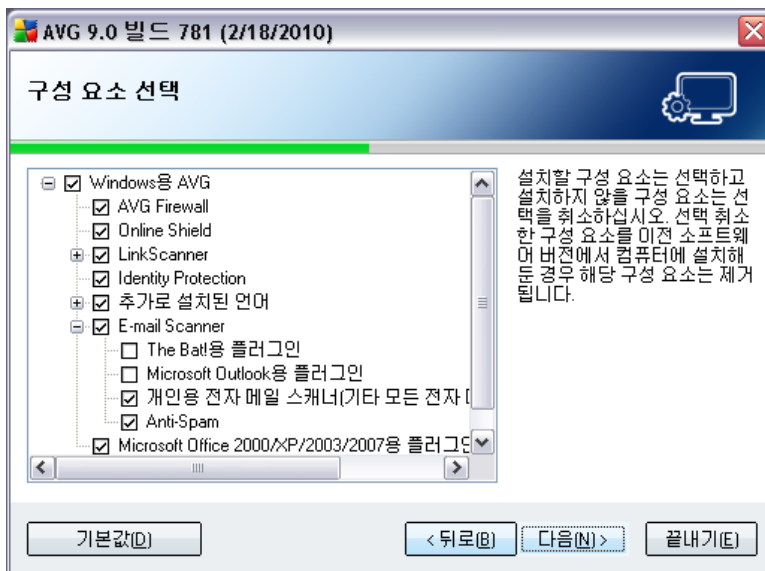


대상 폴더 대화 상자에서 **AVG 9 Internet Security** 응용 프로그램을 설치할 위치를 지정할 수 있습니다. 기본적으로 AVG는 C: 드라이브에 위치한 Program Files 폴더에 설치됩니다. 해당 폴더가 존재하지 않는 경우에는 AVG에서 지금 폴더를 만드는 것에 동의하는지 묻는 새 대화 상자가 나타납니다.

이 위치를 변경하려면 **찾아보기** 단추를 사용하여 드라이브 구조를 표시한 다음 해당 폴더를 선택합니다.

다음 단추를 눌러 계속합니다.

5.7. 사용자 지정 설치 - 구성 요소 선택



구성 요소 선택 대화 상자에서는 설치할 수 있는 모든 **AVG 9 Internet Security** 구성 요소에 대한 개요를 표시합니다. 기본 설정이 사용자에게 맞지 않으면 특정 구성 요소를 제거하거나 추가할 수 있습니다.

그러나 구입한 AVG 버전에 포함된 구성 요소에서만 선택할 수 있습니다. 이러한 구성 요소는 구성 요소 선택 대화 상자 내에서 설치하도록 제공됩니다.

• 언어 선택

설치할 구성 요소 목록에서 AVG를 설치할 언어를 정의할 수 있습니다. **추가로 설치된 언어** 항목을 선택한 다음 해당 메뉴에서 원하는 언어를 선택합니다.

• 전자 메일 스캐너 플러그인

전자 메일 스캐너 항목을 클릭하여 해당 항목을 열고 전자 메일 보안을 유지하기 위해 설치할 플러그인을 결정할 수 있습니다 . 기본적으로 **Microsoft Outlook용 플러그인** 이 설치됩니다 . **Anti-Spam**을 포함하는 라이선스를 구매한 경우 해당 구성 요소가 자동으로 설치됩니다 . 다른 특정 옵션은 **The Bat!용 플러그인** 입니다 . 다른 전자 메일 클라이언트 (*MS Exchange, Qualcomm Eudora* 등)를 사용하는 경우 **개인용 전자 메일 스캐너** 옵션을 설정하여 실행하는 전자 메일 프로그램에 관계없이 전자 메일 통신을 자동으로 보호할 수 있습니다 .

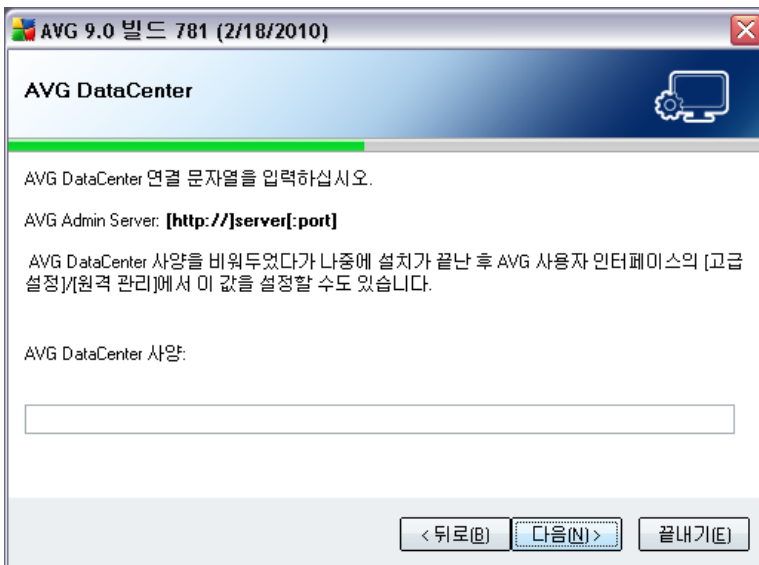
• 원격 관리

나중에 컴퓨터를 AVG Remote Administration에 연결할 계획이라면 해당 항목도 설치되도록 선택하십시오 .

다음 단추를 눌러 계속합니다 .

5.8. AVG DataCenter

AVG 네트워크 라이선스를 사용하고 이전의 **사용자 지정 설치 - 구성 요소 선택** 대화 상자에서 **원격 관리** 항목을 설치하도록 선택한 경우 **AVG DataCenter** 매개 변수를 지정해야 합니다 .



AVG DataCenter 사양 텍스트 필드에 **서버:포트** 형식으로 AVG DataCenter 연결 문자열을 입력합니다 . 아직 이 정보를 모르는 경우에는 필드를 비워두고 나중에 **고급 설정/원격 관리** 대화 상자에서 구성을 설정할 수 있습니다 .

참고 : AVG 원격 관리에 대한 자세한 정보는 AVG Network Edition 사용자 설명서를 참조

하십시오 . 이 설명서는 AVG 웹 사이트 (<http://www.avg.com/>) 에서 다운로드할 수 있습니다.

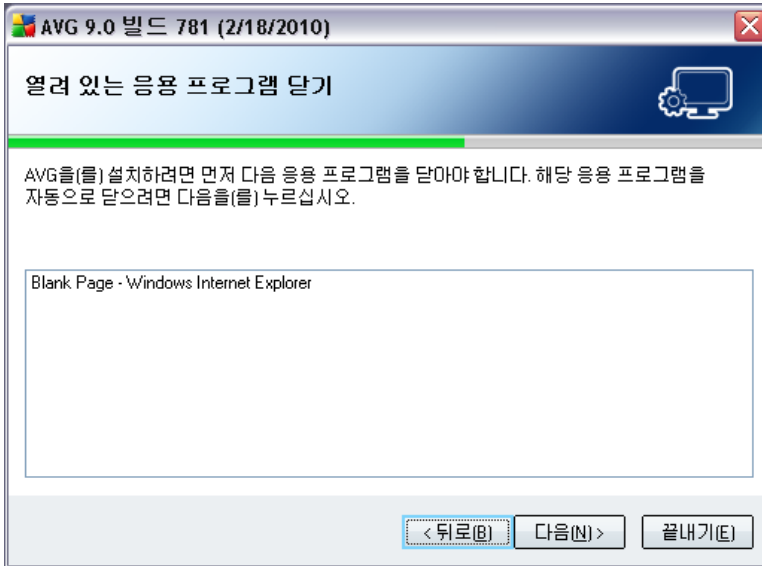
5.9. AVG Security Toolbar



AVG Security Toolbar 대화 상자에서 **AVG Security Toolbar**를 설치할지 결정하십시오 (지원되는 인터넷 검색 엔진의 검색 결과 확인). 기본 설정을 변경하지 않으면 이 구성 요소가 인터넷 브라우저에 자동으로 설치되어 인터넷을 서핑하는 동안 포괄적인 온라인 보호 기능을 사용할 수 있게 됩니다 . 현재 지원되는 브라우저는 Microsoft Internet Explorer 6.0 버전 이상 및 Mozilla Firefox 2.0 버전 이상입니다 .

또한 Yahoo!를 기본 검색 공급자로 선택할지 여부를 결정하는 옵션도 제공됩니다 . Yahoo!를 기본 검색 공급자로 선택하려면 해당 확인란을 선택합니다 .

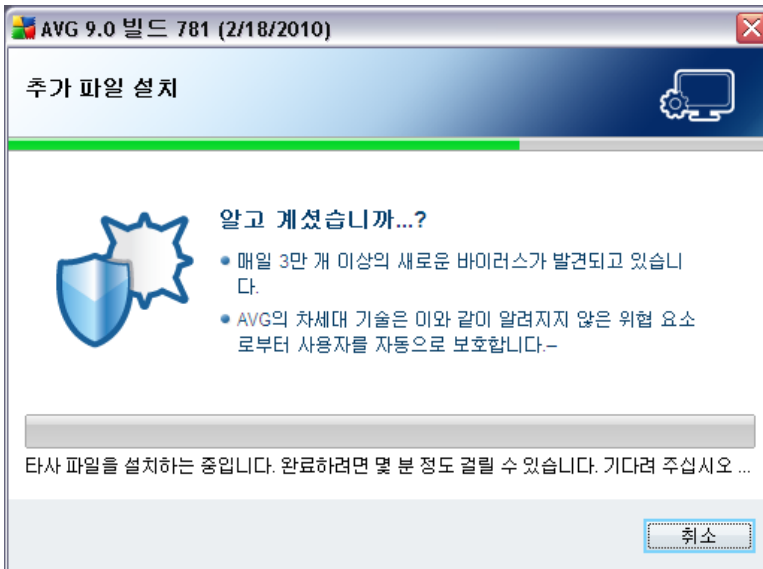
5.10. 열려 있는 응용 프로그램 닫기



열려 있는 응용 프로그램 닫기 대화 상자는 설치 프로세스 동안 컴퓨터에 몇 개의 다른 충돌 프로그램이 실행 중인 경우에만 표시됩니다. 그런 다음 설치 프로세스를 성공적으로 끝내기 위해 닫아야 하는 프로그램 목록이 제공됩니다. 해당 응용 프로그램을 닫고 다음 단계를 계속하는 것에 동의한다면 **다음** 단추를 누르십시오.

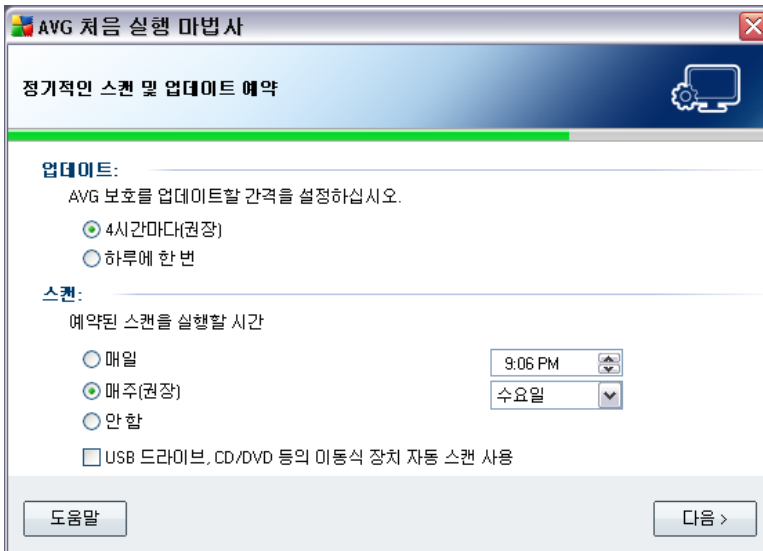
5.11. AVG 설치

AVG 설치 중 대화 상자는 설치 프로세스의 진행률을 보여 주며, 별도의 작업이 필요하지 않습니다.



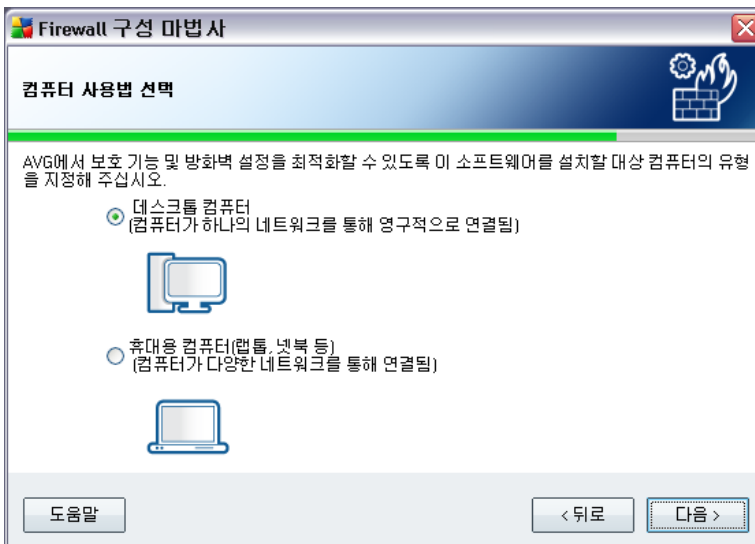
설치 프로세스가 완료되면 자동으로 다음 대화 상자로 이동합니다.

5.12. 정기적 스캔 및 업데이트 예약



정기적 스캔 및 업데이트 예약 대화 상자에서 새로운 업데이트 파일 액세스 가능성 검사를 위한 간격을 설정하고 **예약된 스캔**을 시작할 시간을 정의합니다 . 기본값을 그대로 유지하는 것이 좋습니다 . 계속하려면 **다음** 단추를 누릅니다 .

5.13. 컴퓨터 사용법 선택



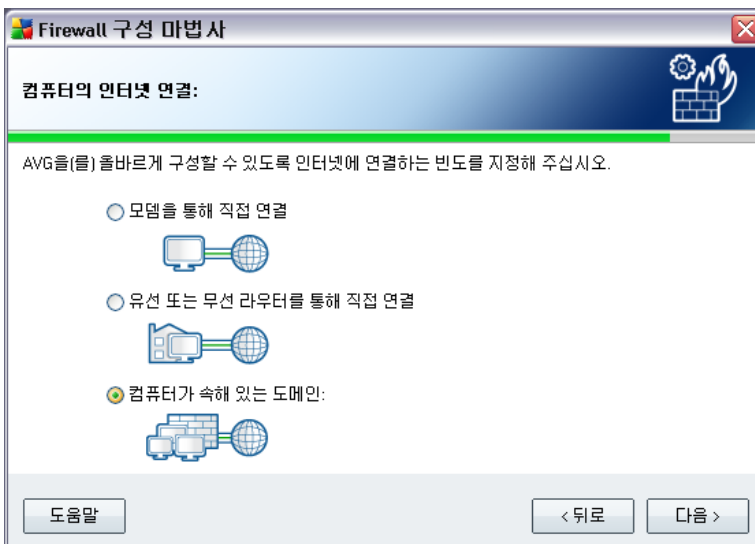
이 대화 상자의 **방화벽 구성 마법사** 에서 어떤 종류의 컴퓨터를 사용하고 있는지 묻는 메시지가 나타납니다 . 예를 들어 **공항, 호텔 객실** 등 다양한 위치에서 인터넷에 연결하는 노트북은 특정 도메인 (**회사 네트워크** 등). 선택한 컴퓨터 사용 유형에 따라 **방화벽** 기본 규칙이 다른 보안 수준으로 정의됩니다 .

다음과 같은 두 가지 옵션 중에서 선택할 수 있습니다 .

- **데스크톱 컴퓨터**
- **휴대용 컴퓨터**

다음 단추를 눌러 선택 항목을 확인하고 다음 대화 상자로 진행합니다 .

5.14. 컴퓨터의 인터넷 연결:



이 대화 상자에서 **방화벽 구성 마법사** 는 컴퓨터의 인터넷 연결 방식을 확인합니다 . 선택한 연결 유형에 따라 **방화벽** 기본 규칙에서 다른 보안 수준이 정의됩니다 .

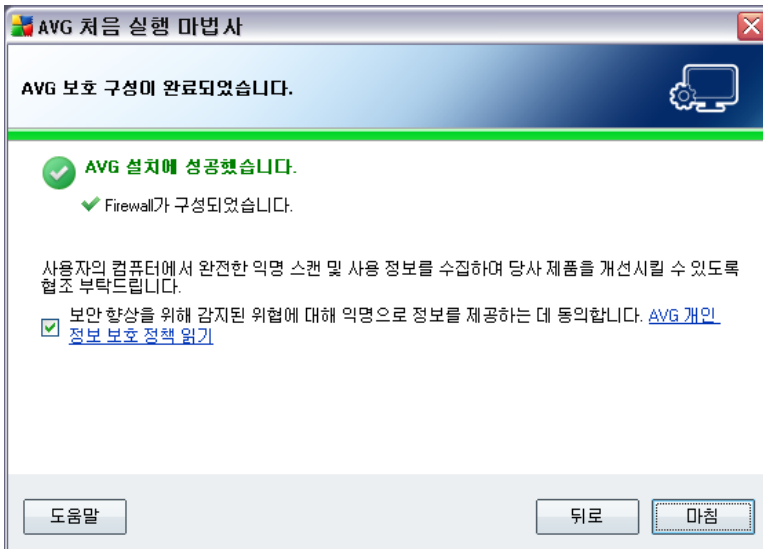
다음과 같은 세 가지 옵션이 있습니다 .

- **모뎀을 통해 직접 연결**
- **유선 또는 무선 라우터를 통해 직접 연결**
- **컴퓨터가 속해 있는 도메인 :**

컴퓨터가 인터넷에 연결하는 방식을 가장 잘 설명하는 연결 유형을 선택합니다 .

다음 단추를 눌러 선택 항목을 확인하고 다음 대화 상자로 진행합니다 .

5.15. AVG 보호 구성이 완료되었습니다 .



이제 **AVG 9 Internet Security** 구성이 완료되었습니다 .

이 대화 상자에서 익스플로잇과 유해 사이트를 익명으로 AVG 바이러스 연구실에 보고할 수 있는 옵션을 사용할 수 있습니다 . 익명 보고를 허용하려면 **내 보안 수준을 항상 시키기 위해서 발견된 위협 요소에 대한 익명 정보를 제공하기로 동의합니다** . 옵션을 선택합니다 .

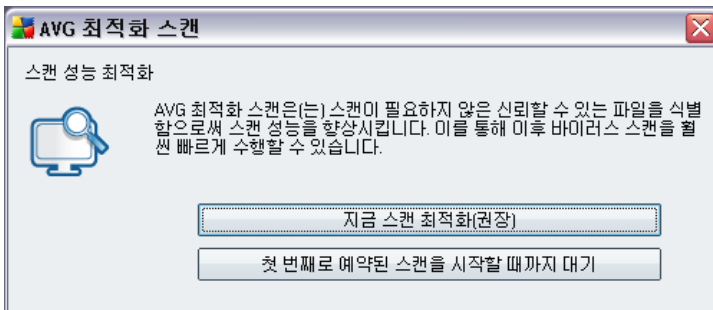
마지막으로 **마침** 단추를 누릅니다 . AVG를 사용하려면 컴퓨터를 다시 시작해야 할 수 있습니다 .

6. 설치 후 작업

6.1. 스캔 최적화

스캔 최적화 기능에서는 적절한 파일 (*.exe, *.dll 및 *.sys 파일)을 탐지하여 이러한 파일에 대한 정보를 저장할 Windows 및 Program files 폴더를 검색합니다. 다음 번 액세스에서는 이러한 파일이 다시 스캔되지 않으므로 스캔 시간이 상당히 줄어듭니다.

설치 프로세스가 끝나면 새 대화 상자 창을 통해 스캔을 최적화할 수 있습니다.



이 옵션을 사용하고 **지금 스캔 최적화** 단추를 눌러 스캔 최적화 프로세스를 실행하는 것이 좋습니다.

6.2. 제품 등록

AVG 9 Internet Security 설치를 마친 후에는 AVG 웹 사이트 (<http://www.avg.com/>)의 **등록** 페이지 (*해당 페이지의 지침 참조*)에서 제품을 온라인으로 등록하십시오. 등록이 끝나면 AVG 사용자 계정, AVG 업데이트 뉴스레터 및 등록된 사용자에게만 제공되는 기타 서비스를 전반적으로 이용할 수 있습니다.

6.3. 사용자 인터페이스 액세스

AVG 사용자 인터페이스 는 다음과 같은 여러 가지 방법으로 액세스할 수 있습니다.

- 시스템 트레이에서 AVG 아이콘 두 번 클릭
- 바탕 화면에서 AVG 아이콘 두 번 클릭
- **시작 / 프로그램 / AVG 9.0 / AVG 사용자 인터페이스 메뉴에서 액세스**

6.4. 전체 컴퓨터 스캔

AVG 9 Internet Security 설치 전에 컴퓨터 바이러스가 이미 사용자 컴퓨터에 전송되었을 위험이 있습니다. 따라서 전체 컴퓨터 스캔을 실행하여 사용자 PC가 감염되지 않았는지 확인해야 합니다.

전체 컴퓨터 스캔 실행 지침은 AVG 스캔 장을 참조하십시오.

6.5. EICAR 테스트

EICAR 테스트를 실행하면 **AVG 9 Internet Security** 제품이 올바르게 설치되었는지 확인할 수 있습니다.

EICAR 테스트는 바이러스 백신 시스템 기능을 테스트하는 데 사용되는 표준 방법으로 매우 안전합니다. EICAR는 실제 바이러스가 아니며 어떠한 바이러스 코드 조각도 포함되어 있지 않으므로 실행해도 안전합니다. 통상적으로 EICAR는 "EICAR-AV-Test"와 같이 분명히 구별되는 이름으로 보고되지만 대부분의 제품은 EICAR가 바이러스인 것처럼 반응합니다. EICAR 웹 사이트 (www.eicar.com)에서 EICAR 바이러스를 다운로드할 수 있으며 해당 사이트에서 EICAR 테스트에 필요한 모든 정보도 확인할 수 있습니다.

ecar.com 파일을 다운로드하고 로컬 디스크에 저장합니다. 테스트 파일 다운로드를 확인하는 즉시 Online Shield가 그에 반응하여 경고 메시지를 표시합니다. 이 알림은 AVG가 사용자 컴퓨터에 올바르게 설치되었는지 여부를 표시합니다.



<http://www.eicar.com> 웹 사이트에서 압축된 버전의 EICAR '바이러스' (예: *ecar_com.zip* 형식)를 다운로드할 수도 있습니다. 상주 보호를 사용하면 이 파일을 다운로드하여 로컬 디스크에 저장할 수 있지만 파일 압축을 풀려고 할 때 상주 보호에서 해당 파일을 '바이러스'로 탐지합니다. AVG가 EICAR 테스트 파일을 바이러스로 식별하는 데 실패할 경우 프로그램 구성을 다시 확인해야 합니다.

6.6. AVG 기본 구성

AVG 9 Internet Security의 기본 구성 (즉, 설치 직후 응용 프로그램이 설정되는 방식) 은 소프트웨어 공급업체에 의해 설정되어 모든 구성 요소 및 기능이 최적의 성능을 낼 수 있도록 조정되어 있습니다 .

특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 .

[AVG 구성 요소](#) 설정 중 일부만 편집하려면 특정 구성 요소 사용자 인터페이스에서 직접 액세스하면 됩니다 . 사용자 요구 사항에 맞춰 AVG 구성을 변경해야 한다면 [AVG 고급 설정](#)으로 이동합니다 . 시스템 메뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

7. AVG 사용자 인터페이스

AVG 9 Internet Security은 (는) 기본 창으로 열립니다 .



기본 창은 여러 섹션으로 나뉩니다 .

- **시스템 메뉴** (창의 상단 시스템 줄)는 모든 AVG 구성 요소 , 서비스 및 기능에 액세스할 수 있는 표준 탐색 메뉴입니다 . - [세부 정보 >>](#)
- **보안 상태 정보** (창의 상단 섹션)에는 AVG 프로그램의 현재 상태에 대한 정보가 나와 있습니다 . - [세부 정보 >>](#)
- **빠른 링크** (창의 왼쪽 섹션)에서는 가장 중요하고 자주 사용하는 AVG 작업에 빠르게 액세스할 수 있습니다 . - [세부 정보 >>](#)

- **구성 요소 개요** (창의 중앙 섹션)에서는 설치된 모든 AVG 구성 요소에 대한 개요를 제공합니다 . - [세부 정보 >>](#)
- **통계** (창의 왼쪽 하단 섹션)에는 프로그램 작업과 관련한 모든 통계 데이터가 나와 있습니다 . - [세부 정보 >>](#)
- **시스템 트레이 아이콘** (모니터 오른쪽 아래 모서리 , 시스템 트레이에 위치)은 AVG 현재 상태를 보여 줍니다 . - [세부 정보 >>](#)

7.1. 시스템 메뉴

시스템 메뉴 는 모든 Windows 응용 프로그램에서 사용되는 표준 탐색 메뉴입니다 . **AVG 9 Internet Security** 기본 창의 맨 위 부분에 가로로 위치합니다 . 시스템 메뉴를 사용하여 특정 AVG 구성 요소 , 기능 및 서비스에 액세스할 수 있습니다 .

시스템 메뉴는 다섯 개의 기본 섹션으로 나뉩니다 .

7.1.1. 파일

- **끝내기** - **AVG 9 Internet Security**의 사용자 인터페이스를 닫습니다 . 그러나 AVG 응용 프로그램은 백그라운드에서 계속 실행되며 사용자 컴퓨터도 지속적으로 보호됩니다 .

7.1.2. 구성 요소

시스템 메뉴의 [구성 요소](#) 항목에는 설치된 모든 AVG 구성 요소에 대한 링크가 포함되어 있습니다 . 이 링크를 누르면 사용자 인터페이스에서 해당 기본 대화 상자 페이지가 열립니다 .

- **시스템 개요** - [설치된 모든 구성 요소 및 해당 상태에 대한 개요가 포함된 기본 사용자 인터페이스 대화 상자로 전환합니다 .](#)
- **Anti-Virus** - [Anti-Virus](#) 구성 요소의 기본 페이지를 엽니다 .
- **Anti-Rootkit** - [Anti-Rootkit](#) 구성 요소의 기본 페이지를 엽니다 .
- **Anti-Spyware** - [Anti-Spyware](#) 구성 요소의 기본 페이지를 엽니다 .
- **방화벽** - [방화벽](#) 구성 요소의 기본 페이지를 엽니다 .
- **Link Scanner** - [Link Scanner](#) 구성 요소의 기본 페이지를 엽니다 .
- **시스템 도구** - [시스템 도구의 기본 페이지를 엽니다 .](#)
- **Anti-Spam** - [Anti-Spam](#) 구성 요소의 기본 페이지를 엽니다 .

- **전자 메일 스캐너** - [전자 메일 스캐너](#) 구성 요소의 기본 페이지를 엽니다 .
- **ID Protection** - [ID Protection](#) 구성 요소의 기본 페이지를 엽니다 .
- **라이선스** - [라이선스](#) 구성 요소의 기본 페이지를 엽니다 .
- **Online Shield** - [Online Shield](#) 구성 요소의 기본 페이지를 엽니다 .
- **상주 보호** - [상주 보호](#) 구성 요소의 기본 페이지를 엽니다 .
- **업데이트 관리자** - [업데이트 관리자](#) 구성 요소의 기본 페이지를 엽니다 .

7.1.3. 기록

- **스캔 결과** - AVG 테스트 인터페이스 , 특히 [스캔 결과 개요](#) 대화 상자로 전환합니다 .
- **상주 보호 검색** - [상주 보호에서 검색한 위협 요소에 대한 개요가 있는 대화 상자를 엽니다 .](#)
- **전자 메일 스캐너 검색** - [전자 메일 스캐너](#) 구성 요소에서 위협 요소로 검색한 전자 메일 메시지 첨부 파일에 대한 개요가 있는 대화 상자를 엽니다
- **Online Shield 검색 결과** - [Online Shield에서 검색한 위협 요소에 대한 개요가 있는 대화 상자를 엽니다 .](#)
- **바이러스 저장소** - 자동으로 치료되지 않는 발견된 감염을 모두 제거하는 검역소 공간 ([바이러스 저장소](#)) 인터페이스를 엽니다 . 이 검역소 내에서 감염된 파일은 별도로 격리되므로 컴퓨터의 안전이 보장되며 , 동시에 감염된 파일은 나중에 복구할 수 있도록 저장됩니다 .
- **이벤트 기록 로그** - 기록된 모든 **AVG 9 Internet Security** 작업에 대한 개요가 있는 기록 로그 인터페이스를 엽니다 .
- **방화벽** - 모든 방화벽 작업에 대한 상세한 개요가 있는 [로그](#) 탭에서 방화벽 설정 인터페이스를 엽니다 .

7.1.4. 도구

- **컴퓨터 스캔** - [AVG 스캔 인터페이스](#) 로 전환하여 전체 컴퓨터 스캔을 실행합니다
- **선택한 폴더 스캔** - [AVG 스캔 인터페이스](#) 로 전환하여 컴퓨터의 트리 구조 내에서 스캔할 파일 및 폴더를 정의할 수 있습니다

- **파일 스캔** - 디스크의 트리 구조에서 선택한 단일 파일에 대해 요청 시 테스트를 실행할 수 있습니다 .
- **업데이트** - 자동으로 업데이트 프로세스를 실행합니다 . **AVG 9 Internet Security**
- **디렉터리에서 업데이트** - 로컬 디스크의 지정된 폴더에 있는 업데이트 파일에서 업데이트 프로세스를 실행합니다 . 하지만 이 옵션은 인터넷에 연결할 수 없는 상황 등의 긴급한 경우에만 사용하는 것이 좋습니다 (예: 컴퓨터가 감염되었고 인터넷 연결이 끊긴 경우, 컴퓨터가 인터넷에 액세스할 수 없는 네트워크에 연결된 경우 등). 새로 열린 창에서 이전에 업데이트 파일을 두었던 폴더를 선택한 다음 업데이트 프로세스를 실행합니다 .
- **고급 설정** - **AVG 고급 설정** 대화 상자가 열리며 여기에서 **AVG 9 Internet Security** 구성을 편집할 수 있습니다 . 일반적으로 소프트웨어 공급업체가 정의한 응용 프로그램의 기본 설정을 유지하는 것이 좋습니다 .
- **방화벽 설정** - **방화벽** 구성 요소의 고급 구성에 대한 독립 실행형 대화 상자가 열립니다 .

7.1.5. 도움말

- **목차** - AVG 도움말 파일을 엽니다 .
- **온라인 도움말 보기** - AVG 웹 사이트 (<http://www.avg.com/>)의 고객 지원 센터 페이지를 엽니다 .
- **AVG 웹** - AVG 웹 사이트 (<http://www.avg.com/>)를 엽니다 .
- **바이러스 및 위협 요소 정보** - 식별된 바이러스에 대한 자세한 정보를 검색할 수 있는 온라인 **바이러스 백과 사전**을 엽니다 .
- **다시 활성화** - **설치 프로세스 중에** AVG 개인 설정 *** 대화 상자에 입력한 데이터를 사용하여 AVG 활성화 *** 대화 상자를 엽니다 . 이 대화 상자에서 판매 번호 (AVG 설치 번호)를 대체하거나 이전 라이선스 번호를 대체 (예: 새 AVG 제품으로 업그레이드하는 경우)할 라이선스 번호를 입력할 수 있습니다 .
- **지금 등록** - AVG 웹 사이트 (<http://www.avg.com/>)의 등록 페이지로 연결합니다 . 등록 데이터를 입력하십시오 . AVG 제품을 등록하는 고객만이 무료 기술 지원을 받을 수 있습니다 .

참고 : **AVG 9 Internet Security** 평가판을 사용 중인 경우 마지막 두 항목이 **지금 구매** 및 **활성화**로 표시되므로 프로그램의 정식 버전을 즉시 구매할 수 있습니다 . 판매 번호로 설치된 **AVG 9 Internet Security**의 경우에는 두 항목이 **등록** 및 **활성화**로 표시됩니다 . 자세한 내용은 이 설명서의 **라이선스** 섹션을 참조하십시오 .

- **AVG 정보** - 프로그램 이름, 프로그램 및 바이러스 데이터베이스 버전, 시스템 정보, 라이선스 계약, **AVG Technologies CZ**의 연락처 정보 등에 대한 데이터가 있는 5개의 탭으로 구성된 **정보** 대화 상자를 엽니다.

7.2. 보안 상태 정보

보안 상태 정보 섹션은 AVG 기본 창의 위쪽 부분에 있습니다. 이 섹션 내에서 사용자는 언제든지 **AVG 9 Internet Security**의 현재 보안 상태에 대한 정보를 확인할 수 있습니다. 이 섹션에 표시되는 아이콘 및 그 의미에 대한 개괄적인 설명을 참조하십시오.



녹색 아이콘은 AVG가 완전하게 기능하고 있음을 나타냅니다. 컴퓨터가 최신 상태로 완벽히 보호되고 있으며 모든 설치된 구성 요소도 제대로 동작하고 있습니다.



주황색 아이콘은 하나 이상의 구성 요소가 잘못 구성되었음을 경고하므로 사용자는 해당 속성 / 설정을 살펴보아야 합니다. 심각한 문제는 아니며 특별한 이유로 사용자가 일부 구성 요소의 설정을 해제했을 수 있습니다. 컴퓨터는 여전히 AVG의 보호를 받습니다. 하지만 문제된 구성 요소의 설정을 살펴보시기 바랍니다. 해당 구성 요소의 이름은 **보안 상태 정보** 섹션에서 확인할 수 있습니다.

이 아이콘은 어떤 이유로 사용자가 구성 요소의 오류 상태를 무시하기로 결정했을 때에도 나타날 수 있습니다. "구성 요소 상태 무시" 옵션은 AVG 기본 창의 구성 요소 개요에 있는 해당 구성 요소의 아이콘을 마우스 오른쪽 단추로 클릭할 때 열리는 상황에 맞는 메뉴에서 사용할 수 있습니다. 특정 상황에서 이 옵션을 사용할 필요가 있을 수 있으나 가능한 한 빨리 "구성 요소 상태 무시" 옵션의 설정을 해제하는 것이 좋습니다.



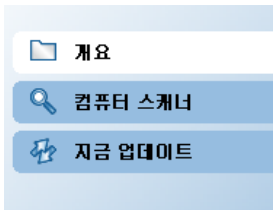
빨간색 아이콘은 AVG가 심각한 상태에 있음을 나타냅니다. 하나 이상의 구성 요소가 올바르게 작동하지 않으므로 AVG가 컴퓨터를 보호할 수 없습니다. 보고된 문제의 해결 방법을 즉시 살펴보시기 바랍니다. 오류를 스스로 해결할 수 없다면 AVG 기술 지원 팀에 문의하십시오.

보안 상태 정보에 주의를 기울여야 하며 보고서에 문제가 표시되는 경우에는 망설이지 말고 즉시 문제 해결을 시도하십시오. 그렇지 않을 경우 컴퓨터가 위험합니다.

참고 : AVG 상태 정보는 시스템 트레이 아이콘에서도 언제든지 확인할 수 있습니다.

7.3. 빠른 링크

빠른 링크 ([AVG 사용자 인터페이스](#) 왼쪽 섹션)를 이용하면 가장 중요하고 많이 사용되는 AVG 기능에 바로 액세스할 수 있습니다 .



- **개요** - 이 링크를 사용하면 현재 열려 있는 AVG 인터페이스가 설치된 모든 구성 요소의 개요가 표시된 화면으로 전환됩니다 . [구성 요소 개요](#) 장을 참조하십시오 . >>
- **컴퓨터 스캐너** - 이 링크를 사용하면 바로 테스트를 실행하고 , 스캔을 예약하고 매개 변수를 편집할 수 있는 AVG 스캔 인터페이스가 열립니다 . [AVG 스캔](#) >>
- **지금 업데이트** - 이 링크를 클릭하면 업데이트 인터페이스가 열리고 AVG 업데이트 프로세스가 바로 실행됩니다 . [AVG 업데이트](#) 장을 참조하십시오 . >>

사용자 인터페이스에서는 항상 이러한 링크에 액세스할 수 있습니다 . 특정한 프로세스를 실행하기 위해 빠른 링크를 사용할 경우 GUI에서 새로운 대화 상자로 전환되지만 빠른 링크는 여전히 화면에 표시됩니다 . 또한 실행되는 프로세스가 알기 쉽게 그래픽으로 표시됩니다 .

7.4. 구성 요소 개요

구성 요소 개요 섹션은 [AVG 사용자 인터페이스](#) 의 가운데 부분에 있습니다 . 이 섹션은 다음 두 부분으로 나뉩니다 .

- 설치된 모든 구성 요소의 개요는 구성 요소 아이콘과 각각의 구성 요소가 활성 상태인지 또는 비활성 상태인지를 보여 주는 정보가 포함된 하나의 패널로 구성되어 있습니다 .
- 선택된 구성 요소에 대한 설명

AVG 9 Internet Security의 구성 요소 개요 섹션에는 다음 구성 요소에 대한 정보가 포함되어 있습니다 .

- **Anti-Virus**는 컴퓨터에 침입하려고 하는 바이러스로부터 컴퓨터를 보호합니다 . - [세부 정보](#) >>

- **Anti-Spyware**는 응용 프로그램을 실행할 때 이를 백그라운드에서 스캔합니다 .
- [세부 정보 >>](#)
- **Anti-Spam**은 모든 들어오는 전자 메일 메시지를 검사하고 원치 않는 전자 메일을 스팸으로 표시합니다 . - [세부 정보 >>](#)
- **방화벽**은 컴퓨터가 인터넷이나 로컬 네트워크에서 다른 컴퓨터와 데이터를 교환하는 방식을 제어합니다 . - [세부 정보 >>](#)
- **Link Scanner**는 인터넷 브라우저에 표시된 검색 결과를 검사합니다 . - [세부 정보 >>](#)
- **Anti-Rootkit**은 맬웨어를 위장하려는 프로그램 및 기술을 검색합니다 . - [세부 정보 >>](#)
- **시스템 도구**는 AVG 환경에 대한 자세한 요약 정보와 운영 체제 정보를 제공합니다 . - [세부 정보 >>](#)
- **전자 메일 스캐너**는 바이러스가 있는지 확인하기 위해 들어오는 메일 및 나가는 메일 모두를 검사합니다 . - [세부 정보 >>](#)
- **ID Protection** - ID 도용자가 개인의 디지털 자산을 훔치지 못하도록 방지하는데 주력하는 맬웨어 백신 구성 요소입니다 . - [세부 정보 >>](#)
- **라이선스**는 라이선스 번호, 유형 및 만료 날짜를 표시합니다 . - [세부 정보 >>](#)
- **Online Shield**는 웹 브라우저에서 다운로드되는 모든 데이터를 스캔합니다 . - [세부 정보 >>](#)
- **상주 보호**는 백그라운드로 실행되며 복사되거나 열리거나 저장되는 파일을 스캔합니다 . - [세부 정보 >>](#)
- **업데이트 관리자**는 모든 AVG 업데이트를 제어합니다 . - [세부 정보 >>](#)

구성 요소 개요에서 특정 구성 요소를 강조 표시하려면 해당 구성 요소 아이콘을 한 번 클릭합니다 . 이와 동시에 구성 요소의 기본 기능 설명이 사용자 인터페이스 하단에 표시됩니다 . 기본 통계 데이터 목록과 함께 구성 요소 자체 인터페이스를 열려면 아이콘을 두 번 클릭합니다 .

상황에 맞는 메뉴를 확장하려면 구성 요소 아이콘을 마우스 오른쪽 단추로 클릭합니다 . 또한 구성 요소 그래픽 인터페이스를 열면 **구성 요소 상태 무시**를 선택할 수도 있습니다 . 이 옵션은 [구성 요소 오류 상태](#)를 알고 있지만 특정 이유로 AVG 상태를 그대로 유지하고 [시스템 트레이 아이콘](#)으로 경고를 표시하지 않으려고 할 때 선택합니다 .

7.5. 통계

통계 섹션은 [AVG 사용자 인터페이스](#)의 왼쪽 아래 부분에 있습니다. 프로그램의 작업에 대한 정보의 목록을 제공합니다.

- **마지막 스캔 날짜** - 마지막으로 스캔이 수행된 날짜를 표시합니다.
- **마지막 업데이트 날짜** - 마지막으로 업데이트가 실행된 날짜를 표시합니다.
- **바이러스 DB** - 현재 설치된 바이러스 데이터베이스의 버전을 알려 줍니다.
- **AVG 버전** - 설치된 AVG 버전을 알려 줍니다. 번호는 9.0.xx 형식으로 지정되며, 9.0은 제품군 버전을, xx는 빌드 번호를 의미합니다.
- **라이선스 만료 날짜** - AVG 라이선스 만료 날짜를 제공합니다.

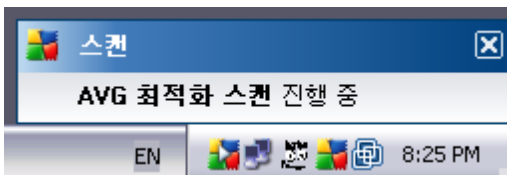
7.6. 시스템 트레이 아이콘

시스템 트레이 아이콘 (Windows 작업 표시줄에 위치)은 **AVG 9 Internet Security**의 현재 상태를 나타냅니다. AVG 기본 창이 열려 있거나 닫혀 있더라도 시스템 트레이에 항상 표시됩니다.

여러 가지 색으로 표시된 의 경우  **시스템 트레이 아이콘**은 모든 AVG 구성 요소가 활성 상태이며 완벽하게 작동하고 있음을 나타냅니다. 또한 AVG가 오류 상태지만 사용자가 이 상황을 파악하고 있으며 일부러 [구성 요소 상태를 무시](#)하기로 결정한 경우에도 AVG 시스템 트레이 아이콘이 여러 가지 색으로 표시될 수 있습니다.

느낌표가 있는 아이콘은  문제가 있음을 나타냅니다 (비활성 구성 요소, 오류 상태 등). **시스템 트레이 아이콘**을 두 번 클릭하여 기본 창을 열고 구성 요소를 편집합니다.

시스템 트레이 아이콘은 현재 AVG의 동작 및 프로그램의 가능한 상태 변화 (예: 예약된 스캔 또는 업데이트의 자동 실행, Firewall 프로파일 전환, 구성 요소의 상태 변화, 오류 상태 발생 등)를 AVG 시스템 트레이 아이콘에서 열리는 팝업 창을 통해 상세하게 알려 줍니다.



또한 아이콘을 두 번 클릭하면 **시스템 트레이 아이콘**을 통해 AVG 기본 창에 빠르게 역



세스할 수 있습니다 . **시스템 트레이 아이콘** 을 마우스 오른쪽 단추로 클릭하면 다음과 같은 옵션이 있는 간략한 상황에 맞는 메뉴가 열립니다 .

- **AVG 사용자 인터페이스 열기** - 클릭하면 [AVG 사용자 인터페이스가 열립니다.](#)
- **업데이트** - 즉시 [업데이트가 시작됩니다.](#)



8. AVG 구성 요소

8.1. Anti-Virus

8.1.1. Anti-Virus 원리

바이러스 백신 소프트웨어의 스캔 엔진은 모든 파일 및 파일 활동 (파일 열기 / 닫기 등) 에서 알려진 바이러스를 스캔합니다 . 발견된 모든 바이러스는 활동할 수 없도록 차단한 후 치료 또는 격리합니다 . 대부분의 바이러스 백신 소프트웨어는 지능형 스캔을 사용하여 파일에서 바이러스 서명이라는 일반적인 바이러스 특성을 스캔합니다 . 따라서 바이러스 백신 스캐너는 알 수 없는 새 바이러스에 기존 바이러스의 일반적인 특성이 있는 경우에 이를 바이러스로 검색할 수 있습니다 .

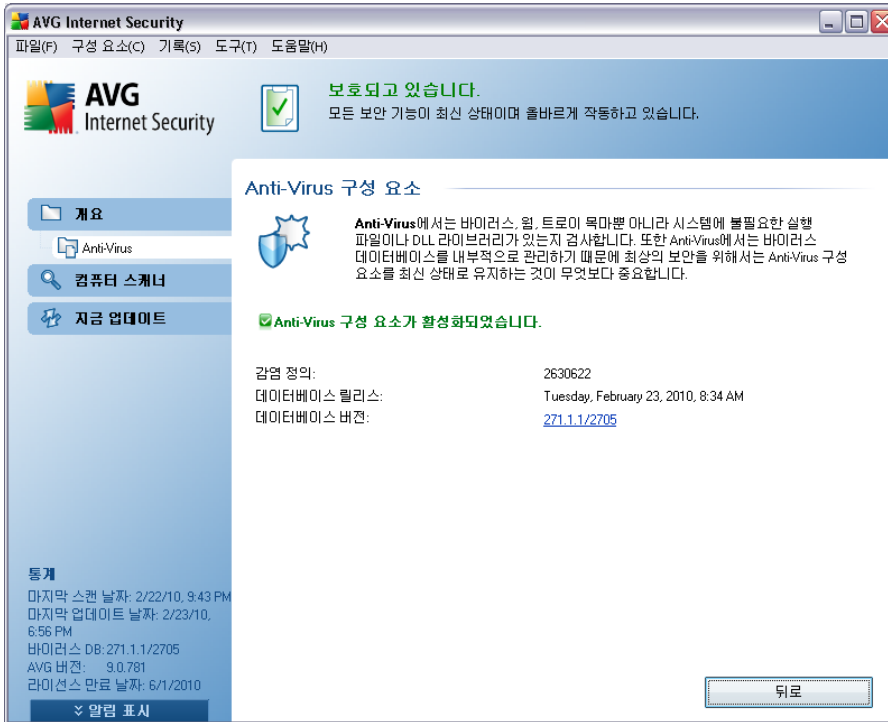
바이러스 백신 보호의 중요한 기능은 알려진 바이러스가 컴퓨터에서 실행되지 못하게 하는 것입니다 .

단일 기술만으로는 바이러스를 검색하거나 식별하기 어려운 경우 **Anti-Virus**는 다음과 같은 여러 기술을 함께 사용하여 사용자의 컴퓨터를 바이러스로부터 보호합니다 .

- 스캔 - 지정된 바이러스의 특성 문자열을 검색합니다 .
- 지능형 분석 - 가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침입니다 .
- 일반 검색 - 지정된 바이러스 / 바이러스 그룹의 지침 특성을 검색합니다 .

AVG는 시스템에서 원치 않는 실행 가능 응용 프로그램 또는 DLL 라이브러리를 분석하고 검색할 수도 있습니다 . 그러한 위협 요소를 원치 않는 프로그램 (다양한 종류의 스파이웨어 , 애드웨어 등)이라고 합니다 . 또한 AVG는 시스템 레지스트리에서 의심스러운 항목, 임시 인터넷 파일 및 추적 쿠키를 스캔하여 다른 감염과 같은 방법으로 잠재적으로 해로운 항목을 모두 처리할 수 있도록 합니다 .

8.1.2. Anti-Virus 인터페이스



Anti-Virus 구성 요소 인터페이스에서는 구성 요소 기능에 대한 몇 가지 기본적인 정보, 구성 요소의 현재 상태 정보 (**Anti-Virus 구성 요소가 활성화되었습니다**) 및 다음과 같은 **Anti-Virus** 통계에 대한 간략한 개요를 확인할 수 있습니다 .

- **감염 정의** - 이 숫자는 최신 바이러스 데이터베이스 버전에 정의된 바이러스 수를 나타냅니다 .
- **최신 데이터베이스 업데이트** - 바이러스 데이터베이스가 마지막으로 업데이트된 시기 및 시간을 지정합니다 .
- **데이터베이스 버전** - 최신 바이러스 데이터베이스 버전 번호를 정의합니다 . 이 번호는 바이러스 데이터베이스가 업데이트될 때마다 증가합니다 .

이 구성 요소 인터페이스에서는 하나의 작동 단추 (**뒤로**)만 사용할 수 있습니다 . 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갈 수 있습니다 .

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다 . 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 . AVG 구성을 변경해야 하는 경우 시스템 메



뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

8.2. Anti-Spyware

8.2.1. Anti-Spyware 원리

스파이웨어는 사용자 모르게 또는 사용자 동의 없이 사용자 컴퓨터에서 정보를 수집하는 일종의 맬웨어 (즉, 소프트웨어)로 정의됩니다 . 일부 스파이웨어 응용 프로그램은 의도적으로 설치할 수 있으며 여기에는 주로 광고 , 창 팝업 또는 다양한 종류의 원치 않는 소프트웨어가 포함됩니다 .

현재 가장 일반적인 감염 출처는 잠재적으로 위험한 콘텐츠가 포함된 웹 사이트라고 할 수 있습니다 . 또한 전자 메일이나 웹 및 바이러스를 통한 기타 전송 방법을 통해서도 감염됩니다 . 이를 위한 가장 효과적인 보호 수단은 항상 켜져 있는 백그라운드 스캐너인 **Anti-Spyware**를 사용하는 것입니다 . Anti-Spyware는 상주 보호처럼 작동하여 실행되는 응용 프로그램을 백그라운드에서 스캔합니다 .

AVG를 설치하기 전에 맬웨어가 이미 컴퓨터에 전송되었거나 최신 **데이터베이스 및 프로그램 업데이트**로 AVG 9 Internet Security [을\(를\) 업데이트하지 못하는 등의 잠재적인 위험 가능성도 있습니다](#) . 따라서 AVG의 스캔 기능을 통해 맬웨어 /스파이웨어가 있는지 컴퓨터를 완전히 스캔할 수 있습니다 . 또한 다운로드되었으나 아직 활성화되지 않은 맬웨어와 같이 대기 중인 비활성 맬웨어도 검색합니다 .

8.2.2. Anti-Spyware 인터페이스



Anti-Spyware 구성 요소 인터페이스에서는 구성 요소 기능에 대한 간략한 개요, 구성 요소의 현재 상태에 대한 정보 (**Anti-Spyware 구성 요소가 활성화되었습니다**) 및 다음과 같은 일부 **Anti-Spyware** 통계를 제공합니다.

- **스파이웨어 정의** - 숫자는 최신 스파이웨어 데이터베이스 버전에 정의된 스파이웨어 샘플 수를 나타냅니다.
- **최신 데이터베이스 업데이트** - 스파이웨어 데이터베이스가 업데이트된 시기 및 시간을 지정합니다.
- **데이터베이스 버전** - 최신 스파이웨어 데이터베이스 버전을 정의합니다. 이 번호는 바이러스 데이터베이스가 업데이트될 때마다 증가합니다.

이 구성 요소 인터페이스에서는 하나의 작동 단추 (**뒤로**)만 사용할 수 있습니다. 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갈 수 있습니다.

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다. AVG 구성을 변경해야 하는 경우 시스템 메

뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

8.3. Anti-Spam

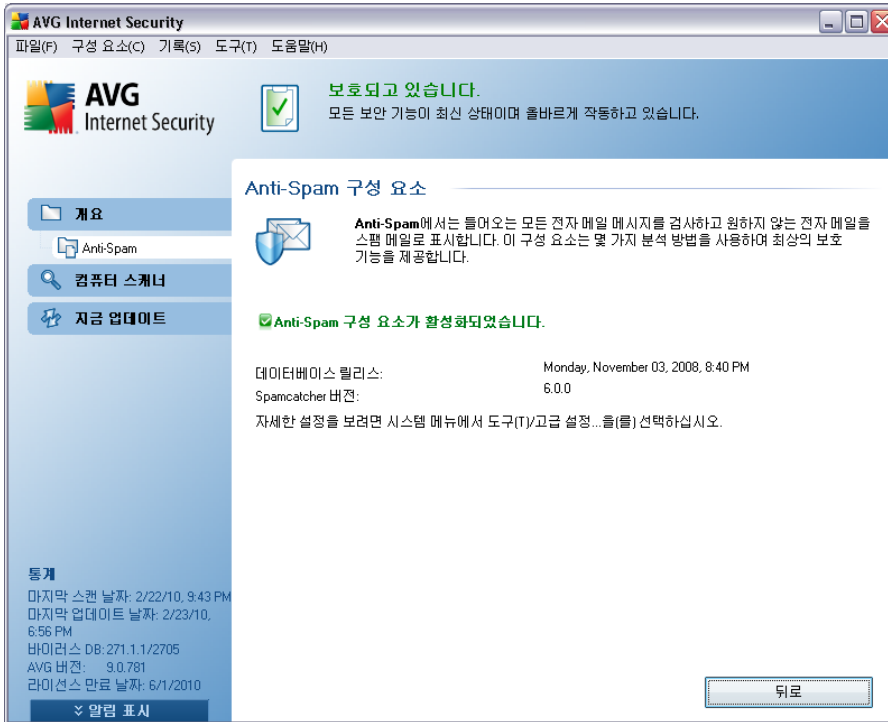
스팸 메일은 대부분 제품 또는 서비스의 광고를 위해 한꺼번에 대량의 전자 메일 주소로 발송되어 수신자의 편지함을 채우는 원치 않는 전자 메일입니다 . 스팸은 소비자의 동의를 얻은 합법적인 상업용 전자 메일과는 다릅니다 . 스팸은 성가실 뿐 아니라 사기성 메일 , 바이러스 또는 공격적 콘텐츠를 포함하는 경우가 많습니다 .

8.3.1. Anti-Spam 원리

Anti-Spam에서는 들어오는 모든 전자 메일 메시지를 검사하고 원치 않는 전자 메일을 스팸 메일로 표시합니다 . **AVG Anti-Spam**에서는 특수한 텍스트 문자열을 추가하여 전자 메일 (스팸으로 식별된 전자 메일)의 제목을 수정할 수 있습니다 . 따라서 전자 메일 클라이언트에서 쉽게 전자 메일을 필터링할 수 있습니다 .

AVG Anti-Spam 구성 요소는 여러 가지 분석 방법을 사용하여 각각의 전자 메일 메시지를 처리하며 원치 않는 전자 메일 메시지에 대해 최대한 모든 보호 기능을 제공합니다 . **AVG Anti-Spam**에서는 스팸을 검색하기 위해 정기적으로 업데이트되는 데이터베이스를 사용합니다 . 또한 [RBL 서버](#) ("알려진 스팸머 " 전자 메일 주소에 대한 공용 데이터베이스)를 사용하거나 [허용 목록](#) (스팸으로 표시 안 함) 및 [차단 목록](#) (항상 스팸으로 표시)에 수동으로 전자 메일 주소를 추가할 수도 있습니다 .

8.3.2. Anti-Spam 인터페이스



Anti-Spam 구성 요소의 대화 상자에서는 구성 요소 기능에 대한 간략한 설명, 구성 요소의 현재 상태에 대한 정보 (**Anti-Spam 구성 요소가**) 및 다음과 같은 통계 수치를 확인할 수 있습니다 .

- **데이터베이스 릴리스** - 스팸 데이터베이스가 업데이트되고 게시된 시기 및 시간을 지정합니다 .
- **Spam catcher 버전** - Anti-Spam 엔진의 최신 버전 번호를 정의합니다 .

이 구성 요소 인터페이스에서는 하나의 작동 단추 (**뒤로**)만 사용할 수 있습니다 . 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갈 수 있습니다 .

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다 . 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 . AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

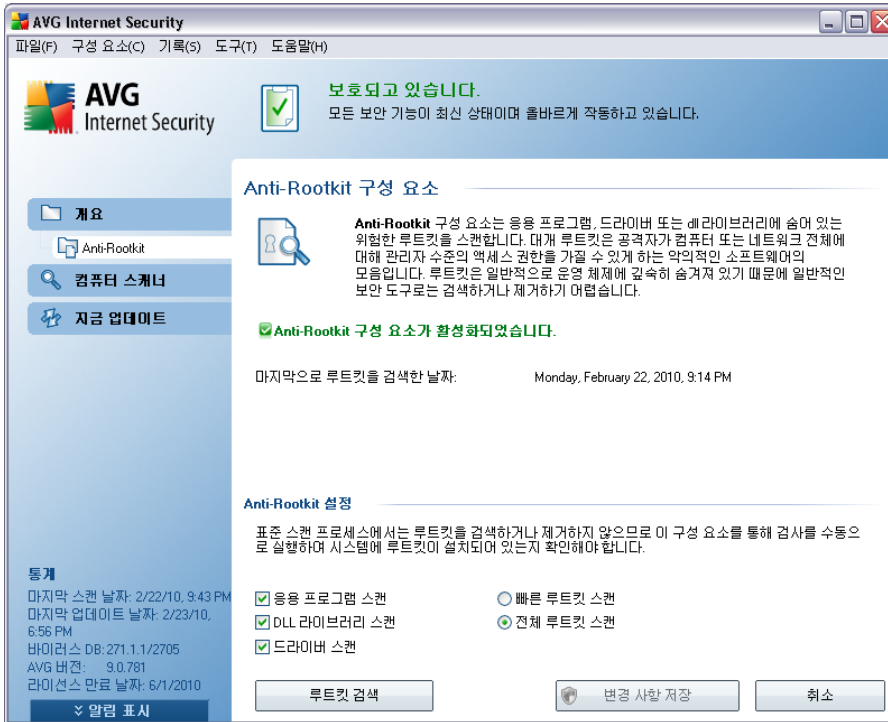
8.4. Anti-Rootkit

루트킷이란 시스템 소유자 및 합법적인 관리자의 허가 없이 컴퓨터 시스템을 근본적으로 제어하도록 설계된 프로그램입니다. 루트킷은 하드웨어에서 실행되는 운영 체제를 제어하므로 하드웨어 자체에 대한 액세스가 필요한 경우는 거의 없습니다. 일반적으로 루트킷은 표준 운영 체제 보안 메커니즘을 파괴하거나 우회함으로써 시스템에서 자신의 존재를 숨깁니다. 많은 경우 루트킷은 사용자를 속여 시스템에서 안전하게 실행할 수 있는 프로그램이라고 믿게 만드는 트로이 목마이기도 합니다. 이를 위해 사용되는 기술로는 모니터링 프로그램으로부터 실행 중인 프로세스를 숨기거나 운영 체제로부터 파일 또는 시스템 데이터를 숨기는 방법이 있습니다.

8.4.1. Anti-Rootkit 원리

AVG Anti-Rootkit은 위험한 루트킷 (즉, 컴퓨터에서 악의적인 소프트웨어의 존재를 위장할 수 있는 프로그램 및 기술)을 검색하고 효과적으로 제거하는 전문적인 도구입니다. **AVG Anti-Rootkit**은 미리 정의된 규칙 집합을 기준으로 루트킷을 검색할 수 있습니다. 모든 루트킷이 검색된다는 점에 주의하십시오 (*감염된 루트킷만 검색되는 것이 아님*). **AVG Anti-Rootkit**에서 루트킷으로 발견했다고 해서 해당 루트킷이 감염되었다는 의미는 아닙니다. 드라이버 또는 정상적인 응용 프로그램의 일부로 루트킷이 사용되는 경우가 있습니다.

8.4.2. Anti-Rootkit 인터페이스



Anti-Rootkit 사용자 인터페이스에서는 구성 요소의 기능에 대한 간략한 설명을 제공하고 구성 요소의 현재 상태에 대해 안내하며 (**Anti-Rootkit 구성 요소가 활성화되었습니다**) **Anti-Rootkit** 테스트가 마지막으로 실행된 시기에 대한 정보도 표시합니다 .

대화 상자의 아래쪽에는 **Anti-Rootkit 설정** 섹션이 있으며 , 여기에서 루트킷 상태 스캔의 기본적인 기능 몇 가지를 설정할 수 있습니다 . 먼저 각 확인란을 선택하여 스캔할 개체를 지정합니다 .

- 응용 프로그램 스캔
- DLL 라이브러리 스캔
- 드라이버 스캔

또한 루트킷 스캔 모드도 선택할 수 있습니다 .

- 빠른 루트킷 스캔 - 모든 실행 중인 프로세스 , 로드된 드라이버 및 시스템 폴더 (일반적으로 c:\Windows)를 스캔합니다 .

- **전체 루트킷 스캔** - 모든 실행 중인 프로세스, 로드된 드라이버 및 시스템 폴더 (일반적으로 c:\Windows)와 모든 로컬 디스크 (플래시 디스크 포함, 플로피 디스크/CD 드라이브 제외)를 스캔합니다.

사용 가능한 제어 단추는 다음과 같습니다.

- **루트킷 검색** - 루트킷 스캔은 [전체 컴퓨터 스캔](#)에 포함된 부분이 아니므로 이 단추를 사용하여 **Anti-Rootkit** 인터페이스에서 직접 루트킷 스캔을 실행할 수 있습니다.
- **변경 사항 저장** - 이 단추를 누르면 이 인터페이스에서 변경한 내용을 모두 저장하고 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갈 수 있습니다.
- **취소** - 이 단추를 누르면 변경한 내용을 저장하지 않고 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갈 수 있습니다.

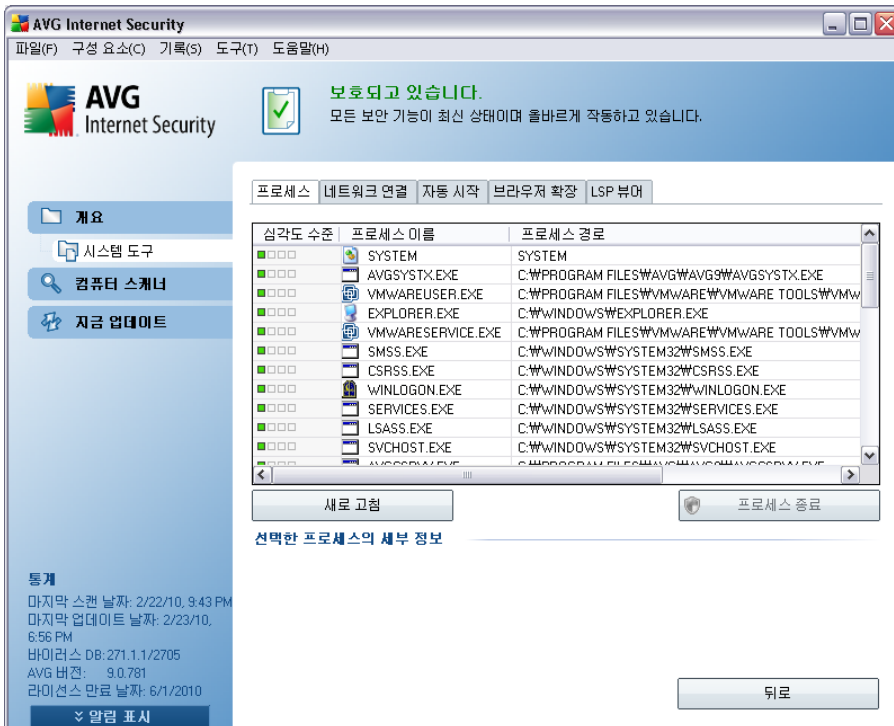
8.5. 시스템 도구

시스템 도구는 **AVG 9 Internet Security** 환경 및 운영 체제에 대한 자세한 요약 정보를 제공하는 도구입니다. 구성 요소에 다음 개요가 표시됩니다.

- [프로세스](#) - 현재 컴퓨터에서 활성 상태인 프로세스 (예: 실행 중인 응용 프로그램)의 목록
- [네트워크 연결](#) - 현재 활성 연결의 목록
- [자동 시작](#) - Windows 시스템을 시작할 때 실행되는 모든 응용 프로그램의 목록
- [브라우저 확장](#) - 인터넷 브라우저에 설치되어 있는 플러그인 (예: 응용 프로그램)의 목록
- [LSP 뷰어](#) - LSP(계층적 서비스 공급자)의 목록

또한 특정 개요를 편집할 수 있지만 이 기능은 고도로 숙련된 사용자만 사용하는 것이 좋습니다.

8.5.1. 프로세스



프로세스 대화 상자에는 현재 컴퓨터에서 활성 상태인 프로세스 목록 (예: 실행 중인 응용 프로그램)이 있습니다. 이 목록은 여러 개의 열로 구분됩니다.

- **심각도 수준** - 관련 프로세스의 심각도를 유해하지 않은 수준 (■□□□)부터 심각한 수준 (■□□■)에 이르기까지 네 단계로 나타내는 그래픽 표시
- **프로세스 이름** - 실행 중인 프로세스의 이름
- **경로** - 실행 중인 프로세스의 실제 경로
- **창** - 해당되는 경우 응용 프로그램 창 이름을 나타냅니다.
- **인터넷** - 실행 중인 프로세스가 인터넷에 연결되어 있는지 여부를 예/아니오로 나타냅니다.
- **서비스** - 실행 중인 프로세스가 서비스인지 여부를 예/아니오로 나타냅니다.
- **PID** - PID(프로세스 식별 번호)는 고유한 Windows 내부 프로세스 ID입니다.

제어 단추

시스템 도구 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **새로 고침** - 현재 상태에 따라 프로세스 목록을 업데이트합니다 .
- **프로세스 종료** - 하나 이상의 응용 프로그램을 선택한 다음 이 단추를 눌러 선택한 응용 프로그램을 종료할 수 있습니다 . **응용 프로그램이 확실하게 실제 위험 요소를 나타내는 경우가 아니라면 응용 프로그램을 종료하지 않는 것이 좋습니다** .
- **뒤로** - 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다 .

8.5.2. 네트워크 연결



네트워크 연결 대화 상자에는 현재 활성화되어 있는 연결 목록이 표시됩니다 . 목록은 다음 열로 구분됩니다 .

- **응용 프로그램** - 연결과 관련된 응용 프로그램 이름입니다 (정보가 제공되지 않는 Windows 2000은 예외)

- **프로토콜** - 연결에 사용되는 전송 프로토콜 유형입니다 .
 - o TCP - IP(인터넷 프로토콜)와 함께 사용되며 인터넷을 통해 정보를 전송하는 프로토콜입니다 .
 - o UDP - TCP 프로토콜을 대체하는 프로토콜입니다 .
- **로컬 주소** - 로컬 컴퓨터의 IP 주소 및 사용되는 포트 번호입니다 .
- **원격 주소** - 원격 컴퓨터의 IP 주소 및 연결된 포트 번호입니다 . 가능한 경우 원격 컴퓨터의 호스트 이름도 찾습니다 .
- **상태** - 가능성이 가장 높은 현재 상태 (연결됨 , 서버 닫기 , 수신 , 자동 닫기 완료 , 수동 닫기 , 자동 닫기)를 나타냅니다 .

외부 연결만 나열하려면 대화 상자 아래쪽의 목록 아래에 있는 **로컬 연결 숨기기** 확인란을 선택합니다 .

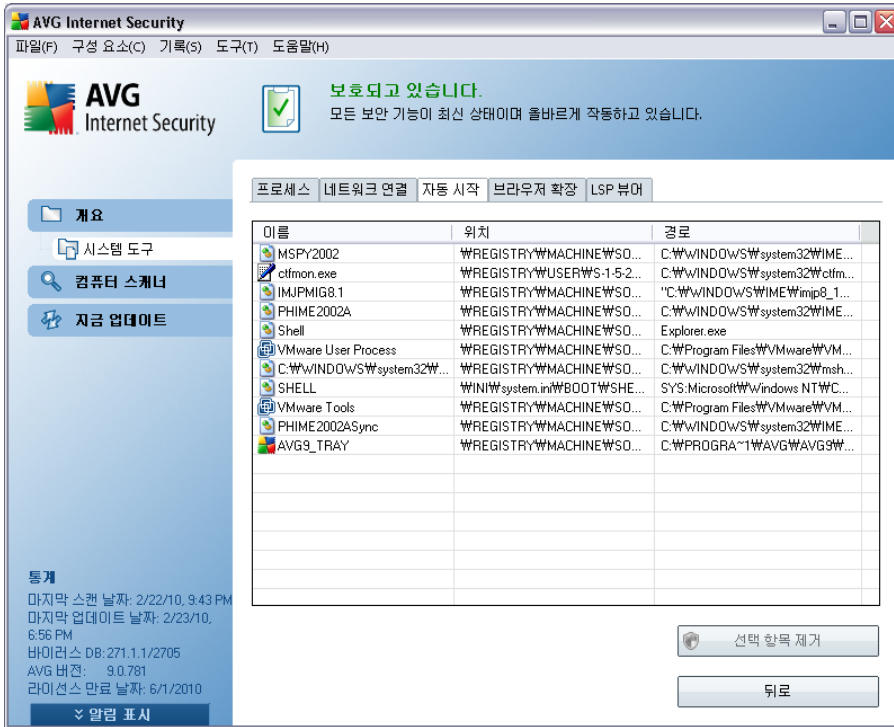
제어 단추

사용할 수 있는 제어 단추는 다음과 같습니다 .

- **연결 종료** - 목록에서 선택된 연결을 닫습니다 .
- **프로세스 종료** - 목록에서 선택한 연결과 관련된 하나 이상의 응용 프로그램을 닫습니다 .
- **뒤로** - 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갑니다 .

현재 연결된 상태인 응용 프로그램만 종료할 수도 있습니다 . 그러나 연결이 확실하게 실제 위협 요소를 나타내는 경우가 아니라면 연결을 종료하지 않는 것이 좋습니다 .

8.5.3. 자동 시작



자동 시작 대화 상자에는 Windows 시스템이 시작되는 동안 실행되는 모든 응용 프로그램 목록이 표시됩니다. 몇몇 맬웨어 응용 프로그램은 빈번하게 시작 레지스트리 항목에 자동으로 추가됩니다.

이들 항목을 선택하고 **선택 항목 제거** 단추를 눌러 삭제할 수 있습니다. **뒤로** 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다.

목록에 있는 응용 프로그램이 확실하게 실제 위협 요소를 나타내는 경우가 아니라면 응용 프로그램을 삭제하지 않는 것이 좋습니다.

8.5.4. 브라우저 확장



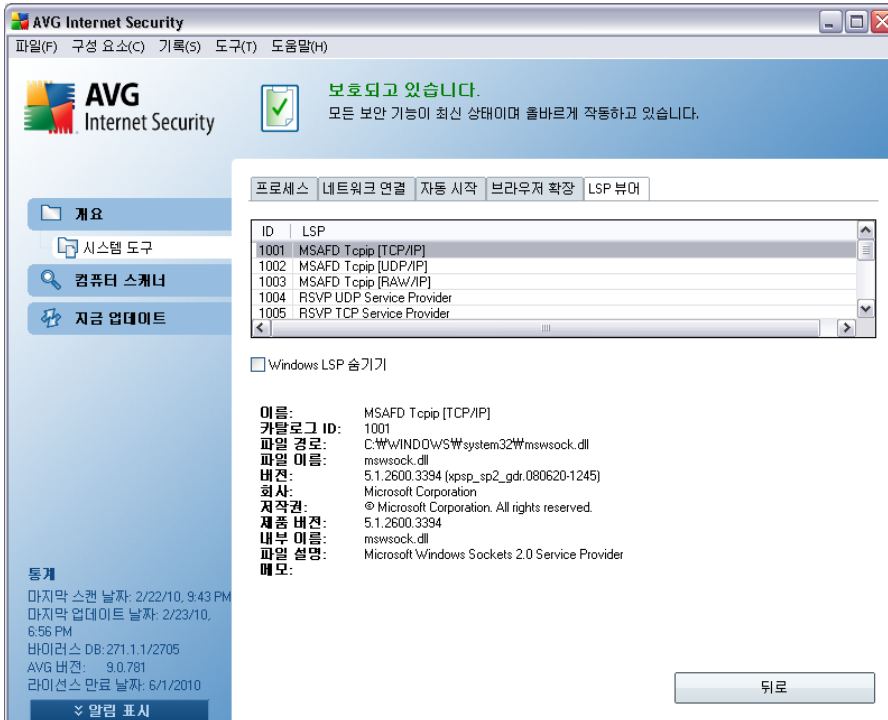
브라우저 확장 대화 상자에는 인터넷 브라우저 내에 설치되어 있는 플러그인 (예: 응용 프로그램) 목록이 포함되어 있습니다. 이 목록에는 정규 응용 프로그램 플러그인뿐 아니라 잠재적인 맬웨어 프로그램이 포함되어 있을 수 있습니다. 목록에서 개체를 클릭하면 대화 상자 하단 섹션에 선택한 플러그인에 대한 자세한 정보가 표시됩니다.

제어 단추

브라우저 확장 탭에서 다음과 같은 제어 단추를 사용할 수 있습니다.

- **선택한 개체 제거** - 현재 목록에서 강조 표시된 플러그인을 제거합니다. 목록에 있는 플러그인이 확실하게 실제 위협 요소를 나타내는 경우가 아니라면 플러그인을 삭제하지 않는 것이 좋습니다.
- **뒤로** - 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다.

8.5.5. LSP 뷰어



LSP 뷰어 대화 상자에는 LSP(계층적 서비스 공급자)의 목록이 표시됩니다.

LSP(계층적 서비스 공급자)는 Windows 운영 체제의 네트워크 서비스에 연결되어 있는 시스템 드라이버입니다. LSP는 컴퓨터에서 들어오고 나가는 모든 데이터에 액세스할 수 있으며 이 데이터를 수정할 수도 있습니다. Windows가 인터넷을 비롯하여 다른 컴퓨터에 연결하려면 몇 가지 LSP가 필요합니다. 그러나 일부 맬웨어 응용 프로그램이 스스로 LSP로 설치되어 사용자 컴퓨터가 전송하는 모든 데이터에 액세스할 수도 있습니다. 그러므로 이러한 검토를 통해 모든 가능한 LSP 위협 요소를 검사하면 도움이 됩니다.

특정한 상황에서는 손상된 LSP를 복구해야 할 수도 있습니다 (예: 파일은 제거되었지만 레지스트리 항목이 그대로 남아 있는 경우). 복구 가능한 LSP가 발견되면 해당 문제를 수정하기 위한 새 단추가 표시됩니다.

목록에 Windows LSP를 포함하려면 **Windows LSP 숨기기** 확인란의 선택을 취소합니다. **뒤로** 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다.

8.6. 방화벽

방화벽은 트래픽을 차단/허용하는 방법으로 두 개 이상의 네트워크 간에 액세스 제어 정책을 적용하는 시스템입니다. 방화벽에는 외부에서 발생한 공격 (일반적으로 인터넷 공격)으로부터 내부 네트워크를 보호하고 각각의 단일 네트워크 포트의 커뮤니케이션을 모두 제어하는 규칙 집합이 포함되어 있습니다. 이러한 커뮤니케이션은 정의된 규칙에 따라 평가된 다음 허용되거나 차단됩니다. 방화벽에서 침입 시도를 인지한 경우 이러한 시도를 "차단"하며 침입자가 컴퓨터에 액세스하지 못하도록 합니다.

방화벽은 정의된 포트를 통해 내부/외부 커뮤니케이션 (양방향 또는 들어오거나 나가는 단방향)을 허용하거나 거부하도록 구성되며, 정의된 소프트웨어 응용 프로그램에 대해서도 마찬가지입니다. 예를 들어, Microsoft Explorer를 사용하여 들어오고 나가는 웹 데이터만 허용하도록 방화벽을 구성할 수 있습니다. 다른 모든 브라우저를 통해 웹 데이터를 전송하려는 시도는 모두 차단됩니다.

방화벽은 개인 식별 정보가 사용자의 허가 없이 사용자 컴퓨터에서 전송되지 않도록 보호합니다. 방화벽은 사용자 컴퓨터가 인터넷 또는 로컬 네트워크의 다른 컴퓨터와 데이터를 교환하는 방법을 제어합니다. 조직 내에서 방화벽은 네트워크의 다른 컴퓨터에 있는 내부 사용자가 공격을 시도할 경우 단일 컴퓨터를 보호해 주는 역할도 합니다.

권장 사항 : 한 컴퓨터에서 여러 개의 방화벽을 사용하는 것은 권장되지 않습니다. 방화벽을 여러 개 설치해도 컴퓨터의 보안이 향상되지 않으며, 두 응용 프로그램 간에 충돌이 발생할 가능성만 많아집니다. 따라서 컴퓨터에서 방화벽 하나만 사용하고 나머지 방화벽은 비활성화하여 충돌 가능성 및 다른 관련 문제를 방지하는 것이 좋습니다.

8.6.1. 방화벽 원리

AVG에서 **방화벽** 구성 요소는 사용자 컴퓨터의 네트워크 포트 상의 모든 트래픽을 제어합니다. 정의된 규칙을 기반으로 **방화벽**은 사용자 컴퓨터에서 실행되며 인터넷/로컬 네트워크에 연결하려는 응용 프로그램이나, 외부에서 사용자 PC에 연결하여 사용자 컴퓨터에 접근하려는 응용 프로그램을 평가합니다. 그런 다음 이러한 각 응용 프로그램에 대해 **방화벽**은 네트워크 포트에서의 커뮤니케이션을 허용하거나 차단합니다. 응용 프로그램이 알려져 있지 않은 경우 (즉, 정의된 **방화벽** 규칙이 없는 경우) **방화벽**은 기본적으로 해당 커뮤니케이션 시도를 허용할 것인지 아니면 차단할 것인지를 사용자에게 물어봅니다.

참고 : AVG Firewall은 서버 플랫폼용이 아닙니다.

AVG Firewall에서 수행할 수 있는 작업

- 알려진 [응용 프로그램](#)의 커뮤니케이션 시도를 자동으로 허용 또는 차단하거나 사용자에게 확인을 요구합니다.

- 사용자의 필요에 따라 미리 정의된 규칙이 포함된 완전한 프로필을 사용합니다.
- 다양한 네트워크에 연결하거나 다양한 네트워크 어댑터를 사용할 때 자동으로 프로필을 전환 합니다.

8.6.2. 방화벽 프로필

방화벽을 사용하면 사용자 컴퓨터가 도메인에 있는지, 독립 실행형 컴퓨터인지 또는 노트북인지에 따라 특정 보안 규칙을 정의할 수 있습니다. ******* 이러한 옵션 각각에는 다른 수준의 보호가 필요하며, 보호 수준은 관련 프로필에 따라 결정됩니다. 간단히 말해 방화벽 프로필은 방화벽 구성 요소의 특정 구성이며 이러한 미리 정의된 구성을 많이 사용할 수 있습니다.

사용 가능한 프로필

- **모두 허용** - 제조업체에서 미리 설정한 방화벽 시스템 프로필이며 항상 존재합니다. 이 프로필이 활성화되면 방화벽 보호 기능이 사용되지 않는 것과 마찬가지로 모든 네트워크 커뮤니케이션이 허용되며 안전 정책 규칙이 전혀 적용되지 않습니다 (즉, 모든 응용 프로그램이 허용되지만 패킷은 계속 확인됩니다. 모든 필터링을 전혀 사용하지 않으려면 방화벽을 사용하지 않도록 설정해야 합니다). 이 시스템 프로필은 복제하거나 삭제할 수 없으며 해당 설정을 수정할 수 없습니다.
- **모두 차단** - 제조업체에서 미리 설정한 방화벽 시스템 프로필이며 항상 존재합니다. 이 프로필이 활성화되면 모든 네트워크 커뮤니케이션이 차단되므로 컴퓨터가 외부 네트워크에 액세스하거나 외부와 커뮤니케이션할 수 없습니다. 이 시스템 프로필은 복제하거나 삭제할 수 없으며 해당 설정을 수정할 수 없습니다.
- **사용자 지정 프로필** :
 - **인터넷에 직접 연결** - 인터넷에 직접 연결된 일반 가정용 데스크톱 컴퓨터 또는 안전한 회사 네트워크 외부에서 인터넷에 연결하는 노트북에 적합합니다. 집에서 연결하거나 중앙 통제가 이루어지지 않는 소규모 회사 네트워크인 경우에 이 옵션을 선택합니다. 또한 출장 중에 위험에 노출될 수 있는 다양한 장소 (예: 인터넷 카페, 호텔)에서 노트북으로 연결하는 경우에도 이 옵션을 선택합니다. 이러한 컴퓨터에는 추가 보호 기능이 없어 최대한의 보호가 필요하다고 간주되기 때문에 더욱 제한적인 규칙이 만들어집니다.
 - **도메인의 컴퓨터** - 학교 또는 회사 네트워크 등 로컬 네트워크의 컴퓨터에 적합합니다. 이러한 네트워크는 다른 추가적인 방법으로 네트워크를

보호하므로 보안 수준이 독립 실행형 컴퓨터보다 낮다고 가정합니다 .

- o **소규모 가정용 또는 사무실 네트워크** - 가정이나 소규모 사무실 같이 "중앙" 관리자 없이 몇 개의 컴퓨터만 연결되어 있는 소규모 네트워크의 컴퓨터에 적합합니다 .

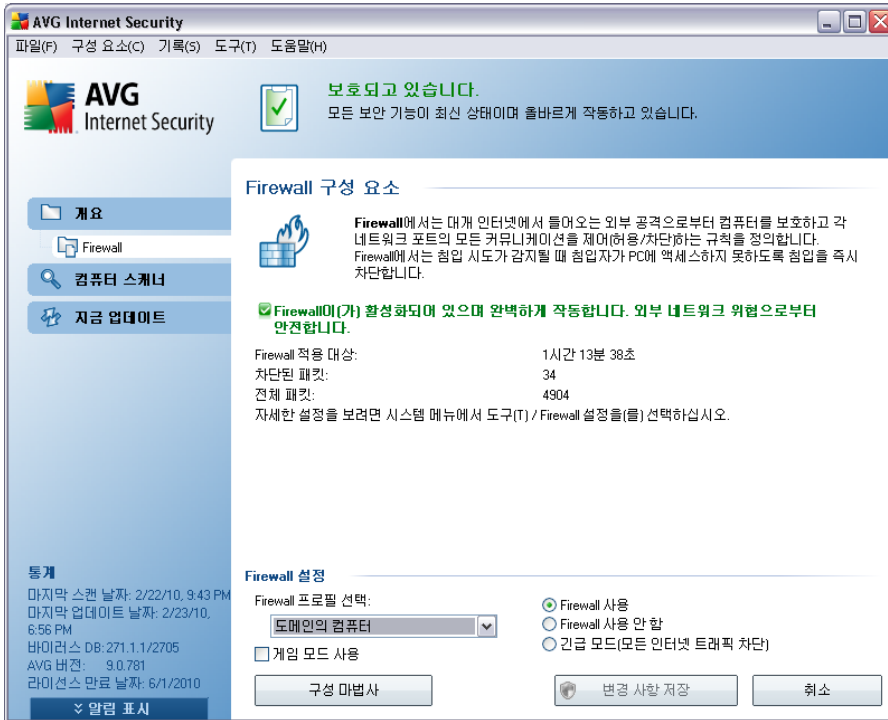
프로필 전환

프로필 전환 기능을 사용하면 특정 네트워크 어댑터를 사용하거나 특정 유형의 네트워크에 연결될 때 **방화벽**이 자동으로 정의된 프로필로 전환됩니다 . 네트워크 영역에 프로필이 할당되어 있지 않으면 다음 번에 해당 영역에 연결할 때 **방화벽**에서 프로필 할당을 요구하는 대화 상자를 표시합니다 .

영역 및 어댑터 프로필 대화 상자에서 모든 로컬 네트워크 인터페이스 또는 영역에 프로필을 할당하고 세부 설정을 지정할 수 있으며 , 이 기능을 원하지 않는 경우 사용하지 않도록 설정할 수도 있습니다 . *이렇게 하면 모든 종류의 연결에 기본 프로필이 사용됩니다.*

일반적으로 , 노트북을 가지고 있으면서 다양한 유형의 연결을 사용하는 사용자에게 이 기능이 유용합니다 . 데스크톱 컴퓨터를 가지고 있으면서 한 가지 유형의 연결만 사용하는 경우에는 (예: 인터넷에 대한 케이블 연결) 프로필 전환을 사용할 일이 거의 없으므로 이 기능이 필요 없습니다 .

8.6.3. 방화벽 인터페이스



방화벽 인터페이스에서는 해당 구성 요소의 기능에 대한 기본 정보 및 **방화벽** 통계에 대한 간략한 개요를 제공합니다 .

- **방화벽 적용 대상** - 방화벽이 마지막으로 시작된 후 경과된 시간입니다 .
- **차단된 패킷** - 확인된 전체 패킷 중 차단된 패킷의 개수입니다 .
- **전체 패킷** - 방화벽 실행 중 검사된 모든 패킷의 개수입니다 .

기본 구성 요소 구성

- **방화벽 프로필 선택** - 롤다운 메뉴에서 정의된 프로필 중 하나를 선택합니다 . 항상 두 가지 프로필이 제공됩니다 (기본 프로필인 **모두 허용** 및 **모든 차단**). 기타 프로필은 [방화벽 설정](#)의 [프로필](#) 대화 상자에서 프로필을 편집하여 수동으로 추가합니다 .
- **게임 모드 사용** - 이 옵션을 선택하면 전체 화면 응용 프로그램 (게임, PowerPoint 프레젠테이션 등)이 실행 중일 때 [방화벽](#)에서 알 수 없는 응용 프로

그럼과의 커뮤니케이션을 허용할지 아니면 차단할지를 묻는 대화 상자를 표시하지 않습니다. 그 시점에 알 수 없는 응용 프로그램이 네트워크를 통해 커뮤니케이션하려고 시도하면 [방화벽](#)에서 현재 프로필의 설정에 따라 그러한 시도를 자동으로 허용하거나 차단합니다.

• **방화벽 상태는 다음과 같습니다.**

- **방화벽 사용** - 이 옵션을 선택하면 선택한 [방화벽](#) 프로필에 정의된 규칙 집합에서 "허용"으로 지정된 해당 응용 프로그램과 커뮤니케이션할 수 있습니다.
- **방화벽 사용 안 함** - 이 옵션은 [방화벽](#)을 완전히 사용하지 않도록 설정하여 모든 네트워크 트래픽이 허용되나 검사되지는 않습니다.
- **긴급 모드 (모든 인터넷 트래픽 차단)** - 이 옵션을 선택하면 각 단일 네트워크 포트의 트래픽이 모두 차단됩니다. [방화벽](#)은 계속 실행되지만 모든 네트워크 트래픽은 중지됩니다.

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다. 방화벽 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 방화벽 설정**을 선택하고 새로 열린 [방화벽 설정](#) 대화 상자에서 방화벽 구성을 편집합니다.

제어 단추

- **구성 마법사** - 이 단추를 누르면 [방화벽](#) 구성 요소 구성을 지정할 수 있는 [컴퓨터 사용법 선택](#)이라는 관련 대화 상자 (**설치 프로세스에서 사용됨**)로 전환됩니다.
- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다.
- **취소** - 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (**구성 요소 개요**)로 돌아갑니다.

8.7. 전자 메일 스캐너

바이러스 및 트로이 목마가 유입되는 가장 일반적인 원인 중 하나는 전자 메일입니다. 피싱 및 스팸은 그러한 전자 메일의 위험성을 더욱 증가시키는 요소가 되고 있습니다. 무료 전자 메일 계정은 스팸 방지 기술을 거의 사용하지 않으므로 악성 전자 메일이 전달될 확률이 높으며, 개인 사용자의 경우 그러한 전자 메일을 많이 사용합니다. 또한 알 수 없는 사이트를 서핑하고 개인 데이터 (예: 전자 메일 주소)를 온라인 양식에 입력하

는 개인 사용자들의 경우 전자 메일을 통한 공격에 노출될 가능성이 높습니다 . 기업에서는 일반적으로 이러한 위험을 줄이기 위해 회사 전자 메일 계정을 사용하고 스팸 방지 필터 등을 적용합니다 .

8.7.1. 전자 메일 스캐너 원리

전자 메일 스캐너 구성 요소가 자동으로 들어오고 나가는 전자 메일을 스캔합니다 . Outlook Express, Mozilla, Incredimail 등과 같이 AVG의 고유한 플러그인이 없는 전자 메일 클라이언트에서 이 구성 요소를 사용할 수 있습니다 .).

AVG [설치](#) 중에 전자 메일을 제어하기 위한 자동 서버가 만들어집니다 . 하나는 들어오는 전자 메일을 확인하기 위한 서버이고 다른 하나는 나가는 전자 메일을 확인하기 위한 서버입니다 . 이 두 서버를 사용하면 포트 110 및 25(전자 메일 송/수신을 위한 표준 포트)에서 자동으로 전자 메일이 확인됩니다 .

전자 메일 스캐너 는 인터넷에서 전자 메일 클라이언트와 전자 메일 서버 간의 인터페이스로 작동합니다 .

- **들어오는 메일** : 서버에서 메시지를 받는 동안 **전자 메일 스캐너** 구성 요소가 메시지에 바이러스가 있는지 테스트하고 감염된 첨부 파일을 제거하며 인증을 추가합니다 . 발견된 바이러스는 즉시 [바이러스 저장소](#)로 이동됩니다 . 그런 다음 메시지가 전자 메일 클라이언트로 전달됩니다 .
- **나가는 메일** : 메시지가 전자 메일 클라이언트에서 전자 메일 스캐너로 전송됩니다 . 전자 메일 스캐너는 메시지와 첨부 파일에 바이러스가 있는지 테스트한 후 메시지를 SMTP 서버로 전송합니다 (나가는 전자 메일의 스캔은 기본적으로 비활성화되어 있으며 수동으로 설정할 수 있음).

참고 : AVG 전자 메일 스캐너는 서버 플랫폼용이 아닙니다 .

8.7.2. 전자 메일 스캐너 인터페이스



전자 메일 스캐너 구성 요소 대화 상자에서는 구성 요소 기능에 대한 간략한 설명, 구성 요소의 현재 상태에 대한 정보 (전자 메일 스캐너가 활성화되었습니다) 및 다음과 같은 통계 수치를 확인할 수 있습니다.

- **스캔한 총 전자 메일 수 - 전자 메일 스캐너**가 마지막으로 시작된 후 스캔된 전자 메일 메시지의 개수입니다. (필요한 경우 이 값은 다시 설정할 수 있습니다(예: 통계를 위한 값 다시 설정)).
- **발견되거나 차단된 위협 요소 수 - 전자 메일 스캐너**가 마지막으로 시작된 후 전자 메일 메시지에서 발견된 감염 수입니다.
- **설치되어 있는 전자 메일 보호 기능** - 사용자 컴퓨터에 기본으로 설치된 전자 메일 클라이언트와 관련된 특정 전자 메일 보호 플러그인에 대한 정보입니다.

기본 구성 요소 구성

대화 상자의 아래쪽 부분에서 구성 요소 기능 중 일부 기본 기능을 편집할 수 있는 **전자 메일 스캐너 설정**이라는 섹션을 찾을 수 있습니다.

- **들어오는 메시지 스캔** - 사용자 계정에서 수신한 모든 전자 메일에 대해 바이러스를 스캔하도록 지정하려면 이 항목을 선택합니다 . 이 항목은 기본적으로 사용되며 , 이 설정을 변경하지 않는 것이 좋습니다 .
- **나가는 메시지 스캔** - 사용자 계정에서 발송한 모든 전자 메일에 대해 바이러스를 스캔하게 하려면 이 항목을 선택합니다 . 기본적으로 이 항목은 사용되지 않습니다 .
- **전자 메일을 스캔하는 동안 알림 아이콘 표시** - [전자 메일 스캐너](#) 구성 요소를 통해 메일을 스캔하는 동안 시스템 트레이의 AVG 아이콘 위에 표시되는 알림 대화 상자를 통해 정보를 받으려면 이 항목을 선택합니다 . 이 항목은 기본적으로 사용되며 , 이 설정을 변경하지 않는 것이 좋습니다 .

시스템 메뉴의 **도구 / 고급 설정** 항목을 통해 **전자 메일 스캐너** 구성 요소의 고급 구성에 액세스할 수 있습니다 . 그러나 숙련된 사용자가 아닌 경우에는 고급 구성을 사용하지 않는 것이 좋습니다 .

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다 . 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 . AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

제어 단추

전자 메일 스캐너 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다 .
- **취소** - 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갑니다 .

8.7.3. 전자 메일 스캐너 검색



기록 / 전자 메일 스캐너 검색 시스템 메뉴 옵션을 통해 액세스할 수 있는 전자 메일 스캐너 검색 대화 상자에서는 전자 메일 스캐너 구성 요소에서 발견된 모든 결과 목록을 볼 수 있습니다. 발견된 각 개체에 대해 다음 정보가 제공됩니다.

- **감염** - 발견된 개체에 대한 설명 (및 이름)
- **개체** - 개체 위치
- **결과** - 발견된 개체에 수행된 작업
- **검색 시간** - 의심스러운 개체가 발견된 날짜 및 시간
- **개체 유형** - 발견된 개체의 유형

대화 상자의 아래쪽 부분의 목록에서 위에 나와 있는 발견된 개체의 총 개수를 확인할 수 있습니다. 또한 발견된 개체의 전체 목록을 파일로 내보내고 (**파일로 목록 내보내기**), 발견된 개체의 모든 항목을 삭제 (**목록 비우기**) 할 수 있습니다.

제어 단추

전자 메일 스캐너 검색 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **목록 새로 고침** - 발견된 위협 요소 목록을 업데이트합니다 .
- **뒤로** - 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다 .

8.8. ID Protection

AVG Identity Protection은 ID 도용자가 사용자 PC를 대상으로 하는 모든 종류의 악의적인 소프트웨어 (*맬웨어*)를 통해 사용자의 암호, 은행 계좌 정보, 신용 카드 번호 및 기타 개인 디지털 자산의 도난을 방지하는 데 주력하는 맬웨어 백신 제품입니다 . 또한, PC에서 실행되는 모든 프로그램이 올바르게 작동하도록 보호합니다 . **AVG Identity Protection**은 지속적으로 의심스러운 동작을 검색하고 차단하며 컴퓨터를 새로운 모든 맬웨어로부터 보호합니다 .

8.8.1. ID Protection 원리

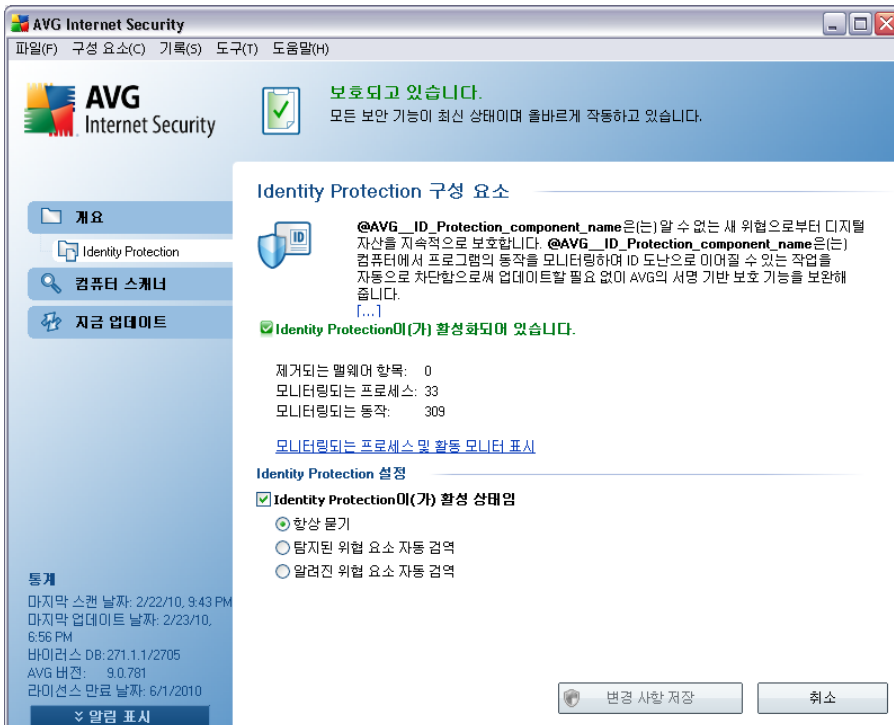
AVG Identity Protection은 맬웨어 백신 구성 요소로, 동작 분석 기술을 사용하여 모든 종류의 맬웨어 (*스파이웨어* , *봇* , *ID 도난* 등)를 차단하며 새로운 바이러스에 대한 제로 데이 보호 기능을 제공합니다 . 맬웨어는 정교해지고 있으며, ID를 도난하려는 원격 공격자에게 PC를 노출할 수 있는 정상적인 프로그램의 형태로 나타나고 있습니다 . **AVG Identity Protection**은 이러한 새로운 실행 기반 맬웨어로부터 사용자를 보호합니다 . 이는 서명 메커니즘과 스캔을 사용하여 파일 기반 바이러스와 알려진 바이러스를 차단하는 [AVG Anti-Virus](#)를 보완하는 보호 기능입니다 .

PC를 완벽하게 보호하려면 [AVG Anti-Virus](#)와 **AVG Identity Protection** 구성 요소를 모두 설치하는 것이 좋습니다 .

8.8.2. ID Protection 인터페이스

Identity Protection 구성 요소 인터페이스에는 구성 요소의 기본적인 기능에 대한 간략한 설명, 구성 요소 상태 (*AVG Identity Protection이 활성화되었으며 모든 기능이 작동합니다* .) 및 몇 가지 통계 데이터가 표시됩니다 .

- **제거되는 맬웨어 항목** - 맬웨어로 검색되어 제거된 응용 프로그램의 수
- **모니터링되는 프로세스** - IDP에서 모니터링되고 있는 현재 실행 중인 응용 프로그램의 수
- **모니터링되는 동작** - 모니터링되는 응용 프로그램 내에서 실행되고 있는 특정 동작의 수



기본 구성 요소 구성

대화 상자의 아래쪽 부분에서 구성 요소 기능 중 일부 기본 기능을 편집할 수 있는 **Identity Protection 설정** 섹션을 찾을 수 있습니다 .

- **Identity Protection이 활성화되었습니다** . - (기본적으로 설정되어 있음): IDP 구성 요소를 활성화하고 자세한 편집 옵션을 열려면 선택합니다 .

Identity Protection에서 일부 정상적인 파일을 의심스러운 파일이나 위험한 파일로 보고하는 경우가 있습니다 . **Identity Protection**은 동작을 기준으로 위협 요소를 검색하기 때문에 프로그램이 키보드 작동을 모니터링하거나 , 컴퓨터에 다른 프로그램이나 새 드라이버를 설치하려는 경우 이러한 현상이 발생할 수 있습니다 .

따라서 다음 옵션 중 하나를 선택하여 의심스러운 활동이 감지된 경우를 대비한 **Identity Protection** 구성 요소의 동작을 지정해야 합니다 .

- **항상 묻기** - 응용 프로그램이 맬웨어로 탐지된 경우 항상 사용자에게 차단 여부를 묻습니다 (이 옵션은 기본적으로 설정되어 있으며 특별한 이유가 없다면 변경하지 않는 것이 좋음) .

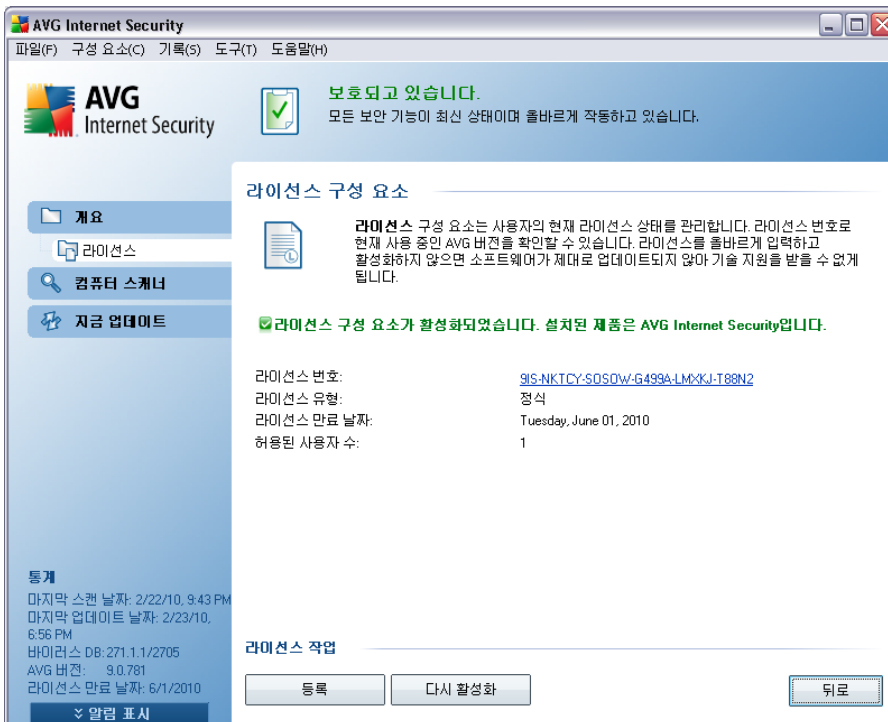
- **발견된 위협 요소 자동 검역** - 맬웨어로 감지된 모든 응용 프로그램을 자동으로 차단합니다 .
- **알려진 위협 요소 자동 검역** - 탐지된 응용 프로그램이 맬웨어라고 확신되는 경우에만 해당 응용 프로그램을 차단합니다 .

제어 단추

Identity Protection 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다 .
- **취소** - 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갑니다 .

8.9. 라이선스



라이선스 구성 요소 인터페이스에서는 구성 요소 기능에 대한 간략한 설명 , 구성 요소

의 현재 상태에 대한 정보 (라이선스 구성 요소가 활성화되었습니다) 및 다음과 같은 정보를 확인할 수 있습니다 .

- **라이선스 번호** - 정확한 형식의 라이선스 번호를 제공합니다 . 라이선스 번호를 입력할 때는 번호가 정확해야 하며 화면에 표시된 것과 똑같이 입력해야 합니다 . 따라서 라이선스 번호를 조작할 때에는 항상 "복사하여 붙여넣기 " 방법을 사용하는 것이 좋습니다 .
- **라이선스 유형** - 설치된 제품 유형을 지정합니다 .
- **라이선스 만료 날짜** - 이 날짜에 따라 라이선스의 유효 기간이 결정됩니다 . 이 날짜 이후에 **AVG 9 Internet Security** 제품을 계속 사용하려면 라이선스를 갱신해야 합니다 . 라이선스 갱신은 AVG 웹 사이트 (<http://www.avg.com/>)에서 온라인으로 수행할 수 있습니다 .
- **허용된 사용자 수** - **AVG 9 Internet Security** 제품을 설치할 수 있는 워크스테이션의 개수입니다 .

제어 단추

- **등록** - AVG 웹 사이트 (<http://www.avg.com/>)의 등록 페이지로 연결됩니다 . 등록 데이터를 입력하십시오 . AVG 제품을 등록하는 고객만이 무료 기술 지원을 받을 수 있습니다 .
- **다시 활성화** - **설치 프로세스** 중 AVG 개인 설정 *** 대화 상자에 입력한 데이터를 사용하여 AVG 활성화 *** 대화 상자를 엽니다 . 이 대화 상자에서 판매 번호 (AVG 설치 번호)를 대체하거나 이전 라이선스 번호를 대체 (예: 새 AVG 제품으로 업그레이드하는 경우)할 라이선스 번호를 입력할 수 있습니다 .

참고 : **AVG 9 Internet Security** 평가판을 사용 중인 경우 단추가 **지금 구매 및 활성화** 로 표시되므로 프로그램의 정식 버전을 즉시 구매할 수 있습니다 . 판매 번호로 설치된 **AVG 9 Internet Security**의 경우에는 단추가 **등록 및 활성화** 로 표시됩니다 .

- **뒤로** - 이 단추를 누르면 기본 AVG 사용자 인터페이스 (구성 요소 개요)로 돌아갑니다 .

8.10. Link Scanner

8.10.1. Link Scanner 원리

LinkScanner 구성 요소는 웹 브라우저나 웹 브라우저 플러그인을 사용하여 컴퓨터에 맬웨어를 설치하도록 고안된 웹 사이트로부터 사용자를 보호합니다. **LinkScanner** 기술은 **AVG Search-Shield** 및 **AVG Active Surf-Shield**의 두 가지 기능으로 구성되어 있습니다.

- **AVG Search Shield**는 위험하다고 알려진 웹 사이트 (URL 주소)의 목록을 가지고 있습니다. Google, Yahoo!, Bing, Baidu, Altavista 또는 Yandex에서 검색할 때 이 목록을 기준으로 모든 검색 결과를 확인하여 판정 아이콘을 표시합니다 (Yahoo! 검색 결과의 경우 "익스플로잇된 웹 사이트" 판정 아이콘만 표시됨). 또한 브라우저에 직접 주소를 입력하거나, 웹 사이트 또는 전자 메일의 링크를 클릭한 경우 자동으로 링크를 확인하여 필요한 경우 차단합니다.
- **AVG Active Surf-Shield**는 웹 사이트의 주소에 관계없이 방문하는 모든 웹 사이트의 내용을 스캔합니다. 일부 웹 사이트가 **AVG Search Shield**에서 검색되지 않는 경우 (예: 악성 웹 사이트가 새로 만들어졌거나 깨끗했던 웹 사이트에 맬웨어가 포함된 경우)에도 사용자가 웹 사이트를 방문하면 **AVG Active Surf-Shield**가 위협 요소를 검색하여 차단합니다.

참고 : AVG Link Scanner는 서버 플랫폼용이 아닙니다.

8.10.2. Link Scanner 인터페이스

LinkScanner 구성 요소는 **LinkScanner 구성 요소** 인터페이스에서 설정 또는 해제할 수 있는 두 부분으로 구성됩니다.

LinkScanner 구성 요소 인터페이스에는 구성 요소의 기능에 대한 간략한 설명과 구성 요소의 현재 상태에 대한 정보 (**LinkScanner 구성 요소가 활성화되었습니다**). 또한 최신 **LinkScanner** 데이터베이스 버전 번호에 대한 정보 (**LinkScanner 버전**)를 찾을 수 있습니다.



대화 상자의 아래쪽 부분에서 몇 가지 옵션을 편집할 수 있습니다 .

- **AVG Search-Shield** 사용 (기본적으로 설정되어 있음) - Google, Yahoo!, Bing, Baidu, Yandex 또는 Altavista 검색 엔진에서 반환하는 사이트의 내용을 미리 검사하여 해당 검색 엔진에서 수행하는 검색에 대한 안전도를 알려 주는 아이콘입니다 .
- **AVG Active Surf-Shield** 사용 - (기본적으로 설정되어 있음): 악의적인 사이트의 액세스를 차단하는 활성 (실시간) 보호 기능입니다 . 알려진 악의적인 사이트 연결 및 이와 관련된 악의적인 내용은 사용자가 웹 브라우저 (또는 HTTP를 사용하는 다른 모든 응용 프로그램)를 통해 액세스할 때 차단됩니다 .
- **발견된 위협 요소를 AVG에 보고** - 웹 상에서의 악의적인 활동에 대한 데이터베이스 수집 정보를 제공하기 위해 **Safe Surf** 또는 **Safe Search**를 통해 사용자가 발견한 익스플로잇과 악성 사이트를 보고하도록 하려면 이 항목을 선택합니다 .

8.10.3. AVG Search-Shield

AVG Search-Shield를 실행한 상태에서 인터넷을 검색하는 경우 Yahoo!, Google, Bing, Altavista, Yandex 등의 자주 사용되는 대부분의 검색 엔진에서 반환되는 모든 검색 결과가 위험한 링크인지 또는 의심스러운 링크인지 평가됩니다 . 이러한 링크를 확인하고 부적절한 링크로 표시하는 방법으로 **AVG Link Scanner**에서는 사용자가 위험하거나 의심스러운 링크를 클릭하기 전에 사용자에게 이를 경고하여 안전한 웹 사이트로만 연결 되도록 합니다 .

검색 결과 페이지에서 링크가 평가되는 동안 링크 확인이 진행 중임을 알리는 그래픽 기호가 링크 옆에 표시됩니다 . 평가를 마치면 각각의 정보 제공 아이콘이 표시됩니다 .

 연결된 페이지가 안전합니다 . [AVG Security Toolbar](#)에서 Yahoo! 검색 엔진을 사용하는 경우에는 이 아이콘이 표시되지 않습니다 .

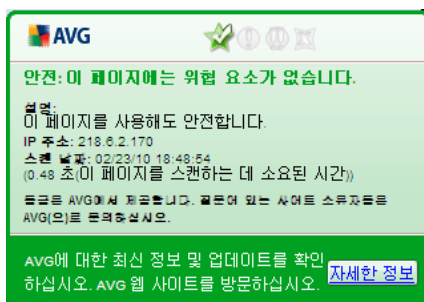
 연결된 페이지가 위험 요소를 포함하고 있지 않지만 다소 의심스럽습니다 . 그 출처나 의도가 불확실해 보이므로 이러한 페이지에서 인터넷 쇼핑과 같은 활동은 하지 않는 것이 좋습니다 .).

 연결된 페이지 자체는 안전할 수 있지만 위험한 페이지에 대한 추가 링크를 포함하고 있거나 현재는 위험 요소가 직접 사용되지 않았지만 코드가 의심스럽습니다 .

 연결된 페이지에 활성 위험 요소가 있습니다 ! 안전상의 이유로 이 페이지에 방문할 수 없습니다 .

 액세스할 수 없는 연결된 페이지이므로 스캔하지 못했습니다 .

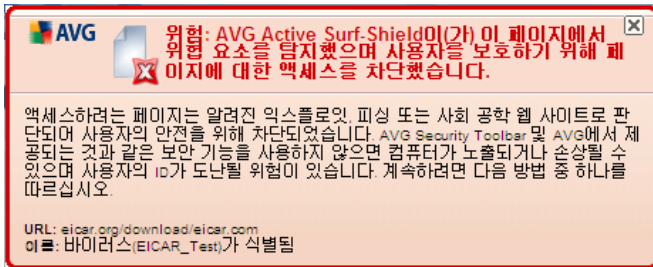
각 등급 아이콘 위에 마우스 포인터를 올려 놓으면 특정 링크에 대한 자세한 정보가 표시됩니다 . 이러한 정보에는 위험 요소에 대한 자세한 정보 (있는 경우), 링크의 IP 주소 및 AVG에서 페이지를 스캔한 시기 등이 포함됩니다 .



8.10.4. AVG Active Surf-Shield

이 강력한 보호 기능은 사용자가 열려는 웹 페이지에서 악의적인 콘텐츠를 차단하여 컴퓨터에 다운로드되지 않도록 합니다. 이 기능을 사용하도록 설정한 경우 위험한 사이트로 연결되는 링크를 클릭하거나 URL을 입력했을 때 해당 웹 페이지가 열리지 않도록 자동으로 차단하므로 컴퓨터의 감염을 막을 수 있습니다. 익스플로잇된 사이트를 방문하면 해당 웹 페이지로 인해 컴퓨터가 감염될 수 있다는 점에 유의해야 합니다. 따라서 익스플로잇 또는 기타 심각한 위협 요소가 있는 위험한 웹 페이지를 요청하는 경우에는 [AVG Link Scanner](#)에서 브라우저에 해당 웹 페이지가 표시되지 않도록 제한합니다.

웹 브라우저에서 악의적인 웹 사이트가 열리면 [AVG Link Scanner](#)에서 화면에 다음과 같은 경고 메시지를 표시합니다.



이 웹 사이트를 방문하는 것은 매우 위험하며 권장되지 않습니다 !

8.11. Online Shield

8.11.1. Online Shield 원리

Online Shield는 방문한 웹 페이지의 콘텐츠 (포함된 파일이 있는 경우 해당 파일도 포함)를 웹 브라우저에 표시하거나 컴퓨터로 다운로드하기 전에 스캔합니다.

Online Shield는 방문하려는 페이지에 위험한 Java 스크립트가 포함되어 있는지 검색하며, 발견된 경우 페이지를 표시하지 않습니다. 또한 페이지에 포함된 맬웨어를 인식하는 즉시 다운로드를 중지함으로써 컴퓨터로 유입되지 않도록 합니다.

참고 : AVG Online Shield는 서버 플랫폼용이 아닙니다.

8.11.2. Online Shield 인터페이스

Online Shield 구성 요소 인터페이스에는 이러한 유형의 보호 동작에 대한 설명이 있습니다. 추가로 구성 요소의 현재 상태에 대한 정보 (**Online Shield가 활성화되었으며 모든 기능이 작동합니다**)를 찾을 수 있습니다. 대화 상자의 아래쪽 부분에서 이 구성 요소의 기능에 대한 기본적인 편집 옵션을 찾을 수 있습니다.

기본 구성 요소 구성

우선 **Online Shield 활성화** 항목을 선택하여 **Online Shield**를 즉시 설정 / 해제할 수 있는 옵션이 있습니다. 이 옵션은 기본적으로 설정되어 있으며 이에 따라 **Online Shield** 구성 요소는 활성화되어 있습니다. 이 설정을 변경해야 할 특별한 이유가 있지 않다면 이 구성 요소를 활성화된 상태로 유지하는 것이 좋습니다. 이 항목을 선택한 경우 **Online Shield**가 실행 중이면 다음 두 탭에서 추가 구성 옵션을 사용하고 편집할 수 있습니다.

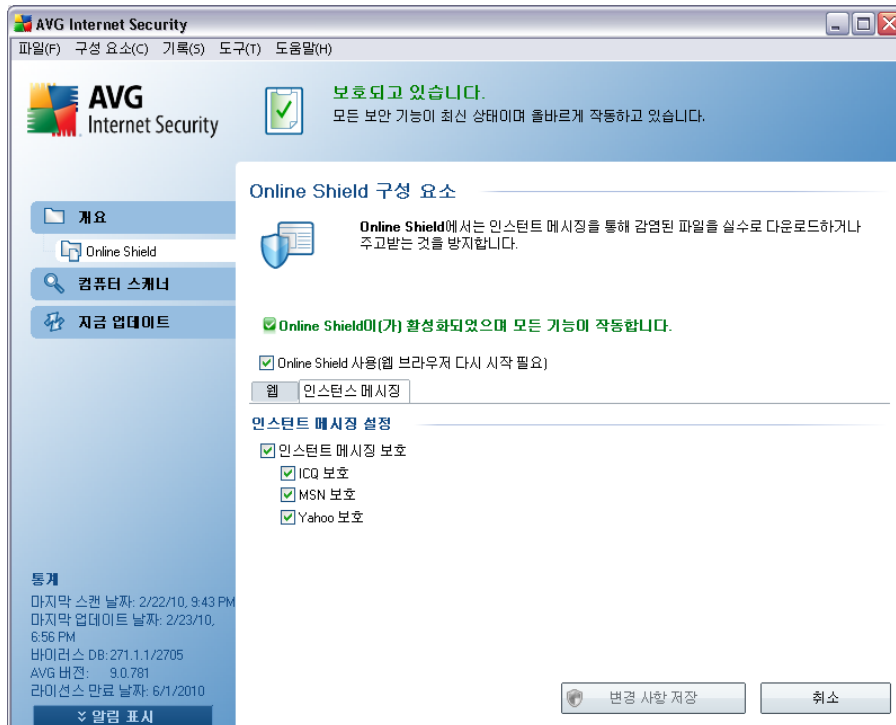
- **웹** - 웹 사이트 콘텐츠 스캔과 관련된 구성 요소의 구성을 편집할 수 있습니다. 편집 인터페이스를 사용하면 다음과 같은 기본적인 옵션을 구성할 수 있습니다.



- o **웹 보호** - 이 옵션을 선택하면 **Online Shield**가 www 페이지 콘텐츠를 스캔하도록 할 수 있습니다. 이 옵션을 선택한 경우 (기본적으로 설정되어 있음) 추가로 다음 항목을 설정 또는 해제할 수 있습니다.

➤ **압축 파일 확인** - 표시할 www 페이지에 포함된 압축 파일의 콘텐츠를 스캔합니다.

- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스�파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위협을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다.](#) 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다.
- **향상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 [스�파이웨어](#)의 확장 패키지를 검색하려면 이 상자를 선택합니다. 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 잘못 사용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.
- **지능형 분석 사용** - 표시할 페이지의 콘텐츠를 지능형 분석 방법 (가상 컴퓨터 환경에서 스캔된 개체의 명령에 대한 시뮬레이션 및 평가)을 사용하여 스캔합니다. 따라서 바이러스 데이터베이스에 정의되지 않은 악의적인 코드를 검색할 수 있습니다 ([Anti-Virus 원리](#) 참조).
- **스캔할 파일의 최대 크기** - 포함된 파일이 표시된 페이지에 존재하는 경우 파일을 컴퓨터로 다운로드하기 전에 파일의 콘텐츠를 스캔할 수도 있습니다. 하지만 큰 파일의 스캔에는 약간의 시간이 걸리며 웹 페이지 다운로드가 상당히 느려질 수 있습니다. 슬라이드 막대를 사용하여 **Online Shield**로 스캔할 파일의 최대 크기를 지정할 수 있습니다. 다운로드한 파일이 지정한 크기보다 커서 **Online Shield**로 스캔할 수 없는 경우라 하더라도 사용자의 컴퓨터는 여전히 보호됩니다. 파일이 감염된 경우에는 [상주 보호](#)가 즉시 이를 검색합니다.
- **인스턴트 메시징** - 인스턴트 메시징 (예: ICQ, MSN Messenger, Yahoo ...) 스캔에 관한 구성 요소 설정을 편집할 수 있습니다.



- o 인스턴트 메시징 보호 - Online Shield를 사용하여 온라인 커뮤니케이션에 바이러스가 없음을 확인하려면 이 항목을 선택합니다. 이 옵션이 설정되어 있으면 제어하려는 인스턴트 메시징 응용 프로그램을 추가로 지정할 수 있습니다. **AVG 9 Internet Security**는 현재 ICQ, MSN 및 Yahoo 응용 프로그램을 지원합니다.

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다. AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 고급 설정**을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다.

제어 단추

Online Shield 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다.

- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다.
- **취소** - 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아

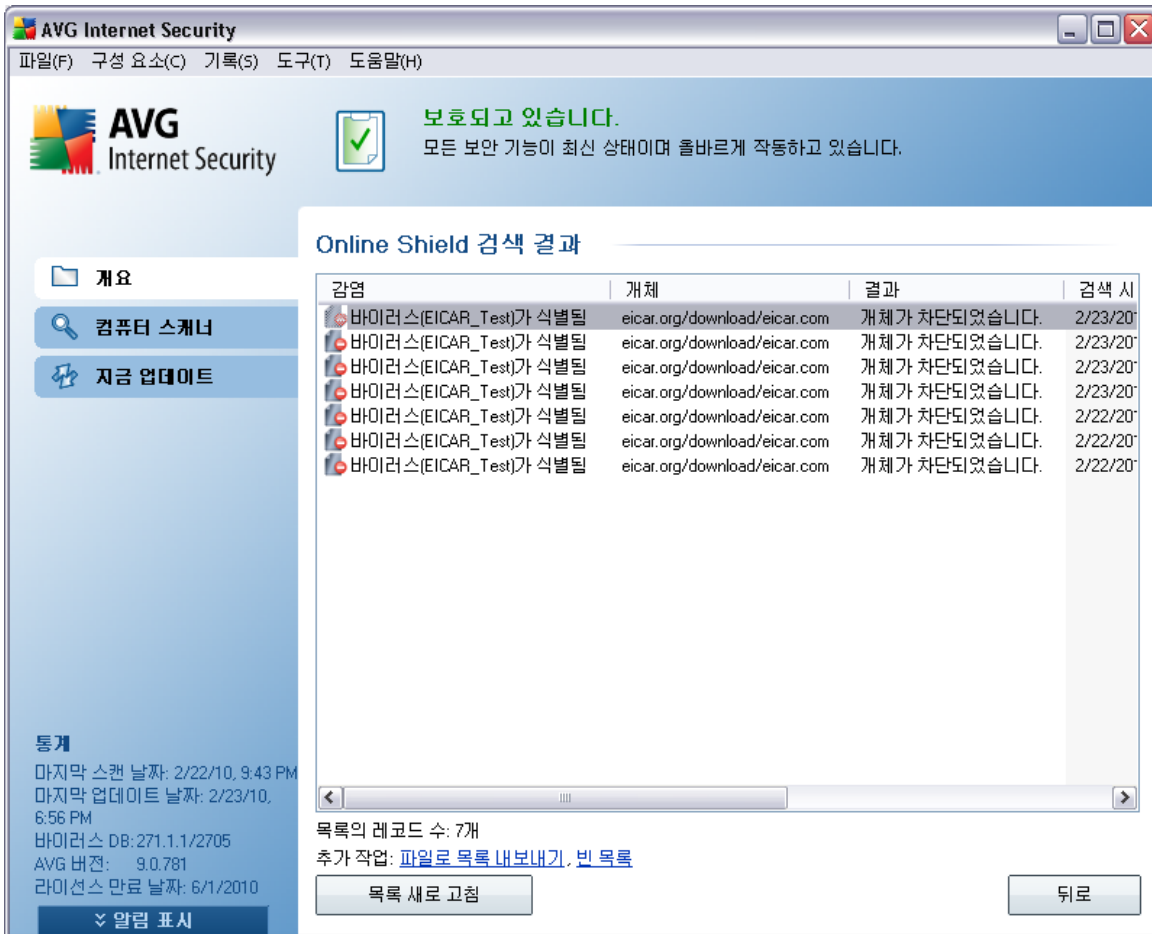
갑니다 .

8.11.3. Online Shield 탐지

Online Shield는 방문한 웹 페이지의 콘텐츠 및 그에 포함된 파일을 웹 브라우저에 표시하거나 컴퓨터로 다운로드하기 전에 스캔합니다 . 위험 요소가 발견되는 즉시 다음과 같은 경고 대화 상자를 표시합니다 .



의심스러운 웹 페이지는 열리지 않으며 위험 요소 검색은 **Online Shield 검색 결과**에 기록됩니다 . 발견된 위험에 대한 개요는 시스템 메뉴 **기록 / Online Shield 검색 결과**에서 액세스할 수 있습니다 .



발견된 각 개체에 대해 다음 정보가 제공됩니다 .

- **감염** - 발견된 개체에 대한 설명 (및 이름)
- **개체** - 개체 출처 (웹 페이지)
- **결과** - 발견된 개체에 수행된 작업
- **검색 시간** - 위협이 요소가 검색되어 차단된 날짜 및 시간
- **개체 유형** - 발견된 개체의 유형
- **프로세스** - 잠재적으로 위험한 개체를 검색할 수 있도록 해당 개체를 불러 내기 위해 수행된 작업

대화 상자의 아래쪽 부분의 목록에서 위에 나와 있는 발견된 개체의 총 개수를 확인할 수 있습니다 . 또한 발견된 개체의 전체 목록을 파일로 내보내고 (**파일로 목록 내보내기**) 발견된 개체에 대한 모든 항목을 삭제 (**목록 비우기**) 할 수 있습니다 . **목록 새로 고침** 단추는 **Online Shield**에서 발견한 결과 목록을 업데이트합니다 . **뒤로** 단추를 누르면 기본 **AVG 사용자 인터페이스** (구성 요소 개요)로 되돌아갑니다 .

8.12. Resident Shield

8.12.1. 상주 보호 원리

Resident Shield 구성 요소를 사용하면 컴퓨터를 지속적으로 보호할 수 있습니다 . 이 구성 요소는 열기, 저장 또는 복사되고 있는 모든 단일 파일을 스캔하고 컴퓨터의 시스템 영역을 보호합니다 . **상주 보호**가 액세스한 파일에서 바이러스를 발견하면 현재 수행 중인 작업을 중단하여 해당 바이러스가 활성화되지 않도록 합니다 . 이 프로세스는 "백그라운드"로 실행되므로 사용자는 대개 프로세스가 있는지조차 알지 못하고 위협 요소가 발견될 경우에만 알림을 받습니다 . 이때 **상주 보호**를 통해 위협 요소의 활성화가 차단되고 위협 요소가 제거됩니다 . **상주 보호**는 시스템을 시작하는 동안 컴퓨터 메모리에 로드됩니다 .

경고 : 상주 보호는 컴퓨터가 시작되는 동안 메모리에 로드되고 항상 실행됩니다 !

8.12.2. 상주 보호 인터페이스



상주 보호 인터페이스는 가장 중요한 통계 데이터 및 구성 요소의 현재 상태에 대한 정보 (**상주 보호가 활성화되었으며 모든 기능이 작동합니다**) 외에도 일부 기본적인 구성 요소 설정 옵션도 제공합니다. 통계는 다음과 같습니다.

- **상주 보호 활성화 시간** - 마지막 구성 요소 시작 이후 경과된 시간을 제공합니다.
- **발견되거나 차단된 위협 요소 수** - 발견된 감염 중에 열기 / 실행이 금지된 감염의 수입니다. 필요한 경우 이 값은 다시 설정할 수 있습니다 (예: 통계를 위한 값 다시 설정).

기본 구성 요소 구성

대화 상자 창의 아래쪽 부분에 있는 **상주 보호 설정** 섹션에서는 구성 요소의 기능에 대한 일부 기본 설정을 편집할 수 있습니다. 다른 모든 구성 요소와 마찬가지로 자세한 구성은 시스템 메뉴의 도구 / 고급 설정 항목을 통해 사용할 수 있습니다.

상주 보호가 활성화되었습니다 옵션으로 상주 보호를 간편하게 설정하거나 해제할 수 있습니다. 기본적으로 이 기능은 설정되어 있습니다. 상주 보호를 설정한 상태에서

사용자는 발견된 감염의 처리 (제거) 방법을 결정할 수 있습니다 .

o 자동 처리 (**모든 위협 요소 자동 제거**)

o 또는 사용자의 승인을 얻은 경우에만 처리 (**위협 요소 제거 전 확인**)

이 옵션은 보안 수준에 영향을 미치지 않으며 사용자의 선호도만을 반영합니다 .

두 경우 모두 **추적 쿠키를 스캔** 할지 여부를 선택할 수 있습니다 . 이 옵션은 기본적으로 해제되어 있지만 특별한 경우에는 설정하여 보안 수준을 극대화할 수 있습니다 . 쿠키 = 서버가 웹 브라우저로 전송한 후 다시 브라우저가 해당 서버에 액세스할 때마다 변경되지 않은 상태 그대로 반환하는 텍스트 꾸러미 . HTTP 쿠키는 사이트 기본 설정이나 전자 쇼핑 카트의 내용물과 같이 사용자와 관련된 정보를 인증하고 , 추적하고 , 유지 관리하는 데 사용됩니다 .

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다 . 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 . AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 **AVG 고급 설정** 대화 상자에서 AVG 구성을 편집합니다 .

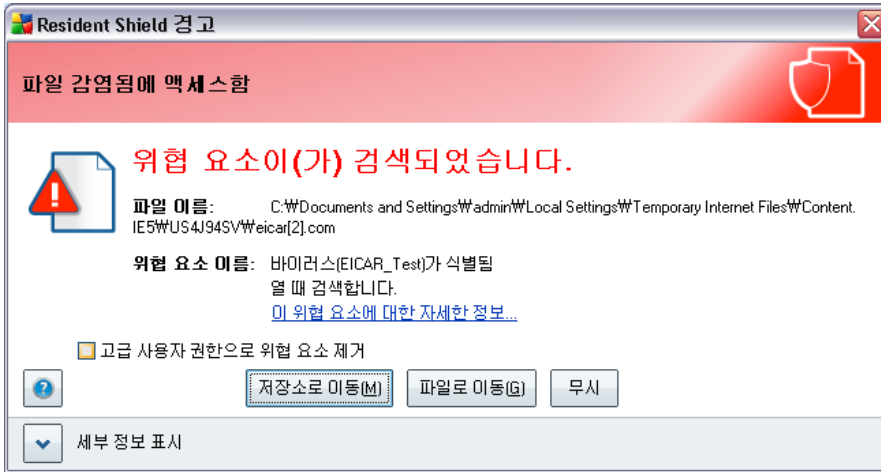
제어 단추

제어 단추는 **상주 보호** 인터페이스에서 다음과 같이 사용할 수 있습니다 .

- **예외 관리** - **상주 보호 - 디렉터리 제외** 대화 상자를 열고 , 여기에서 **상주 보호** 스캔에서 제외시킬 폴더를 정의할 수 있습니다 .
- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다 .
- **취소** - 이 단추를 누르면 기본 **AVG 사용자 인터페이스** (구성 요소 개요)로 돌아갑니다 .

8.12.3. 상주 보호 검색

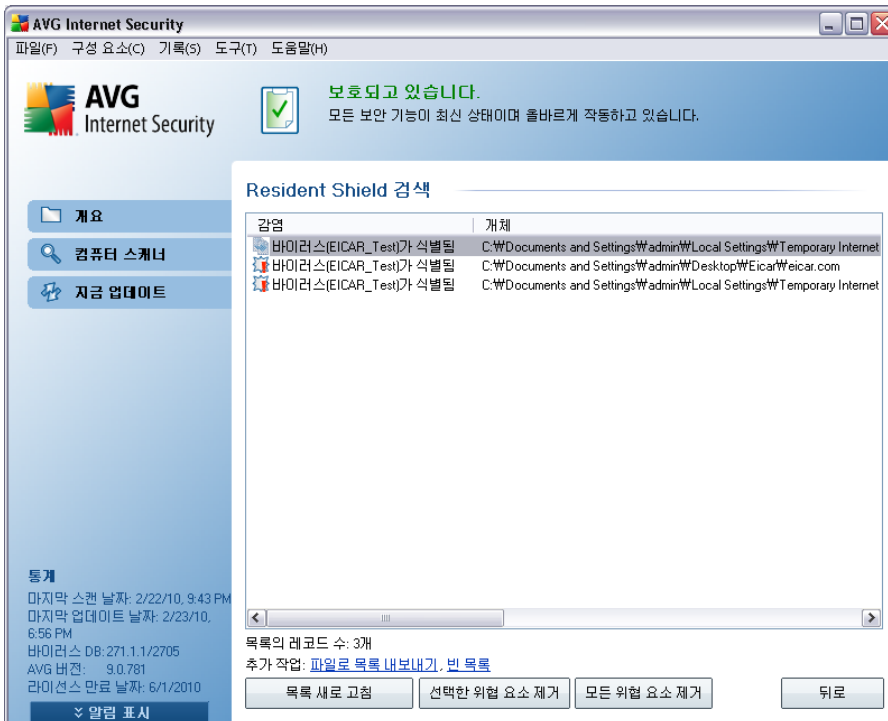
상주 보호 는 파일을 복사하거나 열거나 저장할 때 파일을 스캔합니다 . 바이러스나 다른 종류의 위협 요소가 발견되면 즉각 다음과 같은 대화 상자를 통해 경고가 표시됩니다 .



대화 상자는 발견된 위협 요소에 대한 정보를 제공하고 사용자로 하여금 취해야 할 조치를 결정하도록 안내합니다 .

- **치료** - 치료가 가능한 경우 AVG는 감염된 파일을 자동으로 치료합니다 . 이 옵션을 택하는 것이 좋습니다 .
- **저장소로 이동** - 바이러스를 AVG [바이러스 저장소로 이동합니다](#) .
- **파일로 이동** - 이 옵션을 사용하면 의심스러운 개체의 정확한 위치로 이동할 수 있습니다 (새 Windows 탐색기 창이 열림).
- **무시** - 반드시 필요한 경우를 제외하고 이 옵션은 사용하지 않는 것이 좋습니다 .

[상주 보호](#)에서 발견된 모든 위협에 대한 전체적인 개요는 시스템 메뉴 옵션 [기록 / 상주 보호 검색 결과](#)에서 액세스할 수 있는 [***상주 보호 검색 대화 상자에서](#) 확인할 수 있습니다 .



상주 보호 검색에서는 **상주 보호**에 의해 발견되어 위험한 것으로 평가된 후 치료되거나 **바이러스 저장소**로 이동된 개체에 대한 개요를 제공합니다. 발견된 각 개체에 대해 다음 정보가 제공됩니다.

- **감염** - 발견된 개체에 대한 설명 (및 이름)
- **개체** - 개체 위치
- **결과** - 발견된 개체에 수행된 작업
- **검색 시간** - 개체가 발견된 날짜 및 시간
- **개체 유형** - 발견된 개체의 유형
- **프로세스** - 잠재적으로 위험한 개체를 검색할 수 있도록 해당 개체를 불러 내기 위해 수행된 작업

대화 상자의 아래쪽 부분의 목록에서 위에 나와 있는 발견된 개체의 총 개수를 확인할 수 있습니다. 또한 발견된 개체의 전체 목록을 파일로 내보내고 (**파일로 목록 내보내기**) 발견된 개체에 대한 모든 항목을 삭제 (**목록 비우기**)할 수 있습니다. **목록 새로 고침** 단추는 **상주 보호**에서 검색한 결과 목록을 업데이트합니다. **뒤로** 단추를 누르면 기본



[AVG 사용자 인터페이스](#) (구성 요소 개요)로 되돌아갑니다 .

8.13. 업데이트 관리자

8.13.1. 업데이트 관리자 원리

보안 소프트웨어를 정기적으로 업데이트하지 않으면 다양한 유형의 위협 요소로부터 완벽한 보호를 받을 수 없습니다 . 바이러스 제작자는 소프트웨어와 운영 체제 모두에서 익스플로잇할 수 있는 새 결함을 항상 찾고 있습니다 . 새로운 바이러스 , 맬웨어 , 해킹 공격은 일상적으로 발생합니다 . 이러한 이유로 소프트웨어 공급업체는 새로 발견된 보안 취약점을 해결하기 위해 업데이트 및 보안 패치를 지속적으로 발표합니다 .

따라서 사용자는 AVG를 정기적으로 업데이트해야 합니다 .

업데이트 관리자 를 통해 정기적인 업데이트를 보다 쉽게 관리할 수 있습니다 . 이 구성 요소를 사용하면 인터넷 또는 로컬 네트워크에서 업데이트 파일을 자동으로 다운로드 하도록 예약할 수 있습니다 . 필수적인 바이러스 정의는 가능하면 매일 업데이트해야 합니다 . 긴급도가 낮은 프로그램 업데이트는 매주 진행할 수 있습니다 .

참고 : 업데이트 유형 및 수준에 대한 자세한 내용은 [AVG 업데이트](#) 장을 살펴보십시오 .

8.13.2. 업데이트 관리자 인터페이스



업데이트 관리자 인터페이스에는 구성 요소의 기능 및 현재 상태 (**업데이트 관리자**가 활성화되었습니다)를 제공하고 관련 통계 데이터를 확인할 수 있습니다.

- **마지막 업데이트 날짜** - 데이터베이스의 업데이트 시기와 방법을 지정합니다.
- **바이러스 데이터베이스 버전** - 최신 바이러스 데이터베이스 버전의 번호를 정의하며 이 번호는 바이러스 데이터베이스가 업데이트될 때마다 증가합니다.
- **예약된 다음 업데이트 날짜** - 데이터베이스를 다시 업데이트하도록 예약한 시기 및 시간을 지정합니다.

기본 구성 요소 구성

대화 상자의 아래쪽 부분에는 **업데이트 관리자 설정** 섹션이 있으며, 여기에서 업데이트 프로세스 시작 규칙을 일부 변경할 수 있습니다. 업데이트 파일을 자동으로 다운로드할지 (**자동 업데이트 시작**) 아니면 필요할 때 다운로드할지 정의할 수 있습니다. 기본적으로 **자동 업데이트 시작** 옵션으로 설정되어 있으며 이를 그대로 유지하는 것이 좋습니다. 모든 보안 소프트웨어가 올바르게 작동하려면 최신 업데이트 파일을 정기적

으로 다운로드해야 합니다 .

또한 다음과 같이 업데이트를 시작해야 할 시기를 정의할 수도 있습니다 .

- o **주기적** - 시간 간격을 정의합니다 .
- o **지정한 시간 간격으로** - 정확한 날짜 및 시간을 지정합니다 .

기본적으로 업데이트는 4시간마다 실행되도록 설정되어 있습니다 . 변경해야 할 특별한 이유가 있는 경우를 제외하고 이 설정을 그대로 유지하는 것이 좋습니다 .

참고 : 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG 구성 요소를 설정해 놓았습니다 . 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오 . 모든 설정 변경은 숙련된 사용자가 수행해야 합니다 . AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구 / 고급 설정** 을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다 .

제어 단추

업데이트 관리자 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **지금 업데이트** - 필요할 때 [즉시 업데이트](#) 를 시작합니다 .
- **변경 내용저장** - 이 단추를 누르면 이 대화 상자에서 이루어진 모든 변경 내용이 저장 및 적용됩니다 .
- **취소** - 이 단추를 누르면 기본 [AVG 사용자 인터페이스](#) (구성 요소 개요)로 돌아갑니다 .

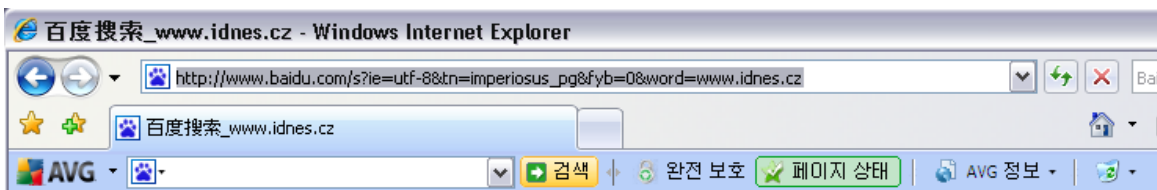
9. AVG Security Toolbar

AVG Security Toolbar는 **AVG Link Scanner** 구성 요소와 함께 작동하여 지원되는 인터넷 검색 엔진 (Yahoo!, Google, Bing, Altavista, Baidu)의 검색 결과를 확인하는 새로운 도구입니다 . **AVG Security Toolbar**는 **AVG Link Scanner** 기능을 제어하고 그 동작을 조정하는 데 사용할 수 있습니다 .

AVG 9 Internet Security 설치 중에 AVG Security Toolbar를 설치하도록 선택하면 웹 브라우저에 자동으로 Security Toolbar가 추가됩니다 . 일부 대체 인터넷 브라우저 (예: Avant Browser)를 사용하는 경우 예기치 않은 동작이 발생할 수 있습니다 .

9.1. AVG Security Toolbar 인터페이스

AVG Security Toolbar는 **MS Internet Explorer**(버전 6.0 이상) 및 **Mozilla Firefox**(버전 2.0 이상)와 함께 작동하도록 설계되었습니다 . **AVG Security Toolbar**를 설치하도록 선택한 경우 (**AVG 설치 프로세스** 중에 구성 요소를 설치할지 묻는 메시지가 나타남) 웹 브라우저의 주소 표시줄 바로 아래에 구성 요소가 나타납니다 .



참고 : AVG Security Toolbar는 서버 플랫폼용이 아닙니다 .

AVG Security Toolbar에는 다음과 같은 항목이 포함되어 있습니다 .

- **AVG 로고** - 이를 통해 일반 도구 모음 항목에 액세스할 수 있습니다 . AVG 웹 사이트 (<http://www.avg.com/>)로 리디렉션하려면 로고 단추를 클릭하십시오 . AVG 아이콘 옆에 있는 포인터를 클릭하면 다음 항목이 열립니다 .
 - **도구 모음 정보** - 도구 모음 보호 기능에 대한 자세한 정보가 나와 있는 **AVG Security Toolbar 홈 페이지로 연결되는 링크입니다** .
 - **시작 AVG 9 Internet Security** - **AVG 9 Internet Security** 사용자 인터페이스를 엽니다 .
 - **옵션** - **AVG Security Toolbar** 설정을 사용자 필요에 맞게 조정할 수 있는 구성 대화 상자가 열립니다 . 자세한 내용은 [AVG Security Toolbar 옵션 장을 참조하십시오](#) .
 - **기록 삭제** - AVG Security Toolbar의 전체 기록 삭제 또는 검색 기록 삭제,

브라우저 기록 삭제, 다운로드 기록 삭제 및 쿠키 삭제를 수행할 수 있습니다.

○ **업데이트** - AVG Security Toolbar에 대한 새 업데이트를 확인합니다

○ **도움말** - 도움말 파일을 열고, 제품 피드백을 제출하고, 도구 모음의 현재 버전에 대한 자세한 정보를 볼 수 있는 옵션을 제공합니다.

- **검색 상자** - 검색 상자에 단어나 구를 입력합니다. **검색**을 눌러 현재 표시된 페이지에 관계없이 지정된 검색 엔진을 사용하여 검색을 시작합니다. [AVG Security Toolbar 고급 옵션](#) 내에서 원하는 검색 엔진을 지정할 수 있으며 Yahoo!, Wikipedia, Baidu, WebHledani 또는 Yandex 중에서 선택할 수 있습니다. 검색 상자에는 검색 기록도 표시됩니다. 검색 상자를 통해 수행하는 검색은 [AVG Search-Shield](#) 보호 기능을 사용하여 분석됩니다.

- **완전 보호** - 이 단추는 구성에 따라 **완전 보호** / **제한적 보호** / **AVG 9 Internet Security** 보호 안 함

- **페이지 상태** - 도구 모음에서 직접 제공되는 이 단추는 [AVG Search-Shield](#) 구성 요소의 조건에 따라 현재 업로드된 웹 페이지의 평가 내용 (**안전한 페이지** / **의심스러운 페이지** / **잠재적으로 위험한 페이지** / **위험 요소가 포함된 페이지** / **스캔하지 못한 페이지**)을 표시합니다. 단추를 클릭하면 특정 웹 페이지에 대한 자세한 정보가 포함된 정보 패널이 열립니다.

- **AVG 정보** - AVG 웹 사이트 (<http://www.avg.com/>)에 있는 중요한 보안 정보에 대한 링크를 제공합니다.

○ **도구 모음 정보** - 도구 모음 보호 기능에 대한 자세한 정보가 나와 있는 [AVG Security Toolbar 홈 페이지](#)로 연결되는 링크입니다.

○ **위협 정보** - 인터넷에 현재 존재하는 바이러스 및 위협 요소에 대한 정보를 제공하는 AVG 웹 페이지를 엽니다.

○ **AVG 뉴스** - AVG 관련 최신 보도 자료를 제공하는 웹 페이지를 엽니다.

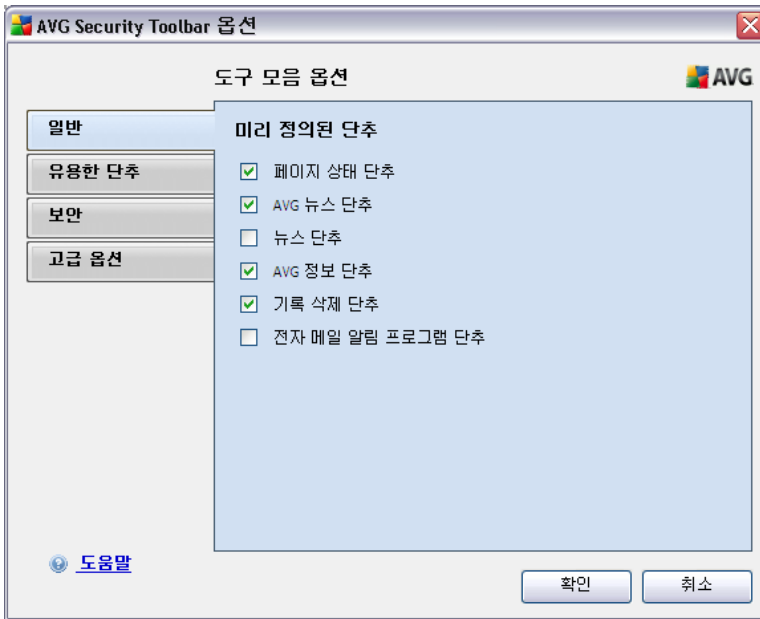
○ **현재 위협 수준** - 웹의 현재 위협 수준을 그래픽으로 보여 주는 바이러스 연구실 웹 페이지를 엽니다.

○ **바이러스 백과 사전** - 이름으로 특정 바이러스를 검색하고 각각에 대한 자세한 정보를 얻을 수 있는 바이러스 백과 사전 페이지를 엽니다.

9.2. AVG Security Toolbar 옵션

모든 **AVG Security Toolbar** 매개 변수 구성은 **AVG Security Toolbar** 패널에서 직접 액세스할 수 있습니다. 편집 인터페이스는 **도구 모음 옵션** 이라고 하는 새 대화 상자의 **AVG/ 옵션** 도구 모음 메뉴 항목을 사용하여 열 수 있습니다. 이 대화 상자에는 다음과 같은 네 개의 섹션이 있습니다.

9.2.1. 탭 일반

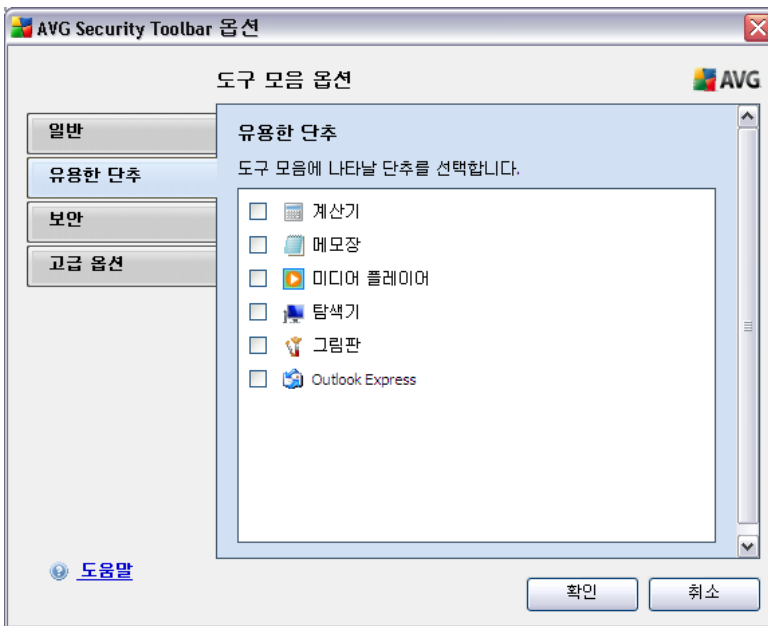


이 탭에서는 **AVG Security Toolbar** 패널에 표시하거나 숨기려는 도구 모음 제어 단추를 지정할 수 있습니다. 개별 단추를 표시하려는 경우 아무 옵션이나 선택합니다. 또한 도구 모음 단추 각각의 기능에 대한 설명은 다음과 같습니다.

- **AVG 뉴스 단추** - 이 단추는 AVG 관련 최신 보도 자료를 제공하는 웹 페이지를 엽니다.
- **뉴스 단추** - 이 단추는 일간 보도 매체의 현재 뉴스에 대한 체계적인 개요를 제공합니다.
- **AVG 정보 단추** - 이 단추는 AVG 도구 모음, 현재 위협 요소 및 인터넷 위협 수준에 대한 정보를 제공하고 바이러스 백과 사전을 열고 AVG 제품 관련 추가 뉴스를 제공합니다.
- **기록 삭제 단추** - 이 단추를 사용하면 AVG Security Toolbar 패널에서 직접 전

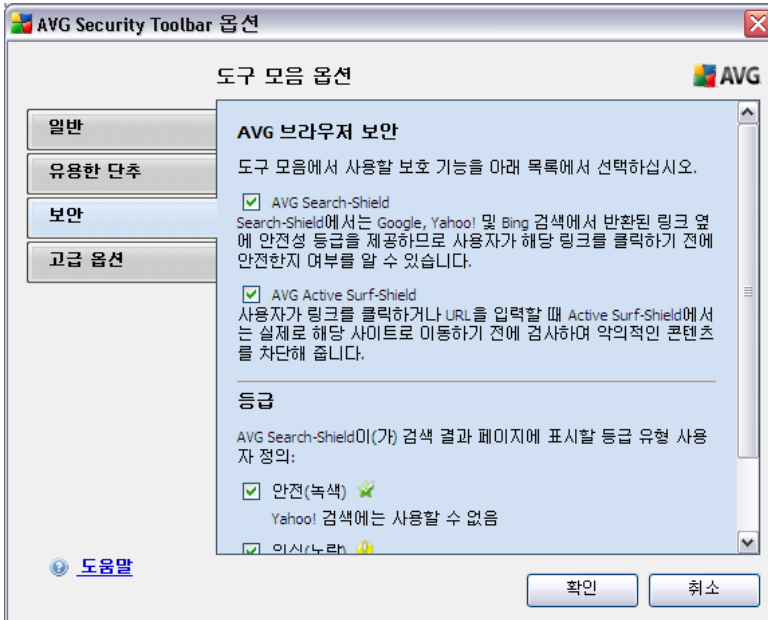
체 기록 삭제 또는 검색 기록 삭제, 브라우저 기록 삭제, 다운로드 기록 삭제 또는 쿠키 삭제를 수행할 수 있습니다.

9.2.2. 탭 유용한 단추



유용한 단추 탭을 사용하면 목록에서 응용 프로그램을 선택하고 해당 아이콘을 도구 모음 인터페이스에 표시할 수 있습니다. 그러면 이러한 아이콘은 빠른 링크로 작동하여 해당 응용 프로그램을 즉시 시작할 있도록 합니다.

9.2.3. 탭 보안



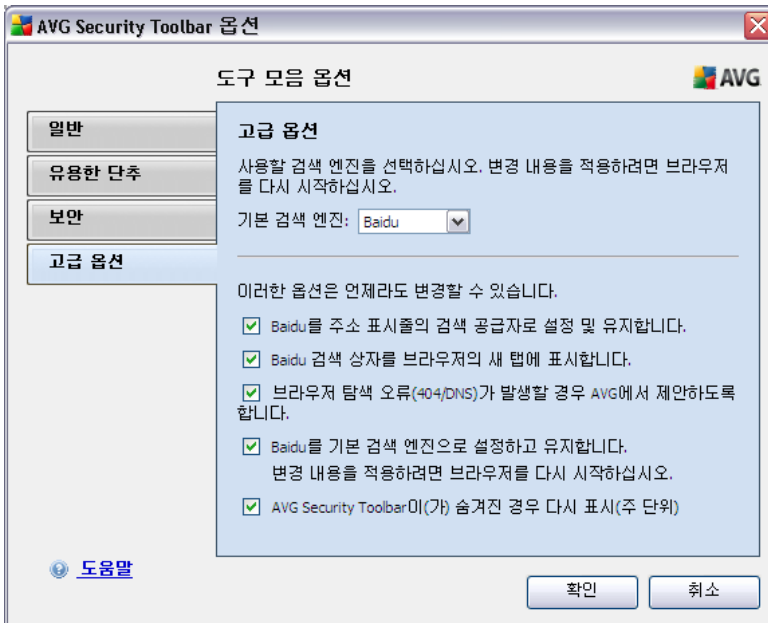
보안 탭은 **AVG 브라우저 보안** 및 **등급**의 두 섹션으로 나뉘어 있으며, 특정 확인란을 선택하여 **AVG Security Toolbar**에서 사용할 기능을 지정할 수 있습니다.

- **AVG 브라우저 보안** - **AVG Search-Shield** 및/또는 **AVG Active Surf-Shield** 서비스를 활성화하거나 비활성화하려면 이 항목을 선택합니다.
- **등급** - **AVG Search-Shield** 구성 요소에서 검색 결과의 등급을 표시하는 그래픽 기호 중 사용할 그래픽 기호를 선택합니다
 - o  안전한 페이지
 - o  의심스러운 페이지
 - o  잠재적으로 위험한 페이지로 연결되는 링크를 포함하는 페이지
 - o  위협 요소를 포함하는 페이지
 - o  액세스할 수 없어 스캔하지 못한 페이지

특정 위협 수준에 대한 알림을 받으려면 해당 옵션을 선택합니다. 위험한 위협 요

소를 포함하는 페이지에 할당되는 빨간색 표식은 해제하여 숨기는 것이 불가능합니다. **반드시 변경해야 할 경우가 아니라면 프로그램 공급업체에서 설정한 기본 구성을 유지하는 것이 좋습니다.**

9.2.4. 탭 고급 옵션



고급 옵션 탭에서 먼저 기본으로 사용할 검색 엔진을 선택합니다. Yahoo!, Baidu, WebHledani 및 Yandex 중에서 선택할 수 있습니다. 기본 검색 엔진을 변경한 후에는 변경 내용이 적용되도록 인터넷 브라우저를 다시 시작합니다.

또한 다른 특정 **AVG Security Toolbar** 설정을 활성화 또는 비활성화할 수 있습니다.

- **Yahoo!를 주소 표시줄의 검색 공급자로 설정 및 유지합니다** . - (기본적으로 설정되어 있음) - 이 옵션을 선택하면 인터넷 브라우저의 주소 표시줄에 직접 검색 키워드를 입력하고 Yahoo! 서비스를 통해 관련 웹 사이트를 자동으로 검색할 수 있습니다 .
- **브라우저 탐색 오류 (404/ DNS) 가 발생할 경우 AVG에서 제안하도록 합니다** . (기본적으로 설정되어 있음) - 웹을 검색할 때 존재하지 않는 페이지나 표시할 수 없는 페이지 (404 오류)를 방문하는 경우 해당 주제와 관련된 대체 페이지의 개요에서 선택할 수 있는 웹 페이지로 자동 리디렉션됩니다 .
- **Yahoo!를 브라우저의 검색 공급자로 설정 및 유지합니다** . - (기본적으로 해제되어 있음) - Yahoo!는 AVG Security Toolbar의 기본 웹 검색 엔진이며 이 옵션



션을 활성화하면 Yahoo!가 웹 브라우저의 기본 검색 엔진으로 사용됩니다 .

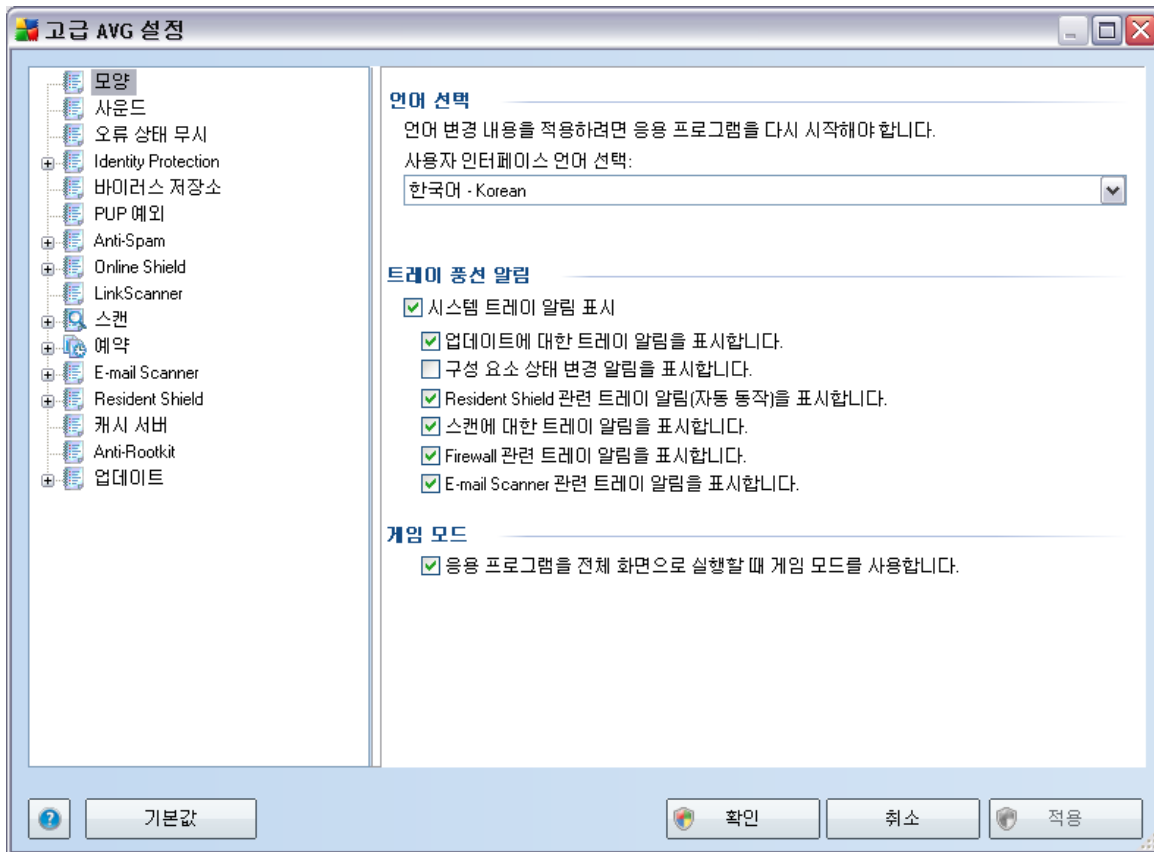
- **AVG Security Toolbar가 숨겨진 경우 다시 표시 (주 단위)** - (기본적으로 설정되어 있음) - 이 옵션은 기본적으로 활성화되며 실수로 **AVG Security Toolbar**를 숨겼을 경우 일주일 내로 다시 표시되게 합니다 .

10. AVG 고급 설정

AVG 9 Internet Security의 고급 구성 대화 상자는 **고급 AVG 설정**이라는 이름의 새 창에서 열립니다. 이 창은 두 개의 섹션으로 나뉘어 있습니다. 왼쪽 부분에는 프로그램 구성 옵션에 대한 정렬된 탐색 트리가 제공됩니다. 구성을 변경할 구성 요소 (또는 해당 특정 부분)를 선택하면 창 오른쪽 섹션에 편집 대화 상자가 열립니다.

10.1. 모양

탐색 트리의 첫 번째 항목인 **모양**은 [AVG 사용자 인터페이스](#)의 일반 설정 및 응용 프로그램 동작의 몇 가지 기본 옵션과 관련이 있습니다.

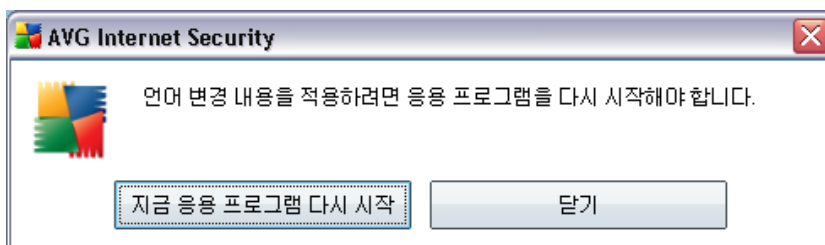


언어 선택

언어 선택 섹션의 드롭다운 메뉴에서 원하는 언어를 선택할 수 있습니다. 여기에서 지정된 언어가 전체 [AVG 사용자 인터페이스](#)에 사용됩니다. 드롭다운 메뉴에는 [설치 프로](#)

[세스](#)에서 설치하기로 이전에 선택한 언어만 표시됩니다 ([사용자 지정 설치 - 구성 요소 선택](#) 장 참조). 하지만 응용 프로그램의 언어를 전환하는 작업을 완료하려면 사용자 인터페이스를 다시 시작해야 합니다. 다음 단계를 수행하십시오.

- 원하는 응용 프로그램 언어를 선택하고 **적용** 단추 (오른쪽 아래 모서리)를 눌러 선택한 사항을 확인합니다.
- **확인** 단추를 눌러 확인합니다.
- AVG 사용자 인터페이스의 언어를 변경하려면 응용 프로그램을 다시 시작해야 한다는 메시지가 표시된 새 대화 상자 창이 나타납니다.



트레이 풍선 알림

이 섹션에서는 응용 프로그램 상태에 대한 시스템 트레이 풍선 알림이 표시되지 않도록 설정할 수 있습니다. 기본적으로 풍선 알림은 표시되도록 허용되며 이 구성을 유지하는 것이 좋습니다. 일반적으로 풍선 알림은 일부 AVG 구성 요소의 상태 변경에 대해 알려 주므로 이 알림에 주의를 기울여야 합니다.

하지만 특별한 이유로 이러한 알림이 표시되지 않게 하거나 특정 알림 (특정 AVG 구성 요소 관련 알림)만 표시되게 하려면 다음 옵션을 선택 / 선택 취소하여 원하는 설정을 정의하고 지정할 수 있습니다.

- **시스템 트레이 알림** 표시 - 기본적으로 이 항목은 선택 (설정)되어 있으므로 알림이 표시됩니다. 모든 풍선 알림의 표시를 완전히 해제하려면 이 항목의 선택을 취소합니다. 이 항목을 설정한 경우에는 표시하려는 특정 알림을 선택할 수 있습니다.
 - [업데이트](#)에 대한 트레이 알림 표시 - AVG 업데이트 프로세스 시작, 진행 상황 및 완료와 관련된 정보를 표시할지 여부를 결정합니다.
 - **구성 요소 상태 변경 알림** 표시 - 구성 요소의 활성화 / 비활성화 또는 그와 관련하여 발생 가능한 문제에 대한 정보를 표시할지 여부를 결정합니다. 구성 요소의 오류 상태를 보고할 때 이 옵션은 AVG 구성 요소에서 문제를 보고하는 [시스템 트레이 아이콘](#) (색 변경)의 정보 기능과 같습니다;

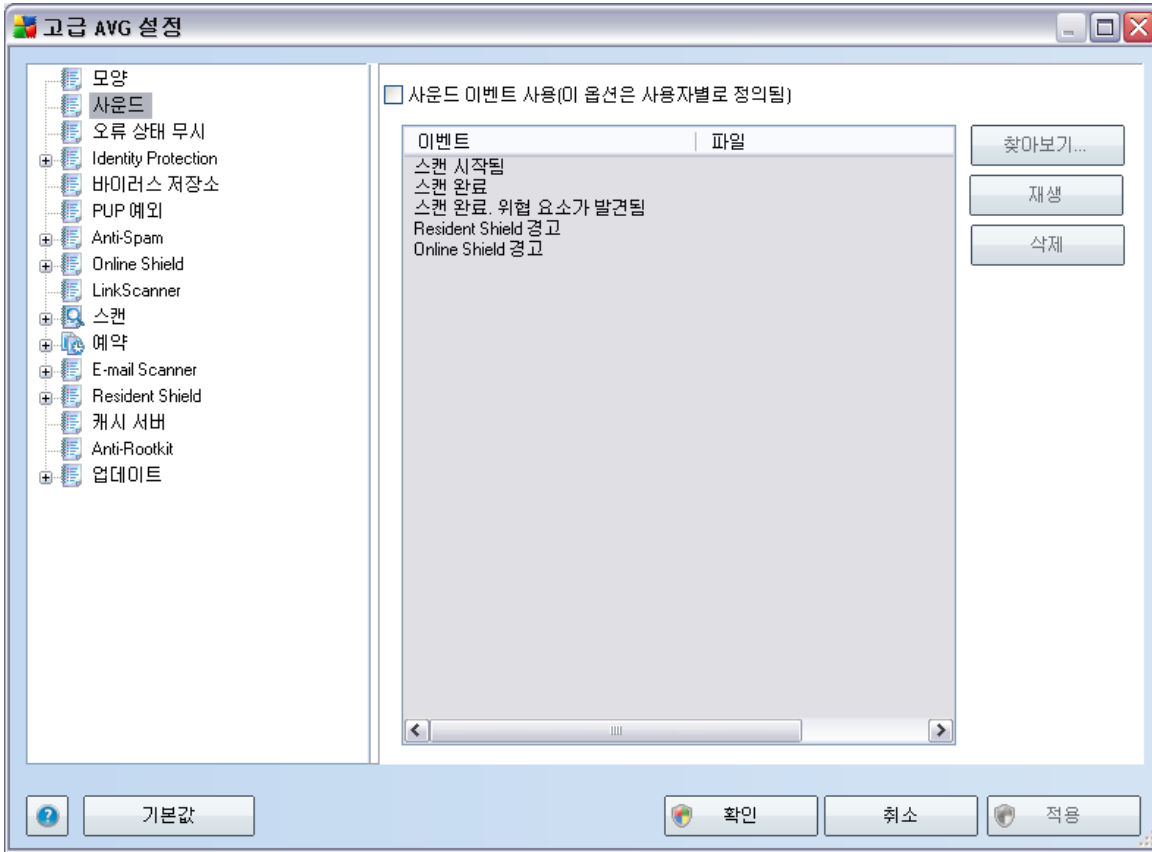
- o **상주 보호** 관련 트레이 알림 표시 - 파일 저장, 복사 및 열기 프로세스 관련 정보를 표시할지 아니면 숨길지 (이 구성에서는 상주 보호 **자동 치료** 옵션의 설정 여부만 표시함)를 결정합니다 .
- o **스캔**에 대한 트레이 알림 표시 - 예약된 스캔의 자동 시작, 진행 상황 및 결과와 관련된 정보를 표시할지 여부를 결정합니다 .
- o **방화벽** 관련 트레이 알림 표시 - 방화벽 상태 및 프로세스 관련 정보 (예: 구성 요소의 활성화 / 비활성화 경고, 발생 가능한 트래픽 차단 등)를 표시할지 여부를 결정합니다 .
- o **전자 메일 스캐너** 관련 트레이 알림 표시 - 들어오거나 나가는 모든 전자 메일 메시지의 스캔에 대한 정보를 표시할지 여부를 결정합니다 .

게임 모드

이 AVG 기능은 AVG 정보 풍선 (예: 예약된 스캔이 시작되는 경우에 표시)으로 인해 방해 (응용 프로그램 최소화 또는 그래픽 손상)를 받을 수 있는 전체 화면 응용 프로그램에 적합하게 설계되었습니다 . 이러한 상황을 방지하려면 **응용 프로그램을 전체 화면으로 실행할 때 게임 모드를 사용합니다** . 옵션 확인란을 선택된 상태 (기본 설정)로 두십시오 .

10.2. 사운드

사운드 대화 상자 내에서 사운드 알림을 통해 특정 AVG 작업에 대한 알림을 받을지 여부를 지정할 수 있습니다 . 알림을 받으려면 **사운드 이벤트 사용** 옵션 (기본적으로 해제되어 있음)을 선택하여 AVG 작업 목록을 활성화합니다 .

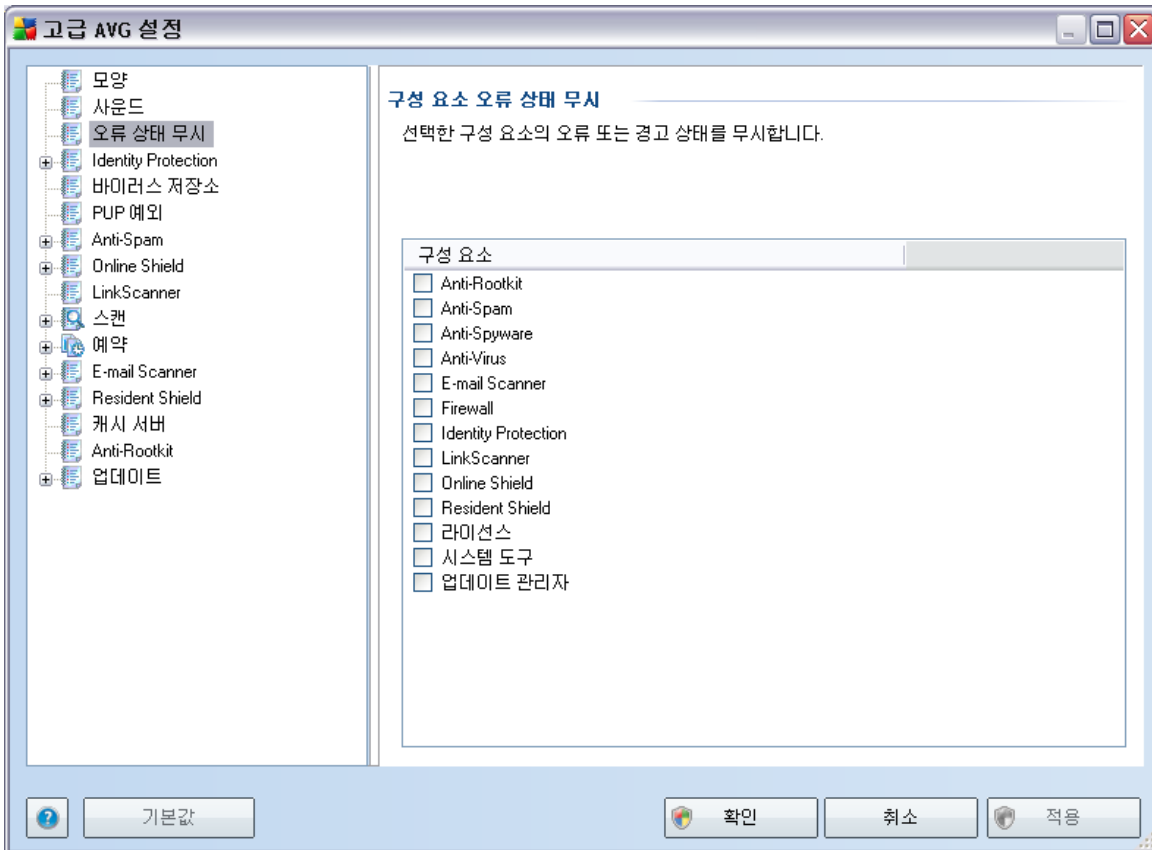


그런 다음 목록에서 해당 이벤트를 선택하고 디스크에서 이 이벤트에 할당할 적절한 사운드를 찾습니다 (**찾아보기**). 선택한 사운드를 들어보려면 목록에서 이벤트를 강조 표시하고 **재생** 단추를 누릅니다. 특정 이벤트에 할당된 사운드를 제거하려면 **삭제** 단추를 사용합니다.

참고 : *.wav 사운드만 지원됩니다 !

10.3. 오류 상태 무시

구성 요소 오류 상태 무시 대화 상자에서 관련된 정보를 받지 않을 구성 요소를 선택할 수 있습니다 .



기본적으로 이 목록에는 구성 요소가 선택되어 있지 않습니다 . 즉, 어떤 구성 요소가 특정한 오류 상태가 되면 사용자는 다음을 통해 즉시 그 사실을 통보받게 됩니다 .

- **시스템 트레이 아이콘** - AVG의 모든 부분이 올바르게 작동하면 아이콘이 4개의 색상으로 표시됩니다 . 하지만 , 오류가 발생하면 아이콘에 노란색 느낌표가 나타납니다 .
- AVG 기본 창의 **보안 상태 정보** 섹션에 문제에 대한 텍스트 설명이 표시됩니다 .

일시적으로 구성 요소를 해제해야 하는 경우가 있을 수 있습니다 . 이 방법은 권장되지 않는 방법으로 사용자는 모든 구성 요소를 기본 구성된 상태로 영구적으로 유지해야 하지만, 그렇지 않고 해제해야 할 수도 있습니다 . 이 경우 자동으로 시스템 트레이 아이콘

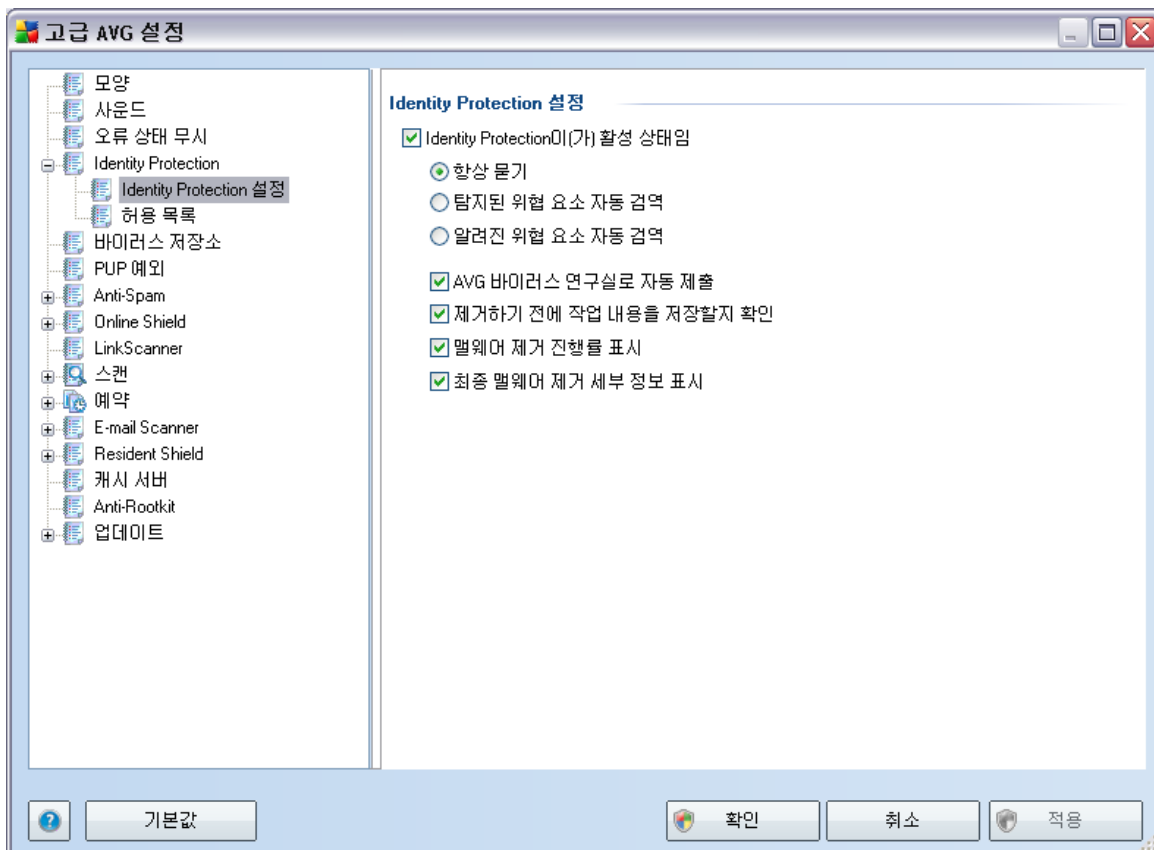
이 구성 요소의 오류 상태를 보고합니다 . 하지만 , 이는 사용자가 의도적으로 오류를 유도하여 잠재적인 위험 상황임을 인식하고 있으므로 실제 오류라고 언급할 만한 경우가 아닙니다 또한 회색으로 표시된 아이콘은 실제로 추가 발생할 수 있는 어떤 오류도 보고하지 못합니다 .

이 경우 위의 대화 상자에서 오류 상태 (또는 *해제된 상태*)에 있지만 해당 상태에 대한 알림을 받지 않으려는 구성 요소를 선택할 수 있습니다 . 같은 옵션인 **구성 요소 상태 무시**도 또한 [AVG 기본 창에 있는 구성 요소 개요](#)에서 바로 특정 구성 요소에 사용할 수 있습니다 .

10.4. Identity Protection

10.4.1. Identity Protection 설정

[Identity Protection 설정](#) 대화 상자에서는 [Identity Protection](#) 구성 요소의 기본 기능을 설정하거나 해제할 수 있습니다 .



Identity Protection이 활성화되었습니다 .(기본적으로 설정되어 있음) – **Identity Protection** 구성 요소를 해제하려면 선택을 취소합니다 .

특별한 경우가 아니면 선택을 취소하지 않는 것이 좋습니다 .

Identity Protection이 활성화되어 있으면 위협 요소가 발견될 때 수행할 작업을 다음과 같이 지정할 수 있습니다 .

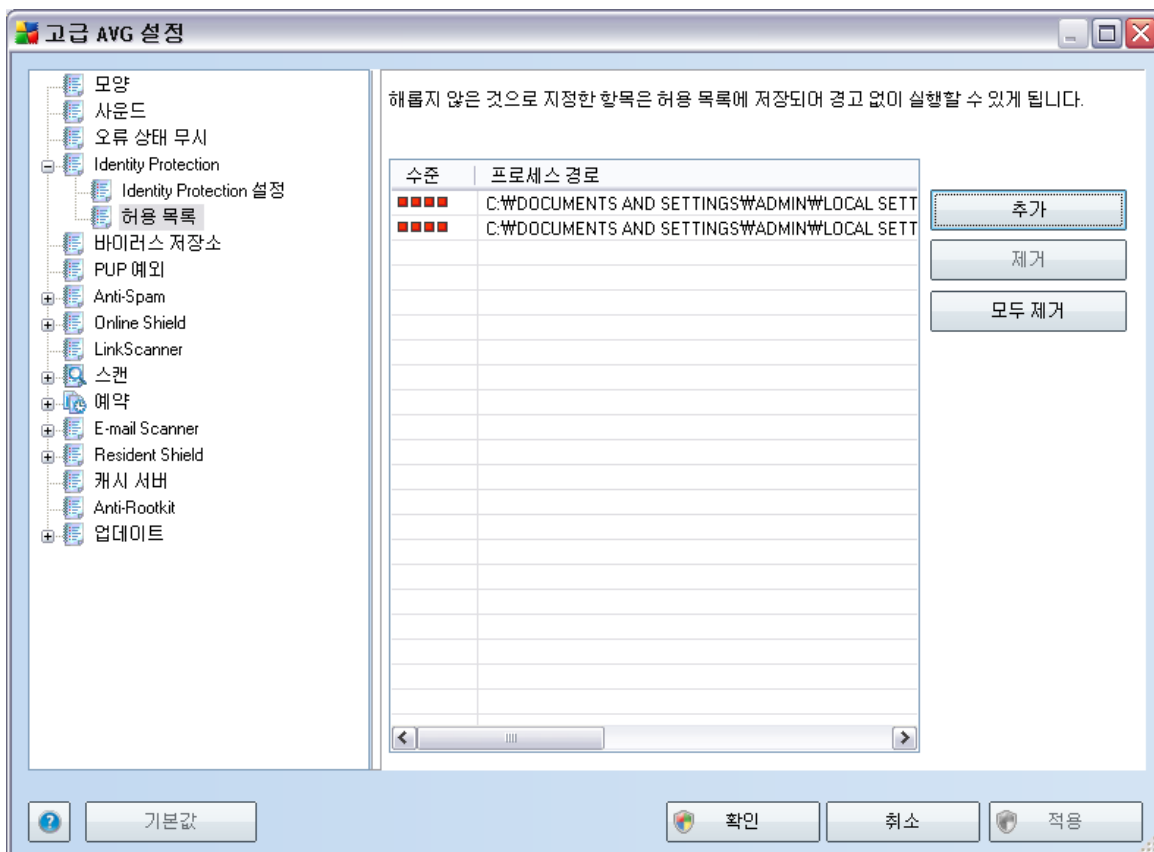
- **항상 묻기** (기본적으로 설정되어 있음) - 위협 요소가 발견될 경우 검역소로 이동할지 여부를 사용자에게 묻게 되므로 실행하고 싶은 응용 프로그램이 자동으로 제거되는 일을 방지할 수 있습니다 .
- **발견된 위협 요소 자동 검역** - 발견된 모든 위협 요소를 즉시 [AVG 바이러스 저장소](#)의 안전한 공간으로 이동하도록 정의하려면 이 확인란을 선택합니다 . 기본 설정을 유지하면 위협 요소가 발견될 경우 검역소로 이동할지 여부를 사용자에게 묻게 되므로 실행하고 싶은 응용 프로그램이 자동으로 제거되는 일을 방지할 수 있습니다 .
- **알려진 위협 요소 자동 검역** - 잠재적인 맬웨어로 탐지된 모든 응용 프로그램을 자동으로 즉시 [AVG 바이러스 저장소](#)로 이동하려면 이 항목을 선택한 상태로 유지합니다 .

또한 특정 항목을 지정하여 **Identity Protection** 기능을 좀 더 활성화할 수도 있습니다 .

- **AVG 바이러스 연구실에 자동 제출** (기본적으로 설정되어 있음): 웹 상에서의 악의적인 활동에 대한 데이터베이스 수집 정보를 제공하여 새로운 위협 요소를 쉽게 식별할 수 있도록 이 확인란을 선택된 상태로 유지합니다 .
- **제거하기 전에 작업 내용을 저장할지 확인** (기본적으로 설정되어 있음) - 잠재적인 맬웨어로 발견된 응용 프로그램을 검역소로 이동하여 제거하기 전에 경고를 받고 싶다면 이 항목을 선택한 상태로 유지합니다 . 응용 프로그램에서 작업하고 있다면 프로젝트가 손실될 수 있으므로 먼저 저장해야 합니다 . 기본적으로 이 항목은 설정되어 있으며 그대로 유지하는 것이 좋습니다 .
- **맬웨어 제거 진행률 표시** (기본적으로 사용) - 이 항목이 설정되어 있으면 잠재적인 맬웨어가 발견된 경우 맬웨어가 검역소로 이동되는 진행 상황을 표시하는 새 대화 상자가 나타납니다 .
- **최종 맬웨어 제거 세부 정보 표시** (기본적으로 사용) - 이 항목이 설정되어 있으면 **Identity Protection**에서 검역소로 이동된 각 개체에 대한 자세한 정보 (심각도 수준, 위치 등)를 표시합니다 .).

10.4.2. 허용 목록

Identity Protection 설정 대화 상자에서 **발견된 위험 요소 자동 검역** 항목을 선택 취소한 상태로 유지한 경우 위험한 맬웨어가 발견될 때마다 제거 여부를 묻는 메시지가 표시됩니다. 의심스러운 응용 프로그램 (동작을 기준으로 검색됨)을 안전한 응용 프로그램으로 지정하고 컴퓨터에 유지하도록 확인하면 해당 응용 프로그램이 **허용 목록**에 추가되고 잠재적으로 위험한 응용 프로그램으로 다시 보고되지 않습니다.



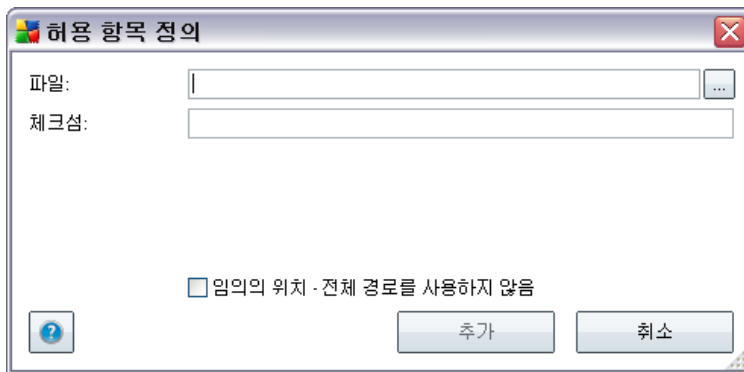
허용 목록에는 각 응용 프로그램에 대한 다음과 같은 정보가 표시됩니다.

- **수준** - 해당 프로세스의 심각도를 유해하지 않은 수준 (■□□□)부터 심각한 수준 (■■■■)에 이르기까지 네 단계로 나타내는 그래픽 표시
- **프로세스 경로** - 응용 프로그램 (프로세스)의 실행 파일이 위치한 경로
- **허용된 날짜** - 수동으로 응용 프로그램을 안전한 응용 프로그램으로 지정한 날짜

제어 단추

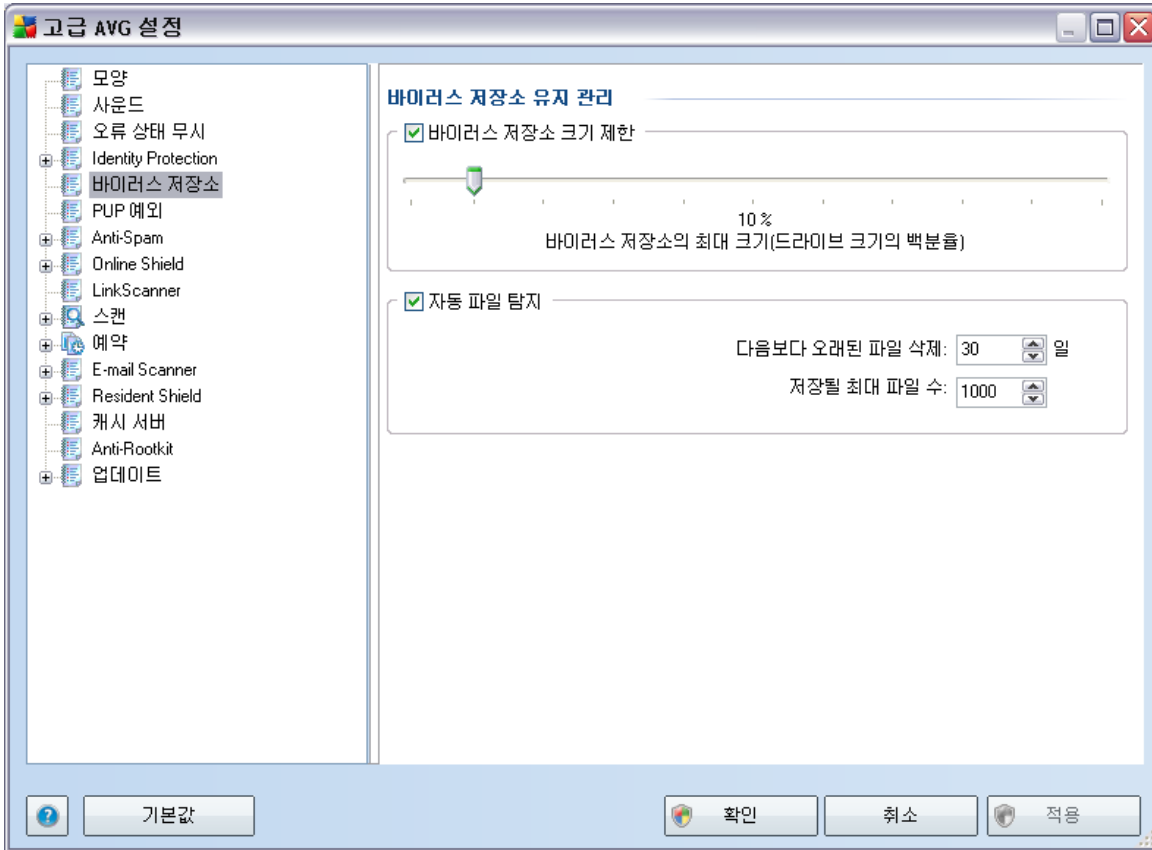
허용 목록 대화 상자에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **추가** - 새 응용 프로그램을 허용 목록에 추가하려면 이 단추를 누릅니다 . 다음 대화 상자가 나타납니다 .



- o **파일** - 예외로 표시할 파일 (응용 프로그램)에 대한 전체 경로를 입력합니다 .
 - o **체크섬** - 선택된 파일의 고유한 '서명'을 표시합니다 . 이 체크섬은 자동으로 생성되는 문자열로 , AVG에서는 체크섬을 통해 선택된 파일을 다른 파일과 구분합니다 . 체크섬은 파일이 추가된 후에 생성되어 표시됩니다 .
 - o **임의의 위치** - 전체 경로를 사용하지 않음 - 특정 위치에 있는 이 파일만을 예외로 정의하려는 경우에는 이 확인란을 선택하지 않은 상태로 두십시오 .
- **제거** - 선택한 응용 프로그램을 목록에서 제거하려면 누릅니다 .
 - **모두 제거** - 목록에 있는 모든 응용 프로그램을 제거하려면 누릅니다 .

10.5. 바이러스 저장소

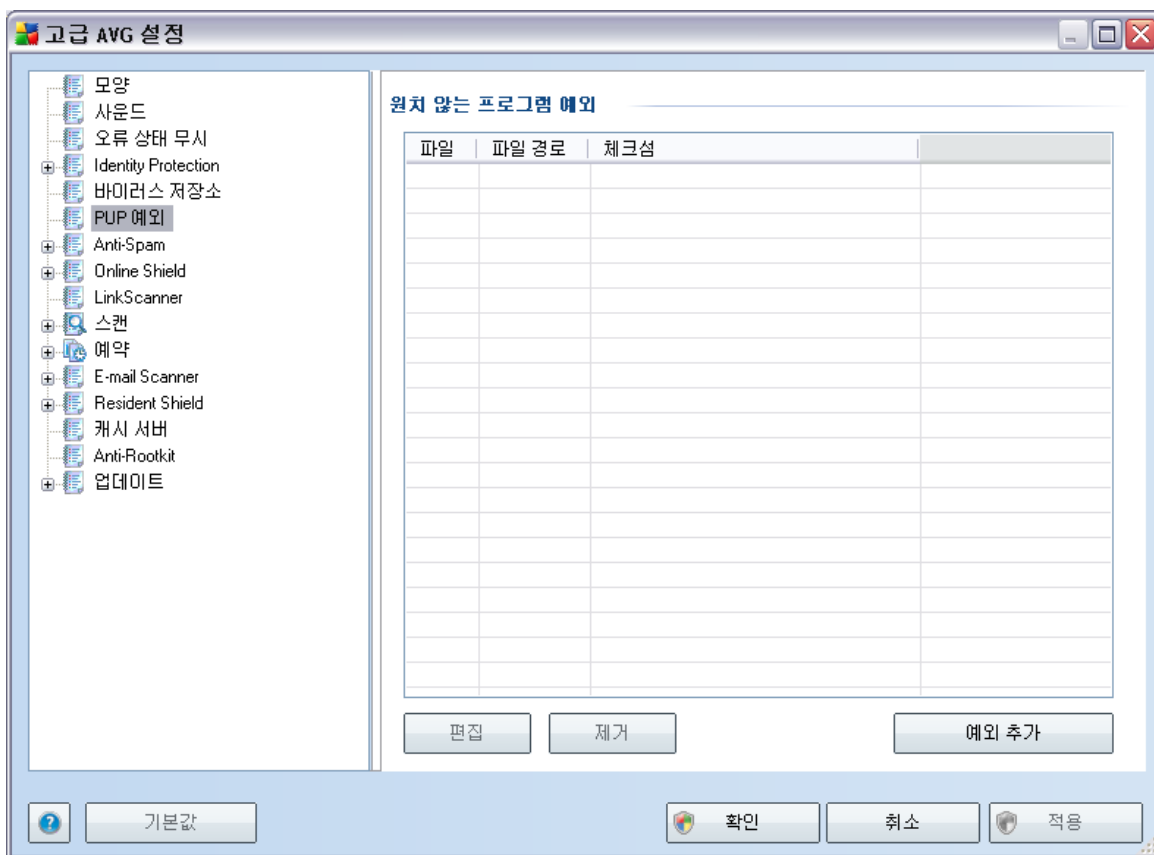


바이러스 저장소 유지 관리 대화 상자를 사용하여 **바이러스 저장소**에 저장된 개체를 관리하기 위한 몇 가지 매개 변수를 정의할 수 있습니다 .

- **바이러스 저장소 크기 제한** - 슬라이더를 사용하여 **바이러스 저장소**의 최대 크기를 설정합니다 . 크기는 로컬 디스크의 크기에 비례하여 지정합니다 .
- **자동 파일 삭제** - 이 섹션에서 개체가 **바이러스 저장소**에 저장되는 최대 기간 (**다음보다 오래된 파일 삭제**) 및 **바이러스 저장소**에 저장되는 파일의 최대 개 수 (저장될 최대 파일 수)를 정의합니다 .

10.6. PUP 예외

AVG 9 Internet Security 제품은 시스템에서 원치 않는 프로그램일 가능성이 있는 실행 가능 응용 프로그램 또는 DLL 라이브러리를 분석하고 검색할 수 있습니다 . 필요한 경우 컴퓨터에서 원치 않는 특정 프로그램을 그대로 유지할 수도 있습니다 (*일부러 설치한 프로그램인 경우*). 무료 프로그램 등의 일부 프로그램은 애드웨어일 수 있습니다 . AVG에서는 그러한 애드웨어를 **원치 않는 프로그램** 으로 검색하여 보고합니다 . 컴퓨터에서 그러한 프로그램을 그대로 유지하고자 할 때는 원치 않는 프로그램에 대한 예외로 정의할 수 있습니다 .



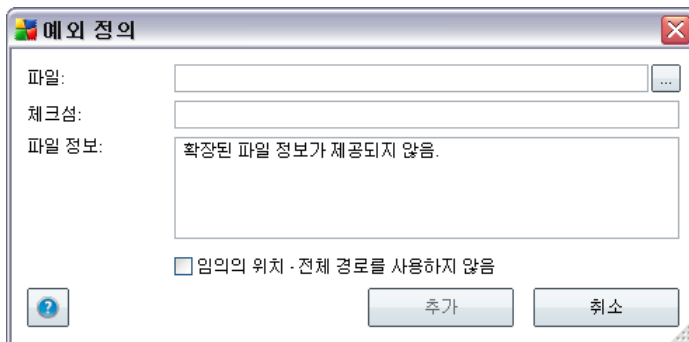
원치 않는 프로그램 예외 대화 상자에는 기존에 이미 원치 않는 프로그램에 대한 예외로 정의되어 현재 사용되고 있는 예외 목록이 표시됩니다 . 목록을 편집하거나 기존 항목을 삭제하거나 새 예외를 추가할 수 있습니다 . 각 예외에 대해 목록에서 다음 정보를 찾을 수 있습니다 .

- **파일** - 해당 응용 프로그램의 이름을 제공합니다 .

- **파일 경로** - 응용 프로그램이 위치한 경로를 표시합니다 .
- **체크섬** - 선택된 파일의 고유한 '서명'을 표시합니다 . 이 체크섬은 자동으로 생성되는 문자열로 , AVG에서는 체크섬을 통해 선택된 파일을 다른 파일과 구분합니다 . 체크섬은 파일이 추가된 후에 생성되어 표시됩니다 .

제어 단추

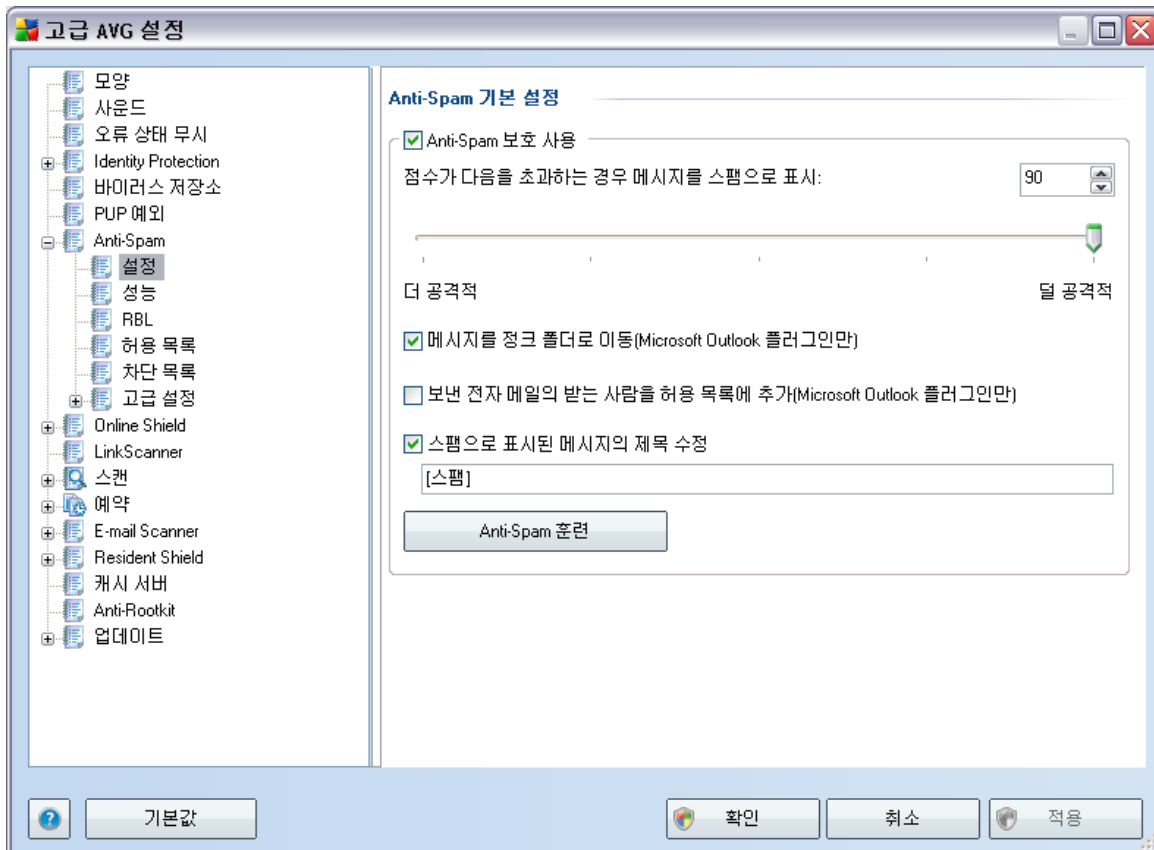
- **편집** - 이미 정의된 예외에 대한 편집 대화 상자를 엽니다 (*아래의 새로운 예외 정의 대화 상자*와 동일). 여기서 예외 매개 변수를 변경할 수 있습니다 .
- **제거** - 예외 목록에서 선택된 항목을 삭제합니다 .
- **예외 추가** - 생성할 새로운 예외 매개 변수를 정의할 수 있는 편집 대화 상자를 엽니다 .



- **파일** - 예외로 지정할 파일에 대한 전체 경로를 입력합니다 .
- **체크섬** - 선택된 파일의 고유한 '서명'을 표시합니다 . 이 체크섬은 자동으로 생성되는 문자열로 , AVG에서는 체크섬을 통해 선택된 파일을 다른 파일과 구분합니다 . 체크섬은 파일이 추가된 후에 생성되어 표시됩니다 .
- **파일 정보** - 파일에 대한 추가적인 정보 (*라이선스 / 버전 정보* 등)를 표시합니다 .
- **임의의 위치 - 전체 경로를 사용하지 않음** - 특정 위치에 있는 이 파일만을 예외로 정의하려는 경우에는 이 확인란을 선택하지 않은 상태로 두십시오 .

10.7. Anti-Spam

10.7.1. 설정



Anti-Spam 기본 설정 대화 상자에서 **Anti-Spam 보호 사용** 확인란을 선택하거나 선택 취소하여 전자 메일 커뮤니케이션의 스팸 방지 스캔을 허용하거나 차단할 수 있습니다 . 이 옵션은 기본적으로 설정되어 있으며 다른 옵션과 마찬가지로 반드시 변경해야 할 경우가 아니라면 이 구성을 유지하는 것이 좋습니다 .

다음으로 공격적인 정도를 나타내는 점수를 선택할 수도 있습니다 . **Anti-Spam** 필터는 몇 가지 동적 스캔 기술을 기반으로 각 메시지에 점수 (즉, 메시지 내용이 스팸과 유사한 정도) 를 할당합니다 . **0에서 100** 사이의 값을 입력하거나 슬라이더를 왼쪽 또는 오른쪽으로 이동하여 (슬라이더를 사용하면 값 범위는 50에서 90 사이로 제한됨) 점수가 다음을 초과하는 경우 메시지를 스팸으로 표시 설정을 조정할 수 있습니다 .

일반적으로 임계값을 50에서 90 사이로 설정하는 것이 좋습니다 . 확신이 없으면 90으로 설정하는 것을 권장합니다 . 점수 임계값을 전반적으로 살펴보면 다음과 같습니다 .

- **90 ~ 99 값** - 대부분의 들어오는 전자 메일 메시지가 정상적으로 전달됩니다 ([스팸](#) 으로 표시되지 않음). 가장 쉽게 식별되는 [스팸](#) 은 필터링되지만 대량의 [스팸](#) 은 허용될 수 있습니다 .
- **80 ~ 89 값** - [스팸](#) 일 가능성이 있는 전자 메일 메시지가 필터링되며 스팸이 아닌 일부 메시지도 잘못 필터링될 수 있습니다 .
- **60 ~ 79 값** - 어느 정도 공격적인 구성으로 간주됩니다 . [스팸](#) 일 가능성이 있는 전자 메일 메시지가 필터링되며 스팸이 아닌 메시지도 필터링될 수 있습니다 .
- **1 ~ 59 값** - 매우 공격적인 구성입니다 . 스팸이 아닌 전자 메일 메시지도 실제 [스팸](#) 메시지로 필터링될 수 있습니다 . 이 임계값 범위는 일반 사용자에게는 권장되지 않습니다 .
- **0 값** - 이 모드에서는 사용자의 [허용 목록](#) 에 포함된 보낸 사람이 전송한 전자 메일 메시지만 받을 수 있습니다 . 그리고 기타 전자 메일 메시지는 [스팸](#) 으로 간주됩니다 . **이 임계값 범위는 일반 사용자에게는 권장되지 않습니다 .**

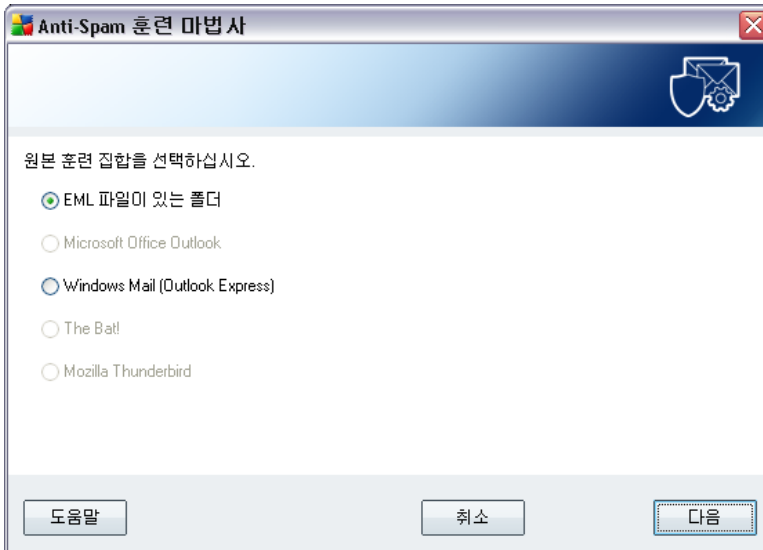
Anti-Spam 기본 설정 대화 상자에서는 발견된 [스팸](#) 전자 메일 메시지를 어떻게 처리할지 세부적으로 정의할 수 있습니다 .

- **메시지를 정크 폴더로 이동** - 이 확인란을 선택하면 발견된 각 스팸 메시지를 사용자 전자 메일 클라이언트 내의 특정 정크 폴더로 자동 이동하도록 지정할 수 있습니다 .
- **보낸 전자 메일의 수신자를 [허용 목록](#) 에 추가** - 이 확인란을 선택하면 보낸 전자 메일의 모든 수신자를 신뢰하고 , 이러한 수신자의 전자 메일 계정에서 들어오는 전자 메일 메시지가 모두 전달되도록 확인할 수 있습니다 .
- **스팸으로 표시된 메시지의 제목 수정** - 이 확인란을 선택하면 [스팸](#) 으로 발견된 모든 메시지의 전자 메일 제목 필드에 특정 단어나 문자를 표시하거나 , 활성화된 텍스트 필드에 원하는 텍스트를 입력할 수 있습니다 .

제어 단추

Anti-Spam 교육 단추를 누르면 [다음 장](#)에 자세한 내용이 설명된 [***Anti-Spam 교육](#) 마법사가 열립니다 .

Anti-spam 교육 마법사의 첫 번째 대화 상자에서는 교육에 사용할 전자 메일 메시지의 원본을 선택하라는 메시지가 나타납니다. 일반적으로 스팸 메일로 잘못 표시된 전자 메일 또는 확인되지 않은 스팸 메시지를 사용해야 할 경우가 있습니다.



선택할 수 있는 옵션은 다음과 같습니다.

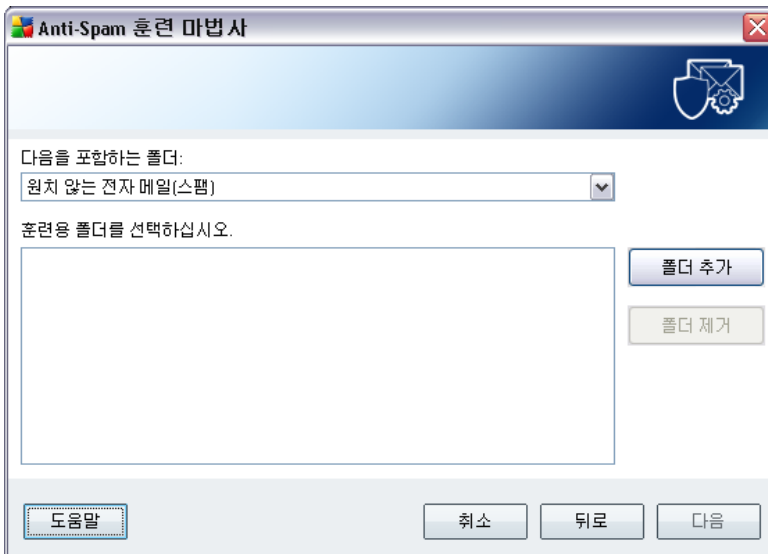
- **특정 전자 메일 클라이언트** - 나열된 전자 메일 클라이언트 (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*) 중 하나를 사용하는 경우 해당 옵션을 선택하면 됩니다.
- **EML 파일이 있는 폴더** - 다른 전자 메일 프로그램을 사용하려면 우선 메시지를 특정 폴더에 *.eml* 형식으로 저장하거나 전자 메일 클라이언트 메시지 폴더의 위치를 알고 있어야 합니다. 그런 다음 **EML 파일이 있는 폴더**를 선택하면 다음 단계에서 원하는 폴더를 찾을 수 있습니다.

교육 프로세스를 보다 빠르고 쉽게 진행하려면 먼저 폴더에서 전자 메일을 정렬하여 교육에 사용할 폴더에 교육 메시지 (원하거나 원치 않는 메시지)만 포함되도록 하는 것이 좋습니다. 그러나 나중에 전자 메일을 필터링할 수 있으므로 이 과정을 수행하지 않아도 됩니다.

해당 옵션을 선택하고 **다음**을 클릭하여 마법사를 계속 진행합니다.

이 단계에서 표시되는 대화 상자는 이전에 선택한 항목에 따라 달라집니다 .

EML 파일이 있는 폴더



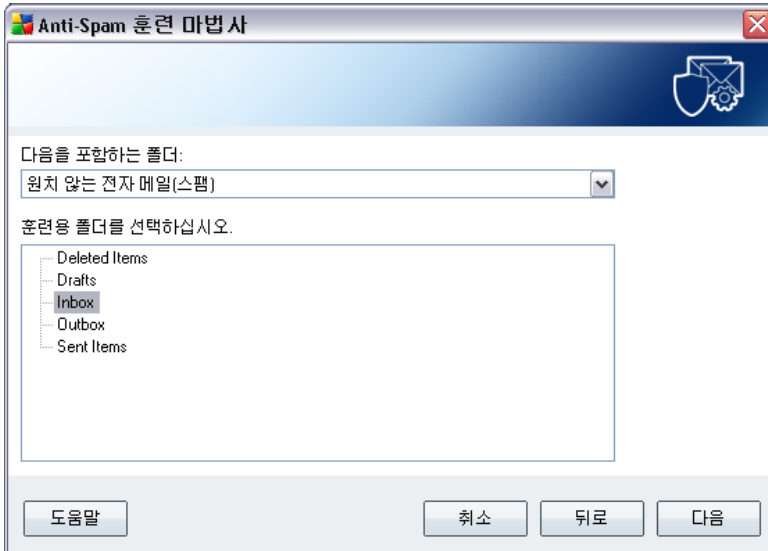
이 대화 상자에서는 교육에 사용할 메시지가 있는 폴더를 선택합니다 . **폴더 추가** 단추를 눌러 .eml 파일 (*저장된 전자 메일 메시지*) 이 있는 폴더를 찾습니다 . 그러면 선택한 폴더가 대화 상자에 나타납니다 .

다음에 포함하는 폴더 드롭다운 메뉴에서 선택한 폴더에 원하는 메시지 (*햄*) 가 포함되었음을 나타내는 옵션 또는 원치 않는 메시지 (*스팸*) 가 포함되었음을 나타내는 옵션 중 하나를 설정합니다 . 다음 단계에서 메시지를 필터링할 수 있으므로 폴더에 교육 전자 메일만 포함되지 않아도 됩니다 . **폴더 제거** 단추를 클릭하면 선택된 원치 않는 폴더를 목록에서 제거할 수도 있습니다 .

완료되면 **다음** 을 클릭한 후 [메시지 필터링 옵션](#) 으로 진행합니다 .

특정 전자 메일 클라이언트

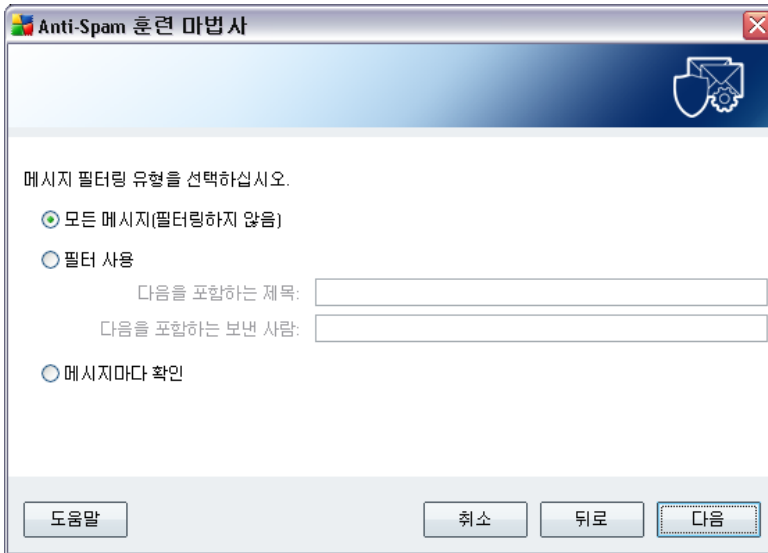
옵션 중 하나를 확인하면 새 대화 상자가 나타납니다 .



참고 : Microsoft Office Outlook의 경우 먼저 MS Office Outlook 프로파일을 선택하라는 메시지가 나타납니다 .

다음에 포함하는 폴더 드롭다운 메뉴에서 선택한 폴더에 원하는 메시지 (햄)가 포함되어 있음을 나타내는 옵션 또는 원치 않는 메시지 (스팸)가 포함되어 있음을 나타내는 옵션 중 하나를 설정합니다 . 다음 단계에서 메시지를 필터링할 수 있으므로 폴더에 교육 전자 메일만 포함되지 않아도 됩니다 . 선택한 전자 메일 클라이언트의 탐색 트리가 대화 상자의 기본 섹션에 표시됩니다 . 트리에서 원하는 폴더를 찾아 마우스로 강조 표시합니다 .

완료되면 **다음** 을 클릭한 후 **메시지 필터링 옵션** 으로 진행합니다 .



이 대화 상자에서는 전자 메일 메시지의 필터링을 설정할 수 있습니다 .

선택한 폴더에 학습에 사용할 메시지만 있는 경우 **모든 메시지 (필터링하지 않음)** 옵션을 선택합니다 .

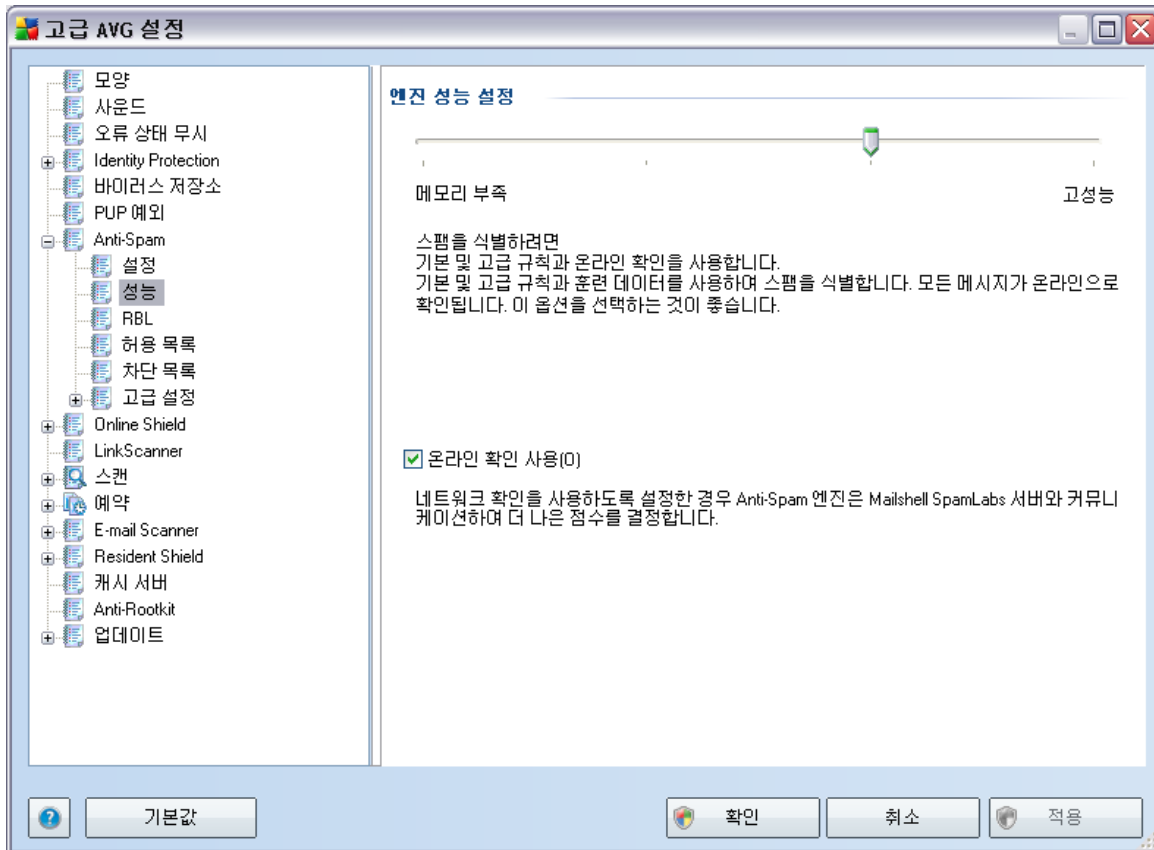
폴더에 어떤 메시지가 포함되어 있는지 확실하지 않아 메시지를 교육에 사용할지 여부를 각 메시지별로 결정하려면 **메시지마다 확인** 옵션을 선택합니다 .

다른 고급 필터링을 사용하려면 **필터 사용** 옵션을 선택합니다 . 전자 메일 제목 및 / 또는 보낸 사람 필드에서 검색할 단어 (*이름*), 단어의 일부 또는 구를 입력할 수 있습니다 . 더 이상 묻는 메시지가 나타나지 않고 입력한 조건과 정확하게 일치하는 모든 메시지가 학습에 사용됩니다 .

주의 !: 두 텍스트 필드를 모두 입력하면 두 조건 중 하나와 일치하는 주소도 역시 사용 됩니다 !

적절한 옵션을 선택한 후에는 **다음** 을 클릭합니다 . 다음 대화 상자는 마법사가 메시지를 처리할 준비가 되었음을 알려줍니다 . 교육을 시작하려면 **다음** 단추를 다시 클릭합니다 . 이제 이전에 선택한 조건에 따라 교육이 시작됩니다 .

10.7.2. 성능



엔진 성능 설정 대화 상자 (왼쪽 탐색 창의 **성능** 항목을 통해 연결)에서는 **Anti-Spam** 구성 요소 성능을 설정할 수 있습니다. 슬라이더를 왼쪽이나 오른쪽으로 옮기면 **메모리 부족**과 **고성능** 모드 사이에서 스캔 성능 수준을 조정할 수 있습니다.

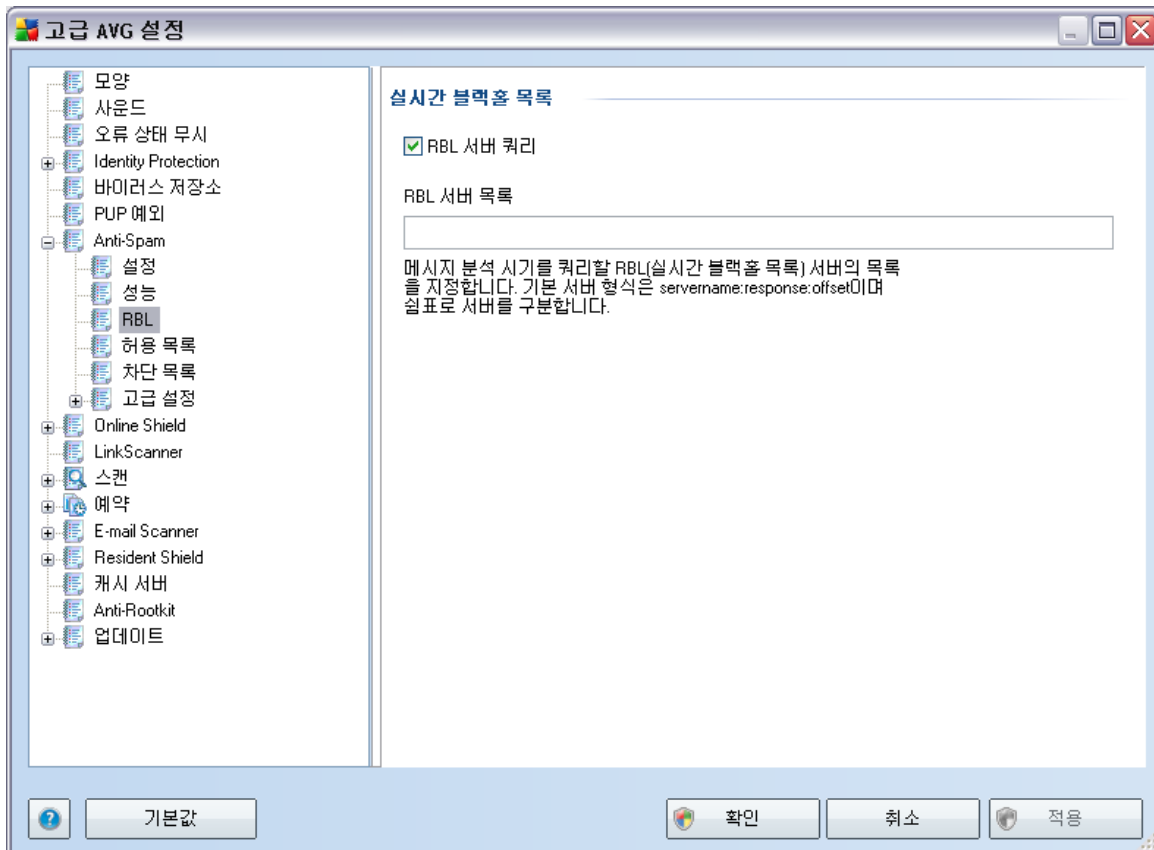
- **메모리 부족** - **스팸**을 식별하는 스캔 프로세스 중에 규칙이 사용되지 않습니다. 교육 데이터만 식별에 사용됩니다. 컴퓨터 하드웨어 성능이 매우 낮은 경우에만 이 모드를 사용하는 것이 좋습니다.
- **고성능** - 이 모드는 많은 양의 메모리를 사용합니다. **스팸**을 식별하는 스캔 프로세스 중에 규칙, **스팸** 데이터베이스 캐시, 기본 및 고급 규칙, 스팸 IP 주소, 스팸 데이터베이스 등의 기능이 사용됩니다.

온라인 확인 사용 항목은 기본적으로 설정되어 있습니다. 이 옵션이 설정된 경우 **Mailshell** 서버와의 커뮤니케이션을 통해 보다 정확한 스팸 ***검색이 가능합니다. 스캔된 데이터는 온라인에서 **Mailshell** 데이터베이스와 비교됩니다.

가급적이면 기본 설정을 그대로 유지하고 타당한 이유가 있는 경우에만 설정을 변경하는 것이 좋습니다 . 모든 구성 변경은 숙련된 사용자가 수행해야 합니다 .

10.7.3. RBL

RBL 항목을 클릭하면 **실시간 블랙홀 목록** 이라는 편집 대화 상자가 열립니다 .



이 대화 상자에서 **RBL 서버 쿼리** 기능을 설정 또는 해제할 수 있습니다 .

RBL(**실시간 블랙홀 목록**) 서버는 스팸을 보내는 사람들에 대한 광범위한 데이터베이스를 가진 DNS 서버입니다 . 이 기능이 설정된 경우 모든 전자 메일 메시지가 RBL 서버 데이터베이스에서 확인되고 데이터베이스에서 동일한 항목이 발견되면 **스팸**으로 표시됩니다 . RBL 서버 데이터베이스에는 가장 최신의 스팸 자료가 포함되어 있으므로 최상의 정확한 **스팸** 검색이 가능합니다 . 이 기능은 보통 **Anti-Spam** 엔진으로 검색할 수 없는 스팸을 다량으로 받는 사용자에게 특히 유용합니다 .

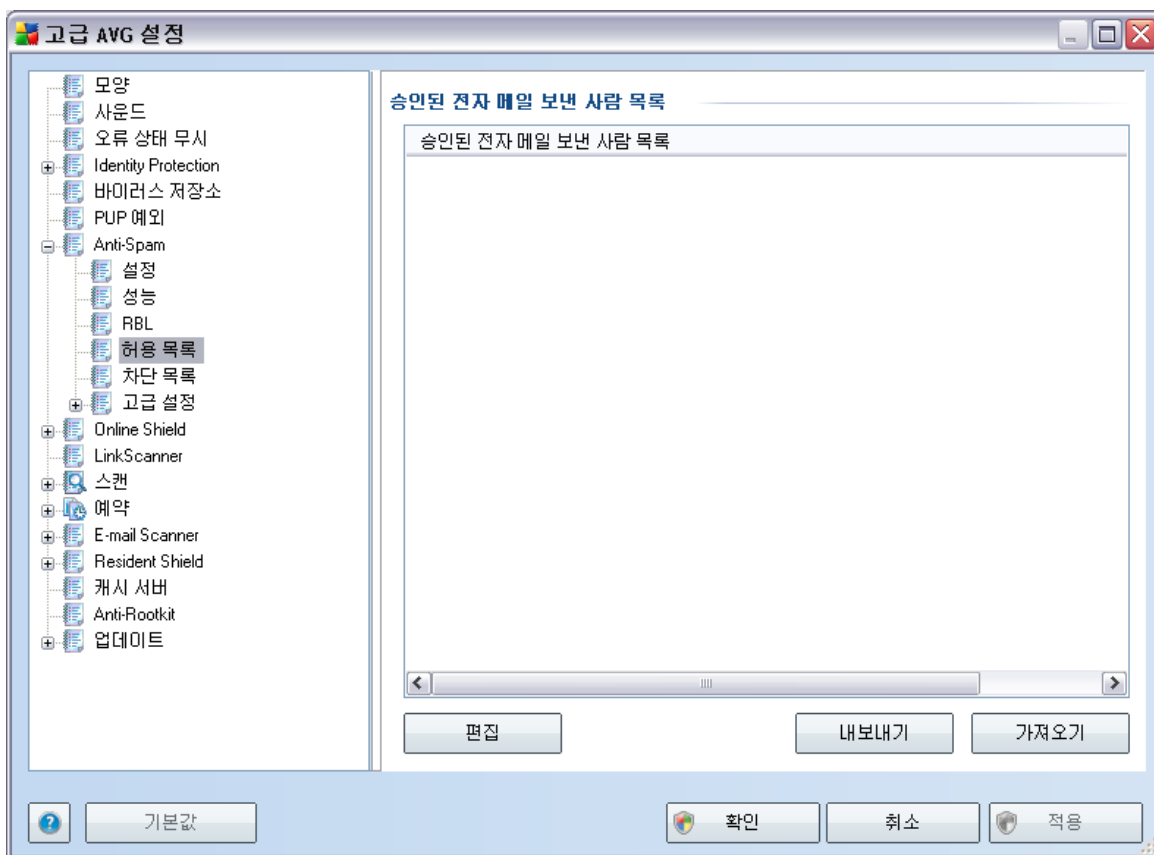
RBL 서버 목록 에 특정 RBL 서버 위치를 정의할 수 있습니다 .

참고 : 일부 시스템 및 구성에서 이 기능을 사용하면 RBL 서버 데이터베이스에서 모든 메시지를 확인하기 때문에 전자 메일 수신 프로세스가 느려질 수 있습니다 .

개인 데이터는 서버에 전송되지 않습니다 .

10.7.4. 허용 목록

허용 목록 항목은 승인된 보낸 사람의 전자 메일 주소 및 도메인 이름에 대한 전역 목록을 포함하는 **승인된 전자 메일 보낸 사람 목록** 대화 상자를 엽니다 . 이러한 보낸 사람으로부터 온 메시지는 스팸으로 표시되지 않습니다 .



편집 인터페이스에서 사용자에게 원치 않는 메시지 (스팸)를 보내지 않을 것으로 예상되는 보낸 사람 목록을 만들 수 있습니다 . 또한 스팸 메시지를 만들지 않는다고 사용자가 알고 있는 전체 도메인 이름 (예: avg.com)의 목록을 만들 수도 있습니다 .

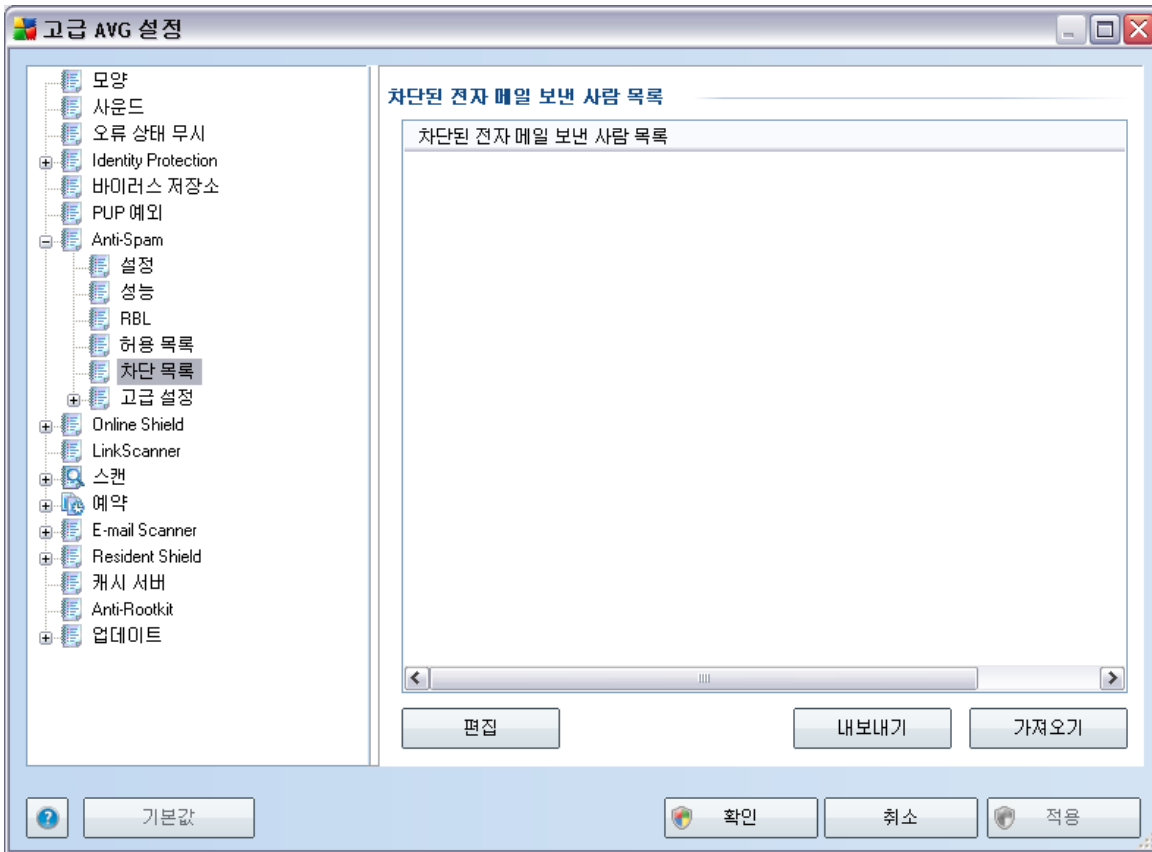
보낸 사람 및/또는 도메인 이름 목록을 준비했으면 각 전자 메일 주소를 직접 입력하거나 전체 주소 목록을 한꺼번에 가져오는 방법으로 이들 항목을 입력할 수 있습니다 . 사

용할 수 있는 제어 단추는 다음과 같습니다 .

- **편집** - 이 단추를 누르면 주소 목록을 수동으로 입력할 수 있는 대화 상자가 열립니다 . 이 대화 상자에서는 복사 및 붙여넣기를 사용할 수도 있습니다 . 한 줄에 한 항목 (보낸 사람, 도메인 이름)씩 입력합니다 .
- **내보내기** - 특정 용도로 레코드를 내보내야 하는 경우 이 단추를 눌러 레코드를 내보낼 수 있습니다 . 모든 레코드는 일반 텍스트 파일로 저장됩니다 .
- **가져오기** - 전자 메일 주소 /도메인 이름으로 구성된 텍스트 파일을 이미 준비한 경우 이 단추를 선택하여 간단하게 파일의 항목을 가져올 수 있습니다 . 입력 파일은 일반 텍스트 형식이어야 하며 해당 내용은 한 줄에 한 항목 (주소, 도메인 이름)만 포함해야 합니다 .

10.7.5. 차단 목록

차단 목록 항목은 차단된 보낸 사람 전자 메일 주소 및 도메인 이름에 대한 전역 목록이 포함된 대화 상자를 엽니다 . 이러한 주소로부터 온 메시지는 항상 [스팸](#)으로 표시됩니다 .



편집 인터페이스에서 원치 않는 메시지 (**스팸**)를 보낼 것으로 예상되는 보낸 사람 목록을 만들 수 있습니다 . 또한 스팸 메시지를 보낼 것으로 예상되는 전체 도메인 이름 (예 : *spammingcompany.com*) 목록을 만들 수도 있습니다 . 이러한 목록에 포함된 주소 /도메인에서 전송되는 전자 메일은 모두 스팸으로 식별됩니다 .

보낸 사람 및 /또는 도메인 이름 목록을 준비했으면 각 전자 메일 주소를 직접 입력하거나 전체 주소 목록을 한꺼번에 가져오는 방법으로 이들 항목을 입력할 수 있습니다 . 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **편집** - 이 단추를 누르면 주소 목록을 수동으로 입력할 수 있는 대화 상자가 열립니다 . 이 대화 상자에서는 복사 및 붙여넣기를 사용할 수도 있습니다 . 한 줄에 한 항목 (보낸 사람, 도메인 이름)씩 입력합니다 .
- **내보내기** - 특정 용도로 레코드를 내보내야 하는 경우 이 단추를 눌러 레코드를 내보낼 수 있습니다 . 모든 레코드는 일반 텍스트 파일로 저장됩니다 .
- **가져오기** - 전자 메일 주소 /도메인 이름으로 구성된 텍스트 파일을 이미 준비

한 경우 이 단추를 선택하여 간단하게 파일의 항목을 가져올 수 있습니다 . 입력 파일은 일반 텍스트 형식이어야 하며 해당 내용은 한 줄에 한 항목 (주소, 도메인 이름)만 포함해야 합니다 .

10.7.6. 고급 설정

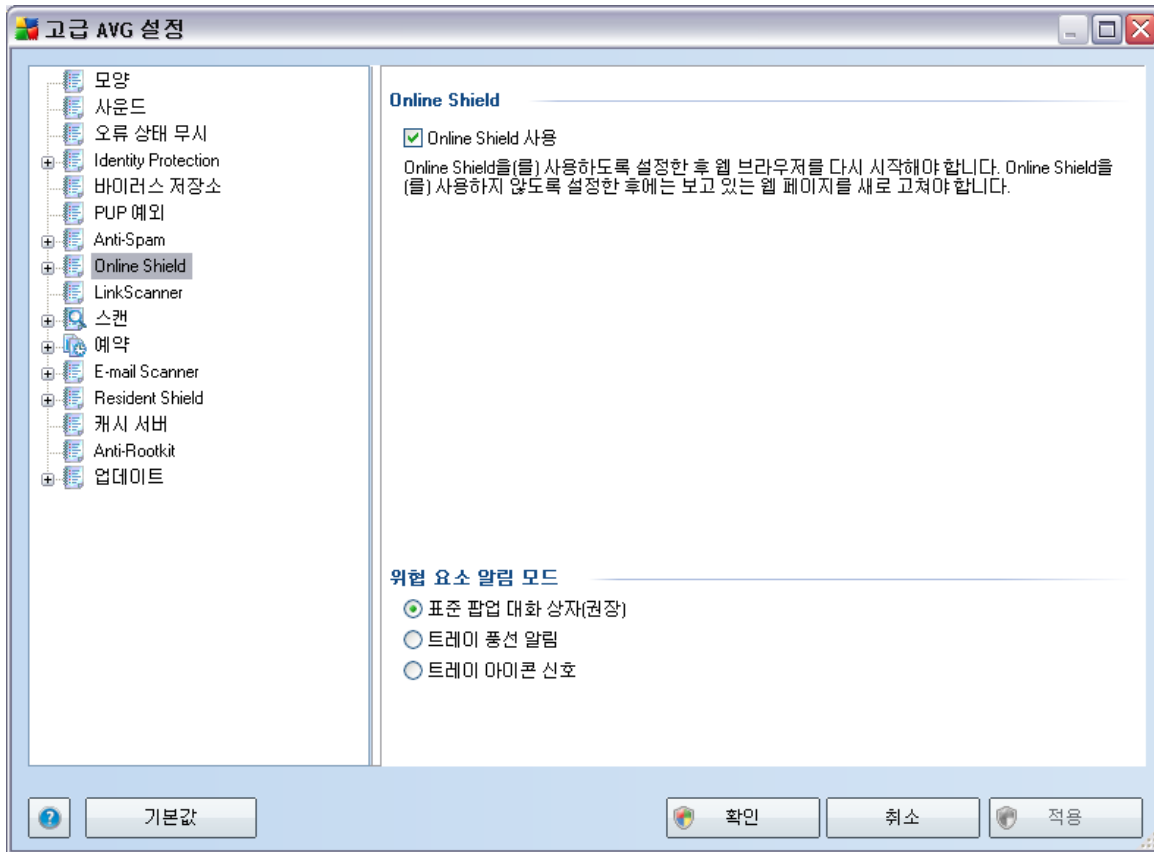
고급 설정 분기에는 **Anti-Spam** 구성 요소에 대한 광범위한 설정 옵션이 들어 있습니다 . 이러한 설정은 일반적으로 전자 메일 서버를 최적으로 보호하기 위해 스팸 방지 보호 기능을 세부적으로 완벽하게 구성해야 하는 네트워크 관리자 같은 숙련된 사용자를 위한 것입니다 . 이러한 이유로 개별 대화 상자에는 추가적인 도움말이 없습니다 . 그러나 사용자 인터페이스에 각 옵션에 대한 간단한 설명이 직접 제공됩니다 .

Spamcatcher(MailShell Inc.)의 고급 설정에 대해 완벽하게 이해하고 있지 않은 경우에는 설정을 변경하지 마십시오 . 파일을 임의로 변경하면 성능이 저하되거나 구성 요소가 제대로 동작하지 않을 수 있습니다 .

그래도 **Anti-Spam** 구성을 세부적으로 변경해야 한다면 사용자 인터페이스에서 직접 제공하는 지침을 따르십시오 . 일반적으로 각 대화 상자는 하나의 특정한 기능을 제공하며 이를 편집할 수 있습니다 . 각 대화 상자에는 항상 지원하는 기능에 대한 설명을 제공합니다 .

- **캐시** - 지문, 도메인 신뢰도, LegitRepute
- **훈련** - 최대 단어 항목 수, 자동 훈련 임계값, 가중치
- **필터링** - 언어 목록, 국가 목록, 승인된 IP, 차단된 IP, 차단된 국가, 차단된 문자 집합, 스푸핑한 보낸 사람
- **RBL** - RBL 서버, 다중 적중, 임계값, 제한 시간, 최대 IP 수
- **인터넷 연결** - 제한 시간, 프록시 서버, 프록시 인증

10.8. Online Shield



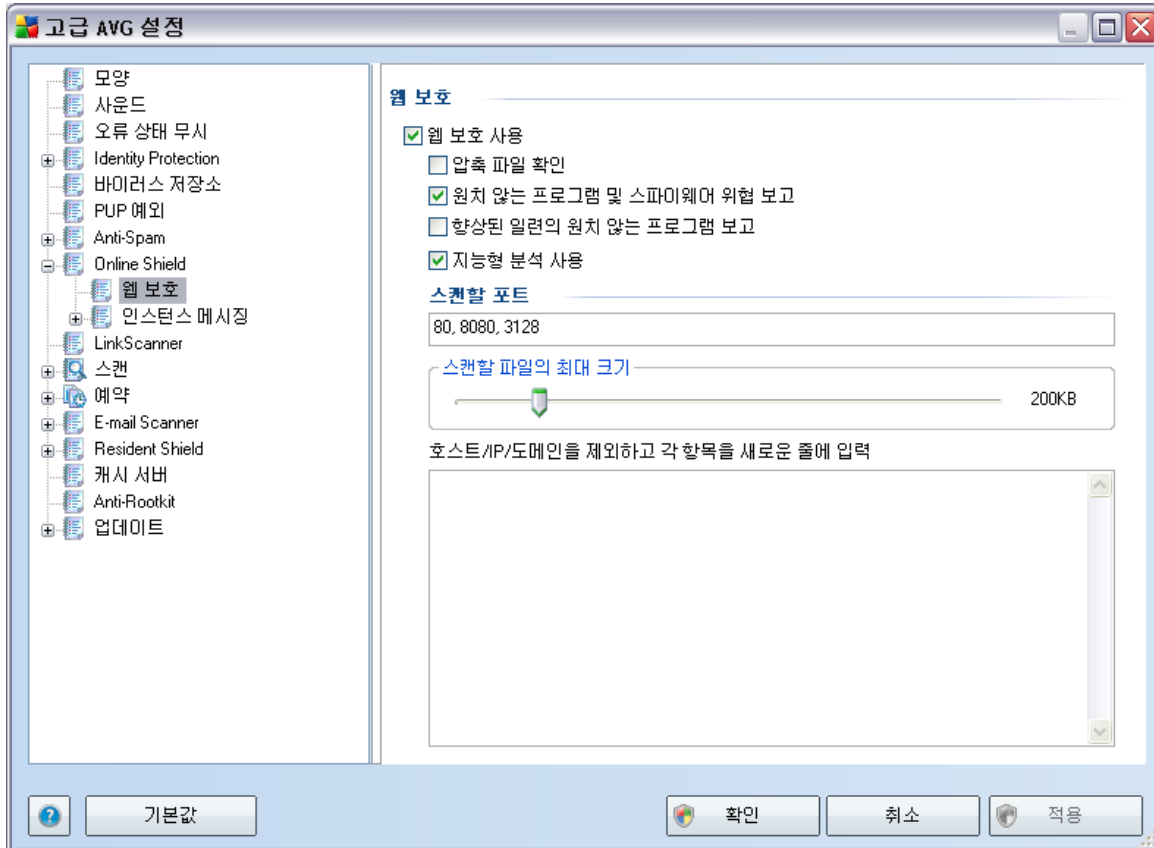
웹 보호 대화 상자에서는 [Online Shield 사용](#) 옵션을 통해 전체 **Online Shield** 구성 요소를 활성화 / 비활성화할 수 있습니다 (기본적으로 활성화되어 있음). 이 구성 요소에 대한 추가 고급 설정은 트리 탐색에 나열되는 이후의 대화 상자에서 계속할 수 있습니다 .

- [웹 보호](#)
- [인스턴트 메시징](#)

알림 모드 처리

발견된 위험 요소를 알릴 때 표준 팝업 대화 상자를 사용할지 , 트레이 풍선 알림을 사용할지 , 트레이 아이콘 정보를 사용할지를 대화 상자의 아래쪽 섹션에서 선택합니다 .

10.8.1. 웹 보호



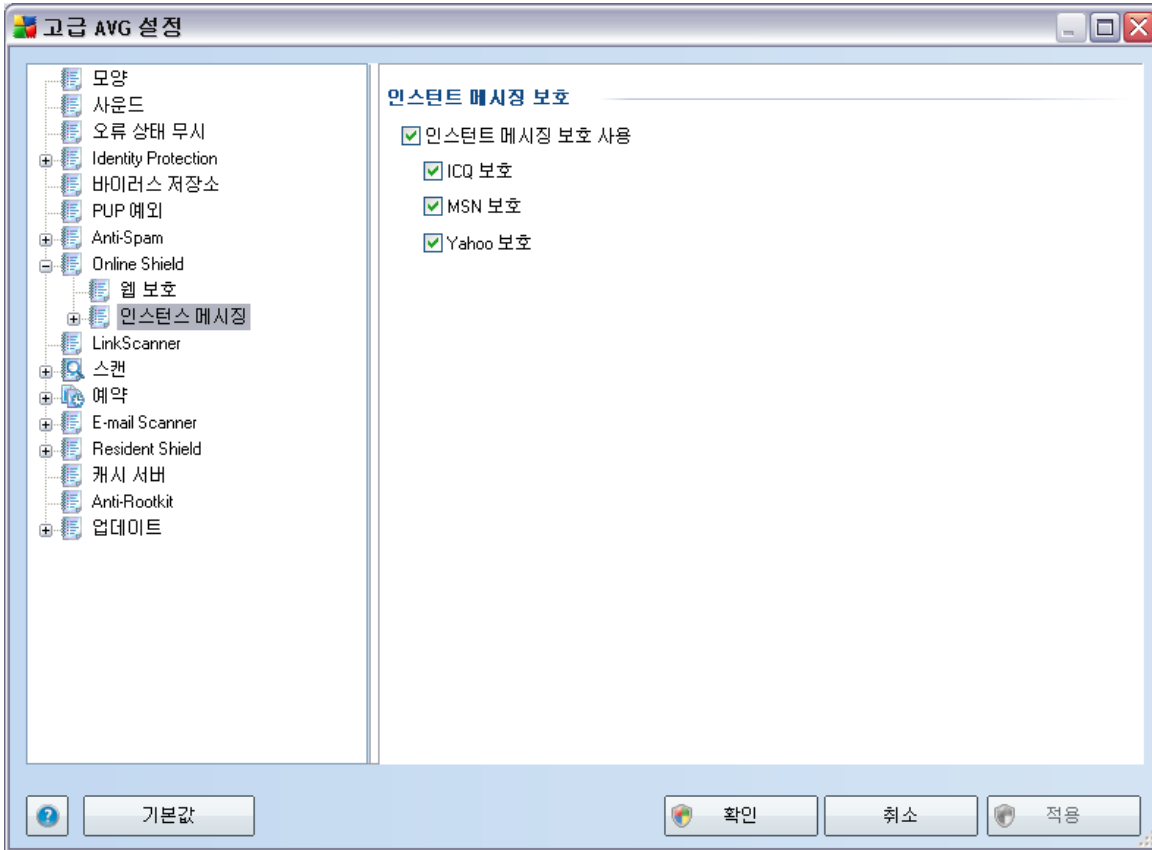
웹 보호 대화 상자에서 웹 사이트 콘텐츠의 스캔에 관한 구성 요소의 구성을 편집할 수 있습니다. 편집 인터페이스를 사용하면 다음과 같은 기본적인 옵션을 구성할 수 있습니다.

- **웹 보호 사용** - 이 옵션을 선택하면 **Online Shield**가 www 페이지의 콘텐츠에 대한 스캔을 수행합니다. 이 옵션을 선택한 경우 (기본적으로 설정되어 있음) 추가로 다음 항목을 설정 또는 해제할 수 있습니다.
 - **압축 파일 확인** - 표시할 www 페이지에 포함된 압축 파일의 콘텐츠를 스캔합니다.
 - **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - **Anti-Spyware** 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위험을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될

수 있습니다. 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다 .

- o **향상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 스파이웨어 의 확장 패키지를 검색하려면 이 상자를 선택합니다 . 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만 , 나중에 악의적인 목적으로 잘못 사용될 수 있습니다 . 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만 , 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다 .
- o **지능형 분석 사용** - 표시할 페이지의 콘텐츠를 지능형 분석 방법 (가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)을 사용하여 스캔합니다 .
- o **스캔할 포트** - 이 필드에는 표준 http 커뮤니케이션 포트 번호가 나열됩니다 . 컴퓨터의 구성이 다른 경우 필요에 따라 포트 번호를 변경할 수 있습니다 .
- o **스캔할 파일의 최대 크기** - 포함된 파일이 표시된 페이지에 존재하는 경우 파일을 컴퓨터로 다운로드하기 전에 파일의 콘텐츠를 스캔할 수도 있습니다 . 하지만 큰 파일의 스캔에는 약간의 시간이 걸리며 웹 페이지 다운로드가 상당히 느려질 수 있습니다 . 슬라이드 막대를 사용하여 Online Shield로 스캔할 파일의 최대 크기를 지정할 수 있습니다 . 다운로드한 파일이 지정한 크기보다 커서 Online Shield로 스캔할 수 없는 경우라 하더라도 사용자의 컴퓨터는 여전히 보호됩니다 . 파일이 감염된 경우에는 상주 보호가 즉시 이를 검색합니다 .
- o **호스트 / IP/ 도메인 제외** - 텍스트 필드에는 Online Shield가 스캔하지 않아도 되는 서버 (호스트 , IP 주소 , 마스크가 있는 IP 주소 또는 URL) 또는 도메인의 정확한 이름을 입력할 수 있습니다 . 따라서 위험한 웹 사이트 콘텐츠를 제공하지 않는다고 확신할 수 있는 호스트만 제외해야 합니다 .

10.8.2. 인스턴트 메시징

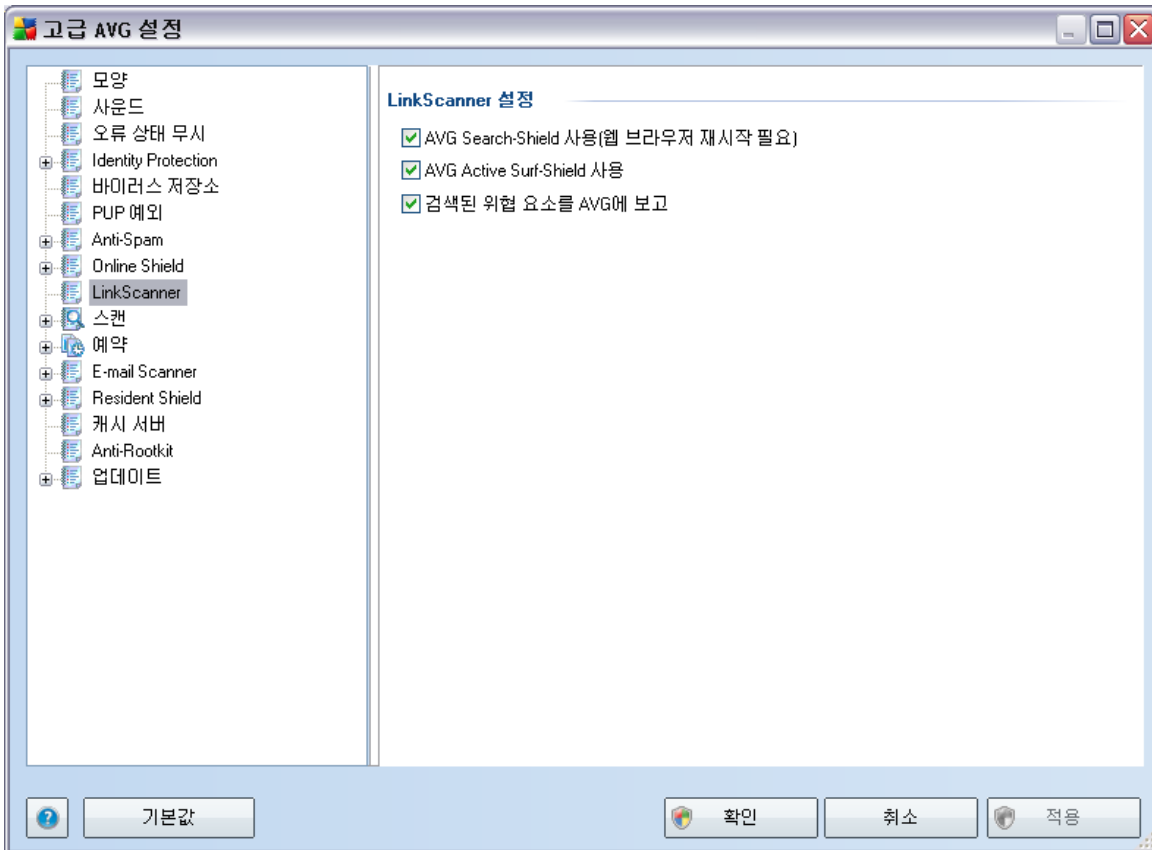


인스턴트 메시징 보호 대화 상자에서는 인스턴트 메시징 스캔을 참조하는 [Online Shield](#) 구성 요소 설정을 편집할 수 있습니다. 현재 지원되는 인스턴트 메시징 프로그램은 **ICQ**, **MSN** 및 **Yahoo** 세 가지입니다. [Online Shield](#)에서 온라인 커뮤니케이션 중에 바이러스가 없는지 확인하려면 이들 각 프로그램의 해당 항목을 선택합니다.

허용되거나 차단되는 사용자에 대한 자세한 내용을 보려면 해당 대화 상자 (**고급 ICQ**, **고급 MSN**, **고급 Yahoo**)를 확인 및 편집한 다음 **허용 목록** (해당 사용자와의 통신이 허용되는 사용자 목록) 및 **차단 목록** (차단된 사용자 목록)을 지정하면 됩니다.

10.9. Link Scanner

LinkScanner 설정 대화 상자에서는 다음과 같은 **LinkScanner**의 기본 기능을 설정하거나 해제할 수 있습니다 .



- **AVG Search-Shield 사용** (기본적으로 설정되어 있음) - Google, Yahoo, Bing, Yandex, Altavista 또는 Baidu 검색 엔진에서 반환하는 사이트의 내용을 미리 검사하여 해당 검색 엔진에서 수행하는 검색에 대한 안전도를 알려주는 아이콘입니다 .
- **AVG Active Surf-Shield 사용** - (기본적으로 설정되어 있음): 악의적인 사이트의 액세스를 차단하는 활성 (실시간) 보호 기능입니다 . 알려진 악의적인 사이트 연결 및 이와 관련된 악의적인 내용은 사용자가 웹 브라우저 (또는 HTTP를 사용하는 다른 모든 응용 프로그램)를 통해 액세스할 때 차단됩니다 .
- **발견된 위협 요소를 AVG에 보고** - (기본적으로 설정되어 있음): 웹 상에서의 악의적인 활동에 대한 데이터베이스 수집 정보를 제공하기 위해 **AVG Active**



Surf-Shield 또는 **AVG Search-Shield**를 통해 사용자가 발견한 익스플로잇과 악성 사이트를 보고하도록 하려면 이 항목을 선택합니다 .

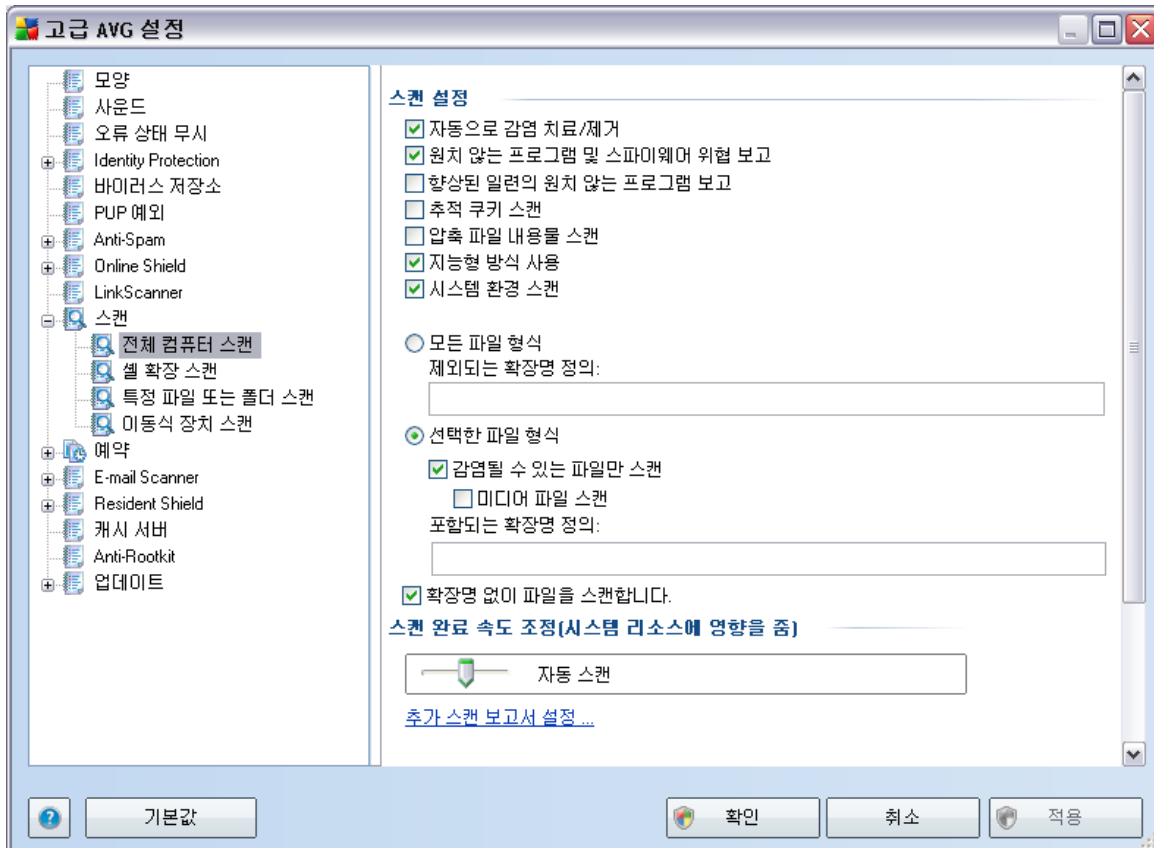
10.10. 스캔

고급 스캔 설정은 소프트웨어 공급업체가 정의한 특정 스캔 유형과 관련하여 다음 세 가지 범주로 나뉩니다 .

- **전체 컴퓨터 스캔** - 전체 컴퓨터에 대해 미리 정의된 표준 스캔
- **선택 확장 스캔** - Windows Explorer 환경에서 직접 선택한 개체에 대한 특정 스캔
- **특정 파일 또는 폴더 스캔** - 컴퓨터의 선택 영역에 대해 미리 정의된 표준 스캔
- **이동식 장치 스캔** - 컴퓨터에 연결된 이동식 장치에 대한 특정 스캔

10.10.1. 전체 컴퓨터 스캔

전체 컴퓨터 스캔 옵션을 사용하여 소프트웨어 공급업체가 미리 정의한 스캔 중 하나인 **전체 컴퓨터 스캔**의 매개 변수를 편집할 수 있습니다.



스캔 설정

스캔 설정 섹션은 선택적으로 설정 또는 해제할 수 있는 스캔 매개 변수의 목록을 제공합니다.

- **자동으로 감염 치료 / 제거** - 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없으면 감염된 개체가 **바이러스 저장소**.
- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - **Anti-Spyware** 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려

는 경우 선택합니다 . 스파이웨어는 의심되는 맬웨어 범주로 , 대개 보안 위험을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다 . 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다 .

- **향상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 스파이웨어 의 확장 패키지를 검색하려면 이 상자를 선택합니다 . 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만 , 나중에 악의적인 목적으로 잘못 사용될 수 있습니다 . 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만 , 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다 .
- **추적 쿠키 스캔** - Anti-Spyware 구성 요소의 이 매개 변수는 스캔 중에 검색할 쿠키를 정의합니다 . HTTP 쿠키는 사이트 기본 설정이나 전자 쇼핑 카트의 내용물과 같이 사용자와 관련된 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다 .
- **압축 파일 내용물 스캔** - 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일에 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다 .
- **지능형 방식 사용** - 지능형 분석 (가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다 .
- **시스템 환경 스캔** - 스캔 시 컴퓨터의 시스템 영역도 검사합니다 .

계속해서 스캔 여부를 결정해야 합니다 .

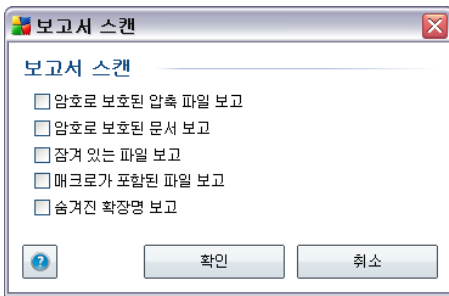
- **모든 파일 형식** - 스캔하지 않아야 할 파일의 확장명을 심표 (저장하면 세미콜론으로 변경됨)로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다 .
- **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔 (일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며 , 이때 미디어 파일 (비디오 , 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여 지정할 수 있습니다 . 이 경우 항상 스캔해야 하는 파일의 확장명을 지정할 수 있습니다 .
- 선택적으로 **확장명이 없는 파일을 스캔**하도록 정할 수 있습니다 . 이 옵션은 기본적으로 설정되어 있으며 반드시 변경해야 할 경우가 아니라면 이 설정을 유지하는 것이 좋습니다 . 확장명이 없는 파일은 의심스러운 경우가 많기 때문에 항상 스캔해야 합니다 .

스캔 프로세스 우선 순위

스캔 프로세스 우선 순위 섹션 내에서 시스템 리소스 사용량에 따라 원하는 스캔 속도를 추가로 지정할 수 있습니다 . 기본적으로 이 옵션 값은 자동 리소스 사용량의 중간 수준으로 설정되어 있습니다 . 스캔을 더 빠르게 실행하려고 하면 스캔 시간이 단축되기는 하지만 시스템의 리소스 사용량이 현저하게 증가하고 PC에서 실행 중인 다른 활동의 진행 속도가 느려지게 됩니다 . 이 옵션은 컴퓨터가 켜져 있지만 아무도 컴퓨터에서 작업을 수행하고 있지 않은 경우에 사용할 수 있습니다 . 반대로 , 스캔 기간을 늘리면 시스템 리소스 사용량을 줄일 수 있습니다 .

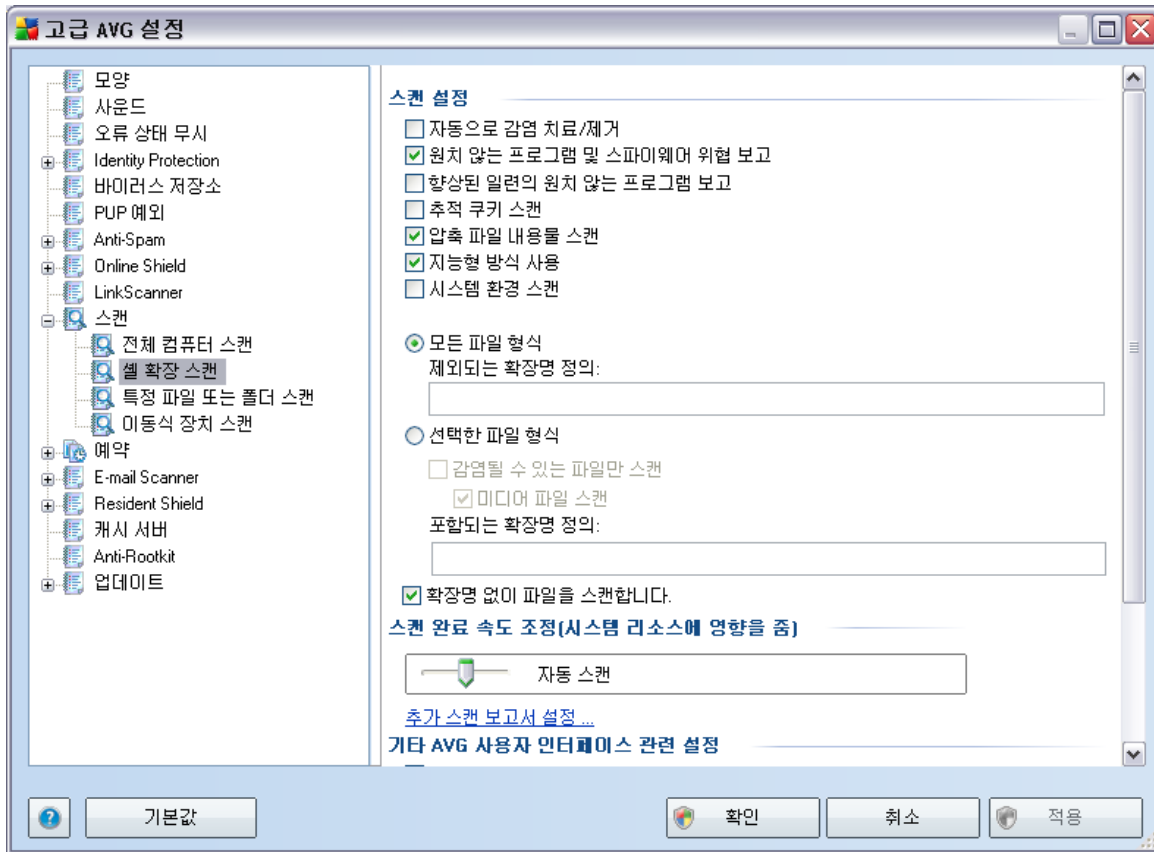
추가 스캔 보고서 설정 ...

추가 스캔 보고서 설정 ... 링크를 클릭하여 **스캔 보고서** 라는 독립 실행형 대화 상자를 열고 보고할 스캔 결과를 정의하는 몇 가지 항목을 선택할 수 있습니다 .



10.10.2. 셀 확장 스캔

이전의 [전체 컴퓨터 스캔](#) 항목과 유사하게 **셀 확장 스캔**이라는 이름의 이 항목 역시 소프트웨어 공급업체가 미리 정의한 스캔을 편집할 수 있는 몇 가지 옵션을 제공합니다 . 이번에는 구성이 [Windows 탐색기](#) 환경 (**셀 확장**)에서 직접 실행되는 특정 개체의 스캔과 연관되므로 [Windows 탐색기에서 스캔](#) 장을 참조하십시오 .

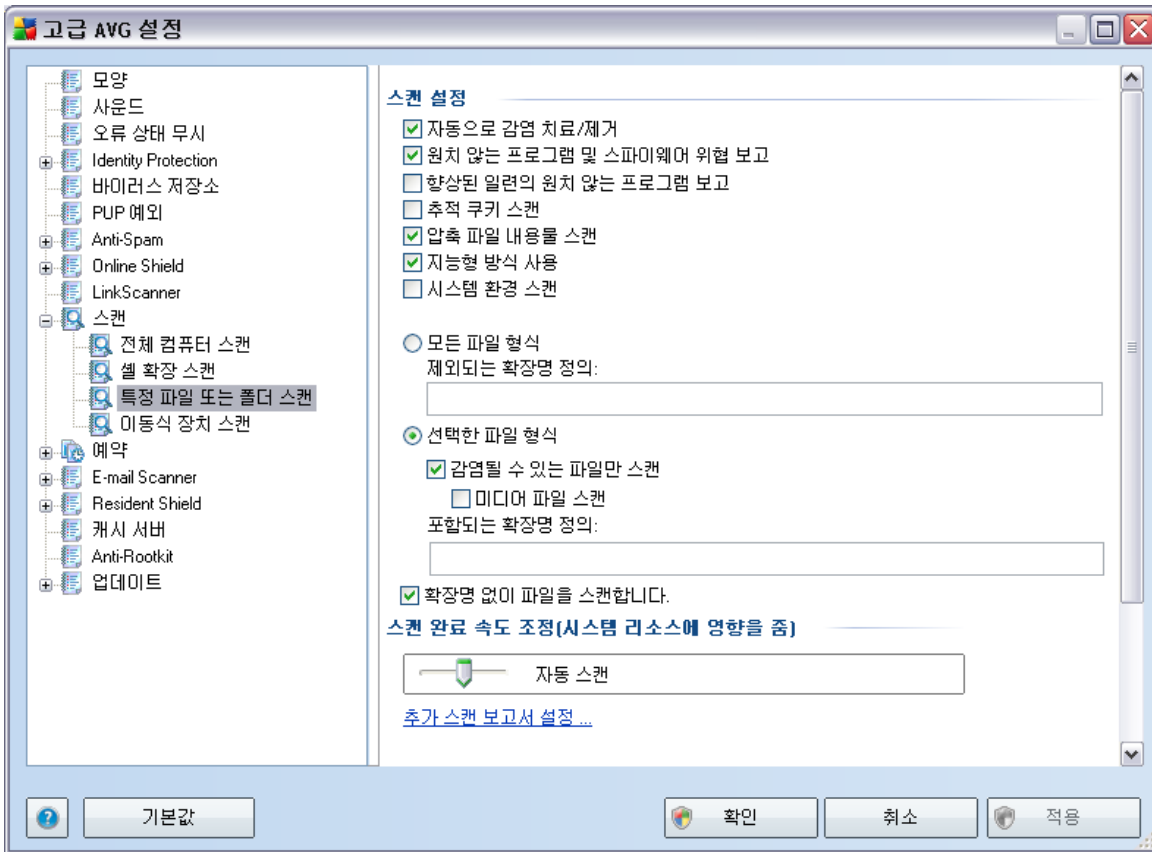


매개 변수의 목록은 [전체 컴퓨터 스캔](#)에서 제공되는 것과 같습니다 . 하지만 기본 설정은 다릅니다 . [전체 컴퓨터 스캔](#)의 경우 대부분의 매개 변수가 선택되는 반면 [선택 확장 스캔 \(Windows 탐색기에서 스캔\)](#)의 경우에는 오직 관련된 매개 변수만 설정됩니다 .

참고 : 특정 매개 변수에 대한 설명은 [AVG 고급 설정 / 스캔 / 전체 컴퓨터 스캔](#) 장을 참조하십시오 .

10.10.3. 특정 파일 또는 폴더 스캔

[특정 파일 또는 폴더 스캔](#)의 편집 인터페이스는 [전체 컴퓨터 스캔](#) 편집 대화 상자와 같습니다 . 모든 구성 옵션이 동일하지만 [전체 컴퓨터 스캔](#)에 대한 기본 설정은 좀 더 엄격합니다 .

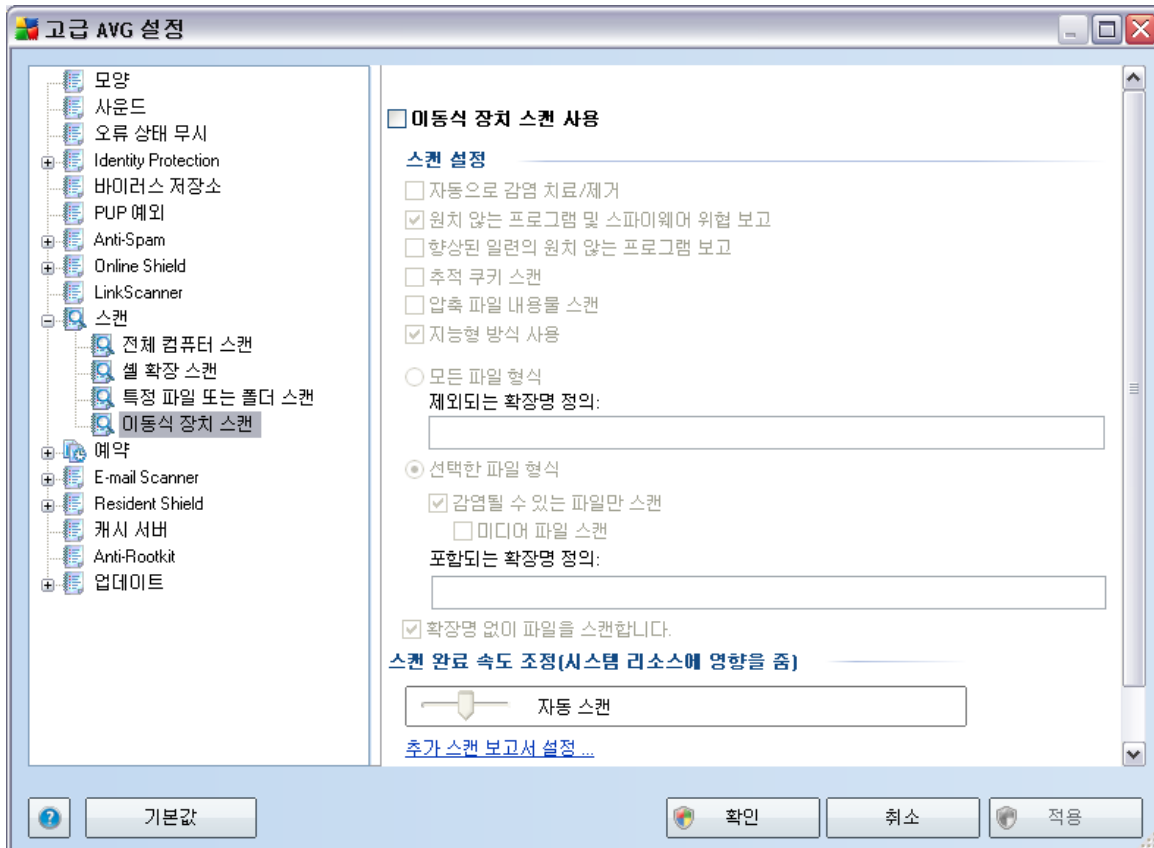


이 구성 대화 상자의 모든 매개 변수 설정은 오직 **특정 파일 또는 폴더 스캔**으로 스캔하기 위해 선택한 영역에만 적용됩니다 .

참고 : 특정 매개 변수에 대한 설명은 [AVG 고급 설정 / 스캔 / 전체 컴퓨터 스캔](#) 장을 참조하십시오 .

10.10.4. 이동식 장치 스캔

이동식 장치 스캔의 편집 인터페이스는 [전체 컴퓨터 스캔](#) 편집 대화 상자와 매우 유사합니다.



컴퓨터에 이동식 장치를 연결하면 **이동식 장치 스캔**이 자동으로 실행됩니다. 기본적으로 이 스캔 옵션은 해제되어 있습니다. 그러나 이동식 장치에서 감염의 주된 원인으로 생각되는 위협 요소는 반드시 스캔해야 합니다. 스캔 준비된 상태를 유지하고 필요할 때 자동으로 실행되게 하려면 **이동식 장치 스캔 사용** 옵션을 선택하십시오.

참고: 특정 매개 변수에 대한 설명은 [AVG 고급 설정 / 스캔 / 전체 컴퓨터 스캔](#) 장을 참조하십시오.

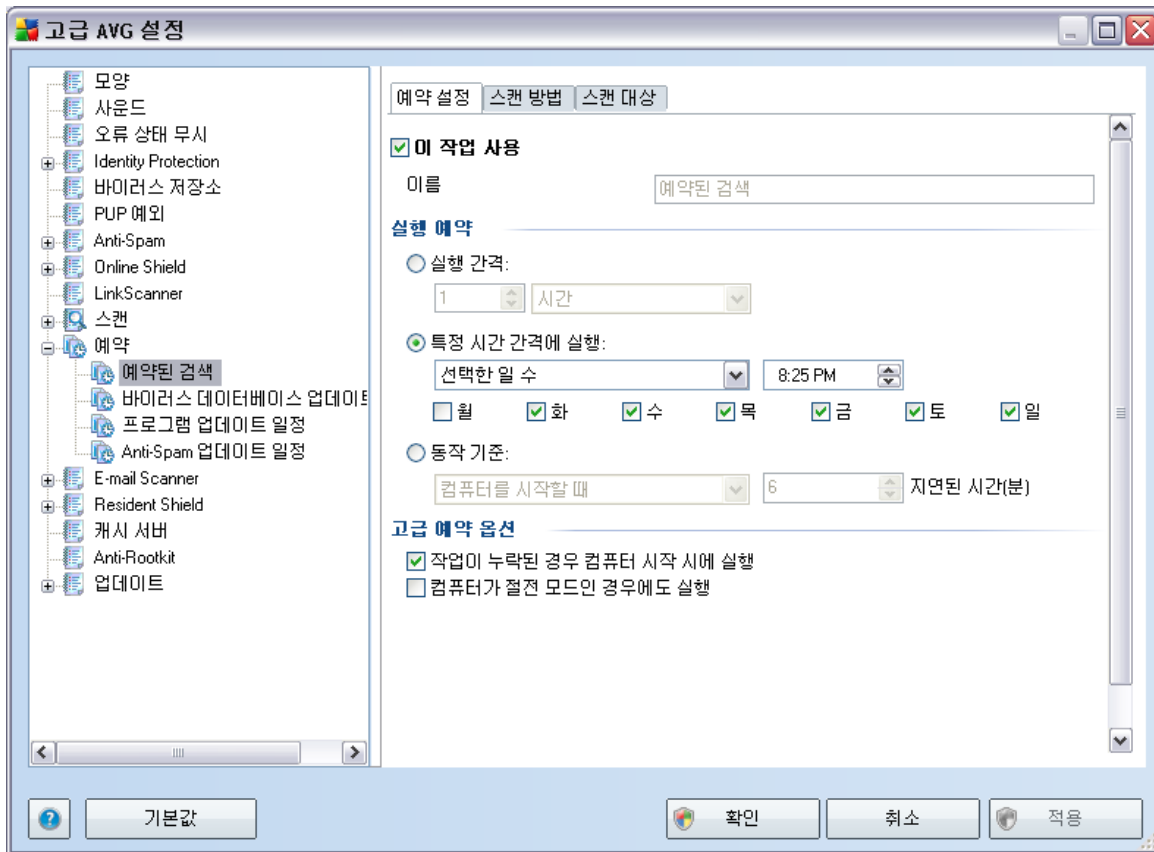
10.11. 예약

예약 섹션에서 다음 기본 설정을 편집할 수 있습니다 .

- [전체 컴퓨터 스캔 일정](#)
- [바이러스 데이터베이스 업데이트 일정](#)
- [프로그램 업데이트 일정](#)
- [Anti-Spam 업데이트 일정](#)

10.11.1. 예약된 스캔

예약된 스캔의 매개 변수 (또는 새 일정 설정)는 다음 세 가지 탭에서 편집할 수 있습니다.



예약 설정 탭에서 먼저 **이 작업 사용** 항목을 선택하거나 선택 취소하여 예약된 테스트를 일시적으로 비활성화하고 필요한 경우에 이를 다시 활성화할 수 있습니다.

다음으로, **모든 기본 일정에 대해 비활성 상태로 표시되는 이름** 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다. 새로 추가된 일정 (왼쪽 탐색 트리에서 **예약된 스캔** 항목을 마우스 오른쪽 단추로 클릭하여 새 일정을 추가할 수 있음)에 대해서는 고유한 이름을 지정할 수 있으며, 이 경우에는 텍스트 필드가 편집할 수 있는 상태로 열립니다. 스캔에 간략하고 설명적인 이름을 사용하여 나중에 해당 스캔을 쉽게 구분할 수 있도록 해야 합니다.

예를 들어 스캔이 실제로 검사하는 대상이 무엇인지 알 수 없는 "새로운 스캔" 또는 "내 스캔" 등의 이름을 붙이는 것은 적절하지 않습니다. 반면, "시스템 영역 스캔" 같은 이름은 설명이 포함된 적절한 이름이라고 할 수 있습니다. 또한 스캔의 이름에 해당 스캔이 전체 컴퓨터 스캔인지, 선택한 파일 스캔인지 아니면 폴더 스캔인지를 지정할 필요는 없습니다. 사용자 자신의 스캔은 언제나 선택한 파일 또는 폴더 스캔의 특정한 버전이 됩니다.

이 대화 상자에서 다음과 같은 스캔 매개 변수를 상세하게 정의할 수 있습니다 .

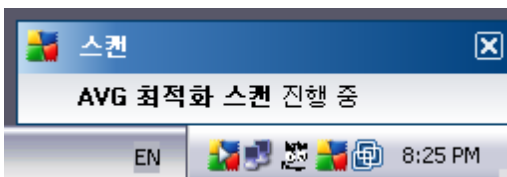
실행 예약

여기서 새로 예약된 스캔이 시작되는 시간 간격을 지정할 수 있습니다 . 특정 시간이 지나면 (**실행 간격 ...**) 스캔 실행이 반복되도록 정의하거나 정확한 날짜 및 시간을 정의 (**특정 시간 간격에 실행 ...**) 하여 스캔이 실행되도록 할 수 있습니다 . 아니면 스캔이 특정 이벤트 (**동작 기준 : 컴퓨터를 시작할 때**) 와 연관되어 실행되도록 지정할 수도 있습니다 .

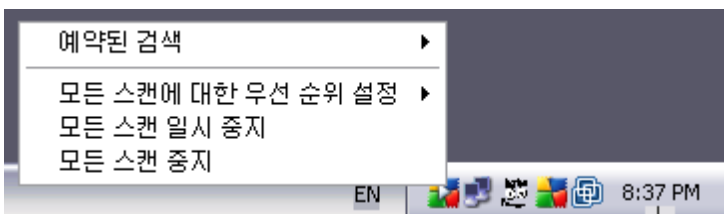
고급 예약 옵션

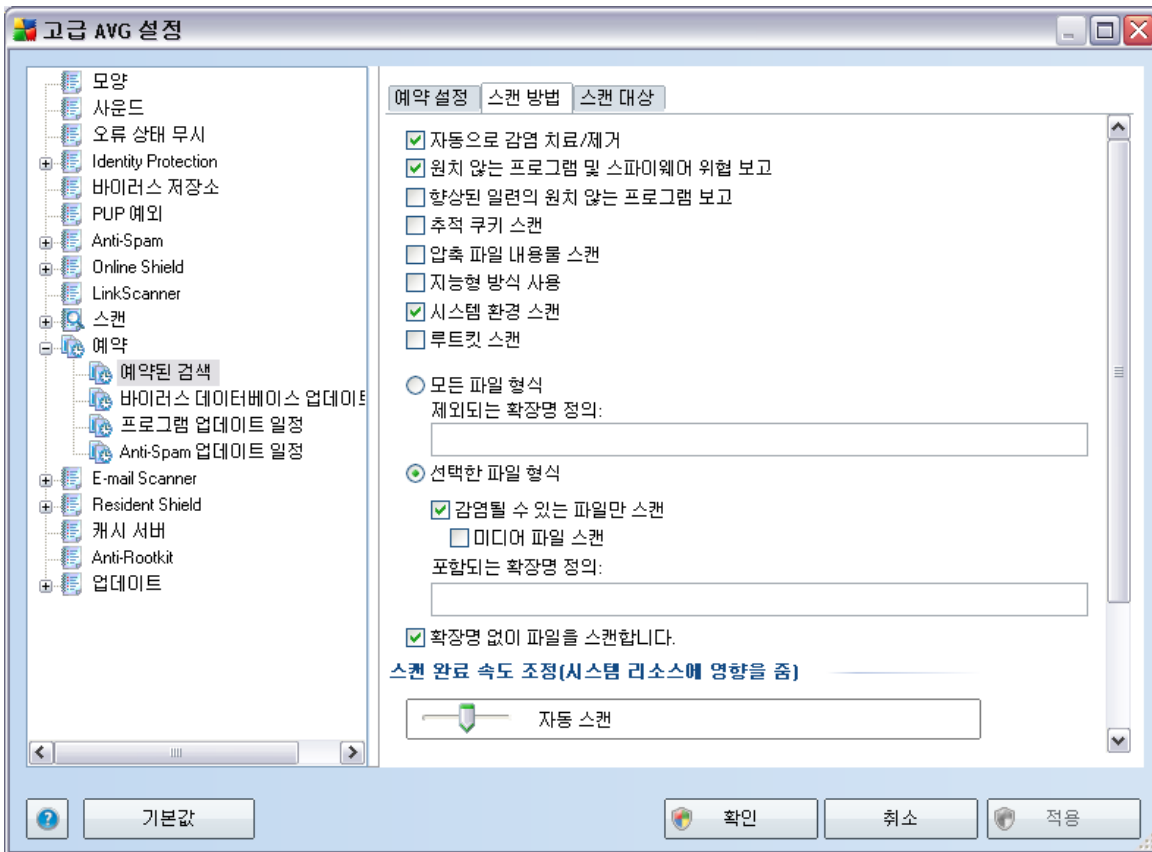
이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 스캔이 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다 .

일단 예약된 스캔이 지정된 시간에 실행되면 [AVG 시스템 트레이 아이콘](#) 위로 팝업 창이 열려 해당 내용을 알립니다 .



그러면 예약된 스캔이 실행 중임을 알리는 새 [AVG 시스템 트레이 아이콘](#) (*흰색 화살표가 있는 여러 가지 색의 아이콘 - 위 그림 참조*) 이 나타납니다 . 실행 중인 스캔 AVG 아이콘을 마우스 오른쪽 단추로 클릭하여 상황에 맞는 메뉴를 열고 실행 중인 스캔을 일시 중지하거나 중지할 수 있습니다 .





스캔 방법 탭에는 선택적으로 설정하거나 해제할 수 있는 스캔 매개 변수의 목록이 있습니다. 기본적으로 대부분의 매개 변수가 설정되어 있으며 스캔하는 동안 해당 기능이 적용됩니다. 이러한 설정을 반드시 변경해야 하는 경우가 아니라면 다음과 같이 미리 정의된 구성을 그대로 유지하는 것이 좋습니다.

- **자동으로 감염 치료 / 제거** - 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없으면 감염된 개체가 [바이러스 저장소](#).
- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위험을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다.](#) 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다.
- **항상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우

스파이웨어의 확장 패키지를 검색하려면 이 상자를 선택합니다. 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 잘못 사용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.

- **추적 쿠키 스캔** (기본적으로 설정되어 있음) - **Anti-Spyware** 구성 요소의 이 매개 변수는 스캔 중에 쿠키가 검색되도록 정의합니다. HTTP 쿠키는 사이트 기본 설정이나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.
- **압축 파일 내용물 스캔** - (기본적으로 설정되어 있음): 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일 형식으로 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.
- **지능형 방식 사용** - (기본적으로 설정되어 있음): 지능형 분석 (가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- **시스템 환경 스캔** - (기본적으로 설정되어 있음): 또한 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- **루트킷 스캔** - 루트킷 검색을 전체 컴퓨터 스캔에 포함하려면 이 항목을 선택합니다. 또한 루트킷 검색은 **Anti-Rootkit** 구성 요소 내에서 단독으로 사용될 수도 있습니다.

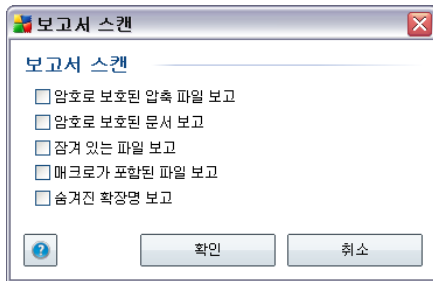
계속해서 스캔 여부를 결정해야 합니다.

- **모든 파일 형식** - 스캔하지 않아야 할 파일의 확장명을 심표 (저장하면 세미콜론으로 변경됨)로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.
- **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔 (일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며, 이때 미디어 파일 (비디오, 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여 지정할 수 있습니다. 이 경우 항상 스캔해야 하는 파일의 확장명을 지정할 수 있습니다.
- 선택적으로 **확장명이 없는 파일을 스캔**하도록 정할 수 있습니다. 이 옵션은 기본적으로 설정되어 있으며 반드시 변경해야 할 경우가 아니라면 이 설정을 유지하는 것이 좋습니다. 확장명이 없는 파일은 의심스러운 경우가 많기 때문에 항상 스캔해야 합니다.

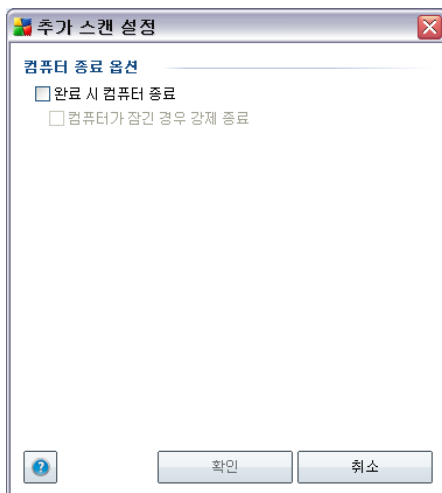
스캔 프로세스 우선 순위

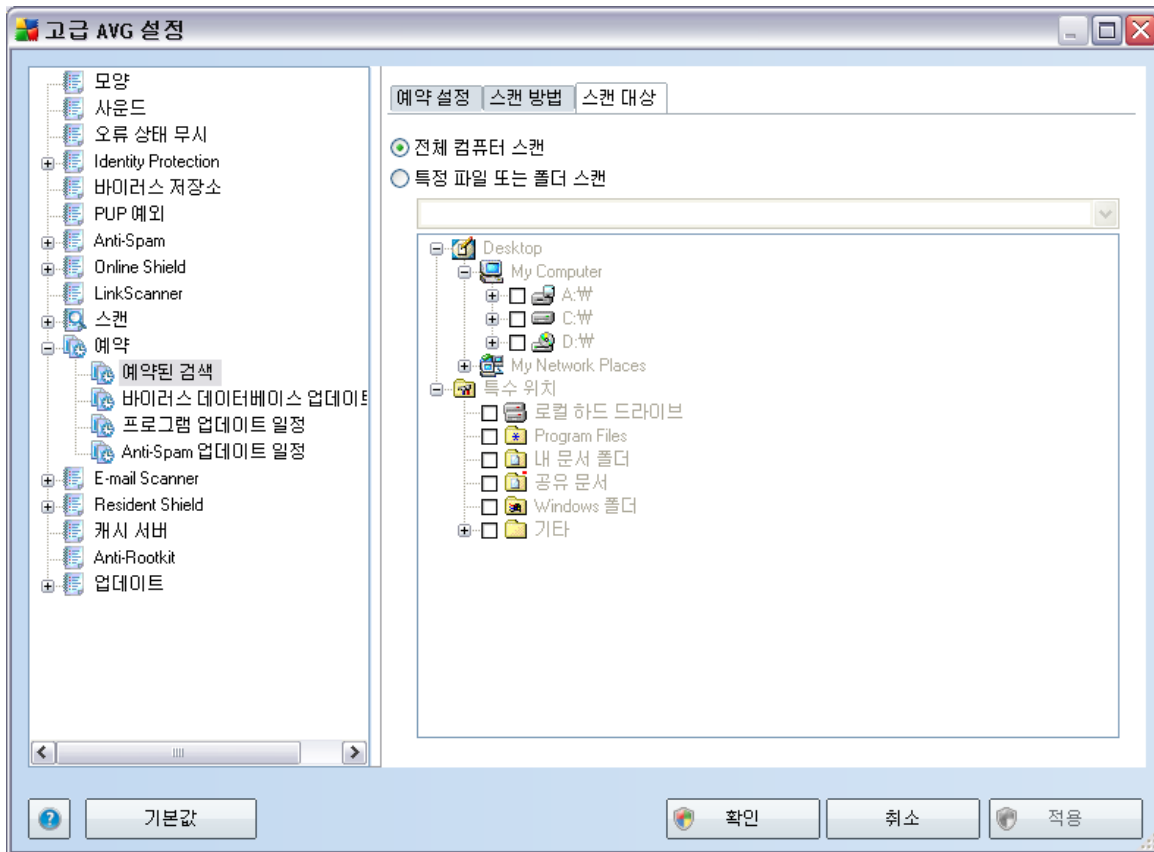
스캔 프로세스 우선 순위 섹션 내에서 시스템 리소스 사용량에 따라 원하는 스캔 속도를 추가로 지정할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 중간 수준으로 설정되어 있습니다. 스캔을 더 빠르게 실행하려고 하면 스캔 시간이 단축되기는 하지만 시스템의 리소스 사용량이 현저하게 증가하고 PC에서 실행 중인 다른 활동의 진행 속도가 느려지게 됩니다. 이 옵션은 컴퓨터가 켜져 있지만 아무도 컴퓨터에서 작업을 수행하고 있지 않은 경우에 사용할 수 있습니다. 반대로, 스캔 기간을 늘리면 시스템 리소스 사용량을 줄일 수 있습니다.

추가 스캔 보고서 설정 ... 링크를 클릭하여 **스캔 보고서** 라는 독립 실행형 대화 상자를 열고 보고할 스캔 결과를 정의하는 몇 가지 항목을 선택할 수 있습니다.



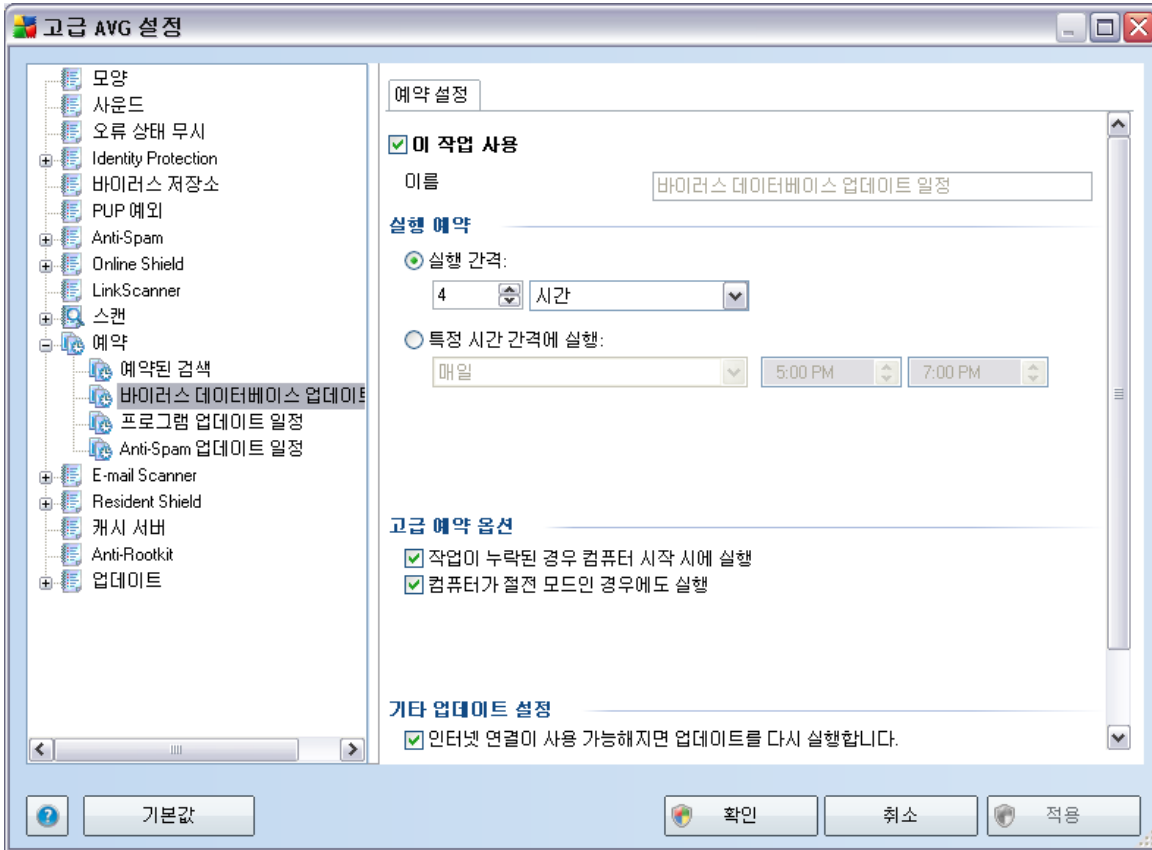
추가 스캔 설정 ... 을 클릭하면 새로운 **컴퓨터 종료 옵션** 대화 상자가 열리므로 스캔 프로세스가 모두 실행된 경우 컴퓨터를 자동으로 종료할 것인지 여부를 결정할 수 있습니다. **스캔 완료 시 컴퓨터 종료** 옵션을 선택하면 컴퓨터가 현재 잠겨 있는 경우에도 종료 (**컴퓨터가 잠긴 경우 강제 종료**)할 수 있는 새로운 옵션이 활성화됩니다.





스캔 대상 탭에서 전체 컴퓨터 스캔 을 예약할지 아니면 특정 파일 또는 폴더 스캔 을 예약할지 여부를 정의할 수 있습니다 . 특정 파일 또는 폴더 스캔을 선택한 경우 표시된 트리 구조가 이 대화 상자의 아래쪽 부분에서 활성화되며 여기서 스캔할 폴더를 지정할 수 있습니다 .

10.11.2. 바이러스 데이터베이스 업데이트 일정



예약 설정 탭에서 **이 작업 사용** 항목을 선택 또는 선택 취소하여 예약된 바이러스 데이터베이스 업데이트를 일시적으로 비활성화했다가 필요할 경우에는 다시 설정할 수 있습니다. 기본 바이러스 데이터베이스 업데이트 일정은 [업데이트 관리자](#) 구성 요소에서 담당합니다. 이 대화 상자에서 바이러스 데이터베이스 업데이트 일정의 세부적인 매개 변수 중 일부를 설정할 수 있습니다. 모든 기본 일정에 대해 **비활성 상태**로 표시되는 이름 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

이 섹션에서는 새로 예약된 바이러스 데이터베이스 업데이트를 시작할 시간 간격을 지정합니다. 특정 시간이 지나면 (**실행 간격...**) 업데이트 실행이 반복되도록 정의하거나 정확한 날짜 및 시간을 정의 (**특정 시간 간격에 실행...**)하여 업데이트가 실행되도록 할 수 있습니다.

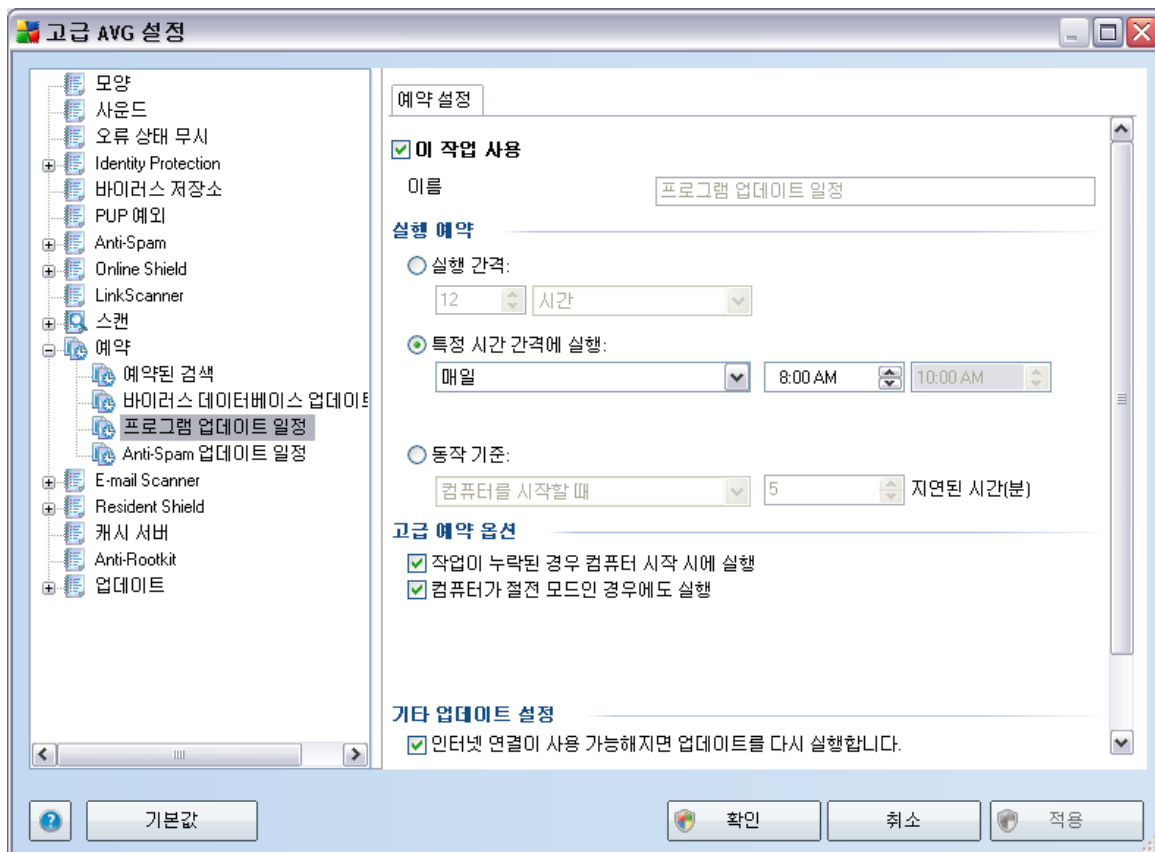
고급 예약 옵션

이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 바이러스 데이터베이스 업데이트가 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다 .

기타 업데이트 설정

마지막으로 , 인터넷 연결이 끊어져 업데이트 프로세스가 실패한 경우 인터넷 연결이 복구되는 즉시 업데이트가 다시 시작되게 만들려면 **인터넷 연결이 사용 가능해지는 즉시 업데이트를 다시 실행합니다** . 옵션을 선택합니다 .

예약된 업데이트가 지정한 시간에 시작되면 [AVG 시스템 트레이 아이콘 \(고급 설정 / 모](#)
[양](#) 대화 상자의 기본 구성을 유지한 경우) 위로 팝업 창이 열려 해당 내용을 알립니다 .



예약 설정 탭에서 **이 작업 사용** 항목을 선택 또는 선택 취소하여 예약된 프로그램의 업데이트를 일시적으로 비활성화했다가 필요할 경우에는 다시 설정할 수 있습니다. **모든 기본 일정에 대해 비활성 상태**로 표시되는 이름 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

여기서 새로 예약된 프로그램 업데이트가 실행되는 주기를 지정합니다. 특정 기간이 지난 후(**실행 간격...**) 또는 정확한 날짜와 시간을 정의(**특정 시간 간격에 실행...**)하여 업데이트 시작이 반복되도록 정의할 수 있습니다. 아니면 업데이트 실행이 특정 이벤트(**동작 기준: 컴퓨터를 시작할 때**)와 연관되어 시작되도록 지정할 수도 있습니다.

고급 예약 옵션

이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 프로그램 업데이트가 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다.

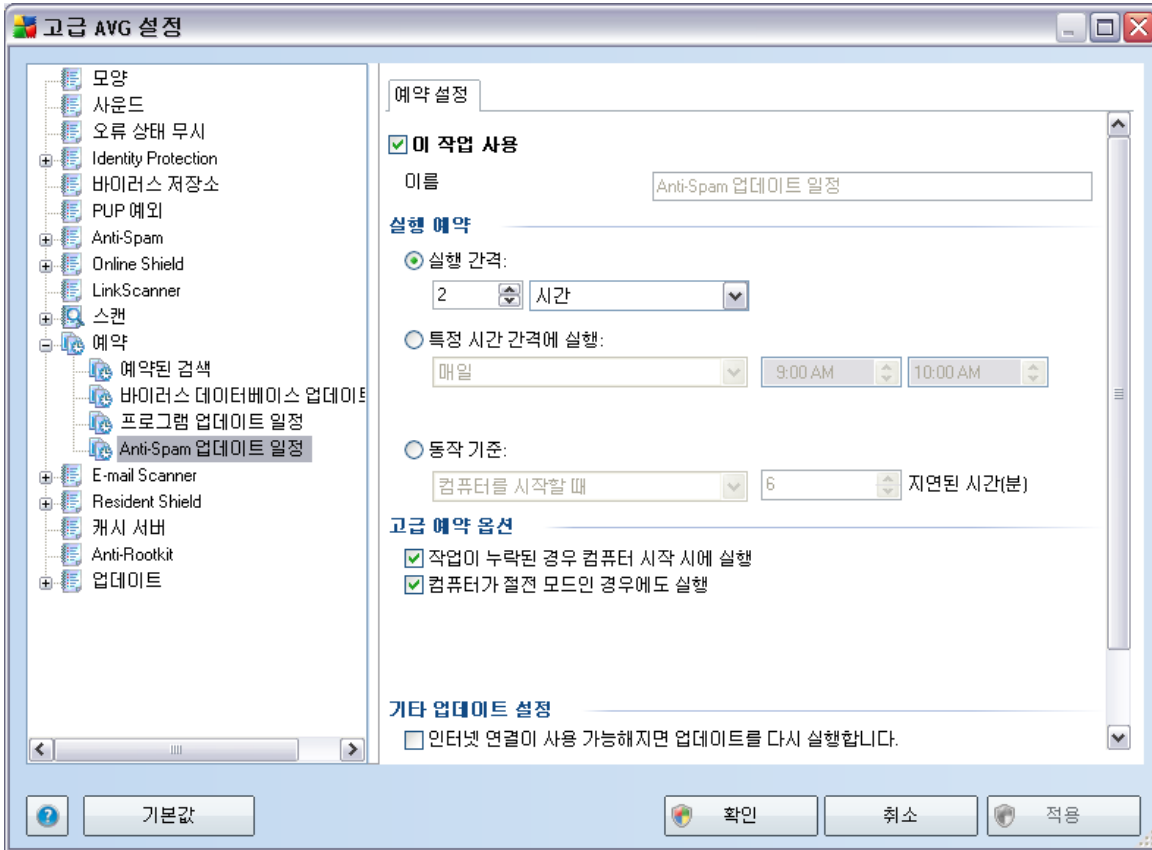
기타 업데이트 설정

인터넷 연결이 끊어져 업데이트 프로세스가 실패한 경우 인터넷 연결이 복구되는 즉시 업데이트가 다시 시작되게 만들려면 **인터넷 연결이 사용 가능해지는 즉시 업데이트를 다시 실행합니다** 옵션을 선택합니다.

예약된 업데이트가 지정한 시간에 시작되면 [AVG 시스템 트레이 아이콘](#) (**고급 설정 / 모**
양 대화 상자의 기본 구성을 유지한 경우) 위로 팝업 창이 열려 해당 내용을 알립니다.

참고: 예약된 프로그램 업데이트와 예약된 스캔이 같은 시간에 수행될 경우 업데이트 프로세스의 우선 순위가 더 높으므로 스캔이 중단됩니다.

10.11.3. Anti-Spam 업데이트 일정



예약 설정 탭에서 먼저 **이 작업 사용** 항목을 선택 / 선택 취소하여 예약된 **Anti-Spam** 업데이트를 일시적으로 비활성화하고 필요한 경우에 이를 다시 활성화할 수 있습니다. 기본 **Anti-Spam** 업데이트 일정은 **업데이트 관리자** 구성 요소에서 설정합니다. 이 대화 상자에서 업데이트 일정의 세부적인 매개 변수 중 일부를 설정할 수 있습니다. 모든 기본 일정에 대해 비활성 상태 **로 표시되는** 이름 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

여기에서 새로 예약된 **Anti-Spam** 업데이트가 실행되는 주기를 지정합니다. 특정 시간 이 지나면 (**실행 간격...**) Anti-Spam 업데이트 실행이 반복되도록 정의하거나 정확한 날짜 및 시간을 정의 (**특정 시간 간격에 실행...**)하여 업데이트가 실행되도록 할 수 있습니다. 아니면 업데이트 실행이 특정 이벤트 (**동작 기준: 컴퓨터를 시작할 때**)와 연관되어 시작되도록 지정할 수도 있습니다.

고급 예약 옵션

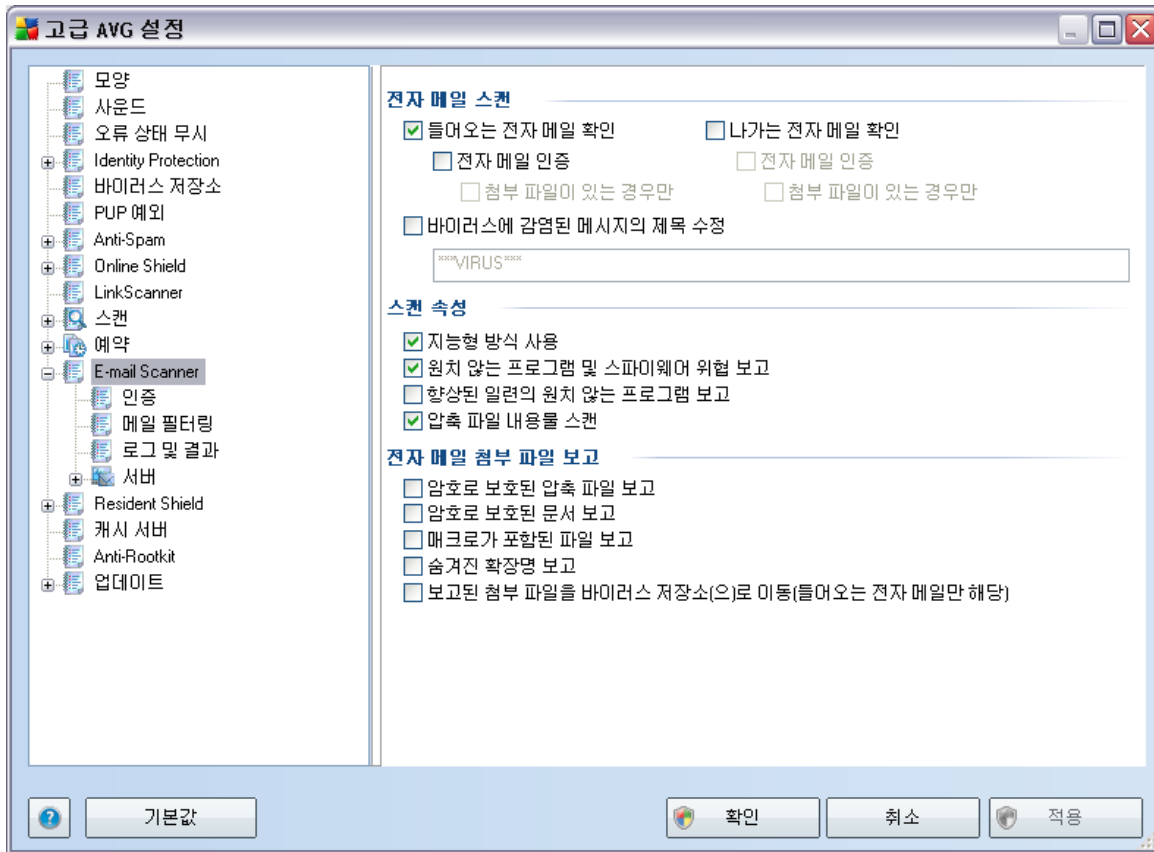
이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 [Anti-Spam](#) 업데이트가 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다 .

기타 업데이트 설정

인터넷 연결이 끊어져 [Anti-Spam 업데이트 프로세스가 실패한 경우 인터넷 연결이 복구되는 즉시 업데이트가 다시 시작되게 만들려면](#) 인터넷 연결이 사용 가능해지는 [즉시 업데이트를 다시 실행합니다](#) . 옵션을 선택합니다 .

지정한 시간에 예약된 스캔이 시작되면 [AVG 시스템 트레이 아이콘](#) (고급 설정 / 모양 대화 상자에서 기본 구성을 유지한 경우) .

10.12. E-mail Scanner



전자 메일 스캐너 대화 상자는 다음 세 개의 섹션으로 나뉘어 있습니다 .

- **전자 메일 스캔** - 이 섹션에서는 들어오고 나가는 전자 메일 메시지에 대해 다음과 같은 기본 사항을 설정할 수 있습니다 .

- o 전자 메일 메시지에서 바이러스를 스캔해야 하는지 여부 .
- o 각 메시지의 끝에 바이러스가 없음을 나타내는 인증 텍스트를 추가해야 하는지 여부 . 텍스트는 [인증](#) 대화 상자에서 조정할 수 있습니다 .
- o 인증 텍스트를 첨부 파일이 있는 메시지에만 추가해야 하는지 여부 .

바이러스에 감염된 메시지의 제목 수정 을 수행하려면 해당 상자를 선택하고 텍스트 필드에 원하는 값을 입력합니다 . 그러면 해당 값이 감염된 전자 메일 메시지의 제목 필드에 추가되어 식별 및 필터링을 용이하게 합니다 . 기본값은

*** VIRUS*** 이며 그대로 유지하는 것이 좋습니다

- **스캔 속성** - 이 섹션에서는 전자 메일 메시지의 스캔 방법을 지정할 수 있습니다.

- **지능형 방식 사용** - 전자 메일 메시지를 스캔할 때 [지능형 검색 방식](#)을 사용하려는 경우 선택합니다. 이 옵션이 선택되어 있으면 전자 메일 첨부 파일을 확장명뿐만 아니라 첨부 파일의 실제 내용으로도 필터링할 수 있습니다. 필터링은 [메일 필터링](#) 대화 상자에서 설정할 수 있습니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스�파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위협을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다.](#) 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다.
- **항상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 [스�파이웨어](#)의 확장 패키지를 검색하려면 이 상자를 선택합니다. 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 잘못 사용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.
- **압축 파일 내용을 스캔** - 전자 메일 메시지에 첨부된 압축 파일의 내용을 스캔하려는 경우 선택합니다.

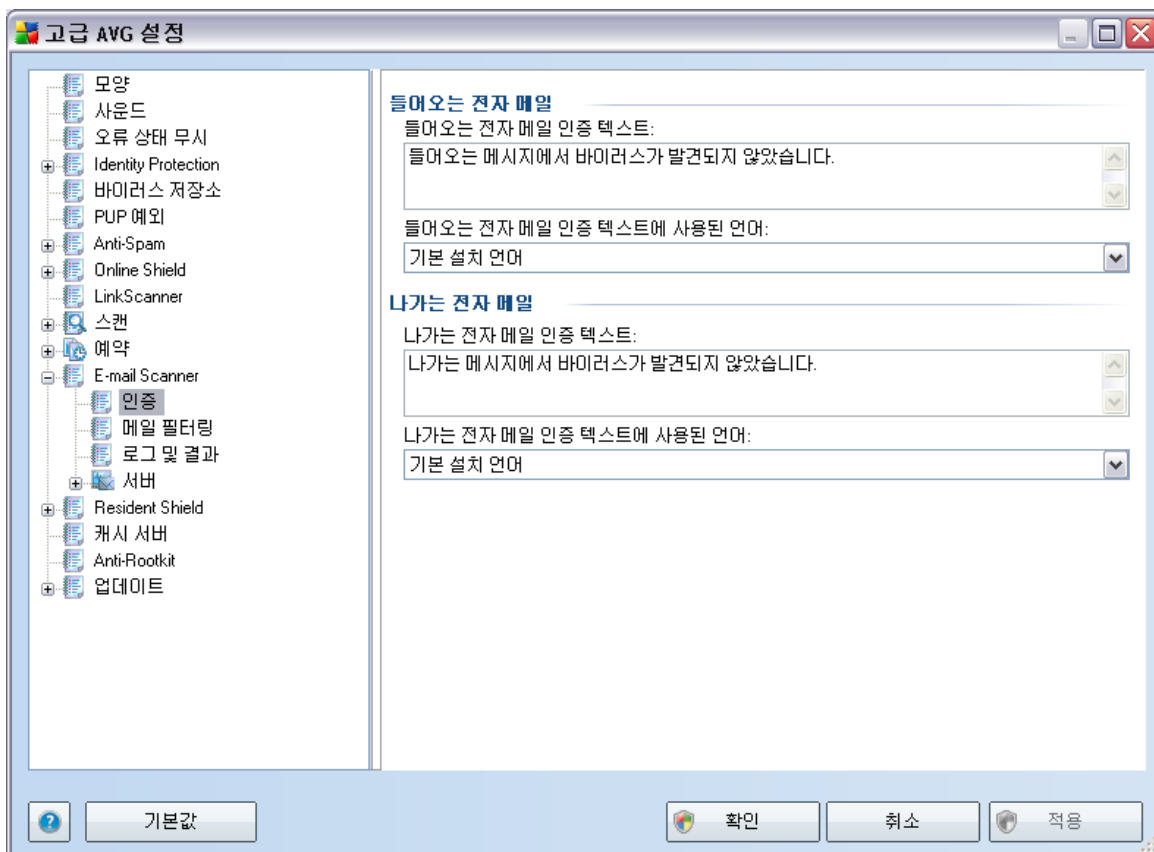
- **전자 메일 첨부 파일 보고** - 이 섹션에서는 잠재적으로 위험하거나 의심스러운 파일에 대한 추가 보고서를 설정할 수 있습니다. 전자 메일 메시지의 끝에 인종 텍스트가 추가되기만 하고 경고 대화 상자가 표시되지 않는다는 점에 주의해야 합니다. 이러한 모든 보고서는 [E-mail Scanner 검색](#) 대화 상자에 나열됩니다:

- **암호로 보호된 압축 파일 보고** - 압축 파일 (ZIP, RAR 등) 암호로 보호된 압축 파일 (ZIP, RAR 등)에서는 바이러스를 스캔할 수 없으므로 이러한 파일을 잠재적으로 위험하다고 보고하려면 상자를 선택합니다.
- **암호로 보호된 문서 보고** - 암호로 보호된 문서에서는 바이러스를 스캔할 수 없으므로 이러한 파일을 잠재적으로 위험하다고 보고하려면 상자를 선택합니다.
- **매크로가 포함된 파일 보고** - 매크로는 사용자가 여러 가지 작업을 편리하게 수행할 수 있도록 미리 정의해 둔 일련의 단계입니다 (MS Word 매크로가 널리 사용됨). 따라서 매크로에는 잠재적으로 위험한 명령이 포함될 수 있으므로 매크로가 포함된 파일을 의심스러운 파일로 보고하도록 하려

면 상자를 선택합니다 .

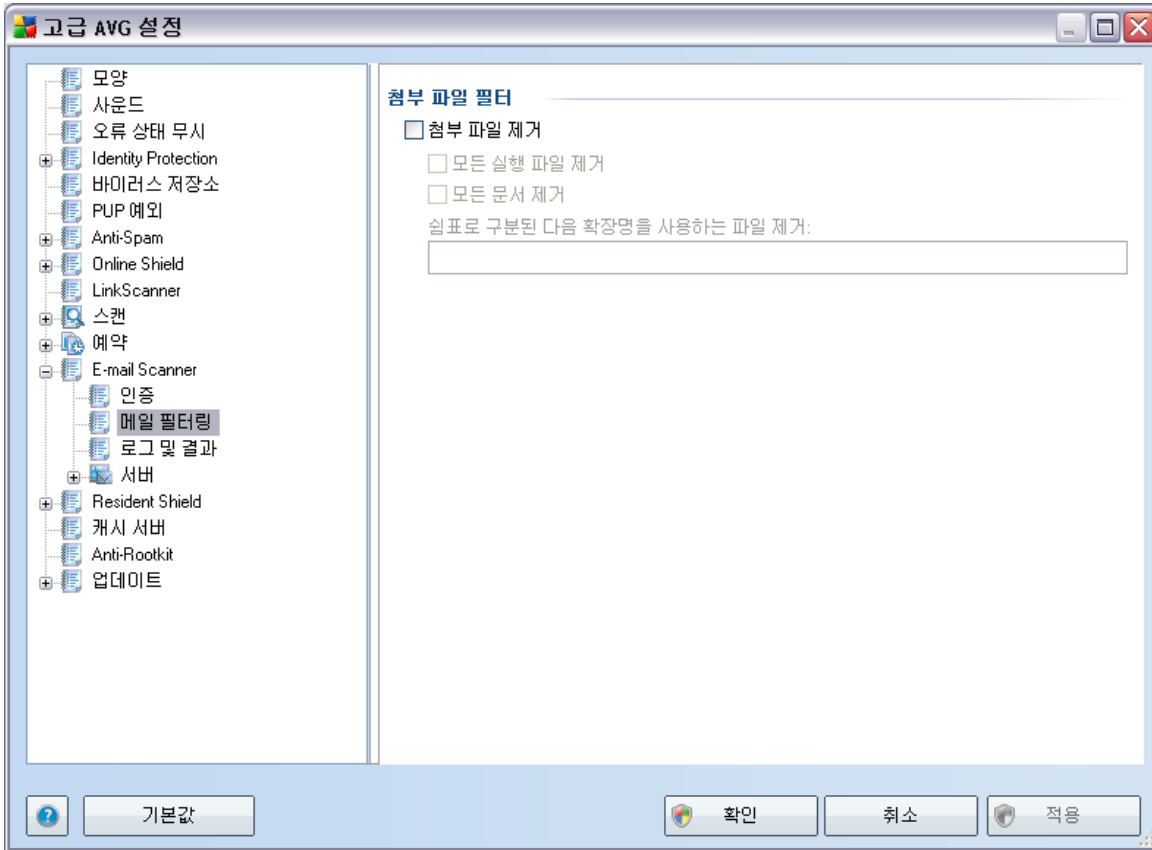
- o **숨겨진 확장명 보고** - 확장명이 숨겨지면 예를 들어 , 의심스러운 실행 파일인 "something.txt.exe"가 안전한 일반 텍스트 파일인 "something.txt"로 표시될 수 있으므로 이러한 파일을 잠재적으로 위험하다고 보고하려면 상자를 선택합니다 .
- o **보고된 첨부 파일을 바이러스 저장소로 이동** - 암호로 보호된 압축 파일 , 암호로 보호된 문서 , 매크로가 포함된 파일 및 / 또는 스캔된 전자 메일 메시지의 첨부 파일로 발견된 확장명이 숨겨진 파일에 대한 전자 메일 알림을 받을지 여부를 지정합니다 . 스캔 중 이러한 메시지가 확인될 경우 발견된 감염 개체를 바이러스 저장소로 이동할지 여부를 정의합니다 .

10.12.1. 인증



인증 대화 상자에서는 인증 메모에 포함할 텍스트 및 해당 언어를 지정할 수 있습니다 . 이는 **들어오는 메일** 및 **나가는 메일**에 대해 각각 따로 지정해야 합니다 .

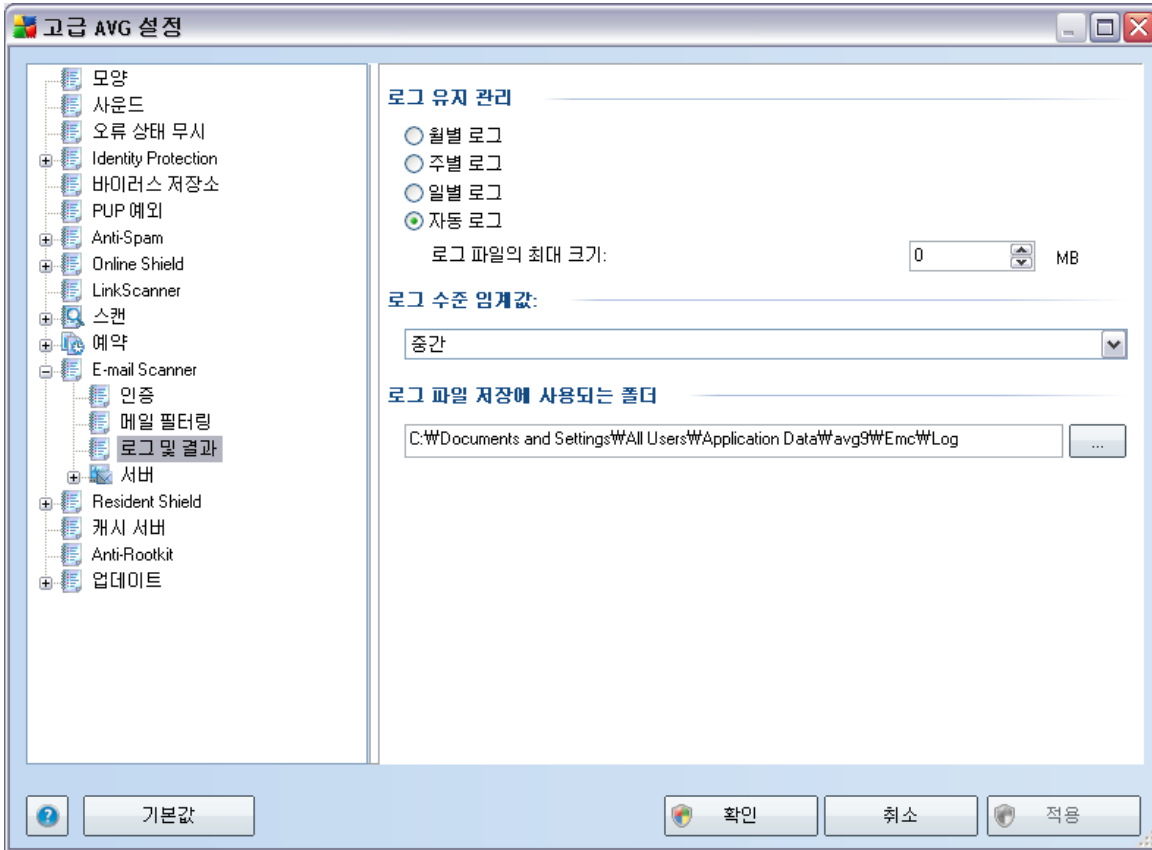
10.12.2. 메일 필터링



첨부 파일 필터 대화 상자에서는 전자 메일 메시지 첨부 파일 스캔을 위한 매개 변수를 설정할 수 있습니다. 기본적으로 **첨부 파일 제거** 옵션은 해제되어 있습니다. 이 옵션을 활성화하면 감염성이나 위험성이 있는 것으로 검색된 모든 전자 메일 메시지 첨부 파일이 자동으로 제거됩니다. 제거하려는 첨부 파일의 특정 유형을 정의하려면 해당 옵션을 선택하십시오.

- **모든 실행 파일 제거** - 모든 *.exe 파일이 삭제됩니다.
- **모든 문서 제거** - 모든 *.doc, *.docx, *.xls, *.xlsx 파일이 삭제됩니다.
- **선택으로 구분된 다음 확장명을 사용하는 파일 제거** - 정의된 확장명을 가진 모든 파일이 제거됩니다.

10.12.3. 로그 및 결과

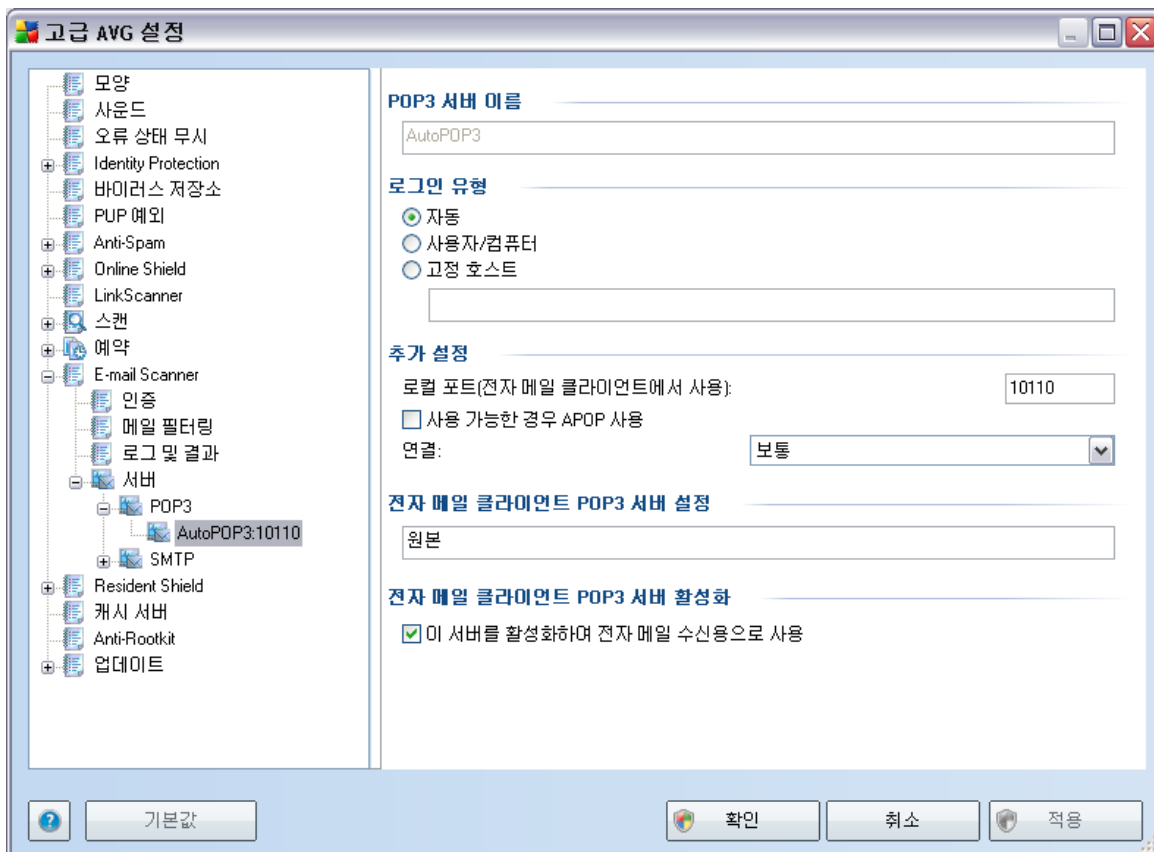


로그 및 결과 탐색 항목을 통해 열린 대화 상자에서는 전자 메일 스캔 결과 유지 관리에 사용되는 매개 변수를 지정할 수 있습니다. 이 대화 상자는 다음과 같이 여러 섹션으로 나뉩니다.

- **로그 유지 관리** - 전자 메일 스캔 정보 기록 간격을 일별, 주별 또는 월별로 정의합니다. 또한 로그 파일의 최대 크기 (MB 단위)를 지정할 수 있습니다.
- **로그 수준 임계값** - 기본적으로 중간 수준이 설정됩니다. 낮은 수준 (기본적인 연결 정보 기록) 또는 높은 수준 (모든 트래픽 기록)을 선택할 수도 있습니다.
- **로그 파일 저장에 사용되는 폴더** - 로그 파일이 저장되는 위치를 정의합니다.

10.12.4. 서버

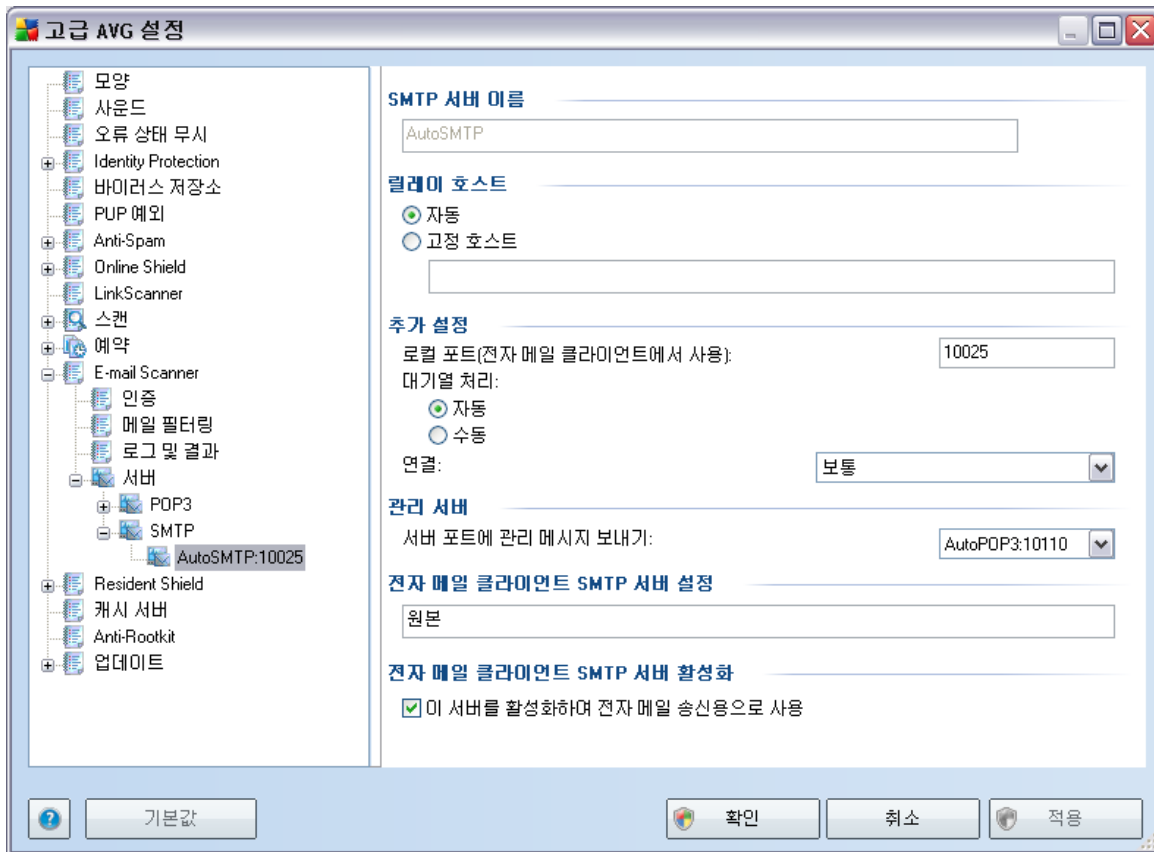
서버 섹션에서 전자 메일 스캐너 구성 요소 서버의 매개 변수를 편집하거나 새 서버 추가 단추를 사용하여 새 서버를 설정할 수 있습니다 .



서버 / POP3을 통해 열린 이 대화 상자에서 들어오는 전자 메일에 대해 POP3 프로토콜을 사용하는 새로운 전자 메일 스캐너 서버를 설정할 수 있습니다 .

- **POP3 서버 이름** - 서버의 이름을 입력하거나 AutoPOP3 기본 이름을 그대로 유지합니다 .
- **로그인 유형** - 들어오는 메일에 사용되는 메일 서버를 결정하는 방법을 정의합니다 .
 - **자동** - 전자 메일 클라이언트 설정에 따라 자동으로 로그인됩니다 .

- o **사용자 / 컴퓨터** - 대상 메일 서버를 결정하는 가장 간단하고 자주 사용되는 방법은 프록시 방법입니다 . 이 방법을 사용하려면 해당 메일 서버의 로그인 사용자 이름 부분에 이름 또는 주소 (또는 포트)를 지정합니다 . 이때 / 문자를 사용하여 이들을 구분합니다 . 예를 들어 서버 pop.acme.com과 포트 8200의 계정 user1의 경우 user1/pop.acme.com:8200을 로그인 이름으로 사용합니다 .
- o **고정 호스트** - 이 경우 프로그램은 항상 여기에 지정된 서버를 사용합니다 . 메일 서버의 주소나 이름을 지정합니다 . 로그인 이름은 변경되지 않은 채로 있습니다 . 이름에는 도메인 이름 (예: pop.acme.com)뿐 아니라 IP 주소 (예: 123.45.67.89)도 사용할 수 있습니다 . 메일 서버에서 비표준 포트를 사용하는 경우 콜론을 구분 기호로 사용하여 이 포트를 서버 이름 다음에 지정할 수 있습니다 (예: pop.acme.com:8200). POP3 커뮤니케이션의 표준 포트는 110입니다 .
- **추가 설정** - 보다 상세하게 매개 변수를 지정합니다 .
 - o **로컬 포트** - 메일 응용 프로그램의 커뮤니케이션이 전달되는 포트를 지정합니다 . 그런 다음 메일 응용 프로그램에서 이 포트를 POP3 커뮤니케이션 포트로 지정해야 합니다 .
 - o **사용 가능한 경우 APOP 사용** - 이 옵션은 보다 안전한 메일 서버 로그인을 지원합니다 . 이렇게 하면 [전자 메일 스캐너](#)에서는 로그인을 위해 사용자 계정 암호를 전달할 때 암호를 열지 않은 상태로 서버에서 받은 변수 체인을 사용하여 암호화된 형식으로 서버에 암호를 보내는 대체 방식을 사용합니다 . 물론 이 기능은 대상 메일 서버에서 이를 지원할 경우에만 사용할 수 있습니다 .
 - o **연결** - 드롭다운 메뉴에서 사용할 연결 유형 (보통 /SSL/SSL 기본값)을 지정할 수 있습니다 . SSL 연결을 선택한 경우 전송되는 데이터가 제3자에 의해 모니터링 또는 추적되지 않도록 암호화됩니다 . 이 기능도 대상 메일 서버에서 이를 지원해야만 사용할 수 있습니다 .
- **전자 메일 클라이언트 POP3 서버 설정??** - [전자 메일 스캐너](#)가 들어오는 모든 메일을 검사할 수 있도록 전자 메일 클라이언트를 올바르게 구성하는 데 필요한 구성 설정에 대한 간략한 정보를 제공합니다 . 이 정보는 이 대화 상자와 다른 대화 상자에서 지정한 매개 변수를 기초로 요약한 것입니다 .
- **전자 메일 클라이언트 POP3 서버 활성화** - 지정된 POP3 서버를 활성화하거나 비활성화하려면 이 항목을 선택하거나 선택 취소합니다 .



서버 / SMTP를 통해 열 수 있는 이 대화 상자에서는 나가는 메일에 SMTP 프로토콜을 사용하는 새로운 **전자 메일 스캐너** 서버를 설정할 수 있습니다 .

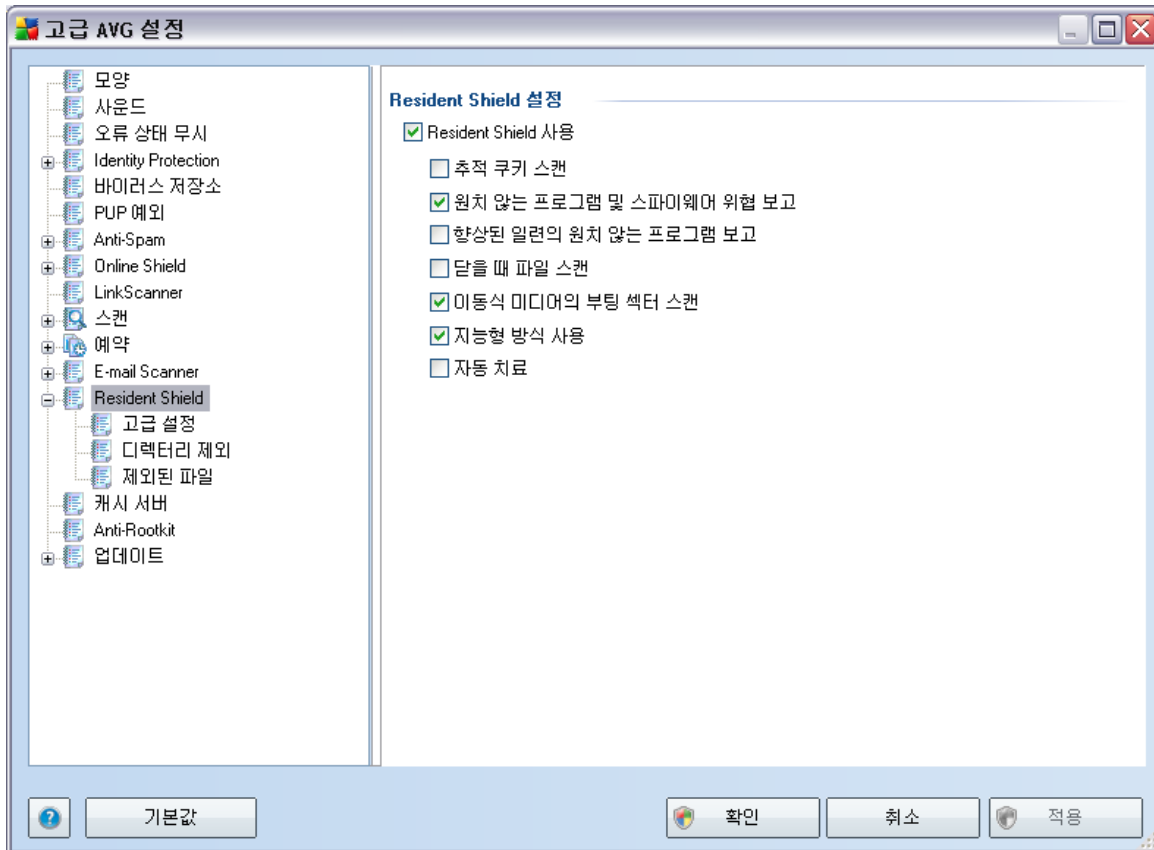
- **SMTP 서버 이름** - 서버의 이름을 입력하거나 AutoSMTP 기본 이름을 유지합니다 .
- **릴레이 호스트** - 나가는 메일에 사용되는 메일 서버를 결정하기 위한 방법을 정의합니다 .
 - **자동** - 전자 메일 클라이언트 설정에 따라 자동으로 로그인됩니다 .
 - **고정 호스트** - 이 경우 프로그램은 항상 여기에 지정된 서버를 사용합니다 . 메일 서버의 주소나 이름을 지정합니다 . 도메인 이름 (예 : smtp.acme.com)이나 도메인 이름의 IP 주소 (예 : 123.45.67.89)를 사용할 수 있습니다 . 메일 서버에서 비표준 포트를 사용할 경우에는 smtp.acme.com:8200 같이 콜론을 구분 기호로 사용하여 서버 이름 뒤에 해당 포트를 입력할 수

있습니다 . SMTP 커뮤니케이션의 표준 포트는 25입니다 .

- **추가 설정** - 보다 상세하게 매개 변수를 지정합니다 .
 - o **로컬 포트** - 메일 응용 프로그램의 커뮤니케이션이 전달되는 포트를 지정합니다 . 그런 다음 메일 응용 프로그램에서 이 포트를 SMTP 커뮤니케이션 포트로 지정해야 합니다 .
 - o **대기열 처리** - 메일 메시지를 보내기 위한 요구 사항을 처리할 때 [전자 메일 스캐너](#)의 동작을 결정합니다 .
 - 자동 - 나가는 메일이 대상 메일 서버에 즉시 전달 (전송)됩니다 .
 - 수동 - 메시지가 나가는 메시지의 대기열에 삽입되고 나중에 전송됩니다 .
 - o **연결** - 이 드롭다운 메뉴에서 사용할 연결 유형 (보통 /SSL/SSL 기본값)을 지정할 수 있습니다 . SSL 연결을 선택한 경우 전송되는 데이터가 제3자에 의해 모니터링 또는 추적되지 않도록 암호화됩니다 . 이 기능은 대상 메일 서버에서 지원되는 경우에만 사용할 수 있습니다 .
- **관리 서버** - 관리 보고서의 역전달에 사용할 서버의 포트 번호가 표시됩니다 . 이러한 메시지는 대상 메일 서버에서 나가는 메시지를 거부하거나 이 메일 서버를 사용할 수 없는 경우 등에 생성됩니다 .
- **전자 메일 클라이언트 SMTP 서버 설정** - 나가는 메일을 확인할 때 현재 수정된 서버를 사용하여 나가는 메일 메시지가 확인되도록 클라이언트 메일 응용 프로그램을 구성하는 방법에 대한 정보를 제공합니다 . 이 정보는 이 대화 상자와 다른 대화 상자에서 지정한 매개 변수를 기초로 요약한 것입니다 .
- **전자 메일 클라이언트 SMTP 서버 활성화** - 위에 지정된 SMTP 서버를 활성화 또는 비활성화하려면 이 확인란을 선택하거나 선택을 취소합니다 .

10.13. Resident Shield

상주 보호 구성 요소는 바이러스, 스파이웨어 및 기타 맬웨어로부터 파일 및 폴더를 실시간으로 보호해 줍니다.



상주 보호 설정 대화 상자에서 **상주 보호 사용** 항목을 선택하거나 선택 취소하여 **상주 보호** 기능을 완전히 활성화하거나 비활성화할 수 있습니다. 이 옵션은 기본적으로 설정되어 있습니다. 또한 어떤 **상주 보호** 기능을 활성화할지 선택할 수도 있습니다.

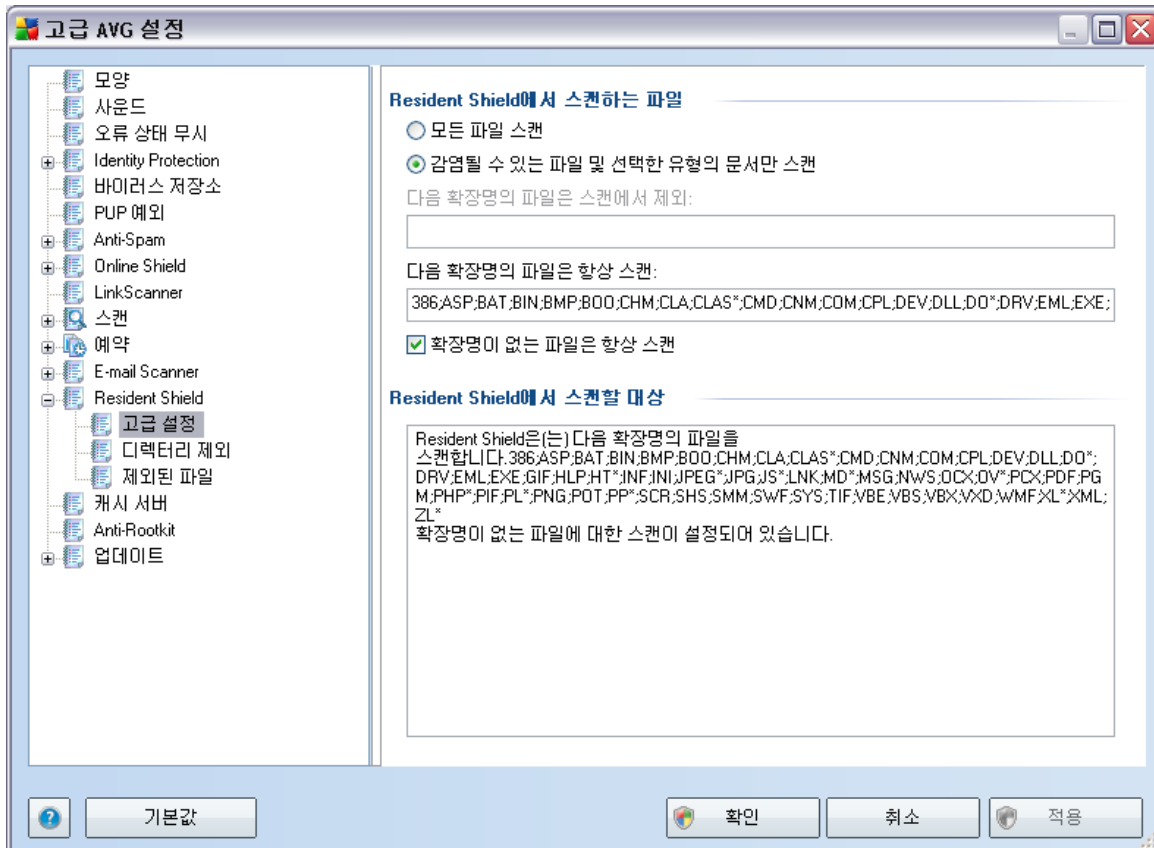
- **추적 쿠키 스캔** - 이 매개 변수는 스캔 중에 쿠키가 발견되도록 정의합니다. HTTP 쿠키는 사이트 기본 설정이나 전자 쇼핑 카트의 내용물과 같이 사용자와 관련된 특정 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - **Anti-Spyware** 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위험을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다. 이 기

능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다 .

- **향상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 [스파이웨어](#)의 확장 패키지를 검색하려면 이 상자를 선택합니다 . 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만 , 나중에 악의적인 목적으로 잘못 사용될 수 있습니다 . 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만 , 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다 .
- **닫을 때 파일 스캔** - 닫을 때 스캔 기능을 사용하면 활성 개체 (예: 응용 프로그램, 문서)를 열 때는 물론 닫을 때도 해당 개체를 스캔할 수 있습니다 . 이 기능은 일부 유형의 복잡한 바이러스로부터 사용자 컴퓨터를 보호하는 데 유용합니다 .
- **이동식 미디어의 부팅 섹터 스캔** - (기본적으로 설정되어 있음)
- **지능형 방식 사용** - (기본적으로 설정되어 있음) [지능형 분석](#)은 검색에 사용됩니다 (가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침) .
- **자동 치료** - 발견된 모든 감염 요소는 치료가 가능한 경우 자동으로 치료됩니다 .

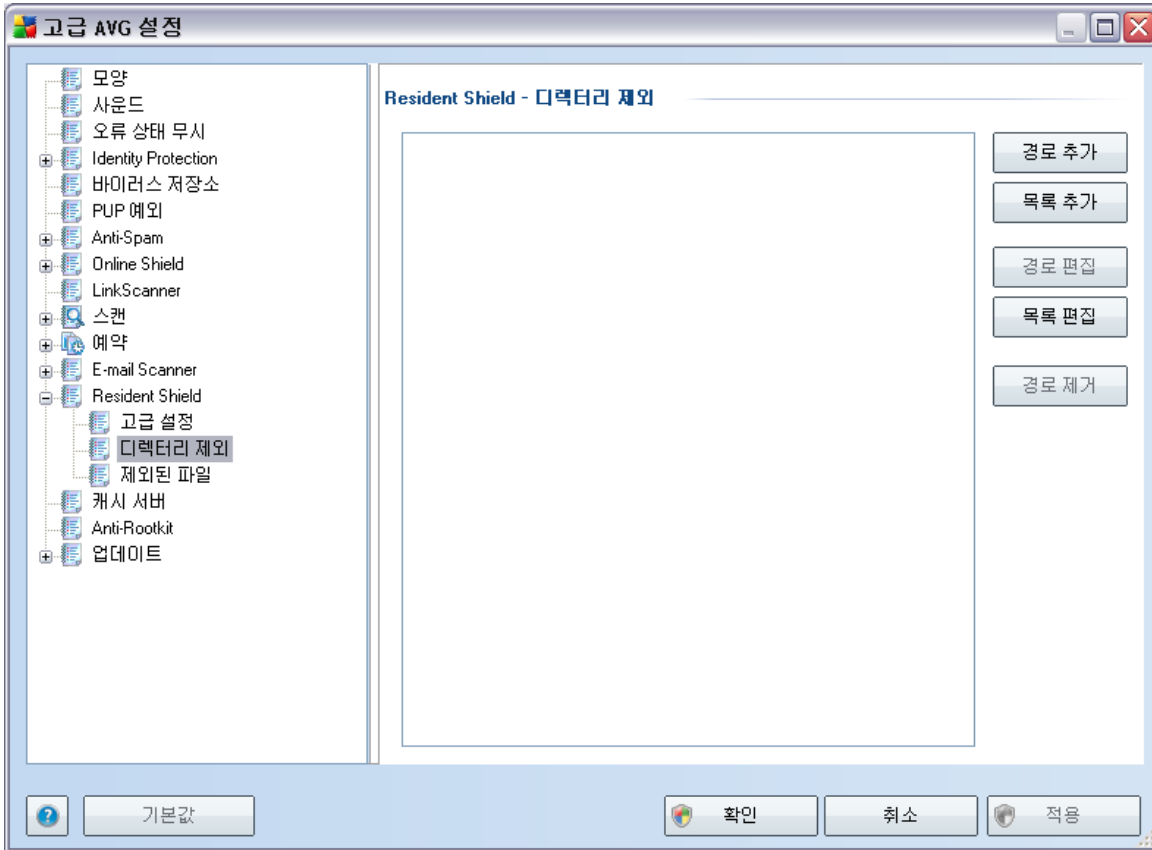
10.13.1. 고급 설정

상주 보호에서 스캔하는 파일 대화 상자에서 스캔할 파일을 구성할 수 있습니다 (특정 확장명 기준).



파일을 모두 스캔할지 아니면 감염 가능한 파일만 스캔할지를 결정합니다 . 감염 가능한 파일만 스캔하는 경우 스캔에서 제외할 파일을 정의하는 확장명 목록과 어떤 상황에서든 스캔되어야 하는 파일을 정의하는 파일 확장명 목록을 추가로 지정할 수 있습니다 .

10.13.2. 디렉터리 제외



상주 보호 - 디렉터리 제외 대화 상자에서는 **상주 보호** 스캔에서 제외시킬 폴더를 정의할 수 있습니다 .

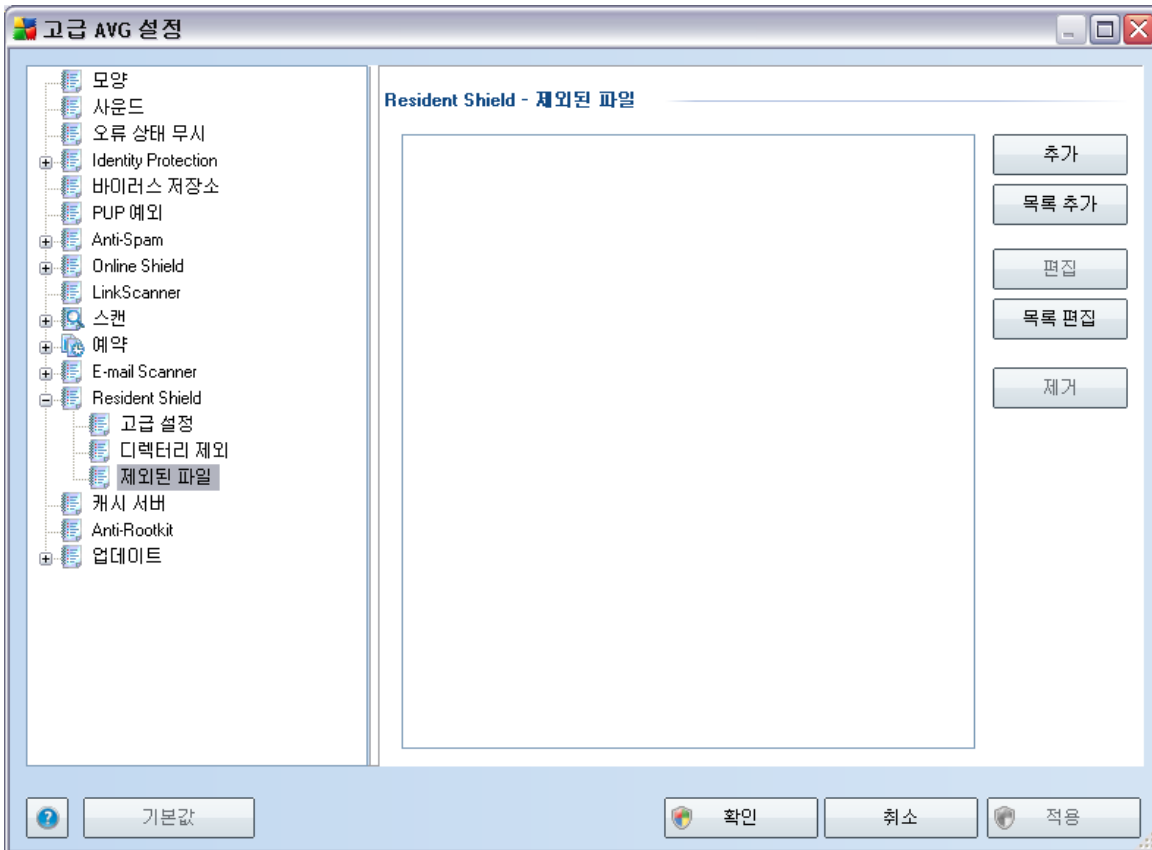
특정 디렉터리를 반드시 제외해야 할 경우가 아니라면 디렉터리를 하나라도 제외하지 않는 것이 좋습니다 .

이 대화 상자에는 다음과 같은 제어 단추가 있습니다 .

- **경로 추가** – 로컬 디스크 탐색 트리에서 디렉터리를 하나씩 선택하여 스캔에서 제외할 디렉터리를 지정할 수 있습니다 .
- **목록 추가** – **상주 보호** 스캔에서 제외할 디렉터리의 전체 목록을 입력할 수 있습니다 .
- **경로 편집** – 선택한 폴더에 대해 지정된 경로를 편집할 수 있습니다 .

- **목록 편집** – 폴더 목록을 편집할 수 있습니다 .
- **경로 제거** – 목록에서 선택한 폴더의 경로를 삭제할 수 있습니다 .

10.13.3. 제외된 파일



상주 보호 - 제외된 파일 대화 상자는 앞서 설명한 **상주 보호 - 디렉터리 제외**와 동일하게 작동하지만 폴더를 지정하는 대신 **상주 보호** 스캔에서 제외할 특정 파일을 정의할 수 있다는 점이 다릅니다 .

특정 파일을 반드시 제외해야 할 경우가 아니라면 파일을 하나라도 제외하지 않는 것이 좋습니다 .

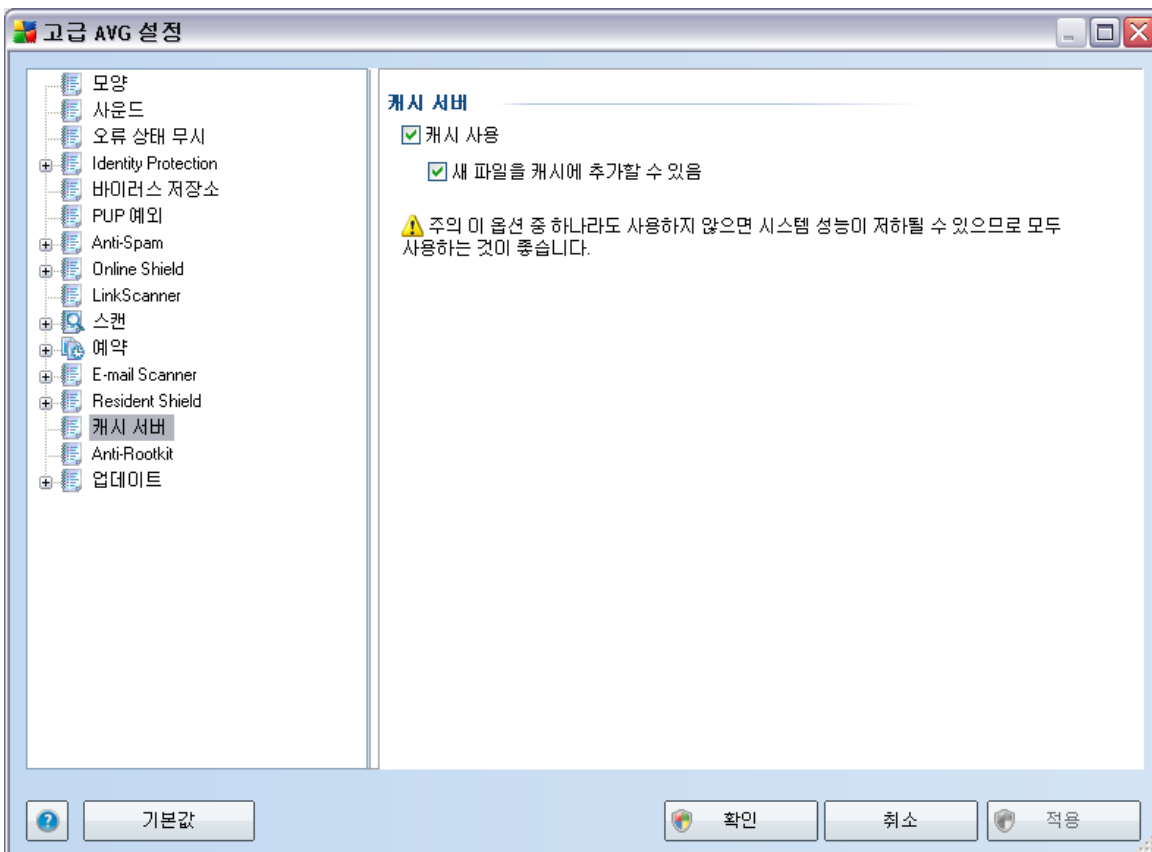
이 대화 상자에는 다음과 같은 제어 단추가 있습니다 .

- **추가** – 로컬 디스크 탐색 트리에서 파일을 하나씩 선택하여 스캔에서 제외할 파일을 지정할 수 있습니다 .

- **목록 추가** - 상주 보호 스캔에서 제외할 파일의 전체 목록을 입력할 수 있습니다.
- **편집** - 선택한 파일에 대해 지정된 경로를 편집할 수 있습니다 .
- **목록 편집** - 파일 목록을 편집할 수 있습니다 .
- **제거** - 목록에서 선택한 파일의 경로를 삭제할 수 있습니다 .

10.14. 캐시 서버

캐시 서버 는 모든 스캔 (요청 시 스캔, 예약된 전체 컴퓨터 스캔, 상주 보호 스캔) 속도를 높이기 위해 고안된 프로세스입니다 . 캐시 서버는 신뢰할 수 있는 파일 정보 (디지털 서명이 포함된 시스템 파일 등)를 수집하고 보관합니다 . 이러한 파일은 안전한 것으로 간주되며 스캔 중 건너뛰게 됩니다 .

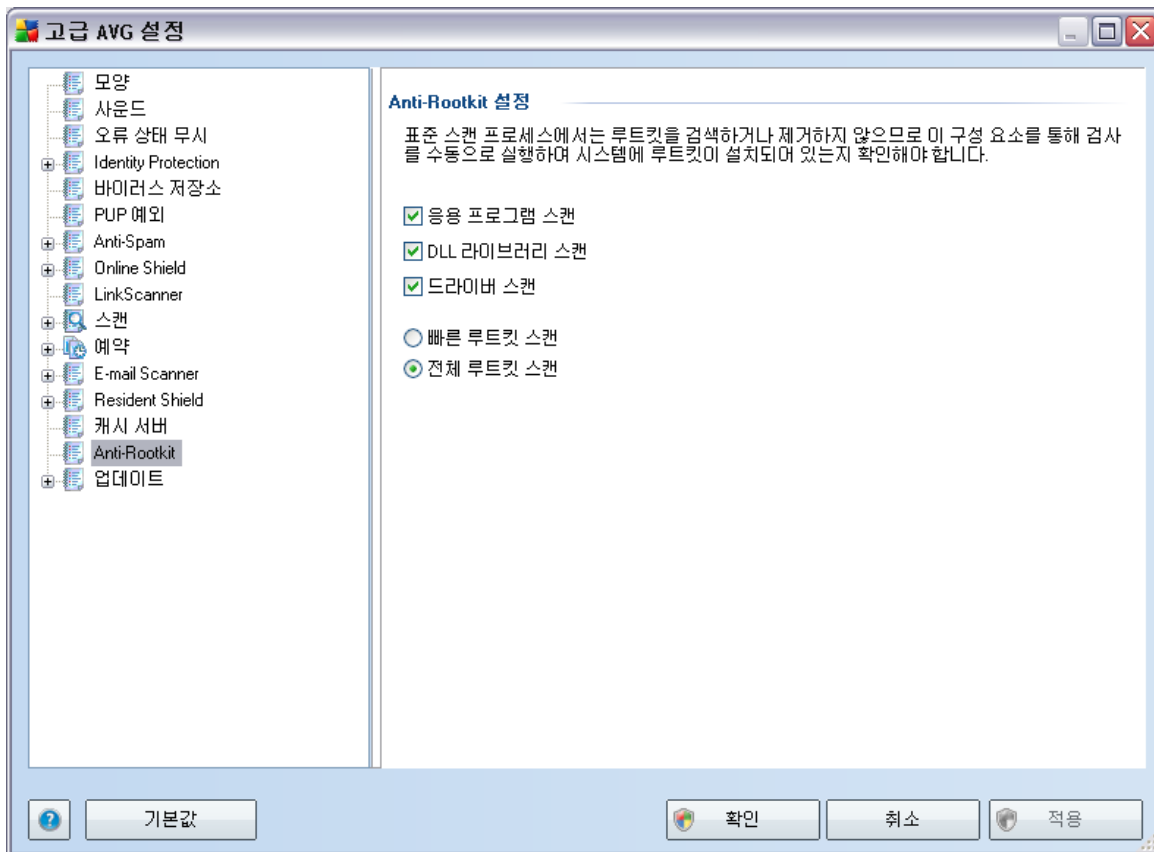


설정 대화 상자에서는 다음 두 가지 옵션을 제공합니다 .

- **캐시 사용** (기본적으로 설정되어 있음) - **캐시 서버** 를 해제하려면 이 상자의 선택을 취소하고 캐시 메모리를 비우십시오 . 처음에는 사용 중인 전체 파일에 대해 하나씩 바이러스 및 스파이웨어 스캔이 진행되므로 , 스캔 속도가 느려질 수 있으며 컴퓨터의 전반적인 성능이 저하될 수 있습니다 .
- **새 파일을 캐시에 추가할 수 있음** (기본적으로 설정되어 있음) - 파일을 캐시 메모리에 더 이상 추가하지 않으려면 이 상자의 선택을 취소하십시오 . 이미 캐시된 모든 파일은 캐시가 완전히 해제되거나 다음 번 바이러스 데이터베이스가 업데이트될 때까지 보관되어 사용됩니다 .

10.15. Anti-Rootkit

이 대화 상자에서 **Anti-Rootkit** 구성 요소의 구성을 편집할 수 있습니다 .



Anti-Rootkit 구성 요소 인터페이스 에서도 직접 액세스하여 이 대화 상자에서 제공된 **Anti-Rootkit** 구성 요소의 모든 기능을 편집할 수 있습니다 .

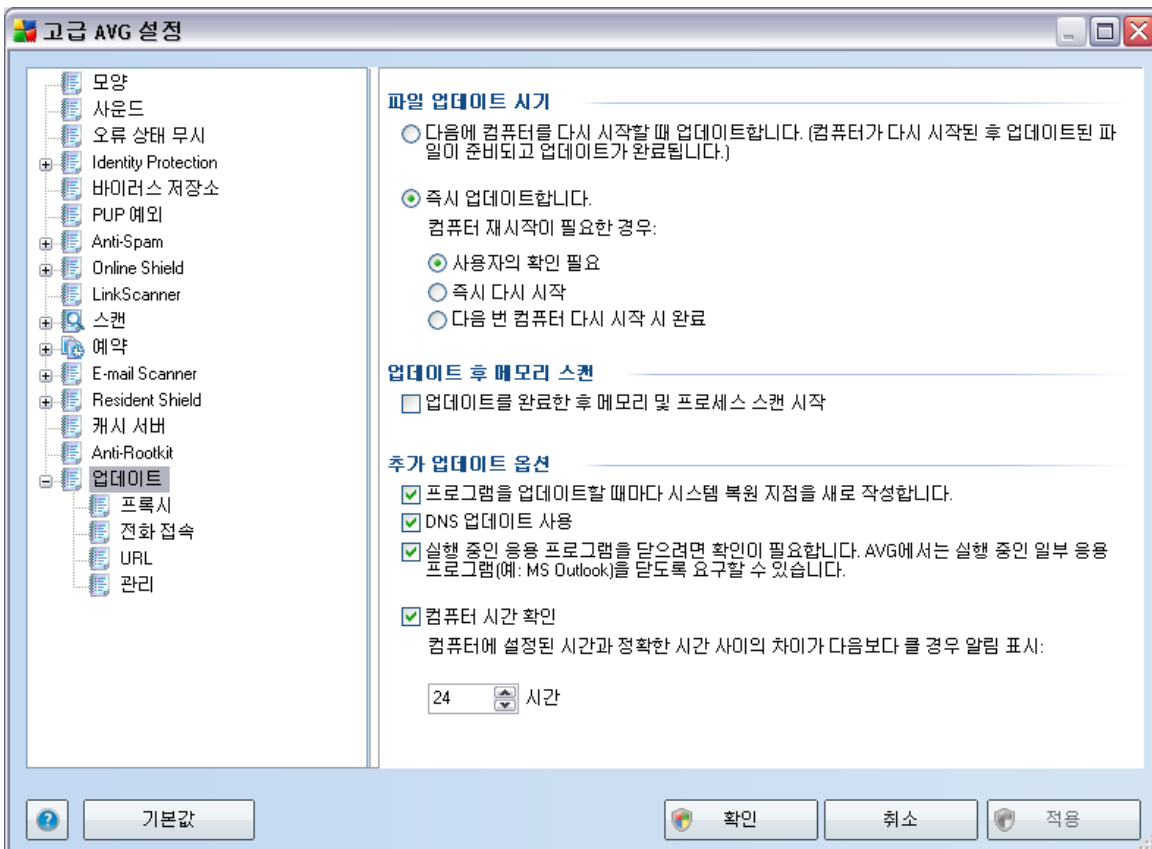
먼저 각 확인란을 선택하여 스캔할 개체를 지정합니다 .

- 응용 프로그램 스캔
- DLL 라이브러리 스캔
- 드라이버 스캔

또한 루트킷 스캔 모드도 선택할 수 있습니다 .

- 빠른 루트킷 스캔 - 모든 실행 중인 프로세스 , 로드된 드라이버 및 시스템 폴더 (일반적으로 c:\Windows)를 스캔합니다 .
- 전체 루트킷 스캔 - 모든 실행 중인 프로세스 , 로드된 드라이버 및 시스템 폴더 (일반적으로 c:\Windows)와 모든 로컬 디스크 (플래시 디스크 포함, 플로피 디스크 /CD 드라이브 제외)를 스캔합니다 .

10.16. 업데이트



업데이트 탐색 항목은 [AVG 업데이트](#)에 관한 일반 매개 변수를 지정할 수 있는 새 대화 상자를 엽니다 .

파일 업데이트 시기

이 섹션에서는 두 옵션 중 하나를 선택할 수 있습니다 . 다음에 PC를 다시 시작할 때 [업데이트](#)하도록 예약하거나 , 아니면 사용자가 즉시 [업데이트](#)를 시작할 수 있습니다 . 기본적으로 즉시 업데이트 옵션이 선택되어 있는데 이런 방식으로 AVG는 보안 수준을 극대화할 수 있습니다 . 다음에 PC를 다시 시작할 때 업데이트하도록 예약하는 옵션은 적어도 매일 정기적으로 컴퓨터를 다시 시작할 수 있는 경우에만 사용하는 것이 좋습니다 .

기본 구성을 유지한 상태로 즉시 업데이트 프로세스를 시작하는 경우에는 컴퓨터를 다시 시작하는 조건을 지정할 수 있습니다 .

- **사용자의 확인 필요** - [업데이트 프로세스를 완료하기 위해 PC를 다시 시작할지 묻는 승인 메시지를 표시합니다](#) .
- **즉시 다시 시작** - 컴퓨터는 [업데이트 프로세스](#)가 완료된 후 즉시 자동으로 다시 시작되며 사용자 승인이 필요 없습니다 .
- **다음 번 컴퓨터 다시 시작 시 완료** - 다음에 컴퓨터가 다시 시작될 때까지 [업데이트 프로세스](#) 완료 시점이 연기됩니다 . 이 옵션은 적어도 매일 정기적으로 컴퓨터를 다시 시작할 수 있는 경우에만 사용하는 것이 좋습니다 .

업데이트 후 메모리 스캔

업데이트가 완료될 때마다 새 메모리 스캔을 시작하도록 정의하려면 이 확인란을 선택합니다 . 최신 다운로드 업데이트에는 새로운 바이러스 정의가 포함되어 있을 수 있으므로 스캔에 즉시 적용하는 것이 좋습니다 .

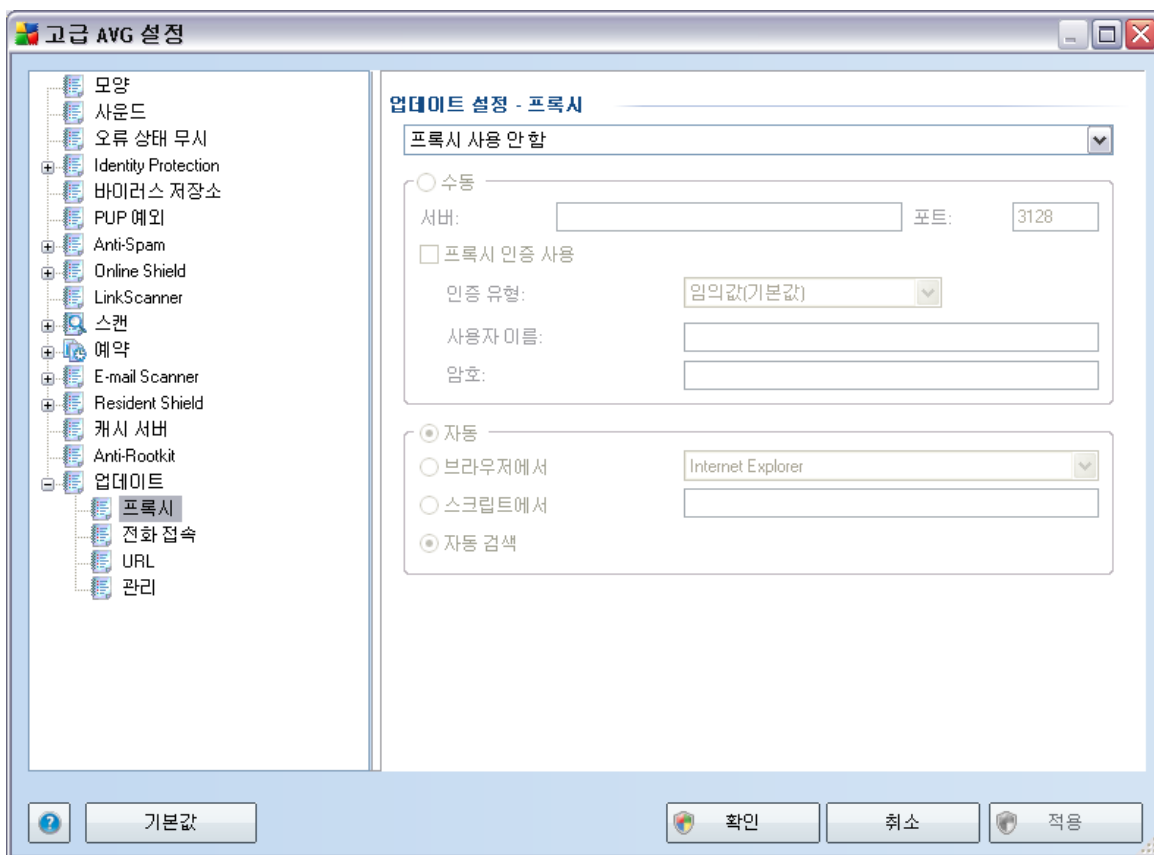
추가 업데이트 옵션

- **프로그램을 업데이트할 때마다 시스템 복원 지점을 새로 작성합니다** . - 각 AVG 프로그램 업데이트가 시작되기 전에 시스템 복원 지점이 만들어집니다 . 업데이트 프로세스가 실패하여 운영 체제가 중단되는 경우 언제든지 OS를 이 지점에서 원래 구성으로 복원할 수 있습니다 . 이 옵션은 시작 /모든 프로그램 /보조 프로그램 /시스템 도구 /시스템 복원을 통해 액세스할 수 있지만 변경은 숙련된 사용자만 하는 것이 좋습니다 . 이 기능을 이용하려면 이 확인란을 선택된 상태로 유지합니다 .
- **DNS 업데이트 사용** - 업데이트 서버와 AVG 클라이언트 사이에 전송된 데이터

를 제거하는 업데이트 파일 검색 방법을 사용하려면 이 확인란을 선택합니다 .

- **실행 중인 응용 프로그램을 닫으려면 확인이 필요합니다** .(기본적으로 설정되어 있음) 옵션을 사용하면 업데이트 프로세스를 완료하기 위해 현재 실행 중인 응용 프로그램을 닫아야 할 경우에는 항상 사용자의 확인을 요구합니다 .
- **컴퓨터 시간 확인** - 컴퓨터 시간과 정확한 시간 사이의 차이가 정해진 시간보다 더 많이 나는 경우 알림이 표시되도록 하려면 이 옵션을 선택합니다 .

10.16.1. 프록시



프록시 서버는 인터넷에 대한 보다 안전한 연결을 보장하기 위해 PC에서 실행되는 서비스 또는 독립 실행형 서버입니다 . 지정된 네트워크 규칙에 따라 프록시 서버를 통과하거나 아니면 직접 인터넷에 액세스할 수 있으며 동시에 두 가지 옵션 모두 사용 가능합니다 . 그러면 **업데이트 설정 - 프록시** 대화 상자의 첫 번째 항목에서 원하는 콤보 상자 메뉴를 선택해야 합니다 .

- **프록시 사용**
- **프록시 서버 사용하지 않음** - 기본 설정
- **프록시를 사용하여 연결을 시도하고 실패할 경우에는 직접 연결**

프록시 서버를 사용하는 옵션을 선택한 경우 몇 가지 데이터를 더 지정해야 합니다 . 서버 설정은 자동으로 구성되기도 하지만 수동으로 구성할 수도 있습니다 .

수동 구성

수동 구성을 선택하는 경우에는 **수동** 옵션을 선택하여 해당 대화 상자 섹션을 활성화 하고 다음 항목을 지정해야 합니다 .

- **서버** - 서버의 IP 주소 또는 서버 이름을 지정합니다 .
- **포트** - 인터넷 액세스를 지원하는 포트 번호를 지정합니다 . 기본적으로 이 번호 는 3128로 설정되지만 , 다른 번호를 설정할 수도 있습니다 . 해당 번호를 알 수 없는 경우 네트워크 관리자에게 문의하십시오 .

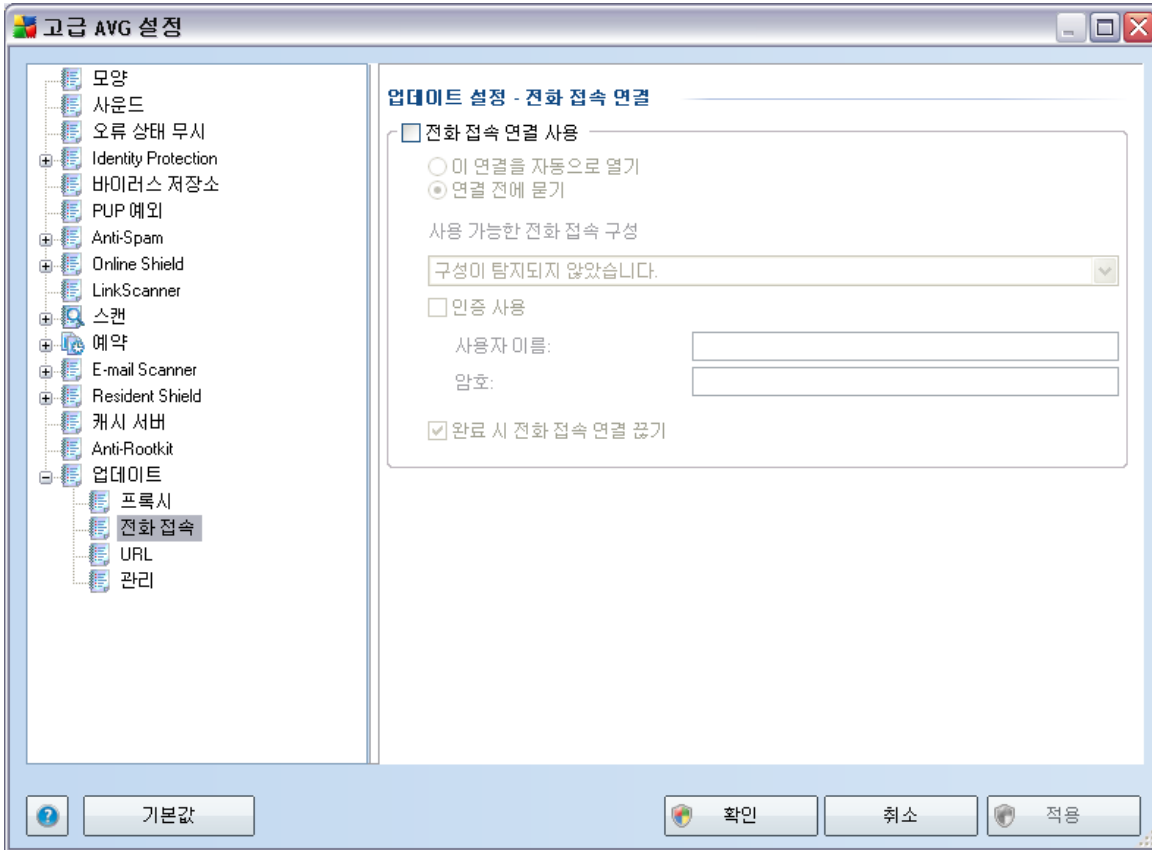
프록시 서버에서는 각 사용자에게 대한 특정 규칙을 구성할 수 있습니다 . 프록시 서버가 이와 같이 설정되어 있으면 **프록시 인증 사용** 옵션을 선택하고 자신의 사용자 이름과 암호를 사용하여 프록시 서버를 통해 인터넷에 연결할 수 있는지 확인하십시오 .

자동 구성

자동 구성을 선택하는 경우에는 **자동** 옵션을 선택하여 해당 대화 상자 섹션을 활성화 하고 프록시 구성을 가져올 위치를 선택하십시오 .

- **브라우저에서** - 기본 인터넷 브라우저에서 구성을 읽습니다 .
- **스크립트에서** - 프록시 주소를 반환하는 기능을 수행하는 다운로드 스크립트 에서 구성을 읽어옵니다 .
- **자동 검색** - 프록시 서버에서 직접 구성을 자동으로 검색합니다 .

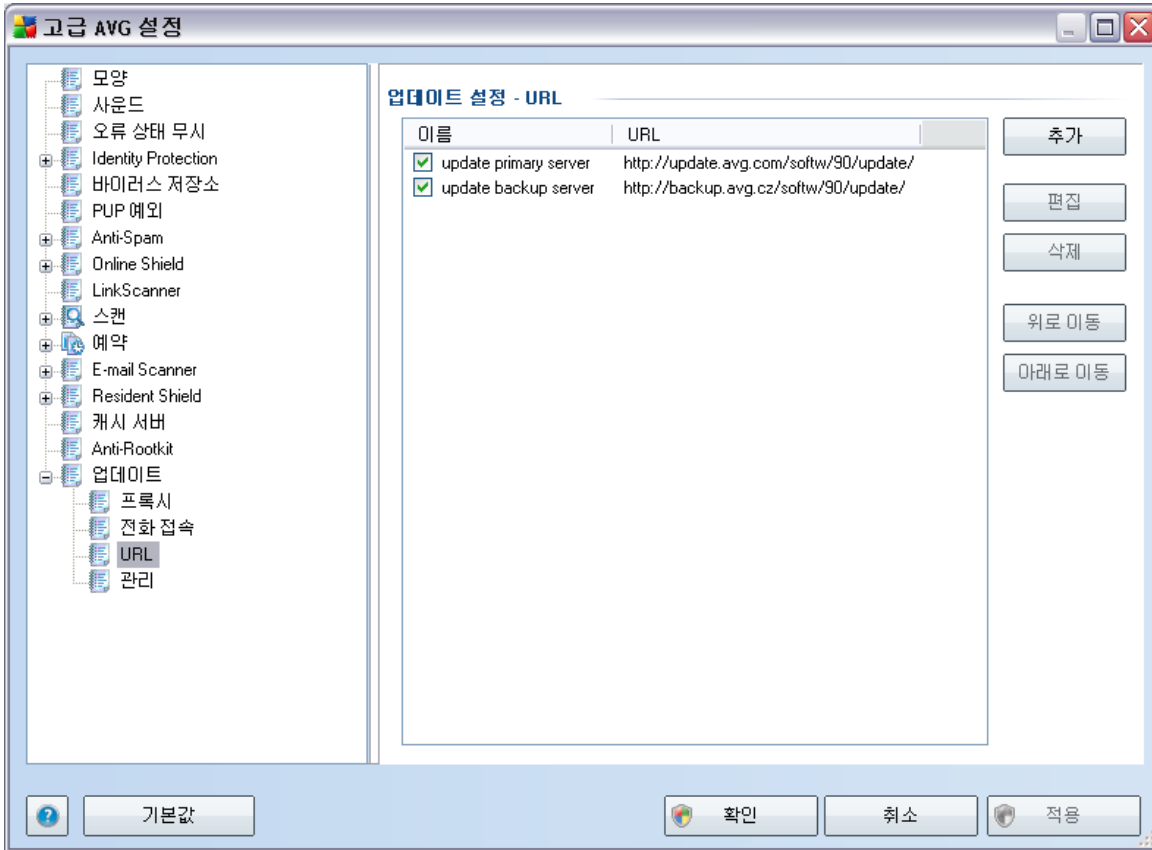
10.16.2. 전화 접속



업데이트 설정 - 전화 접속 연결 대화 상자에서 선택적으로 정의된 모든 매개 변수는 인터넷에 대한 전화 접속 연결과 관련되어 있습니다 . 이 대화 상자의 필드는 **전화 접속 연결 사용** 옵션을 선택하여 필드를 활성화할 때까지 비활성 상태를 유지합니다 .

인터넷에 자동으로 연결할지 (**이 연결을 자동으로 열기**) 아니면 매번 연결을 수동으로 확인할지 (**연결 전에 묻기**)를 지정합니다 . 자동 연결을 하려면 업데이트가 완료된 후 연결을 끊을지 여부를 추가로 선택해야 합니다 (**완료 시 전화 접속 연결 끊기**).

10.16.3. URL

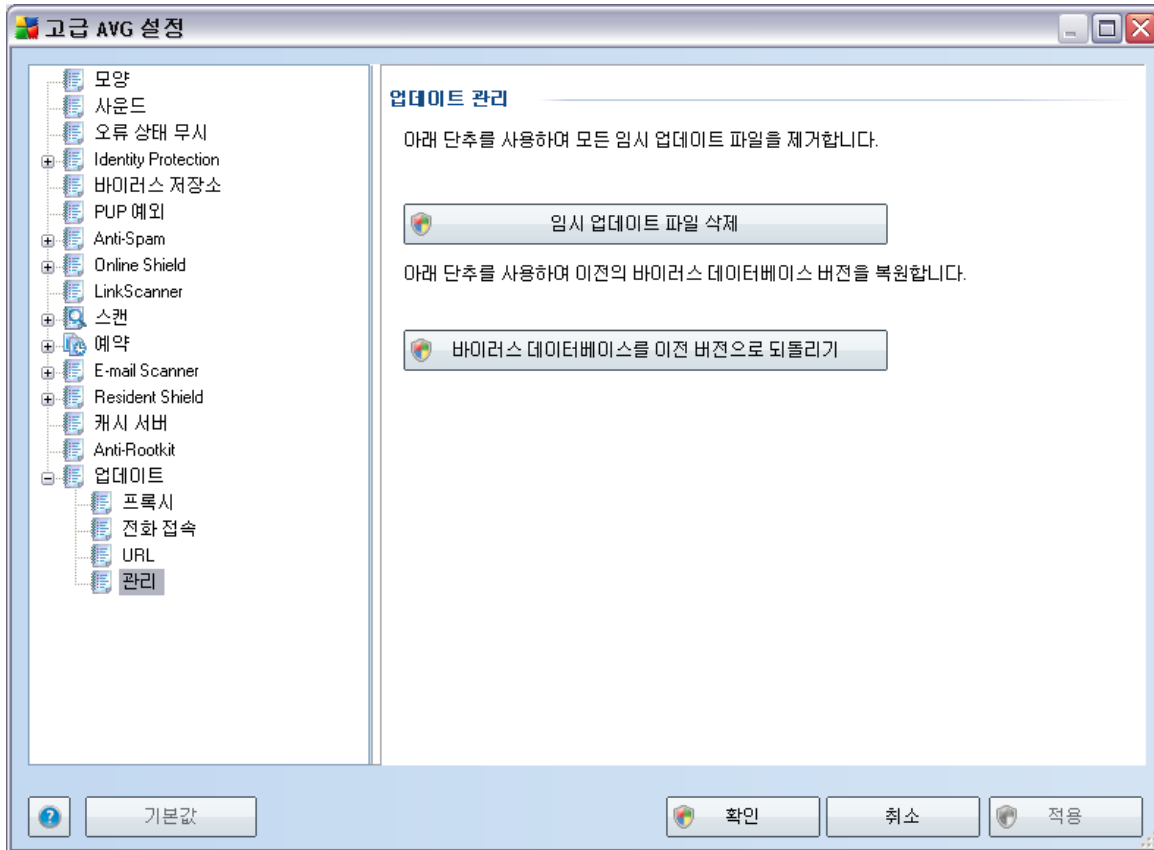


URL 대화 상자에는 업데이트 파일을 다운로드할 수 있는 인터넷 주소의 목록이 제공됩니다. 목록 및 해당 항목은 다음 제어 단추를 사용하여 수정할 수 있습니다.

- **추가** - 목록에 추가할 새 URL을 지정할 수 있는 대화 상자를 엽니다.
- **편집** - 선택한 URL 매개 변수를 편집할 수 있는 대화 상자를 엽니다.
- **삭제** - 선택한 URL을 목록에서 삭제합니다.
- **위로 이동** - 선택한 URL을 목록에서 한 칸 위로 이동합니다.
- **아래로 이동** - 선택한 URL을 목록에서 한 칸 아래로 이동합니다.

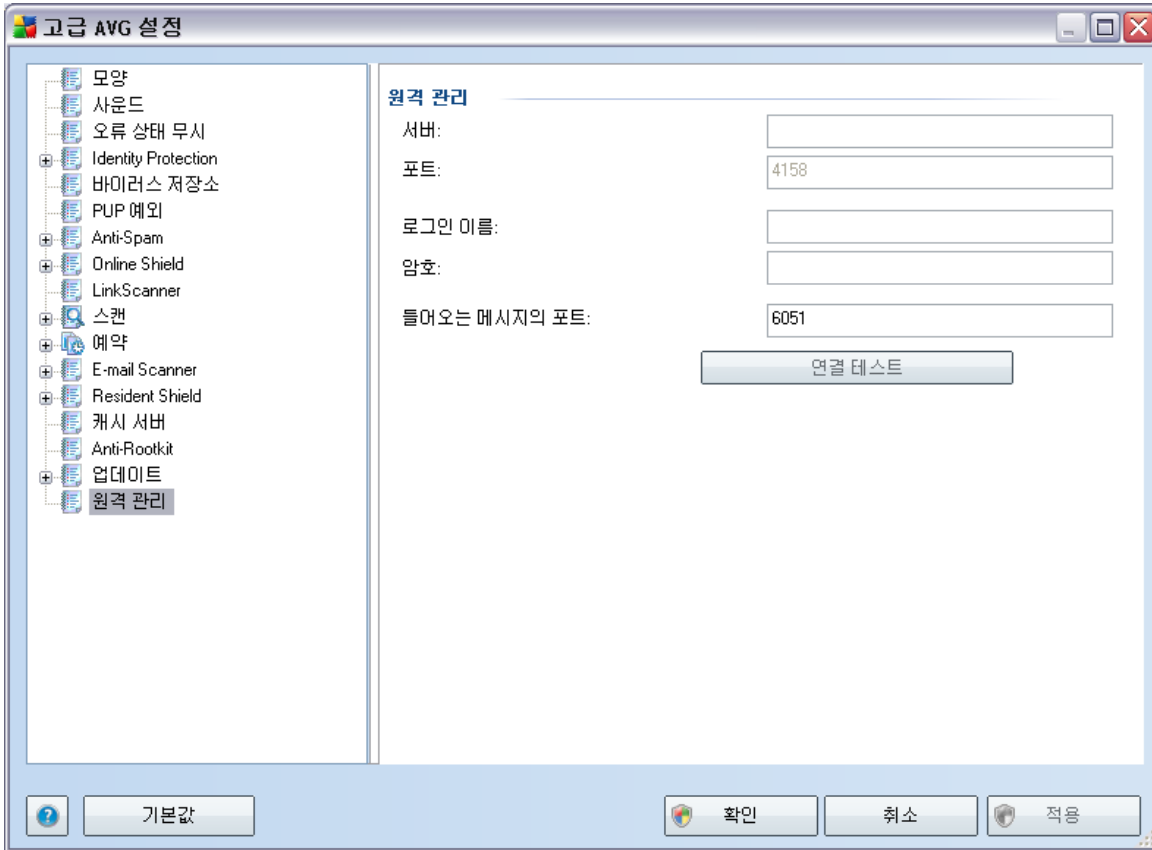
10.16.4. 관리

관리 대화 상자에는 두 개의 단추를 통해 액세스할 수 있는 두 가지 옵션이 있습니다 .



- **임시 업데이트 파일 삭제** - 하드 디스크에서 모든 중복 업데이트 파일을 삭제하려면 이 단추를 누릅니다 . 기본적으로 이 파일은 30일 동안 저장됩니다 .
- **바이러스 데이터베이스를 이전 버전으로 되돌리기** - 이 단추를 누르면 하드 디스크에서 최신 바이러스 데이터베이스 버전을 삭제하고 이전에 저장한 버전으로 돌아갈 수 있습니다 . 새 바이러스 데이터베이스 버전은 다음 업데이트에 포함됩니다 .

10.17. 원격 관리



원격 관리 설정이란 원격 관리 시스템에 대한 AVG 클라이언트 스테이션 연결을 의미합니다. 개별 스테이션에서 원격 관리에 연결하도록 하려면 다음 매개 변수를 지정하십시오.

- **서버** - AVG Admin Server가 설치되어 있는 서버 이름 또는 서버 IP 주소를 지정합니다.
- **포트** - AVG 클라이언트가 AVG Admin Server와 커뮤니케이션하는 포트 번호를 제공합니다. 기본 포트 번호는 4158로, 이 포트 번호를 사용할 경우에는 명시적으로 지정할 필요가 없습니다.
- **로그인** - AVG 클라이언트와 AVG Admin Server 간의 커뮤니케이션이 보안 커뮤니케이션으로 정의된 경우 사용자 이름을 제공해야 합니다.
- **암호** - ... 및 사용자 암호



- **들어오는 메시지의 포트** - AVG 클라이언트가 AVG Admin Server에서 들어오는 메시지를 받는 포트 번호입니다 .

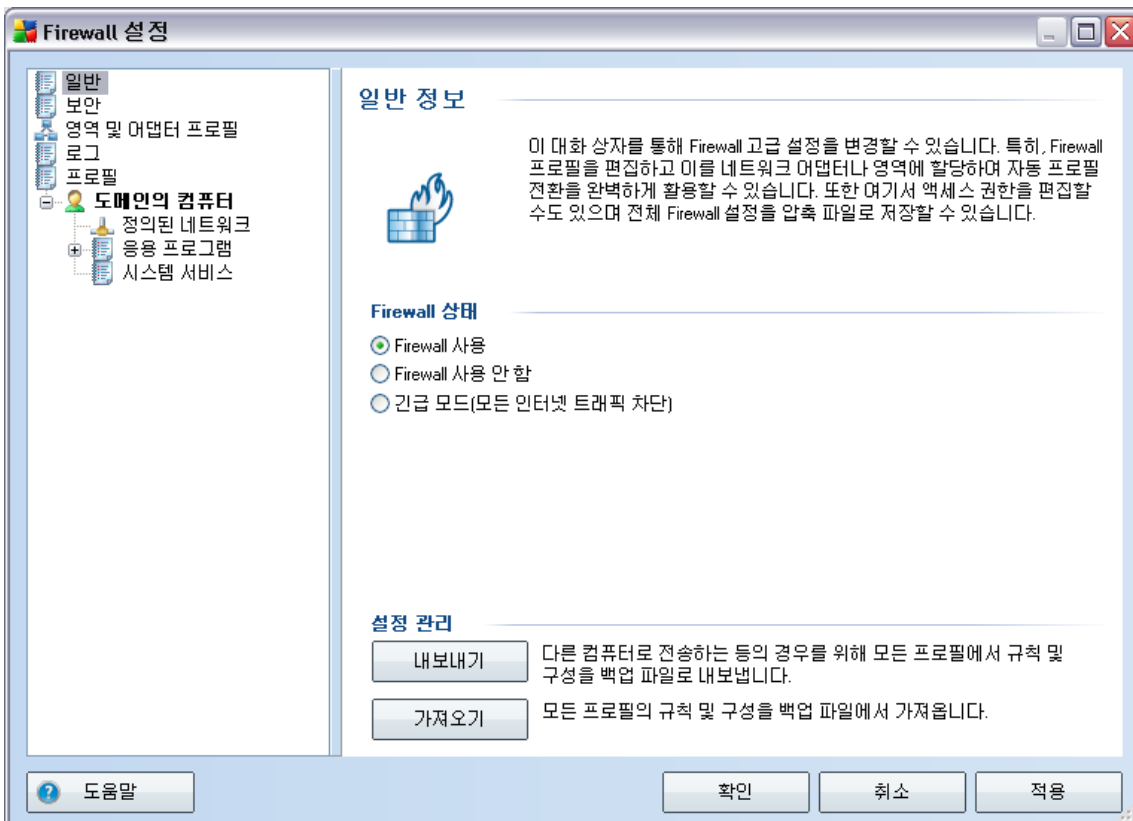
연결 테스트 단추를 사용하면 위의 모든 데이터가 올바르게 DataCenter에 연결할 때 사용 가능한지 확인할 수 있습니다 .

참고 : 원격 관리에 대한 자세한 내용은 AVG Network Edition 설명서를 참조하십시오 .

11. 방화벽 설정

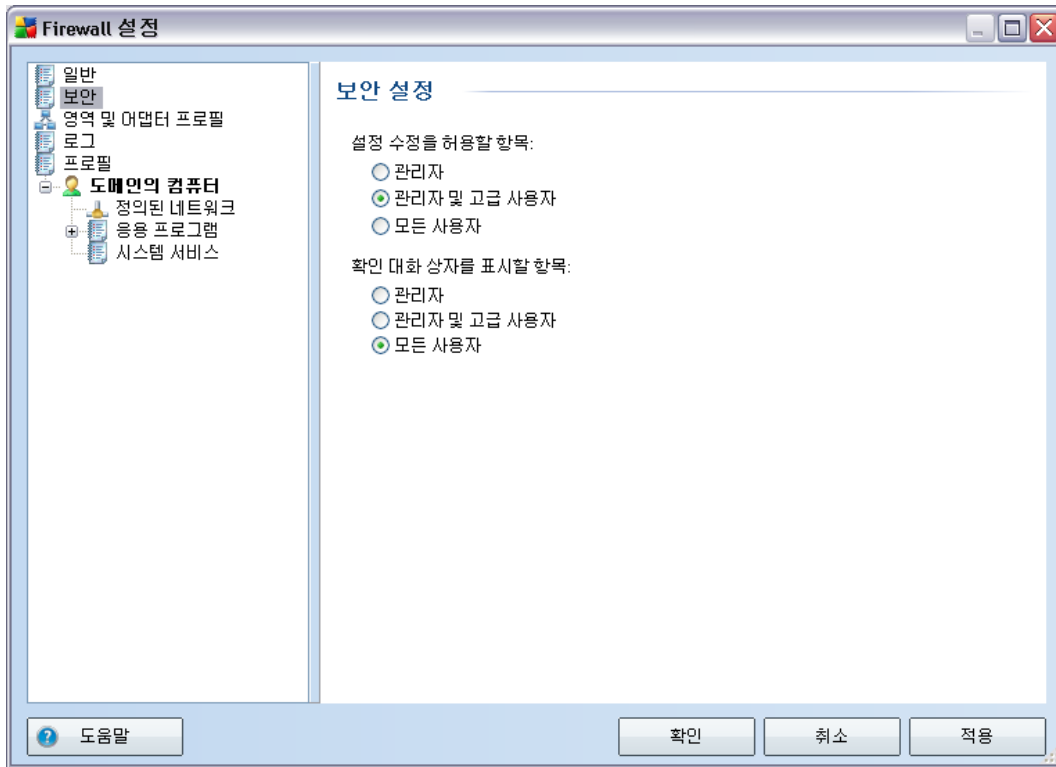
방화벽 구성은 구성 요소의 고급 매개 변수를 설정할 수 있는 여러 개의 대화 상자가 있는 새 창에서 열립니다 . **하지만 이 고급 구성 편집은 숙련된 사용자가 수행해야 합니다 .**

11.1. 일반



일반 정보 에서 방화벽 **구성**의 내보내기 및 가져오기 *******를 수행할 수 있습니다 . 예를 들어 , 정의된 **방화벽** 규칙 및 설정을 백업 파일로 내보내거나 전체 백업 파일을 가져올 수 있습니다 .

11.2. 보안



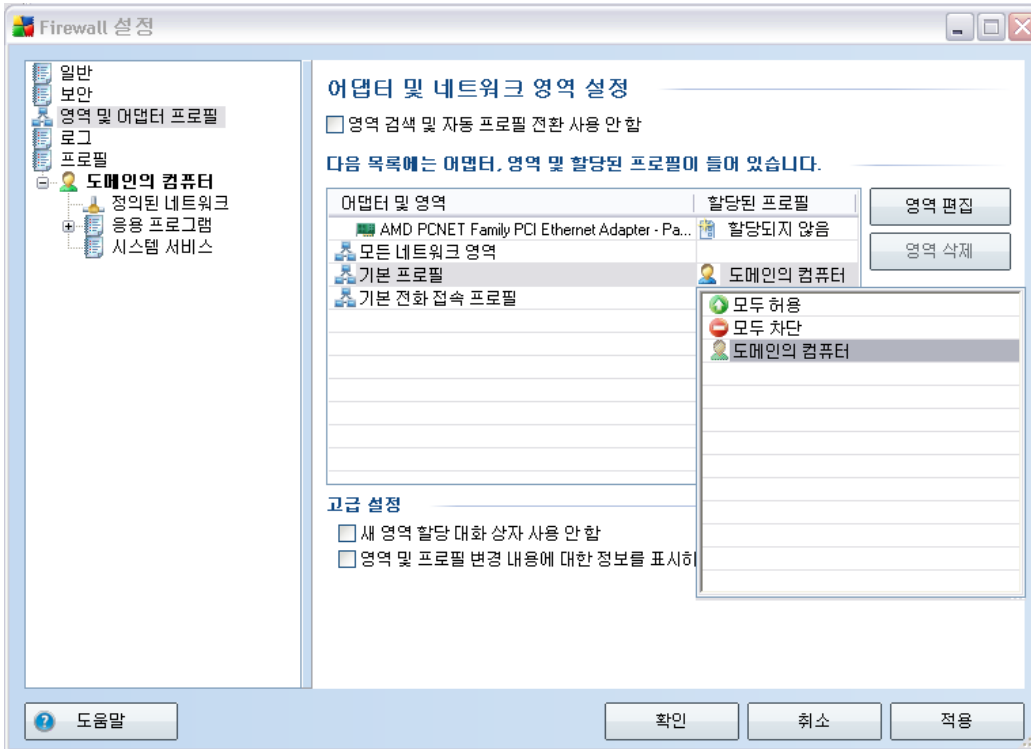
보안 설정 대화 상자에서 **방화벽** 동작에 대한 일반 규칙을 선택된 프로필에 상관없이 정의할 수 있습니다 .

- **설정 수정을 허용할 대상** - **방화벽** 구성을 변경할 수 있는 사람을 지정합니다 .
- **확인 대화 상자를 표시할 항목** - 확인 대화 상자 (정의된 **방화벽** 규칙이 적용되지 않는 상황에서 결정을 요구하는 대화 상자)를 표시할 대상을 지정합니다 .

어느 경우든 다음 사용자 그룹 중 하나에 특정한 권한을 할당할 수 있습니다 .

- **관리자** - PC를 완전히 제어하며 모든 사용자에게 특정하게 정의된 권한을 가진 그룹에 할당할 권한을 가집니다 .
- **관리자 및 고급 사용자** - 관리자는 사용자를 특정한 그룹 (**고급 사용자**)에 할당할 수 있으며 해당 그룹 구성원의 권한을 정의할 수 있습니다 .
- **모든 사용자** - 특정 그룹에 할당되지 않은 그 밖의 사용자입니다 .

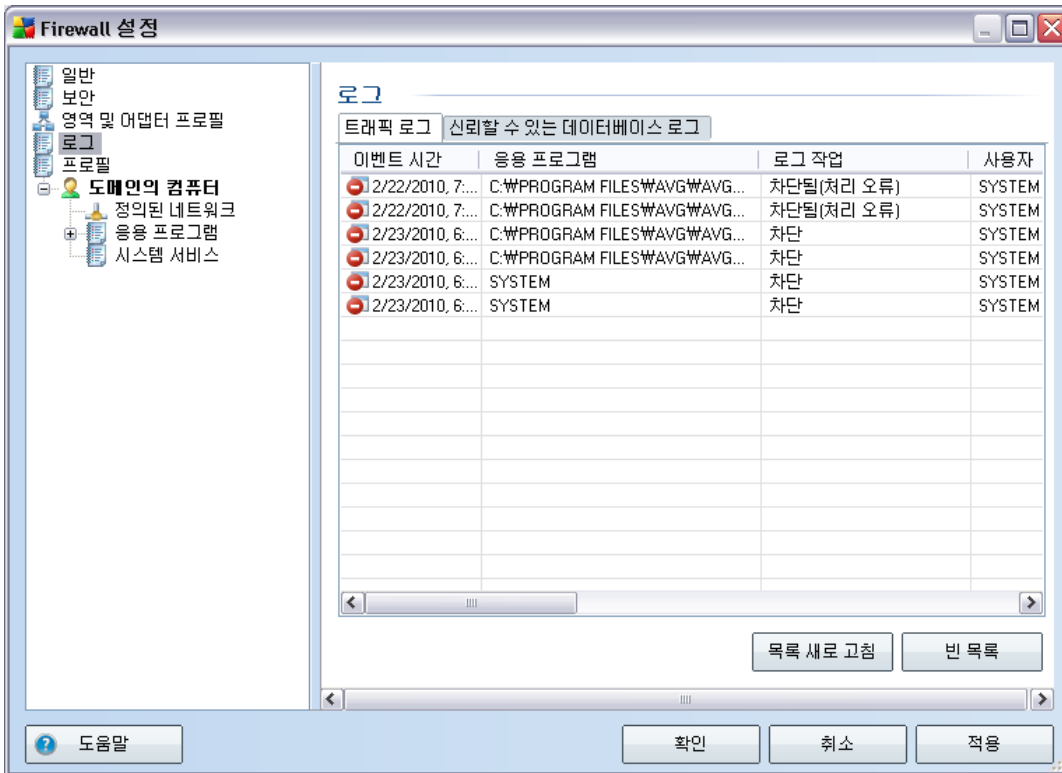
11.3. 영역 및 어댑터 프로필



어댑터 및 네트워크 영역 설정 대화 상자에서 정의된 프로필을 특정 어댑터 및 참조하는 해당 네트워크에 할당하는 작업과 관련된 설정을 편집할 수 있습니다 .

- **영역 검색 및 자동 프로필 전환 사용 안 함** - 정의된 프로필 중 하나를 각 네트워크 인터페이스 유형, 즉 각각의 영역에 할당할 수 있습니다 . 특정 프로필을 정의하지 않은 경우 [설치 프로세스](#) 중에 선택한 [컴퓨터 사용법](#) 및 [컴퓨터 네트워크 설계](#) 를 기준으로 정의되는 공통 프로필 하나가 사용됩니다 . 하지만 각 프로필을 구분하고 이를 특정 어댑터 및 영역에 할당하고 나중에 특별한 이유로 이러한 할당을 일시적으로 전환하려면 **영역 검색 및 자동 프로필 전환 사용 안 함** 옵션을 선택합니다 .
- **어댑터 , 영역 및 할당된 프로필 목록** - 이 목록에서 검색된 어댑터 및 영역에 대한 개요를 찾을 수 있습니다 . 그 각각에 대해 정의된 프로필 메뉴의 특정 프로필을 할당할 수 있습니다 . 이 메뉴를 열려면 어댑터 목록에서 해당 항목을 클릭하고 프로필을 선택합니다 .
- **고급 설정** - 해당 옵션을 선택하면 정보 메시지를 표시하는 기능이 비활성화됩니다 .

11.4. 로그



로그 대화 상자에서는 두 개의 탭을 통해 기록된 모든 **방화벽** 작업 및 이벤트 목록을 관련 매개 변수에 대한 자세한 설명 (이벤트 시간, 응용 프로그램 이름, 관련 로그 작업, 사용자 이름, PID, 트래픽 방향, 프로토콜 유형, 원격 및 로컬 포트 수 등)과 함께 검토할 수 있습니다 .

- **트래픽 로그** - 네트워크에 연결하려고 시도한 모든 응용 프로그램 활동에 대한 정보를 제공합니다 .
- **신뢰할 수 있는 데이터베이스 로그** - 신뢰할 수 있는 데이터베이스 는 온라인 커뮤니케이션이 항상 허용되는 인증되고 신뢰할 수 있는 응용 프로그램에 대해 AVG 내부에서 수집한 데이터베이스 정보입니다 . 새 응용 프로그램을 처음 네트워크에 연결하려고 할 때 (예: 해당 응용 프로그램에 대한 방화벽 규칙이 지정되지 않은 경우) 해당 응용 프로그램에 대한 네트워크 커뮤니케이션을 허용할지 여부를 판단해야 합니다 . AVG는 먼저 **신뢰할 수 있는 데이터베이스** 를 검색하여 응용 프로그램이 목록에 있으면 자동으로 네트워크 액세스 권한을 부여합니다 . 데이터베이스에서 응용 프로그램에 대한 정보를 사용할 수 없는 경우에만 응용 프로그램이 네트워크에 액세스하도록 허용할지 묻는 독립형 대화 상자를 표시

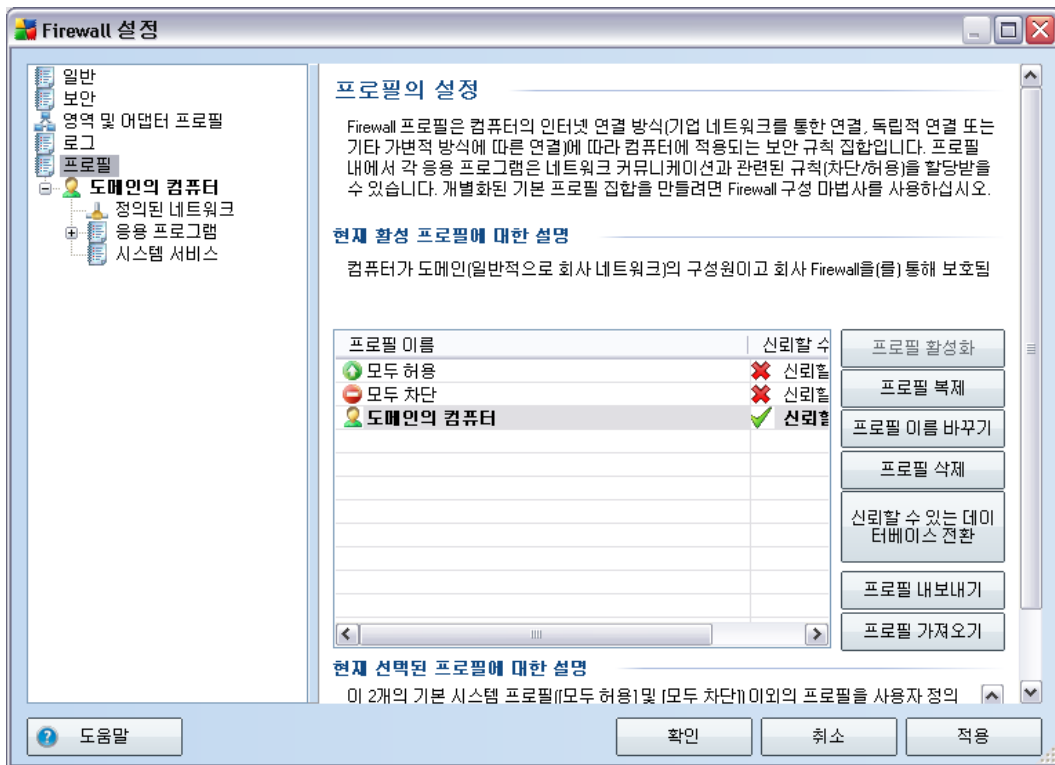
합니다 .

제어 단추

- **도움말** - 대화 상자와 관련된 도움말 파일을 엽니다 .
- **목록 새로 고침** - 해당 열 머리글을 클릭하면 기록된 모든 매개 변수가 선택된 특성에 따라, 발생 순서 (날짜) 또는 알파벳순으로 (기타 열) 정렬됩니다 . **목록 새로 고침** 단추를 사용하면 현재 표시된 정보를 업데이트할 수 있습니다 .
- **목록 비우기** - 차트의 모든 항목을 삭제합니다 .

11.5. 프로필

프로필 설정 대화 상자에는 사용 가능한 모든 프로필 목록이 포함되어 있습니다 .



시스템 **프로필** 이외의 모든 프로필은 다음 제어 단추를 사용하여 이 대화 상자에서 바로 편집할 수 있습니다 .

- **프로필 활성화** - 이 단추는 선택된 프로필을 활성 상태로 설정합니다 . **방화벽**에서는 선택된 프로필 구성을 사용하여 네트워크 트래픽을 제어합니다 .
- **프로필 복제** - 선택된 프로필의 동일한 사본을 만듭니다 . 나중에 이 사본을 편집하고 이름을 바꾸어 복제한 원본 프로필에 기반하는 새로운 프로필을 만들 수 있습니다 .
- **프로필 이름 바꾸기** - 선택된 프로필에 대해 새로운 이름을 정의할 수 있습니다 .
- **프로필 삭제** - 목록에서 선택된 프로필을 삭제합니다 .
- **신뢰할 수 있는 데이터베이스 전환** - 선택한 프로필에 대해 신뢰할 수 있는 데

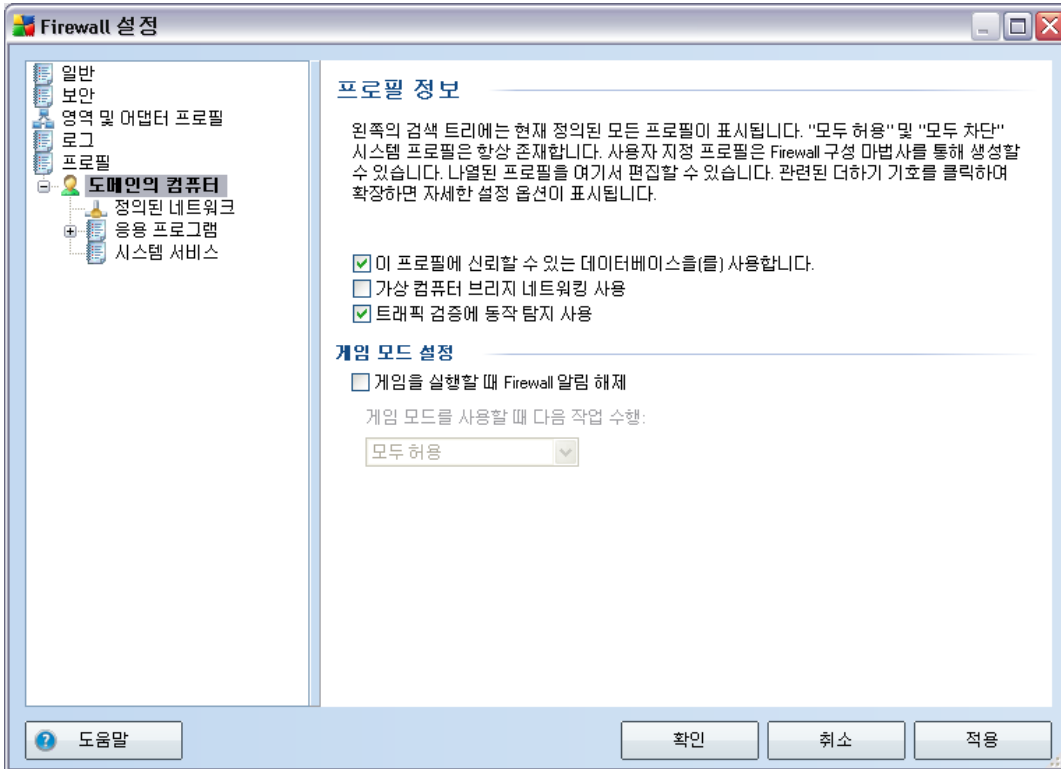
데이터베이스 정보를 사용할지 여부를 결정할 수 있습니다 . 신뢰할 수 있는 데이터베이스는 항상 온라인 커뮤니케이션이 가능한 신뢰할 수 있고 인증된 응용 프로그램에 대해 AVG 내부에서 수집한 데이터베이스 정보입니다 .

- **프로필 내보내기** - 선택된 프로필 구성을 나중에 사용할 수 있도록 파일에 기록하여 저장합니다 .
- **프로필 가져오기** - 백업 구성 파일에서 내보낸 데이터에 기반하여 선택된 프로필 설정을 구성합니다 .
- **도움말** - 대화 상자와 관련된 도움말 파일을 엽니다 .

이 대화 상자의 아래쪽 섹션에는 위 목록에서 선택된 프로필에 대한 설명이 표시됩니다 .

프로필 대화 상자 내의 목록에 나와 있는 정의된 프로필 수에 따라 왼쪽 탐색 메뉴 구조가 바뀝니다 . 각각의 정의된 프로필은 **프로필** 항목 아래에 특정 분기를 만듭니다 . 특정 프로필은 다음 대화 상자에서 편집할 수 있습니다 . 이 대화 상자는 모든 프로필에 대해 동일합니다 .

11.5.1. 프로필 정보



프로필 정보 대화 상자는 프로필의 특정 매개 변수를 가리키는 각각의 대화 상자에서 각 프로필의 구성을 편집할 수 있는 첫 번째 대화 상자입니다 .

- **이 프로필에 신뢰할 수 있는 데이터베이스를 사용합니다 .** (기본적으로 설정되어 있음) - 신뢰할 수 있는 데이터베이스 (즉, 온라인 커뮤니케이션이 가능한 신뢰할 수 있고 인증된 응용 프로그램에 대해 AVG 내부에서 수집한 데이터베이스 정보)를 활성화하려면 이 옵션을 선택합니다 . 해당 응용 프로그램에 대해 지정된 규칙이 아직 없다면 응용 프로그램이 네트워크에 액세스하도록 허용해야 하는지 여부를 판단해야 합니다 . AVG에서는 먼저 신뢰할 수 있는 데이터베이스를 검색하여 응용 프로그램이 목록에 있으면 안전한 것으로 판단하여 네트워크를 통한 커뮤니케이션을 허용합니다 . 목록에 없는 경우, 해당 프로필에 대해 네트워크를 통한 응용 프로그램의 커뮤니케이션 허용 여부를 결정하도록 사용자에게 요청합니다 .
- **가상 컴퓨터 브리지 네트워킹 사용** (기본적으로 해제되어 있음) - 이 항목을 선택하면 VMware의 가상 컴퓨터를 통해 네트워크에 바로 연결할 수 있습니다 .
- **트래픽 검증에 동작 검색 사용** - (기본적으로 설정되어 있음) - [방화벽](#)에서 응

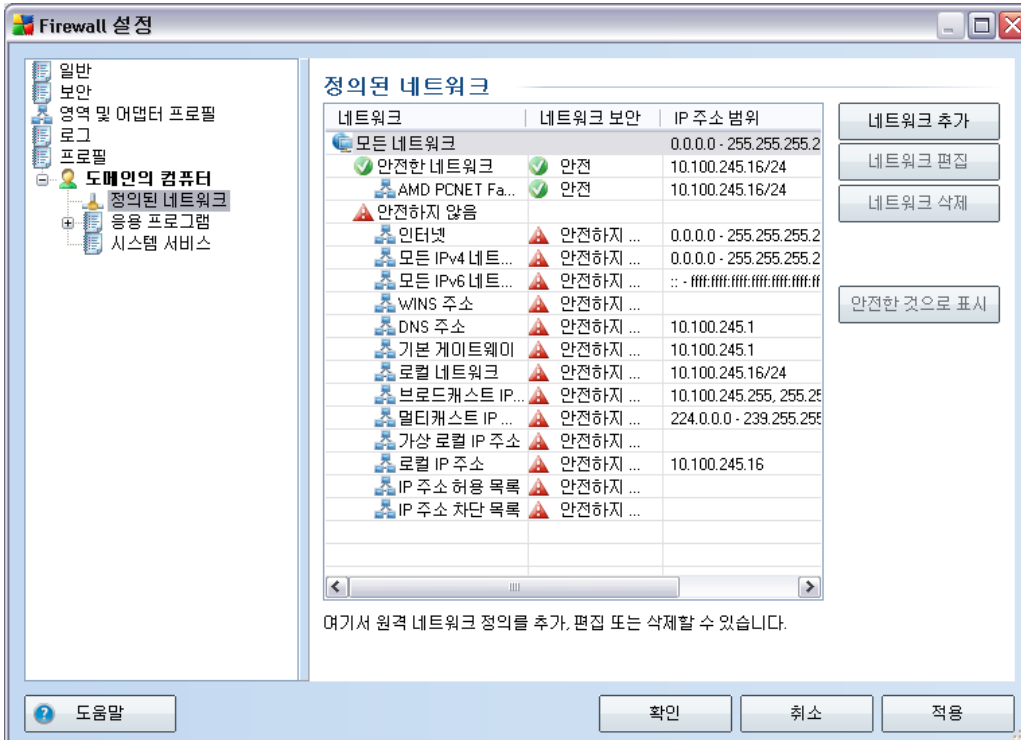
용 프로그램을 평가할 때 **Identity Protection** 기능을 사용하도록 허용하려면 이 옵션을 선택합니다 . **Identity Protection**은 응용 프로그램이 의심스러운 동작을 나타내는지 , 아니면 신뢰할 수 있으며 온라인 커뮤니케이션을 허용할 수 있는 응용 프로그램인지 여부를 알려 줄 수 있습니다 .

게임 모드 설정

게임 모드 설정 섹션에서 해당되는 항목을 선택하여 전체 화면 응용 프로그램이 컴퓨터에서 실행되고 있을 때 **방화벽** 정보 메시지가 표시되도록 할지 여부를 결정할 수 있습니다 . 이 설정은 **게임**과 **PPT 프레젠테이션** 등 전체 화면으로 실행되는 모든 응용 프로그램에 적용됩니다 . 정보 메시지가 방해가 될 수 있으므로 이 기능은 기본적으로 해제되어 있습니다 .

게임을 실행할 때 방화벽 알림 해제 항목을 선택한 경우에는 롤다운 메뉴에서 규칙이 지정되지 않은 새로운 응용 프로그램에서 네트워크를 통해 커뮤니케이션을 시도하는 경우에 수행할 동작을 선택할 수 있습니다 . 이러한 응용 프로그램은 **대개 확인 대화 상자를 표시하는 응용 프로그램** 으로 , 이러한 모든 응용 프로그램을 허용하거나 차단할 수 있습니다 .

11.5.2. 정의된 네트워크



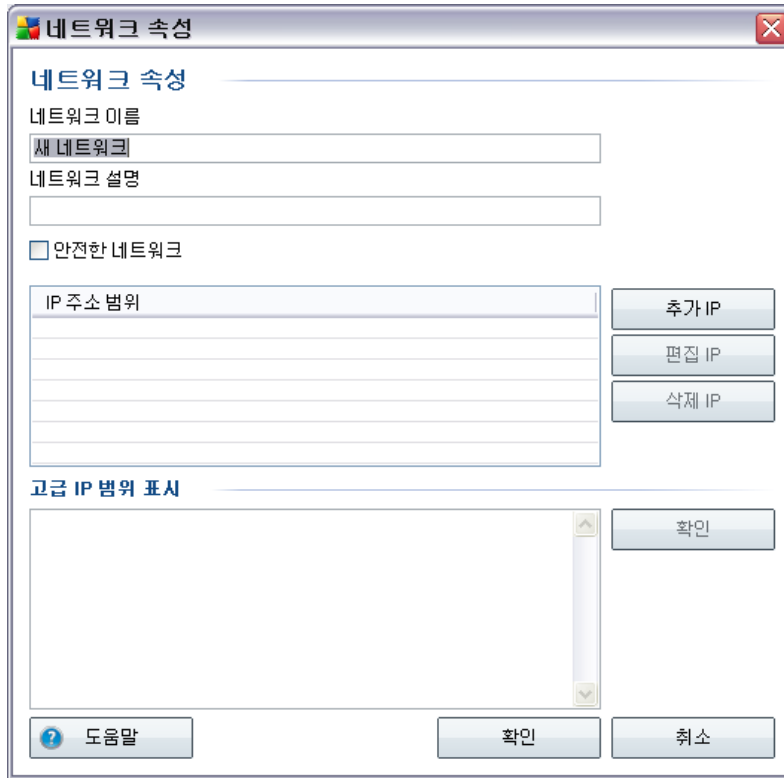
정의된 네트워크 대화 상자에는 사용자 컴퓨터가 연결된 모든 네트워크 목록이 제공됩니다. 발견된 모든 네트워크에 대해 다음 정보가 제공됩니다.

- **네트워크** - 해당 컴퓨터가 연결된 모든 네트워크의 이름을 나열합니다.
- **네트워크 보안** - 기본적으로 모든 네트워크는 안전하지 않은 것으로 간주되며 해당 네트워크가 안전하다고 확신하는 경우에만 이를 지정할 수 있습니다 (목록에서 개별 네트워크를 나타내는 항목을 클릭하고 상황에 맞는 메뉴에서 안전을 선택). 그러면 모든 안전한 네트워크가 응용 프로그램 규칙이 안전한 경우에만 허용으로 설정된 응용 프로그램과 커뮤니케이션할 수 있는 그룹에 포함됩니다.
- **IP 주소 범위** - 각 네트워크는 자동으로 발견되며 IP 주소 범위와 같은 형태로 지정됩니다.

제어 단추

- **네트워크 추가** - 새로 정의된 네트워크의 매개 변수를 편집할 수 있는 **네트워크**

크 속성 대화 상자 창을 엽니다 .



The image shows a Windows-style dialog box titled "네트워크 속성" (Network Properties). It contains several input fields and buttons. At the top, there's a section for "네트워크 이름" (Network Name) with a text box containing "새 네트워크" (New Network) and a "네트워크 설명" (Network Description) text box below it. A checkbox labeled "안전한 네트워크" (Secure Network) is present. Below this is a list box for "IP 주소 범위" (IP Address Range) with three empty rows. To the right of this list are three buttons: "추가 IP" (Add IP), "편집 IP" (Edit IP), and "삭제 IP" (Delete IP). Further down is a section titled "고급 IP 범위 표시" (Advanced IP Range Display) with a large empty text area and an "확인" (OK) button to its right. At the bottom of the dialog are three buttons: "도움말" (Help), "확인" (OK), and "취소" (Cancel).

이 대화 상자에서 **네트워크 이름** 을 지정하고 **네트워크 설명** 을 제공할 수 있으며 네트워크를 안전한 것으로 지정할 수도 있습니다 . **IP 추가** 단추 (또는 **IP 편집 / IP 삭제**)를 통해 독립 실행형 대화 상자에서 새 네트워크를 수동으로 정의할 수 있으며 , 이 대화 상자에서 IP 범위나 마스크를 제공하여 해당 네트워크를 지정할 수 있습니다 .

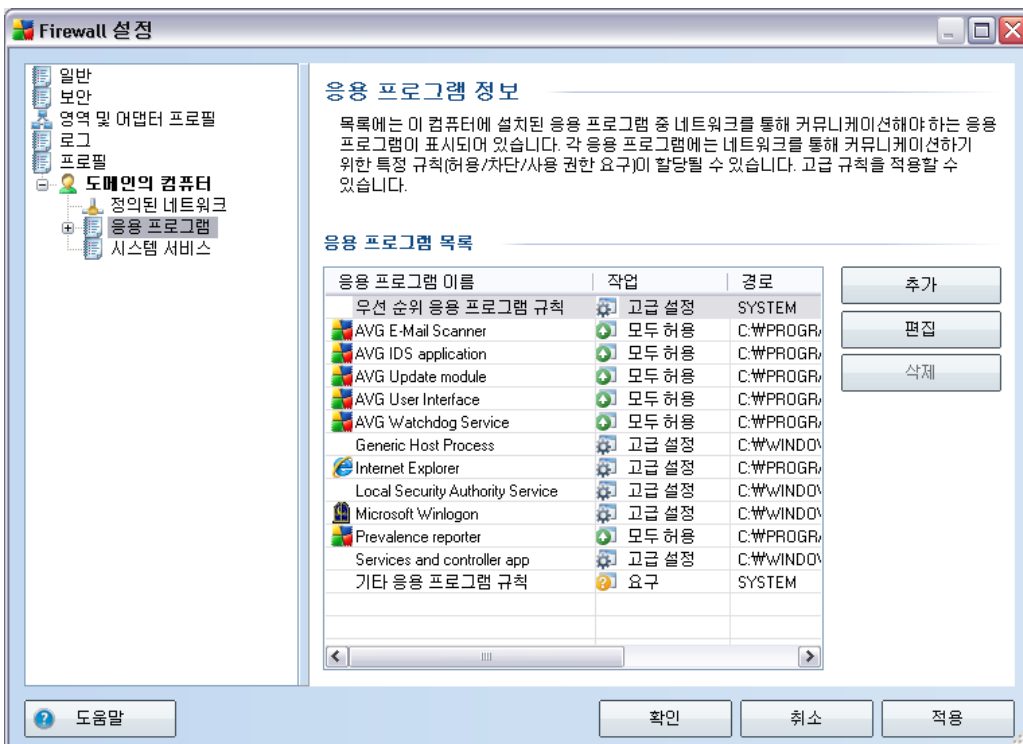
새로 생성된 네트워크의 일부로 다수의 네트워크를 정의해야 하는 경우 **고급 IP 범위 표시** 옵션을 사용할 수 있습니다 . 각 텍스트 필드에 모든 네트워크 목록을 입력하고 (*모든 표준 형식이 지원됨*) **확인** 단추를 눌러 해당 형식이 인식되도록 만듭니다 . 그런 다음 **확인** 을 눌러 확인하고 데이터를 저장합니다 .

- **네트워크 편집** - 이미 정의된 네트워크의 매개 변수를 편집할 수 있는 **네트워크 속성** 대화 상자 창을 엽니다 (위 내용 참조). 이 대화 상자는 새 네트워크 추가에 사용되는 대화 상자과 동일한 것이며 이전 단락에서 해당 설명을 참조하십시오 .
- **네트워크 삭제** - 선택한 네트워크에 대한 정보를 네트워크 목록에서 제거합니다

다.

- **안전한 것으로 표시** - 기본적으로 모든 네트워크는 안전하지 않은 것으로 간주되며 개별 네트워크가 안전하다고 확신하는 경우에만 이 단추를 사용하여 안전한 것으로 지정할 수 있습니다. 반대로, 네트워크가 안전한 것으로 지정되면 단추 텍스트가 "안전하지 않은 것으로 표시"로 변경됩니다.
- **도움말** - 대화 상자와 관련된 도움말 파일을 엽니다.

11.5.3. 응용 프로그램



응용 프로그램 정보 대화 상자에는 네트워크를 통해 커뮤니케이션해야 하는 모든 설치된 응용 프로그램 및 할당된 작업을 위한 아이콘이 나열됩니다.

-  모든 네트워크에 대한 커뮤니케이션 허용
-  안전한 것으로 정의된 네트워크만 커뮤니케이션 허용
-  커뮤니케이션 차단

-  요구 대화 상자 표시 (사용자는 해당 커뮤니케이션을 허용할지 또는 차단할지를 결정할 수 있습니다)
-  고급 설정이 정의됨

목록에 있는 응용 프로그램 (및 할당된 각 작업)이 **방화벽 구성 마법사**가 검색하는 동안 또는 그 이후에 (알 수 없거나 새로 설치된 응용 프로그램의 경우) 사용자 컴퓨터에서 발견되었습니다.

참고 : 이미 설치된 응용 프로그램만 검색할 수 있으므로 새 응용 프로그램을 나중에 설치한 경우 이에 대한 방화벽 규칙을 정의해야 합니다. 기본적으로, 새 응용 프로그램이 처음으로 네트워크를 통해 연결하려고 시도하면 Firewall이 신뢰할 수 있는 데이터베이스에 따라 규칙을 자동으로 만들거나 커뮤니케이션을 허용할지 아니면 차단할지를 사용자에게 묻습니다. 커뮤니케이션의 허용 여부에 대해서는 답을 영구 규칙으로 저장할 수 있습니다 (그러면 해당 규칙이 이 대화 상자에 나열됨).

물론 새 응용 프로그램에 대한 규칙을 즉시 정의할 수도 있습니다. 이 대화 상자에서 **추가**를 누르고 응용 프로그램 세부 정보를 입력합니다.

응용 프로그램과는 별개로 목록에는 두 가지 특수 항목이 포함되어 있습니다.

- **우선 순위 응용 프로그램 규칙** (목록의 맨 위에 있음)이 기본적으로 적용되고 다른 개별 응용 프로그램의 규칙보다 항상 우선적으로 적용됩니다.
- **기타 응용 프로그램 규칙** (목록의 아래쪽에 있음)은 특정 응용 프로그램 규칙이 적용되지 않을 경우 (예: 알려지지 않고 정의되지 않은 응용 프로그램) "마지막 인스턴스"로 사용됩니다.

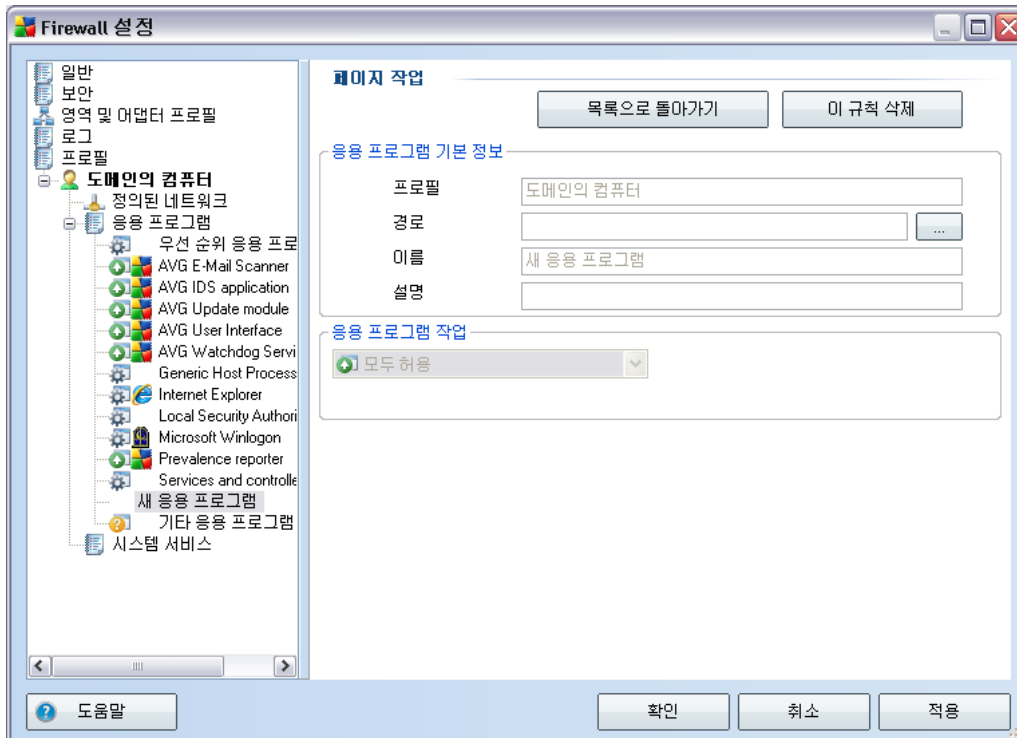
이러한 항목은 일반 응용 프로그램과는 다른 설정 옵션을 가지며 숙련된 사용자만 사용할 수 있습니다. 설정을 수정하지 않는 것이 좋습니다.

제어 단추

다음 제어 단추를 사용하여 목록을 편집할 수 있습니다.

- **추가** - 새 응용 프로그램 규칙을 정의하기 위한 빈 **페이지 작업** 대화 상자를 엽니다.
- **편집** - 기존 응용 프로그램 규칙 집합을 편집할 수 있도록 데이터가 제공된 상태로 같은 **페이지 작업** 대화 상자를 엽니다.
- **삭제** - 선택한 응용 프로그램을 목록에서 제거합니다.

- **도움말** - 대화 상자와 관련된 도움말 파일을 엽니다 .



이 대화 상자에서 각 응용 프로그램의 설정을 상세하게 정의할 수 있습니다 .

페이지 작업

- **목록으로 돌아가기** 단추를 선택하면 정의된 모든 응용 프로그램 규칙의 개요가 표시됩니다 .
- **이 규칙 삭제** 단추를 선택하면 현재 표시된 응용 프로그램 규칙이 삭제됩니다 . 이 작업은 취소할 수 없습니다 .

응용 프로그램 기본 정보

이 섹션에서 응용 프로그램의 **이름** 을 입력하고 원할 경우 **설명** (사용자 정보에 대한 간단한 설명) 을 입력합니다 . **경로** 필드에 디스크에서의 응용 프로그램 (실행 파일) 에 대

한 전체 경로를 입력합니다 . 또는 , "..." 단추를 누른 다음 트리 구조에서 편리하게 응용 프로그램을 찾을 수도 있습니다 .

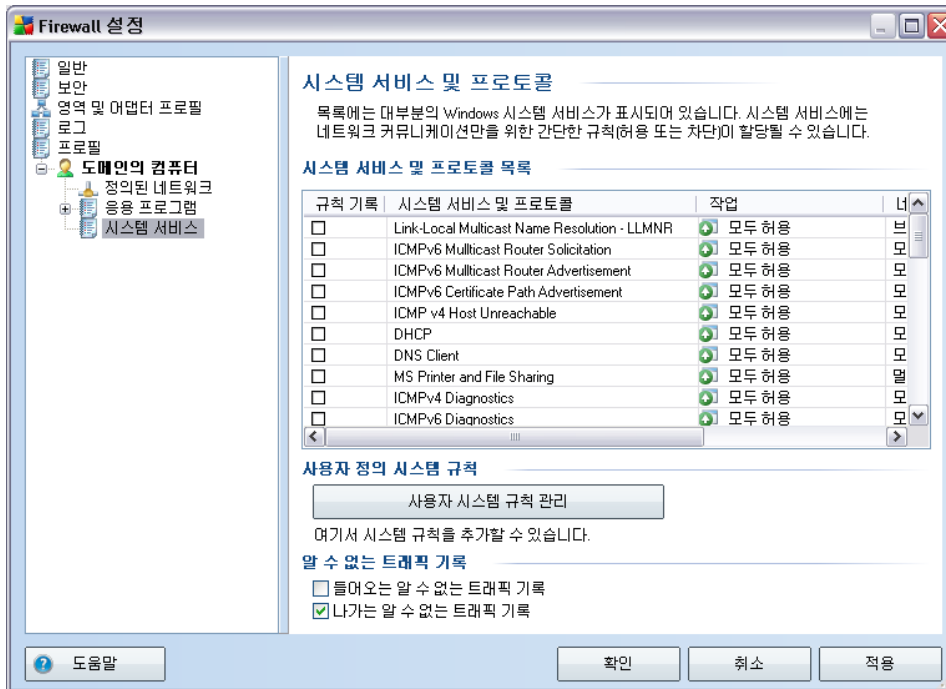
응용 프로그램 작업

드롭다운 메뉴에서 응용 프로그램의 방화벽 규칙을 선택할 수 있습니다 (즉, 응용 프로그램이 네트워크를 통해 커뮤니케이션할 때 사용할 방화벽)

-  **모두 허용** 은 응용 프로그램이 정의된 모든 네트워크 및 어댑터를 통해 제한 없이 커뮤니케이션하도록 허용합니다 .
-  **안전한 경우에만 허용** 은 응용 프로그램이 안전 (신뢰)하다고 정의된 네트워크를 통해서만 커뮤니케이션하도록 허용합니다 .
-  **차단** 은 커뮤니케이션을 자동으로 차단하여 응용 프로그램이 네트워크에 연결되지 못하도록 합니다 .
-  **요구** 는 해당 순간에 커뮤니케이션 시도를 허용 또는 차단할 것인지를 결정할 수 있는 대화 상자를 표시합니다 .
-  **고급 설정** 은 응용 프로그램 세부 규칙 **섹션의** 대화 상자 아래쪽에 광범위한 세부 설정 옵션을 표시합니다 . 세부 정보는 목록 순서대로 적용되므로 목록에서 규칙을 **위로 이동** 또는 **아래로 이동** 하여 우선 순위를 설정할 수 있습니다 . 목록에서 특정 규칙을 클릭하면 규칙 세부 정보에 대한 개요가 대화 상자의 아래쪽에 나타납니다 . 각 설정 대화 상자를 클릭하면 파란색 밑줄이 있는 값을 변경할 수 있습니다 . 강조 표시된 규칙을 삭제하려면 **제거** 를 누르면 됩니다 . 새 규칙을 정의하려면 **추가** 단추를 사용하여 필요한 모든 세부 정보를 지정할 수 있는 **규칙 세부 정보 변경** 대화 상자를 엽니다 .

11.5.4. 시스템 서비스

시스템 서비스 및 프로토콜 대화 상자의 편집 기능은 숙련된 사용자만 사용해야 합니다.



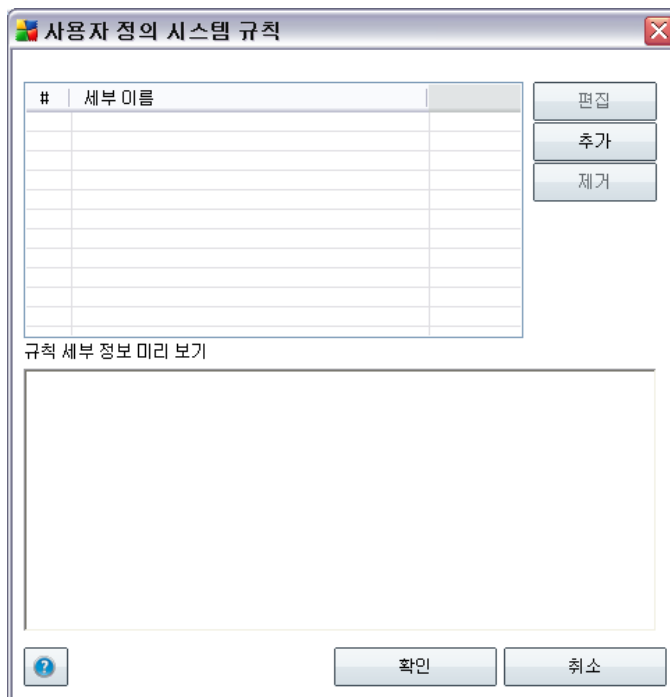
시스템 서비스 및 프로토콜 대화 상자에는 네트워크를 통한 커뮤니케이션을 필요로 하는 Windows 표준 시스템 서비스와 프로토콜의 목록이 표시됩니다. 차트에는 다음과 같은 열이 있습니다.

- **로그 규칙 작업** - 이 상자를 사용하면 규칙이 적용될 때마다 로그에 기록할 수 있습니다.
- **시스템 서비스 및 프로토콜** - 이 열에는 해당 시스템 서비스의 이름이 표시됩니다.
- **작업** - 이 열에는 할당된 작업을 위한 아이콘이 표시됩니다.
 - o  모든 네트워크에 대한 커뮤니케이션 허용
 - o  안전한 것으로 정의된 네트워크만 커뮤니케이션 허용
 - o  커뮤니케이션 차단

- **네트워크** - 이 열에는 시스템 규칙이 적용되는 특정 네트워크가 표시됩니다 .

목록 (*활당된 작업 포함*)은 다음 단추를 사용하여 편집할 수 있습니다 .

- 목록의 항목에 대한 설정 (*활당된 작업 포함*)을 편집하려면 항목을 마우스 오른쪽 단추로 클릭하고 **편집** 을 선택합니다 .
- 고유한 시스템 서비스 규칙을 정의할 수 있는 새 대화 상자를 열려면 (*아래 그림 참조*) **사용자 시스템 규칙 관리** 단추를 누릅니다 . **사용자 정의 시스템 규칙** 대화 상자의 맨 위에는 현재 편집된 시스템 규칙에 대한 모든 세부 정보가 간략히 설명되어 있으며 아래쪽에는 선택한 세부 정보가 표시됩니다 . 각 단추를 눌러 사용자 정의 규칙 세부 정보를 편집, 추가 또는 삭제할 수 있습니다 . 제조업체에서 정의한 규칙 세부 정보는 편집만 가능합니다 .



세부 규칙 설정은 고급 설정으로 , 주로 방화벽 구성을 완전하게 제어할 필요가 있는 네트워크 관리자를 위한 것입니다 . 통신 프로토콜 종류, 네트워크 포트 번호, IP 주소 정의 등에 대해 잘 모르면 이러한 설정을 수정하지 마십시오 ! 구성을 변경해야 하는 경우 개별 대화 상자의 도움말 파일에서 자세한 정보를 참조하십시오 .

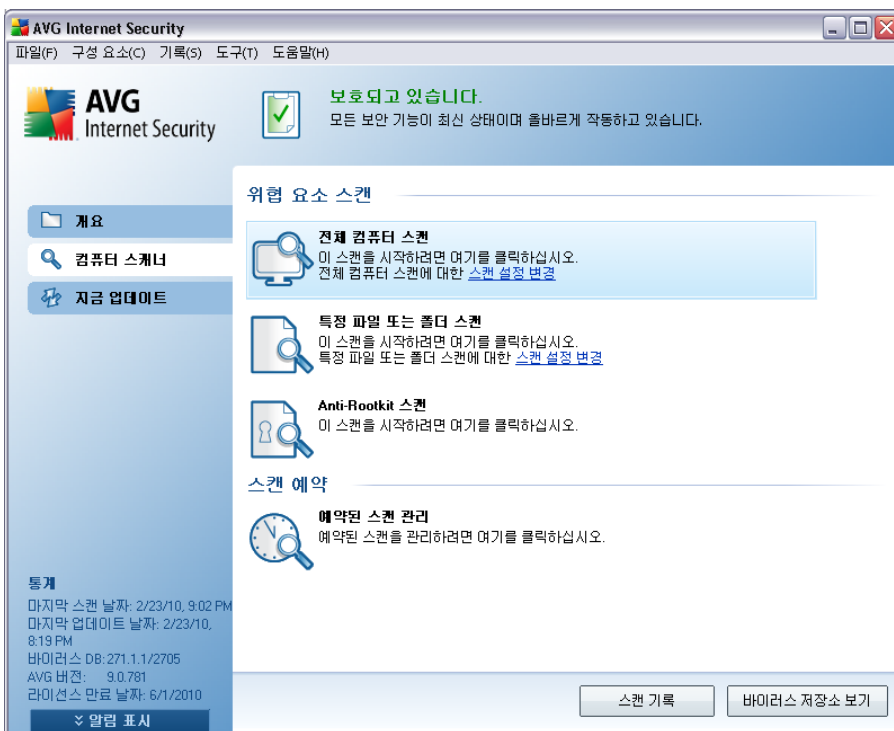
알 수 없는 트래픽 기록

- **들어오는 알 수 없는 트래픽 기록** – 외부에서 컴퓨터에 연결하려는 알 수 없는 시도가 있을 때마다 로그에 기록하려면 상자를 선택합니다 .
- **나가는 알 수 없는 트래픽 기록** – 컴퓨터에서 외부 위치에 연결하려는 알 수 없는 시도가 있을 때마다 로그에 기록하려면 상자를 선택합니다 .

12. AVG 스캔

스캔은 **AVG 9 Internet Security** 기능에서 중요한 부분입니다 . 요청 시 테스트를 실행하거나 원하는 시간에 주기적으로 테스트를 실행하도록 예약 할 수 있습니다 .

12.1. 스캔 인터페이스



AVG 스캔 인터페이스는 **컴퓨터 스캐너 빠른 링크**를 통해 액세스할 수 있습니다 . 이 링크를 클릭하여 **위험 요소 스캔** 대화 상자로 전환합니다 . 이 대화 상자에서는 다음 섹션을 찾을 수 있습니다 .

- 미리 정의된 스캔 개요 - 필요할 때 즉시 또는 예약된 시기에 사용할 수 있는 세 가지 유형의 스캔 (소프트웨어 공급업체가 정의함)이 준비되어 있습니다 .
 - 전체 컴퓨터 스캔
 - 특정 파일 또는 폴더 스캔
 - Anti-Rootkit 스캔
- 스캔 일정 섹션 - 필요한 경우 새 테스트를 정의하고 새 일정을 만들 수 있습니다

다.

제어 단추

테스트 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다 .

- **스캔 기록** - 전체 스캔 기록을 보여 주는 [스캔 결과 개요](#) 대화 상자를 표시합니다 .
- **바이러스 저장소 보기** - 발견된 감염 파일이 격리되는 장소인 [바이러스 저장소](#)를 보여 주는 새로운 창을 엽니다 .

12.2. 미리 정의된 스캔

AVG 9 Internet Security의 주요 기능 중 하나는 요청 시 스캔 기능입니다 . 요청 시 테스트는 바이러스 감염이 의심될 때마다 컴퓨터의 여러 부분을 스캔합니다 . 그러나 바이러스가 컴퓨터에서 발견되지 않을 것으로 생각되는 경우에도 정기적으로 테스트를 수행해야 합니다 .

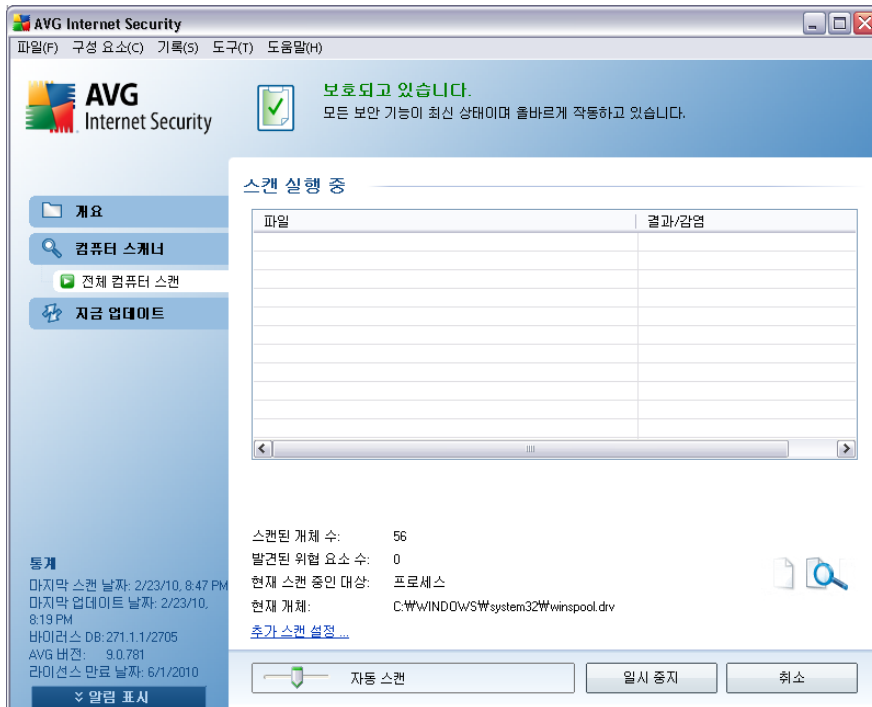
AVG 9 Internet Security에서는 소프트웨어 공급업체에 의해 미리 정의된 두 가지 스캔 유형이 제공됩니다 .

12.2.1. 전체 컴퓨터 스캔

전체 컴퓨터 스캔 - 전체 컴퓨터에서 발생 가능한 감염 및/또는 원치 않는 프로그램을 스캔합니다 . 이 테스트는 컴퓨터의 모든 하드 드라이브를 스캔하고 발견된 모든 바이러스를 검색하여 치료하거나 발견된 감염을 [바이러스 저장소](#)로 이동합니다 . 워크스테이션에서 최소한 매주 한 번씩은 전체 컴퓨터 스캔을 예약해야 합니다 ..

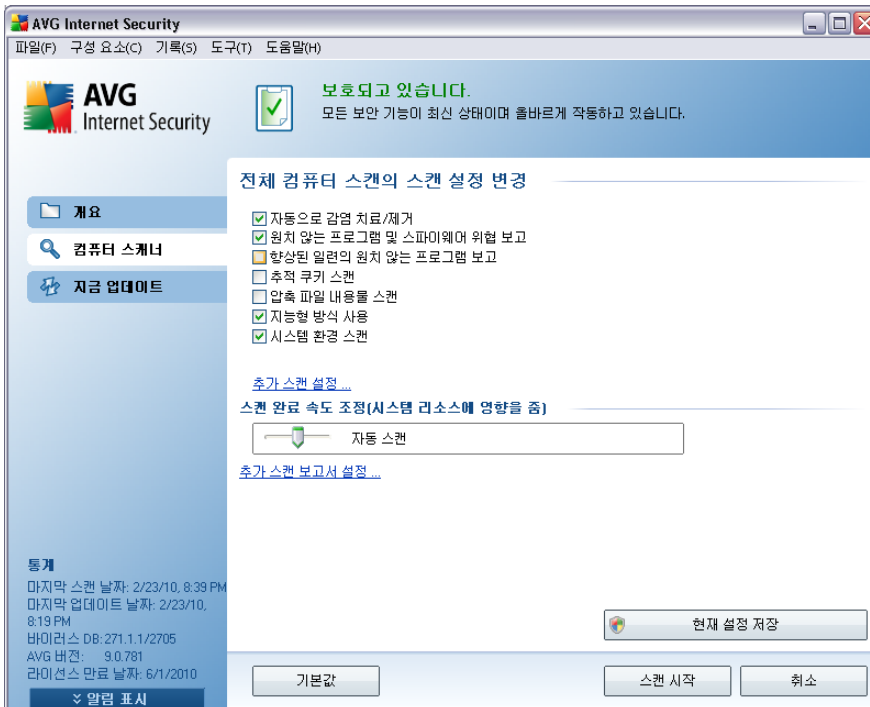
스캔 시작

전체 컴퓨터 스캔은 스캔 아이콘을 클릭하여 [스캔 인터페이스](#)에서 직접 시작할 수 있습니다 . 이 유형의 스캔에 대해 더 이상 특정 설정을 구성할 필요가 없으면 **스캔 실행 중** 대화 상자 ([스크린샷 참조](#))에서 즉시 스캔이 시작됩니다 . 필요한 경우 스캔을 일시적으로 중단 (**일시 중지**)하거나 취소 (**중지**)할 수 있습니다 .



스캔 구성 편집

미리 정의된 **전체 컴퓨터 스캔**의 기본 설정을 편집하는 옵션이 있습니다. **스캔 설정 변경** 링크를 눌러 **전체 컴퓨터 스캔의 스캔 설정 변경** 대화 상자로 이동합니다. **기본 설정을 반드시 변경해야 하는 경우가 아니라면 해당 설정을 그대로 유지하는 것이 좋습니다.**



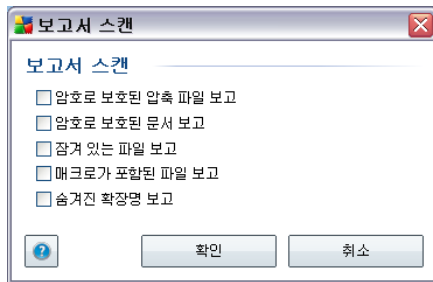
- **스캔 매개 변수** - 스캔 매개 변수 목록에서 필요한 특정 매개 변수를 설정 / 해제할 수 있습니다 . 기본적으로 대부분의 매개 변수가 설정되어 있으며 스캔하는 동안 자동으로 사용됩니다 .
- **추가 스캔 설정** - 이 링크는 다음 매개 변수를 지정할 수 있는 새 **추가 스캔 설정** 대화 상자를 엽니다 .



- **컴퓨터 종료 옵션** - 실행 중인 스캔 프로세스가 종료된 후 자동으로 컴퓨터를 종료할지 여부를 결정합니다 . **스캔 완료 시 컴퓨터 종료** 옵션을 선택하면 컴퓨터가 현재 잠겨 있는 경우에도 종료 (**컴퓨터가 잠긴 경우 강제 종료**) 할 수 있는 새로운 옵션이 활성화됩니다 .
- **스캔할 파일 형식 정의** - 스캔할 항목을 더 자세히 정의할 수 있습니다 .
 - **모든 파일 형식** - 스캔하지 않아야 할 파일의 확장명을 심표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다 .
 - **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔 (일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며 , 이때 미디어 파일 (비디오 , 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여 지정할 수 있습니다 . 이 경우 항상 스캔해야 하는 파일의 확장명을 지정할 수 있습니다 .
 - 선택적으로 **확장명이 없는 파일을 스캔**하도록 정할 수 있습니다 . 이 옵션은 기본적으로 설정되어 있으며 반드시 변경해야 할 경우가 아니라면 이 설정을 유지하는 것이 좋습니다 . 확장명이 없는 파일은 의심스러운 경우가 많기 때문에 항상 스캔해야 합니다 .
- **스캔 프로세스 우선 순위** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다 . 기본적으로 우선 순위는 스캔 프로세스 속도 및 시스템 리소스 사용량을 최적화하는 중간 수준 (**자동 스캔**)으로 설정됩니다 . 또는, 스캔 프로세스를 더 느리게 실행하여 시스템 리소스 부하를 최소화하거나 (**컴퓨터로**

작업해야 할 경우 스캔 소요 시간이 크게 중요하지 않을 때 유용함), 시스템 리소스 요구량이 증가하더라도 스캔 속도를 빠르게 실행하여 합니다 (예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우).

- **추가 스캔 보고서 설정** - 이 링크를 클릭하면 새로운 **보고서 스캔** 대화 상자가 열리므로 가능한 검색 결과 유형 중 보고를 받으려는 유형을 선택할 수 있습니다.



경고 : 이 스캔 설정은 [AVG 스캔 / 스캔 일정 / 스캔 방법](#) 장에 설명된, 새로 정의한 스캔의 매개 변수와 같습니다. **전체 컴퓨터 스캔**의 기본 구성을 변경하기로 결정한 경우 새 설정을 기본 구성으로 저장하여 이후에 전체 컴퓨터를 스캔하는 데 사용할 수 있습니다.

12.2.2. 특정 파일 또는 폴더 스캔

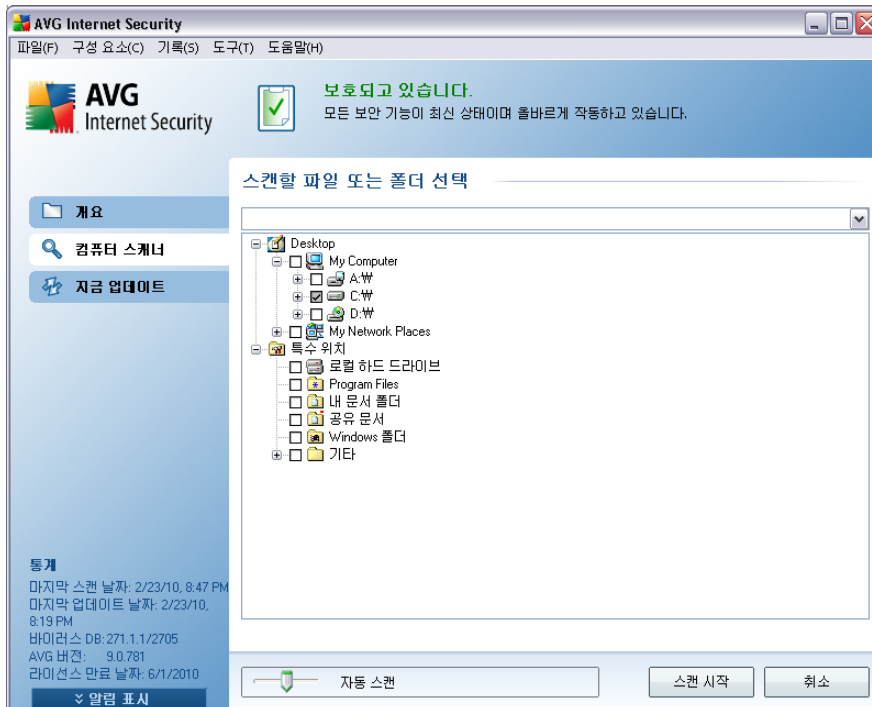
특정 파일 또는 폴더 스캔 - 사용자가 스캔하려고 선택한 컴퓨터 영역 (선택한 폴더, 하드 디스크, 플로피 디스크, CD). 바이러스를 검색하고 이를 처리하는 경우의 스캔 과정은 전체 컴퓨터 스캔과 같습니다. 발견된 바이러스는 모두 치료되거나 [바이러스 저장소](#)로 이동합니다. 특정 파일 또는 폴더 스캔은 사용자 필요에 따라 고유의 테스트 및 해당 일정을 설정하는 데 사용할 수 있습니다.

스캔 시작

특정 파일 또는 폴더 스캔은 스캔 아이콘을 클릭하여 [스캔 인터페이스](#)에서 직접 시작할 수 있습니다. **스캔할 파일 또는 폴더 선택**이라는 새 대화 상자가 열립니다. 컴퓨터의 트리 구조에서 스캔하려는 폴더를 선택합니다. 선택한 각 폴더의 경로는 자동으로 생성되어 이 대화 상자 위쪽에 있는 텍스트 상자에 나타납니다.

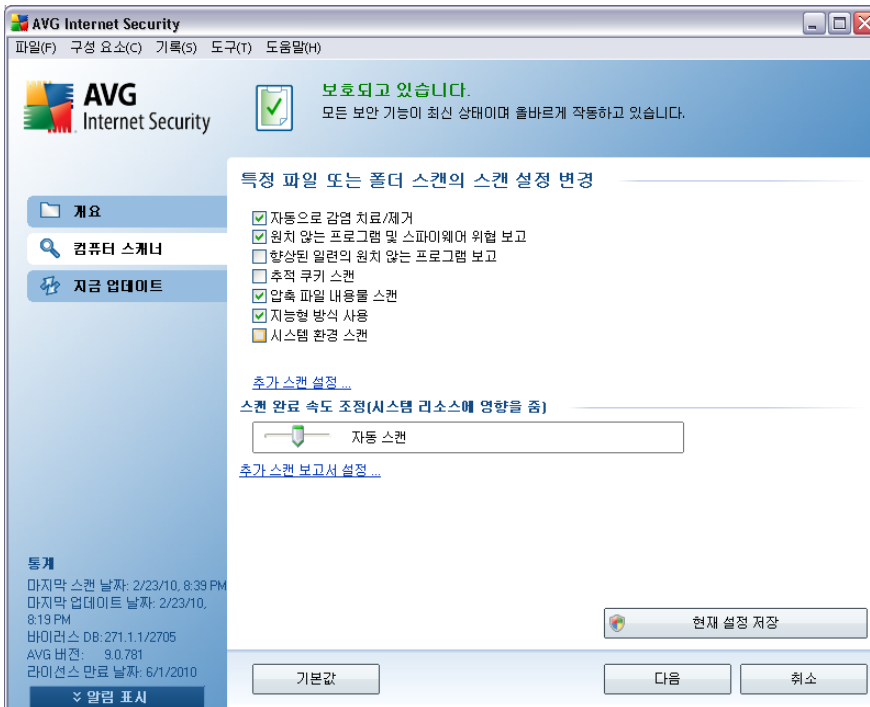
하위 폴더를 제외하고 특정 폴더를 스캔할 수도 있습니다. 그렇게 하려면 자동으로 생성된 경로 앞에 빼기 기호 "-"를 입력합니다 (스크린샷 참조). 스캔에서 전체 폴더를 제외하려면 "!" 매개 변수를 사용합니다.

마지막으로, 스캔을 시작하려면 **스캔 시작** 단추를 누릅니다. 스캔 프로세스 자체는 기본적으로 [전체 컴퓨터 스캔](#)과 같습니다.



스캔 구성 편집

미리 정의된 **특정 파일 또는 폴더 스캔**의 기본 설정을 편집하는 옵션이 있습니다. **스캔 설정 변경** 링크를 눌러 **특정 파일 또는 폴더 스캔의 스캔 설정 변경** 대화 상자로 이동합니다. **기본 설정을 반드시 변경해야 하는 경우가 아니라면 해당 설정을 그대로 유지하는 것이 좋습니다.**



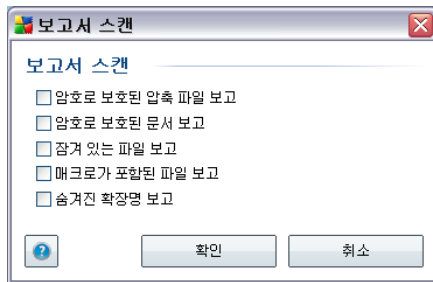
- **매개 변수 스캔** - 필요한 경우 스캔할 매개 변수 목록에서 특정 매개 변수를 설정 / 해제할 수 있습니다 . 이 설정에 대한 자세한 설명은 [AVG 고급 설정/스캔/특정 파일 또는 폴더 스캔](#)을 참조하십시오 .
- **추가 스캔 설정** - 이 링크는 다음 매개 변수를 지정할 수 있는 새 추가 스캔 설정 대화 상자를 엽니다 .



- **컴퓨터 종료 옵션** - 실행 중인 스캔 프로세스가 종료된 후 자동으로 컴퓨터를 종료할지 여부를 결정합니다 . **스캔 완료 시 컴퓨터 종료** 옵션을 선택하면 컴퓨터가 현재 잠겨 있는 경우에도 종료 (**컴퓨터가 잠긴 경우 강제 종료**) 할 수 있는 새로운 옵션이 활성화됩니다 .
- **스캔할 파일 형식 정의** - 스캔할 항목을 더 자세히 정의할 수 있습니다 .
 - **모든 파일 형식** - 스캔하지 않아야 할 파일의 확장명을 심표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다 .
 - **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔 (일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며 , 이때 미디어 파일 (비디오 , 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여 지정할 수 있습니다 . 이 경우 항상 스캔해야 하는 파일의 확장명을 지정할 수 있습니다 .
 - 선택적으로 **확장명이 없는 파일을 스캔** 하도록 정할 수 있습니다 . 이 옵션은 기본적으로 설정되어 있으며 반드시 변경해야 할 경우가 아니라면 이 설정을 유지하는 것이 좋습니다 . 확장명이 없는 파일은 의심스러운 경우가 많기 때문에 항상 스캔해야 합니다 .
- **스캔 프로세스 우선 순위** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다 . 기본적으로 우선 순위는 스캔 프로세스 속도 및 시스템 리소스 사용량을 최적화하는 중간 수준 (**자동 스캔**)으로 설정됩니다 . 또는, 스캔 프로세스를 더 느리게 실행하여 시스템 리소스 부하를 최소화하거나 (**컴퓨터로**

작업해야 할 경우 스캔 소요 시간이 크게 중요하지 않을 때 유용함), 시스템 리소스 요구량이 증가하더라도 스캔 속도를 빠르게 실행하여 합니다 (예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우).

- **추가 스캔 보고서 설정** - 이 링크를 클릭하면 새로운 **보고서 스캔** 대화 상자가 열리므로 가능한 검색 결과 유형 중 보고를 받으려는 유형을 선택할 수 있습니다.



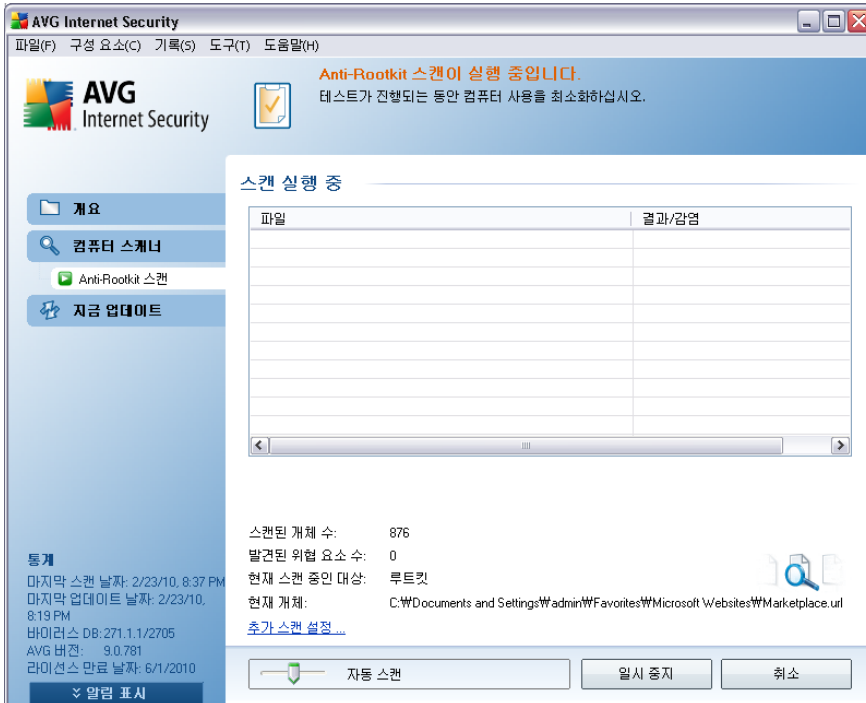
경고 : 이 스캔 설정은 [AVG 스캔 / 스캔 일정 / 스캔 방법](#) 장에 설명된, 새로 정의한 스캔의 매개 변수와 같습니다. **특정 파일 또는 폴더 스캔**의 기본 구성을 변경하기로 한 경우 새 설정을 기본 구성으로 저장하여 이후에 특정 파일 또는 폴더를 스캔하는 데 사용할 수 있습니다. 또한 이 구성을 새로 예약된 모든 스캔의 템플릿으로 사용할 수도 있습니다. 모든 사용자 지정 스캔은 특정 파일 또는 폴더 스캔의 현재 구성을 기준으로 실행됩니다.

12.2.3. Anti-Rootkit 스캔

Anti-Rootkit 스캔은 컴퓨터에서 가능한 루트킷 (컴퓨터에서 맬웨어와 같은 활동을 할 수 있는 프로그램 및 기술)을 검색합니다. 따라서 루트킷이 검색되었다고 해서 컴퓨터가 감염되었다고 단정할 수는 없습니다. 경우에 따라 특정 드라이버나 정상적인 응용 프로그램 부분이 루트킷으로 잘못 검색될 수 있습니다.

스캔 시작

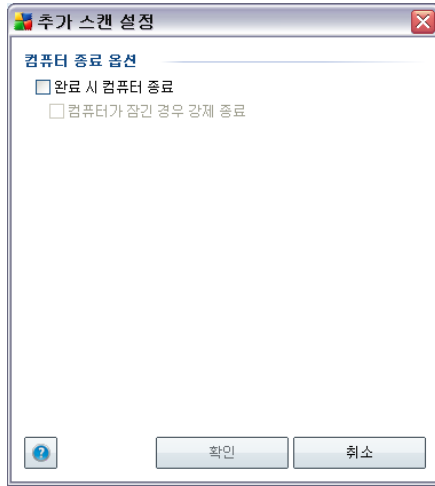
Anti-Rootkit 스캔은 스캔 아이콘을 클릭하여 [스캔 인터페이스](#)에서 직접 시작할 수 있습니다. 이 유형의 스캔에 대해 더 이상 특정 설정을 구성할 필요가 없으면 **스캔 실행 중** 대화 상자 (스크린샷 참조)에서 즉시 스캔이 시작됩니다. 필요한 경우 스캔을 일시적으로 중단 (**일시 중지**)하거나 취소 (**중지**)할 수 있습니다.



스캔 구성 편집

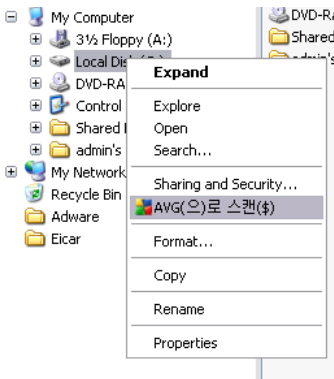
Anti-Rootkit 스캔은 기본적으로 항상 시작되도록 설정되어 있으며 [AVG 고급 설정 / Anti-Rootkit](#) 대화 상자에서만 스캔 매개 변수를 편집할 수 있습니다. [스캔 인터페이스](#)에서는 다음 구성을 사용할 수 있습니다.

- **자동 스캔** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 우선 순위는 스캔 프로세스 속도 및 시스템 리소스 사용량을 최적화하는 중간 수준 (**자동 스캔**)으로 설정됩니다. 또는, 스캔 프로세스를 더 느리게 실행하여 시스템 리소스 부하를 최소화하거나 (**컴퓨터로 작업해야 할 경우 스캔 소요 시간이 크게 중요하지 않을 때 유용함**), 시스템 리소스 요구량이 증가하더라도 스캔 속도를 빠르게 실행하여 합니다 (예: **컴퓨터 일시적으로 무인 모드로 작동하는 경우**).
- **추가 스캔 설정** - 이 링크는 새로운 **추가 스캔 설정** 대화 상자를 엽니다. 이 대화 상자에서 **Anti-Rootkit 스캔**과 관련하여 사용할 수 있는 컴퓨터 종료 조건을 정의할 수 있습니다 (**완료 시 컴퓨터 종료**, 예를 들어 **컴퓨터가 잠긴 경우 강제 종료**).



12.3. Windows 탐색기에서 스캔

전체 컴퓨터 또는 선택한 영역에 대해 미리 정의된 스캔을 시작하는 옵션 외에도 **AVG 9 Internet Security** 제품은 Windows 탐색기 환경에서 직접 특정 개체에 대한 빠른 스캔 옵션을 제공합니다. 알려지지 않은 파일을 열 때 그 내용을 확신할 수 없는 경우 필요하다면 이 옵션을 선택할 수 있습니다. 다음 단계를 수행하십시오.



- Windows 탐색기에서 검사하려는 파일 (또는 폴더)을 강조 표시합니다.
- 개체를 마우스 오른쪽 단추로 클릭하여 상황에 맞는 메뉴를 엽니다.
- **AVG로 스캔** 옵션을 선택하여 파일이 AVG로 스캔되도록 합니다.

12.4. 명령줄 스캔

AVG 9 Internet Security에는 명령줄에서 스캔을 실행하는 옵션이 있습니다. 이 옵션은 서버에서 사용하거나 컴퓨터가 부팅된 후 자동으로 시작되는 일괄 스크립트를 생성할 때 사용할 수 있습니다. 명령줄에서 대부분의 매개 변수를 AVG 그래픽 사용자 인터페이스에 제공되는 것과 같이 사용하여 스캔을 시작할 수 있습니다.

명령줄에서 AVG 스캔을 시작하려면 AVG가 설치된 폴더 내에서 다음 명령을 실행합니다.

- **avgscanx**(32비트 OS의 경우)
- **avgscana**(64비트 OS의 경우)

명령 구문

명령 구문은 다음과 같습니다.

- **avgscanx /parameter ...** 예: **avgscanx /comp**(전체 컴퓨터를 스캔하는 경우)
- **avgscanx /parameter /parameter ..** 여러 매개 변수를 사용하는 경우 한 줄에 입력해야 하며 공백 및 슬래시 문자로 구분해야 합니다.
- 매개 변수에 특정 값을 지정해야 하는 경우 (예: 컴퓨터에서 스캔할 영역에 대한 정보를 제공해야 하는 **/scan** 매개 변수에는 선택한 섹션에 대한 정확한 경로를 지정해야 함) 값을 세미콜론으로 구분합니다 (예: **avgscanx /scan=C:\;D:**).

스캔 매개 변수

사용 가능한 매개 변수에 대한 전체 개요를 표시하려면 매개 변수 **/?** 또는 **/HELP**(예: **avgscanx /?**). 스캔할 컴퓨터 영역을 지정하는 **/SCAN**만 필수 매개 변수입니다. 옵션에 대한 자세한 설명은 [명령줄 매개 변수 개요](#)를 참조하십시오.

스캔을 실행하려면 **Enter** 키를 누르십시오. 스캔하는 동안 **Ctrl+C** 또는 **Ctrl+Pause**를 눌러 프로세스를 중지할 수 있습니다.

그래픽 인터페이스에서 시작되는 CMD 스캔

Windows 안전 모드에서 컴퓨터를 실행하는 경우 그래픽 사용자 인터페이스에서 명령

줄 스캔을 시작할 수도 있습니다 . 스캔 자체가 명령줄에서 시작되며 **명령줄 작성기** 대화 상자를 통해 사용이 간편한 그래픽 인터페이스에서 대부분의 스캔 매개 변수를 지정할 수 있습니다 .

이 대화 상자는 Windows 안전 모드에서만 액세스할 수 있으므로 이 대화 상자에 대한 자세한 설명은 대화 상자에서 직접 열 수 있는 도움말 파일을 참조하십시오 .

12.4.1. CMD 스캔 매개 변수

다음은 명령줄 스캔에 사용할 수 있는 모든 매개 변수의 목록입니다 .

- **/SCAN** [특정 파일 또는 폴더 스캔](#) /SCAN=path;path(예 : /SCAN=C:\;D:\)
- **/COMP** [전체 컴퓨터 스캔](#)
- **/HEUR** [지능형 분석 사용](#)
- **/EXCLUDE** 스캔에서 경로 또는 파일 제외
- **/@** 명령 파일 /file name/
- **/EXT** 다음 확장명 검색 /예 : EXT=EXE,DLL/
- **/NOEXT** 다음 확장명 검색 안 함 /예 : NOEXT=JPG/
- **/ARC** 압축 파일 스캔
- **/CLEAN** 자동 치료
- **/TRASH** 감염된 파일을 [바이러스 저장소로 이동](#)
- **/QT** 빠른 테스트
- **/MACROW** 매크로 보고
- **/PWDW** 암호로 보호된 파일 보고
- **/IGNLOCKED** 잠긴 파일 무시
- **/REPORT** 파일 /file name/(으)로 보고
- **/REPAPPEND** 보고서 파일에 첨부
- **/REPOK** 감염되지 않은 파일을 정상으로 보고

- **/NOBREAK** Ctrl-Break 사용 중지 허용 안 함
- **/BOOT** MBR/BOOT 검사 사용
- **/PROC** 활성 프로세스 스캔
- **/PUP** "[원치 않는 프로그램](#)" 보고
- **/REG** 레지스트리 스캔
- **/COO** 쿠키 스캔
- **/?** 이 항목에 대한 도움말 표시
- **/HELP** 이 항목에 대한 도움말 표시
- **/PRIORITY** 스캔 우선 순위를 /낮음, 자동, 높음 /으로 설정 ([고급 설정 / 스캔](#) 참조)
- **/SHUTDOWN** 스캔 완료 후 컴퓨터 종료
- **/FORCESHUTDOWN** 스캔 완료 후 컴퓨터 자동 종료
- **/ADS** 대체 데이터 스트림 스캔 (NTFS 전용)

12.5. 스캔 일정

AVG 9 Internet Security 제품을 사용하면 필요할 때(예: 컴퓨터가 감염된 것으로 의심되는 경우) 스캔을 실행하거나 예약된 계획에 따라 스캔을 실행할 수 있습니다. 일정에 따라 스캔을 실행하는 것이 좋습니다. 이 방법을 사용하면 일체의 감염 가능성으로부터 컴퓨터를 보호할 수 있으며 스캔 시작 여부 및 시기에 대해 걱정할 필요가 없습니다.

최소한 매주 한 번은 [전체 컴퓨터 스캔](#)을 시작해야 합니다. 하지만 가능하다면 스캔 일정 기본 구성의 설정에 따라 매일 전체 컴퓨터의 스캔을 시작하십시오. 컴퓨터가 "항상 켜져 있는 경우"에는 업무 시간이 아닌 시간에 스캔이 발생하도록 예약할 수 있습니다. .. 컴퓨터를 가끔씩 끄는 경우에는 [스캔 작업 기회를 놓쳤을 때 컴퓨터 시작 시](#) 스캔이 발생하도록 예약하십시오.

새 스캔 일정을 만들려면 [AVG 스캔 인터페이스](#)에서 아래쪽에 있는 **스캔 예약** 섹션을 찾습니다.



스캔 예약

스캔 예약 섹션에 있는 그래픽 아이콘을 클릭하면 현재 예약된 모든 스캔 목록을 볼 수 있는 새 **스캔 예약** 대화 상자가 열립니다 .

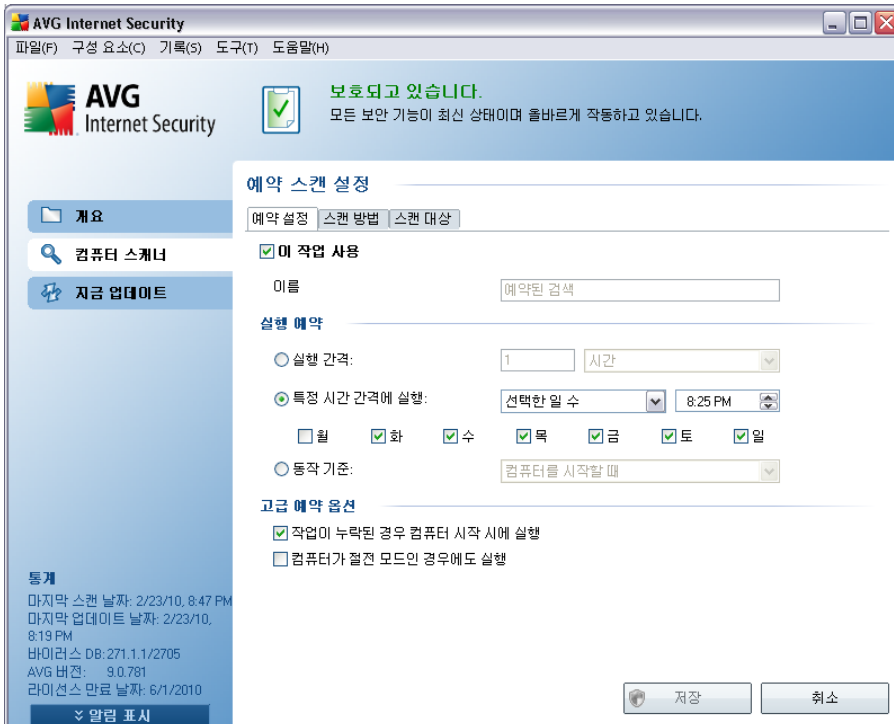


다음 제어 단추를 사용하여 스캔을 편집 / 추가할 수 있습니다 .

- **스캔 일정 추가** - 이 단추를 누르면 **예약 스캔 설정** 대화 상자 및 [예약 설정](#) 탭이 열립니다 . 이 대화 상자에서 새로 정의한 테스트의 매개 변수를 지정할 수 있습니다 .
- **스캔 일정 편집** - 이 단추는 예약된 테스트 목록에서 기존 테스트를 미리 선택한 경우에만 사용할 수 있습니다 . 이 경우 단추가 활성화 상태로 표시됩니다 . 단추를 클릭하면 **예약 스캔 설정** 대화 상자 및 [예약 설정](#) 탭으로 전환할 수 있습니다 . 선택된 테스트의 매개 변수는 여기에 이미 지정되어 있으므로 편집할 수 있습니다 .
- **스캔 일정 삭제** - 이 단추 역시 예약된 테스트 목록에서 기존 테스트를 미리 선택한 경우에만 활성화됩니다 . 이 경우 제어 단추를 눌러 목록에서 해당 테스트를 삭제할 수 있습니다 . 하지만 사용자는 자신의 테스트만 삭제할 수 있으며 기본 설정에서 미리 정의된 **전체 컴퓨터 스캔 일정**은 삭제할 수 없습니다 .
- **뒤로** - [AVG 스캔 인터페이스로 돌아갑니다](#) .

12.5.1. 예약 설정

새로운 테스트를 예약하고 정기적으로 실행하려면 **예약된 테스트 설정** 대화 상자를 엽니다 (**스캔 예약** 대화 상자에서 **스캔 일정 추가** 단추 클릭). 대화 상자는 **예약 설정** (아래 그림 참조), **스캔 방법** 및 **스캔 대상** 탭으로 구성됩니다. 기본 탭인 예약 설정 탭으로 자동 리디렉션됩니다.



예약 설정 탭에서 먼저 **이 작업 사용** 항목을 선택하거나 선택 취소하여 예약된 테스트를 일시적으로 비활성화하고 필요한 경우에 이를 다시 활성화할 수 있습니다.

그런 다음, 생성 및 예약하려는 스캔에 이름을 지정합니다. **이름** 항목 옆의 텍스트 필드에 이름을 입력합니다. 스캔에 간략하고 설명적인 이름을 사용하여 나중에 해당 스캔을 쉽게 구분할 수 있도록 해야 합니다.

예를 들어 스캔이 실제로 검사하는 대상이 무엇인지 알 수 없는 "새로운 스캔" 또는 "내 스캔" 등의 이름을 붙이는 것은 적절하지 않습니다. 반면, "시스템 영역 스캔" 같은 이름은 설명이 포함된 적절한 이름이라고 할 수 있습니다. 또한 스캔의 이름에 해당 스캔이 전체 컴퓨터 스캔인지, 선택한 파일 스캔인지 아니면 폴더 스캔인지를 지정할 필요는 없습니다. 사용자 자신의 스캔은 언제나 **선택한 파일 또는 폴더 스캔**의 특정한 버전이 됩니다.

이 대화 상자에서 다음과 같은 스캔 매개 변수를 상세하게 정의할 수 있습니다 .

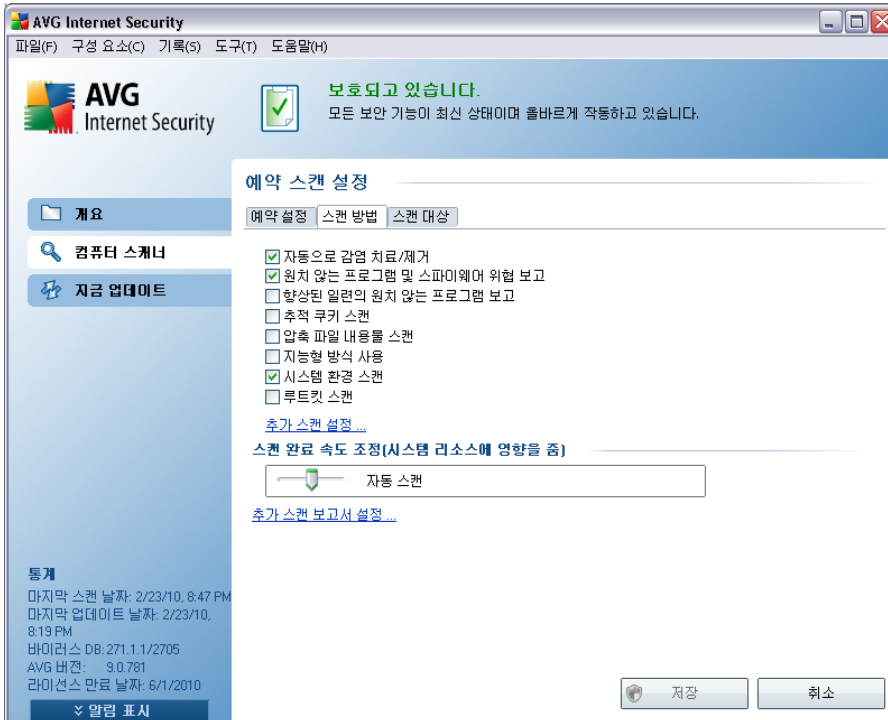
- **실행 예약** - 새로 예약된 스캔이 실행되는 주기를 지정합니다 . 특정 시간이 지나면 (**실행 간격 ...**) 스캔 실행이 반복되도록 정의하거나 정확한 날짜 및 시간을 정의 (**특정 시간 간격에 실행 ...**)하여 스캔이 실행되도록 할 수 있습니다 . 아니면 스캔이 특정 이벤트 (**동작 기준 : 컴퓨터를 시작할 때**)와 연관되어 실행되도록 지정할 수도 있습니다 .
- **고급 예약 옵션** - 이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 스캔이 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다 .

예약 스캔 설정 대화 상자의 제어 단추

예약 스캔 설정 대화 상자에 있는 **예약 설정** , [스캔 방법](#) 및 [스캔 대상](#) 의 세 가지 탭에는 사용 가능한 제어 단추가 두 개 있으며 , 이들 단추는 현재 사용하는 탭과 상관없이 다음과 같은 동일한 기능을 수행합니다 .

- **저장** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 저장하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 . 따라서 , 모든 탭에서 테스트 매개 변수를 구성하려면 모든 요구 사항을 지정한 후에 이 단추를 눌러 매개 변수를 저장합니다 .
- **취소** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 취소하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 .

12.5.2. 스캔 방법



스캔 방법 탭에는 선택적으로 설정하거나 해제할 수 있는 스캔 매개 변수의 목록이 있습니다. 기본적으로 대부분의 매개 변수가 설정되어 있으며 스캔하는 동안 해당 기능이 적용됩니다. 이러한 설정을 반드시 변경해야 하는 경우가 아니라면 다음과 같이 미리 정의된 구성을 그대로 유지하는 것이 좋습니다.

- **자동으로 감염 치료 / 제거** - (기본적으로 설정되어 있음): 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없거나 이 옵션을 해제하기로 선택한 경우에는 바이러스 검색에 대한 알림을 받게 되며 발견된 감염의 처리 방법을 결정해야 합니다. 이 경우 감염된 파일을 [바이러스 저장소](#)로 이동하는 것이 좋습니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고** (기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스파이웨어는 의심되는 맬웨어 범주로, 대개 보안 위험을 나타내지만 이들 프로그램의 일부는 의도적으로 설치될 수 있습니다.](#) 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다.
- **항상된 일련의 원치 않는 프로그램 보고** - 이전 옵션이 활성화되어 있는 경우 [스파이웨어](#)의 확장 패키지를 검색하려면 이 상자를 선택합니다. 스파이웨어 프

로그래밍은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 잘못 사용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.

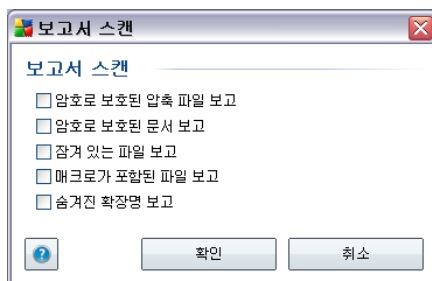
- **추적 쿠키 스캔** - (기본적으로 설정되어 있음): [Anti-Spyware](#) 구성 요소의 이 매개 변수는 스캔 중에 쿠키가 검색되도록 정의합니다. HTTP 쿠키는 사이트 기본 설정이나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.
- **압축 파일 내용물 스캔** - (기본적으로 설정되어 있음): 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일 형식으로 묶여 있는 파일을 포함하여 모든 파일을 검사하도록 정의합니다.
- **지능형 방식 사용** - (기본적으로 설정되어 있음): 지능형 분석 (가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- **시스템 환경 스캔** - (기본적으로 설정되어 있음): 또한 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- **루트킷 스캔** - 루트킷 검색을 전체 컴퓨터 스캔에 포함하려면 이 항목을 선택합니다. 또한 루트킷 검색은 [Anti-Rootkit](#) 구성 요소 내에서 단독으로 사용될 수도 있습니다.

이제 다음과 같이 스캔 구성을 변경할 수 있습니다.

- **추가 스캔 설정** - 이 링크는 다음 매개 변수를 지정할 수 있는 새 **추가 스캔 설정** 대화 상자를 엽니다.



- **컴퓨터 종료 옵션** - 실행 중인 스캔 프로세스가 종료된 후 자동으로 컴퓨터를 종료할지 여부를 결정합니다. **스캔 완료 시 컴퓨터 종료** 옵션을 선택하면 컴퓨터가 현재 잠겨 있는 경우에도 종료 (**컴퓨터가 잠긴 경우 강제 종료**)할 수 있는 새로운 옵션이 활성화됩니다.
- **스캔할 파일 형식 정의** - 스캔할 항목을 더 자세히 정의할 수 있습니다.
 - **모든 파일 형식** - 스캔하지 않아야 할 파일의 확장명을 쉼표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.
 - **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔 (일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며, 이때 미디어 파일 (비디오, 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여 지정할 수 있습니다. 이 경우 항상 스캔해야 하는 파일의 확장명을 지정할 수 있습니다.
 - 선택적으로 **확장명이 없는 파일을 스캔**하도록 정할 수 있습니다. 이 옵션은 기본적으로 설정되어 있으며 반드시 변경해야 할 경우가 아니라면 이 설정을 유지하는 것이 좋습니다. 확장명이 없는 파일은 의심스러운 경우가 많기 때문에 항상 스캔해야 합니다.
- **스캔 프로세스 우선 순위** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 우선 순위는 스캔 프로세스 속도 및 시스템 리소스 사용량을 최적화하는 중간 수준 (자동 스캔)으로 설정됩니다. 또는, 스캔 프로세스를 더 느리게 실행하여 시스템 리소스 부하를 최소화하거나 (컴퓨터로 작업해야 할 경우 스캔 소요 시간이 크게 중요하지 않을 때 유용함), 시스템 리소스 요구량이 증가하더라도 스캔 속도를 빠르게 실행하여 합니다 (예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우).
- **추가 스캔 보고서 설정** - 이 링크를 클릭하면 새로운 **보고서 스캔** 대화 상자가 열리므로 가능한 검색 결과 유형 중 보고를 받으려는 유형을 선택할 수 있습니다.



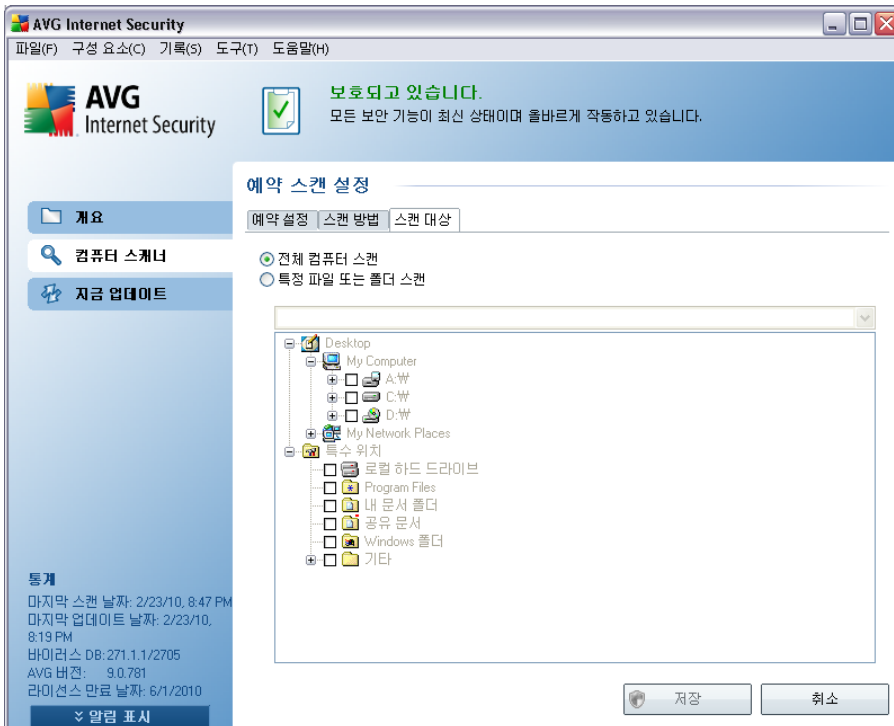
참고 : 기본적으로 스캔 구성은 최적의 성능을 얻을 수 있도록 설정되어 있습니다 . 이러한 스캔 설정을 반드시 변경해야 하는 경우가 아니라면 미리 정의된 구성을 그대로 유지하는 것이 좋습니다 . 모든 구성 변경은 숙련된 사용자가 수행해야 합니다 . 추가적인 스캔 구성 옵션에 대한 자세한 내용은 [고급 설정](#) 대화 상자를 참조하십시오 . 이 대화 상자는 **파일 / 고급 설정** 시스템 메뉴 항목을 통해 액세스할 수 있습니다 .

제어 단추

예약 스캔 설정 대화 상자에 있는 [예약 설정](#), [스캔 방법](#) 및 [스캔 대상](#) 의 세 가지 탭에는 사용 가능한 제어 단추가 두 개 있으며 , 이들 단추는 현재 사용하는 탭과 상관없이 다음과 같은 동일한 기능을 수행합니다 .

- **저장** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 저장하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 . 따라서 , 모든 탭에서 테스트 매개 변수를 구성하려면 모든 요구 사항을 지정한 후에 이 단추를 눌러 매개 변수를 저장합니다 .
- **취소** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 취소하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 .

12.5.3. 스캔 대상



스캔 대상 탭에서 전체 컴퓨터 스캔을 예약할지 아니면 특정 파일 또는 폴더 스캔을 예약할지 여부를 정의할 수 있습니다 .

특정 파일 또는 폴더의 스캔을 선택하는 경우 이 대화 상자의 아래쪽에 표시된 트리 구조가 활성화되고 스캔할 폴더를 선택할 수 있습니다 . 스캔할 폴더를 찾을 때까지 더하기 노드를 클릭하여 항목을 확장합니다 . 해당 상자를 선택하여 여러 폴더를 선택할 수 있습니다 . 선택한 폴더는 대화 상자 위쪽의 텍스트 필드에 나타나며 나중에 사용할 수 있도록 드롭다운 메뉴에는 선택한 스캔 기록이 유지됩니다 . 또는 원하는 폴더의 전체 경로를 직접 입력할 수 있습니다 . 여러 경로를 입력하려면 공백 없이 세미콜론으로 구분해야 합니다 .

트리 구조 내에서 **특수 위치** 라는 분기를 표시할 수도 있습니다 . 해당 확인란을 선택하면 스캔되는 위치의 목록은 다음과 같습니다 .

- **로컬 하드 드라이브** - 컴퓨터의 모든 하드 드라이브
- **프로그램 파일** - C:\Program Files\
- **내 문서 폴더** - C:\Documents and Settings\User\My Documents\

- **공유 문서** - C:\Documents and Settings\All Users\Documents\
- **Windows 폴더** - C:\Windows\
- **기타**
 - o **시스템 드라이브** - 운영 체제가 설치된 하드 드라이브 (일반적으로 C:)
 - o **시스템 폴더** - Windows/System32
 - o **임시 파일 폴더** - Documents and Settings/User/Local Settings/Temp
 - o **임시 인터넷 파일** - Documents and Settings/User/Local Settings/Temporary Internet Files

예약 스캔 설정 대화 상자의 제어 단추

예약 스캔 설정 대화 상자에 있는 [예약 설정](#), [스캔 방법](#) 및 [스캔 대상](#) 의 세 가지 탭에는 사용 가능한 제어 단추가 두 개 있으며, 이들 단추는 현재 사용하는 탭과 상관없이 다음과 같은 동일한 기능을 수행합니다 .

- **저장** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 저장하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 . 따라서, 모든 탭에서 테스트 매개 변수를 구성하려면 모든 요구 사항을 지정한 후에 이 단추를 눌러 매개 변수를 저장합니다 .
- **취소** - 이 탭 또는 이 대화 상자의 다른 탭에 대해 수행한 모든 변경 내용을 취소하고 [AVG 스캔 인터페이스 기본 대화 상자](#) 로 돌아갑니다 .

12.6. 스캔 결과 개요



스캔 결과 개요 대화 상자는 [AVG 스캔 인터페이스](#)에서 **스캔 기록** 단추를 통해 액세스할 수 있습니다. 이 대화 상자는 이전에 시작한 모든 스캔 목록 및 그 결과 정보를 제공합니다.

- **이름** - 스캔 지정. [미리 정의된 스캔](#) 중 하나의 이름 또는 사용자가 [예약된 스캔](#)에 지정한 이름이 될 수 있습니다. 각 이름에는 스캔 결과를 나타내는 아이콘이 표시됩니다.

 녹색 아이콘은 스캔 중 발견된 감염이 없음을 나타냅니다.

 파란색 아이콘은 스캔 중 발견된 감염이 있지만 감염된 개체가 자동으로 제거되었음을 나타냅니다.

 빨간색 아이콘은 스캔 중 발견된 감염이 있지만 이를 제거할 수 없음을 나타냅니다!

각 아이콘은 완전한 모양이거나 중간이 잘린 모양일 수 있습니다. 완전

한 모양의 아이콘은 스캔이 제대로 완료되어 종료되었음을 뜻하며, 중간이 잘린 아이콘은 스캔이 취소되었거나 중단되었음을 뜻합니다.

참고 : 각 스캔에 대한 자세한 정보는 이 대화 상자의 아래쪽 부분에 있는 **세부 정보 보기** 단추를 통해 액세스할 수 있는 [스캔 결과](#) 대화 상자를 참조하십시오.

- **시작 시간** - 스캔이 시작된 날짜 및 시간
- **종료 시간** - 스캔이 끝난 날짜 및 시간
- **테스트된 개체** - 스캔 중 검사된 개체의 수
- **감염** - 검색 / 제거된 [바이러스 감염](#)의 수
- **스파이웨어** - 검색 / 제거된 [스파이웨어](#)의 수
- **경고** - 발견된 개체 중 [의심스러운 개체의 개수](#)
- **루트킷** - 발견된 개체 중 [루트킷](#)
- **스캔 로그 정보** - 스캔 과정 및 결과와 관련된 정보 (일반적으로 스캔 완료 또는 중단에 관한 정보)

제어 단추

스캔 결과 개요 대화 상자의 제어 단추는 다음과 같습니다.

- **세부 정보 보기** - [스캔 결과](#) 대화 상자로 전환하여 선택된 스캔에 대한 세부 데이터를 보려면 누릅니다.
- **결과 삭제** - 스캔 결과 개요에서 선택된 항목을 제거하려면 누릅니다.
- **뒤로** - [AVG 스캔 인터페이스의 기본 대화 상자로 돌아갑니다](#).

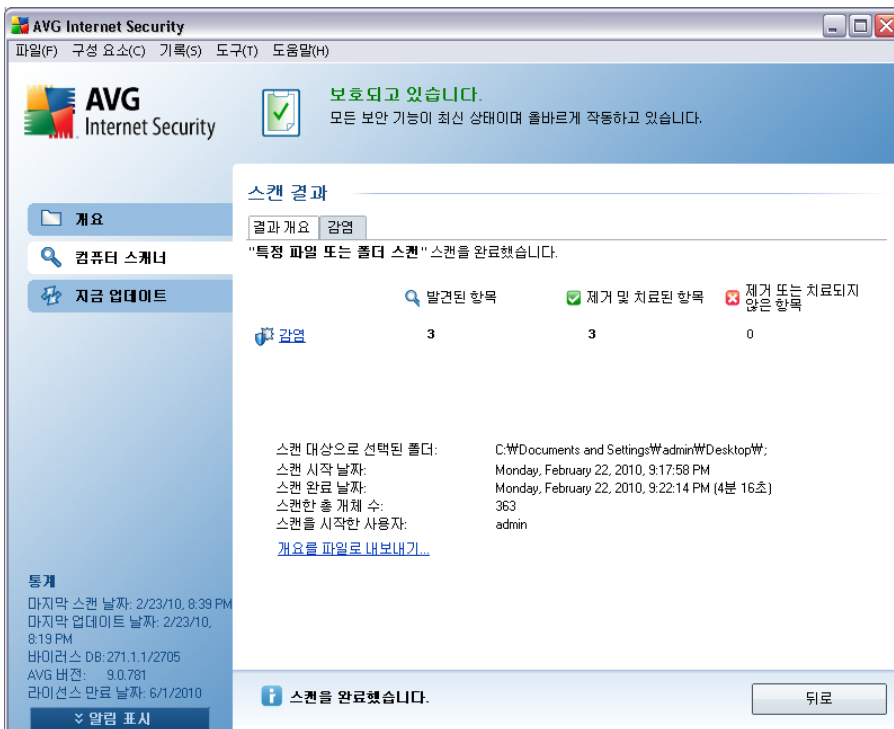
12.7. 스캔 결과 세부 정보

[스캔 결과 개요](#) 대화 상자에서 특정 스캔을 선택하면 **세부 정보 보기** 단추를 클릭하여 선택한 스캔 과정 및 결과에 대한 자세한 데이터를 제공해 주는 **스캔 결과** 대화 상자로 전환할 수 있습니다.

대화 상자는 다음 몇 가지 탭으로 나뉩니다.

- **결과 개요** - 이 탭은 항상 표시되며 스캔 진행을 설명하는 통계 데이터를 제공합니다 .
- **감염** - 이 탭은 스캔 중에 **바이러스 감염**이 발견된 경우에만 표시됩니다 .
- **스파이웨어** - 이 탭은 스캔 중에 **스파이웨어**가 발견된 경우에만 표시됩니다 .
- **경고** - 이 탭은 스캔 중에 쿠키가 검색되는 등의 경우에 표시됩니다 .
- **루트킷** - 이 탭은 스캔 중에 **루트킷**이 발견된 경우에만 표시됩니다 .
- **정보** - 이 탭은 일부 잠재적인 위협 요소를 검색했지만 위의 범주 중 어떤 분류에도 속하지 않는 경우에 표시되며 , 결과에 대한 경고 메시지가 나타납니다 . 또한 스캔할 수 없는 개체 (예: 암호로 보호된 압축 파일)에 대한 정보를 여기서 찾을 수 있습니다 .

12.7.1. 결과 개요 탭



스캔 결과 탭에서는 다음에 대한 자세한 정보 통계를 확인할 수 있습니다 .

- 발견된 **바이러스 감염** / **스파이웨어**

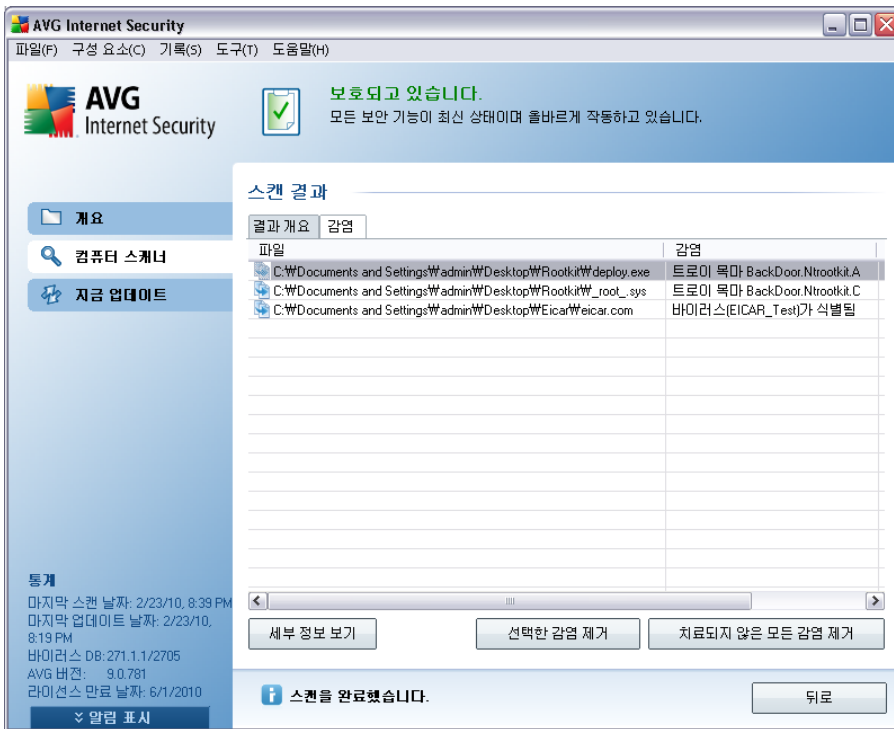
- 제거된 [바이러스 감염 / 스파이웨어](#)
- 제거하거나 치료할 수 없는 [바이러스 감염 / 스파이웨어](#) 의 수

또한 스캔이 시작된 날짜 및 정확한 시간, 스캔된 개체의 총 개수, 스캔 기간 및 스캔 중에 발생한 오류 수에 대한 정보도 찾을 수 있습니다 .

제어 단추

이 대화 상자에서는 하나의 제어 단추만 사용할 수 있습니다 . **결과 닫기** 단추를 누르면 [스캔 결과 개요](#) 대화 상자로 돌아갑니다 .

12.7.2. 감염 탭



감염 탭은 스캔 중에 **바이러스 감염** 이 발견된 경우에만 [스캔 결과](#) 대화 상자에 표시됩니다 . 이 탭은 다음과 같은 정보를 제공하는 세 개의 섹션으로 나뉘어 있습니다 .

- **파일** - 감염된 개체의 원래 위치에 대한 전체 경로입니다 .
- **감염** - 발견된 [바이러스](#) 의 이름입니다 . 특정 바이러스에 대한 자세한 내용은 온

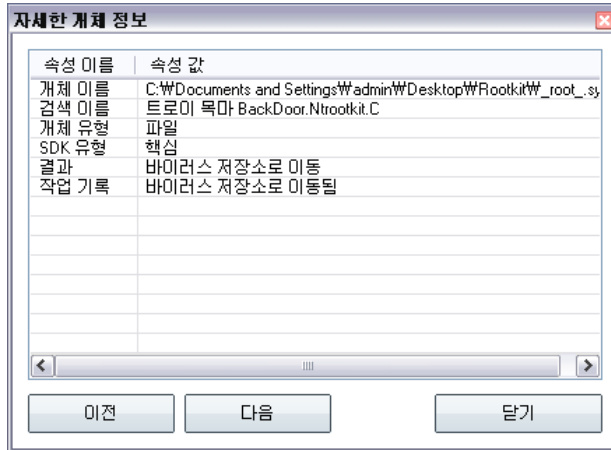
라인 [***바이러스](#) 백과 사전 을 참조하십시오 .

- **결과** - 스캔 중에 발견된 감염된 개체의 현재 상태를 다음과 같이 정의합니다 .
 - o **감염됨** - 감염된 개체가 발견되어 원래 위치에 남아 있습니다 (예: 특정 스캔 설정에서 [***자동 치료 옵션을 해제한 경우](#)).
 - o **치료됨** - 감염된 개체가 자동으로 치료되어 원래 위치에 남아 있습니다 .
 - o **바이러스 저장소로 이동됨** - 감염된 개체가 [바이러스 저장소](#) 검역소로 이동되었습니다 .
 - o **삭제됨** - 감염된 개체가 삭제되었습니다 .
 - o **PUP 예외에 추가됨** - 검색 결과가 예외로 판단되어 PUP 예외 목록 (고급 설정의 [PUP 예외](#) 대화 상자에 구성됨)에 추가되었습니다 .
 - o **잠긴 파일 - 테스트되지 않음** - 해당 개체가 잠겨 있으므로 스캔할 수 없습니다 .
 - o **잠재적으로 위험한 개체** - 개체가 잠재적으로 위험한 것으로 발견되었지만 감염된 것은 아닙니다 (예: 개체에 매크로가 포함된 경우). 이는 경고 정보로 간주할 수 있습니다 .
 - o **작업을 마치려면 다시 부팅해야 함** - 감염된 개체를 제거할 수 없으며 완전히 제거하려면 컴퓨터를 다시 시작해야 합니다 .

제어 단추

이 대화 상자에서 다음 세 개의 제어 단추를 사용할 수 있습니다 .

- **세부 정보 보기** - 이 단추를 클릭하면 **자세한 스캔 결과 정보** 라는 이름의 새 대화 상자 창이 열립니다 .



이 대화 상자에서 발견된 감염 개체의 위치에 대한 정보 (**속성 이름**)를 찾을 수 있습니다. **이전 / 다음** 단추를 사용하여 특정 검색 결과에 대한 정보를 볼 수 있습니다. 이 대화 상자를 닫으려면 **닫기** 단추를 사용합니다.

- **선택한 감염 제거** - 선택한 검색 결과를 바이러스 저장소로 이동하려면 이 단추를 사용합니다.
- **치료되지 않은 모든 감염 제거** - 이 단추를 사용하여 치료할 수 없거나 바이러스 저장소로 이동된 모든 검색 결과를 삭제합니다.
- **결과 닫기** - 자세한 정보 개요를 종료하고 스캔 결과 개요 대화 상자로 돌아갑니다.

12.7.3. 스파이웨어 탭

스�파이웨어 탭은 스캔 중에 **스�파이웨어** 가 발견된 경우에만 스캔 결과 대화 상자에 표시됩니다. 이 탭은 다음과 같은 정보를 제공하는 세 개의 섹션으로 나뉘어 있습니다.

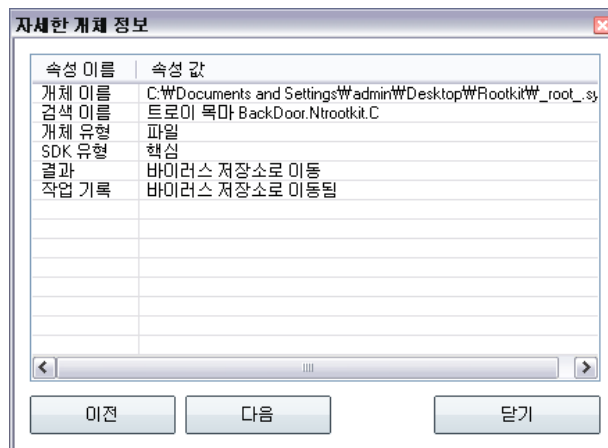
- **파일** - 감염된 개체의 원래 위치에 대한 전체 경로입니다.
- **감염** - 발견된 스�파이웨어 의 이름입니다. 특정 바이러스에 대한 자세한 내용은 온라인 바이러스 백과 사전 을 참조하십시오.
- **결과** - 스캔 중에 발견된 개체의 현재 상태를 정의합니다.
 - **감염됨** - 감염된 개체가 발견되어 원래 위치에 남아 있습니다 (예: 특정 스캔 설정에서 자동 치료 옵션을 해제 한 경우).
 - **치료됨** - 감염된 개체가 자동으로 치료되어 원래 위치에 남아 있습니다.

- **바이러스 저장소로 이동됨** - 감염된 개체가 **바이러스 저장소** 검역소로 이동되었습니다 .
- **삭제됨** - 감염된 개체가 삭제되었습니다 .
- **PUP 예외에 추가됨** - 검색 결과가 예외로 판단되어 PUP 예외 목록 (고급 설정의 **PUP 예외** 대화 상자에 구성됨)에 추가되었습니다 .
- **잠긴 파일 - 테스트되지 않음** - 해당 개체가 잠겨 있으므로 스캔할 수 없습니다 .
- **잠재적으로 위험한 개체** - 개체가 잠재적으로 위험한 것으로 발견되었지만 감염된 것은 아닙니다 (예: 개체에 매크로가 포함된 경우). 이는 경고 정보로 간주할 수 있습니다 .
- **작업을 마치려면 다시 부팅해야 함** - 감염된 개체를 제거할 수 없으며 완전히 제거하려면 컴퓨터를 다시 시작해야 합니다 .

제어 단추

이 대화 상자에서 다음 세 개의 제어 단추를 사용할 수 있습니다 .

- **세부 정보 보기** - 이 단추를 클릭하면 **자세한 스캔 결과 정보** 라는 이름의 새 대화 상자 창이 열립니다 .

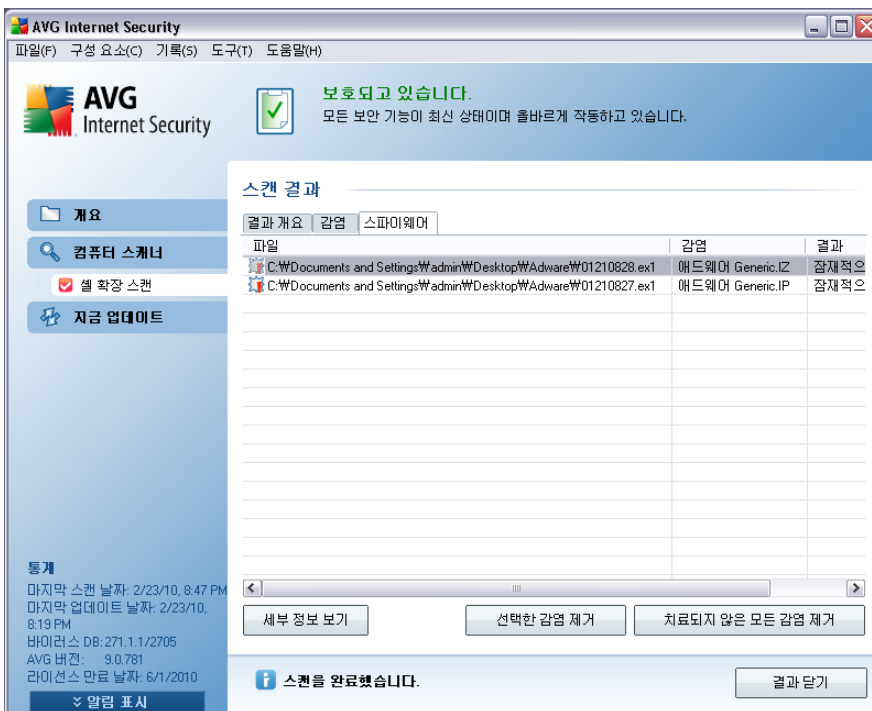


이 대화 상자에서 발견된 감염 개체의 위치에 대한 정보 (**속성 이름**)를 찾을 수 있습니다 . **이전 / 다음** 단추를 사용하여 특정 검색 결과에 대한 정보를 볼 수 있습니다 . 이 대화 상자를 닫으려면 **닫기** 단추를 사용합니다 .

- **선택한 감염 제거** - 선택한 검색 결과를 바이러스 저장소로 이동하려면 이 단추를 사용합니다.
- **치료되지 않은 모든 감염 제거** - 이 단추를 사용하여 치료할 수 없거나 바이러스 저장소로 이동된 모든 검색 결과를 삭제합니다.
- **결과 닫기** - 자세한 정보 개요를 종료하고 스캔 결과 개요 대화 상자로 돌아갑니다.

12.7.4. 경고 탭

경고 탭에는 스캔 중에 검색한 "의심스러운 " 개체 (*일반적으로 파일*)에 대한 정보가 표시됩니다 . 상주 보호에 의해 발견된 이들 파일은 액세스할 수 없도록 차단됩니다 . 그와 같이 검색되는 파일 유형으로는 일반적으로 숨겨진 파일, 쿠키, 의심스러운 레지스트리 키, 암호로 보호되는 문서 또는 압축 파일 등이 있습니다 . 이와 같은 파일은 컴퓨터나 보안에 직접적인 위험이 되지 않습니다 . 일반적으로 이러한 파일에 대한 정보는 컴퓨터에서 애드웨어나 스파이웨어가 발견된 경우에 유용합니다 . AVG 테스트에서 경고만 발견된 경우에는 별도의 작업이 필요치 않습니다 .



다음은 그러한 개체의 가장 일반적인 사례에 대한 간략한 설명입니다 .

- **숨겨진 파일** - 숨겨진 파일은 기본적으로 Windows에 표시되지 않으며 , 일부 바

이러스나 위협 요소는 자신이 검색되지 않도록 하기 위해 파일이 저장될 때 이러한 특성을 이용합니다 . AVG에서 악의적인 파일로 의심되는 숨겨진 파일을 보고하는 경우 이를 [AVG 바이러스 저장소](#)로 이동할 수 있습니다 .

- **쿠키** - 쿠키는 웹 사이트에서 사용자 관련 정보를 저장하여 나중에 사용자 지정 웹 사이트 레이아웃을 로드하거나 사용자 이름을 미리 입력하는 등의 용도로 사용되는 일반 텍스트 파일입니다 .
- **의심스러운 레지스트리 키** - 일부 맬웨어는 시작 시 로드되어 운영 체제 전체에 영향을 미치기 위해 자신의 정보를 Windows 레지스트리에 저장합니다 .

12.7.5. 루트킷 탭

Anti-Rootkit 스캔 을 시작하거나 Anti-Rootkit 스캔 옵션을 [전체 컴퓨터 스캔](#) 에 수동으로 추가한 경우 ([이 옵션은 기본적으로 해제되어 있음](#)) 루트킷 탭에 스캔 중 발견된 루트킷 관련 정보가 표시됩니다 .

[루트킷](#)이란 시스템 소유자 및 합법적인 관리자의 허가 없이 컴퓨터 시스템을 근본적으로 제어하도록 설계된 프로그램입니다 . 루트킷은 하드웨어에서 실행되는 운영 체제를 제어하므로 하드웨어 자체에 대한 액세스가 필요한 경우는 거의 없습니다 . 일반적으로 루트킷은 표준 운영 체제 보안 메커니즘을 파괴하거나 우회함으로써 시스템에서 자신의 존재를 숨깁니다 . 많은 경우 루트킷은 사용자를 속여 시스템에서 안전하게 실행할 수 있는 프로그램이라고 믿게 만드는 트로이 목마이기도 합니다 . 이를 위해 사용되는 기술로는 모니터링 프로그램으로부터 실행 중인 프로세스를 숨기거나 운영 체제로부터 파일 또는 시스템 데이터를 숨기는 방법이 있습니다 .

이 탭의 구조는 기본적으로 [감염 탭](#) 또는 [스파이웨어 탭](#)과 같습니다 .

12.7.6. 정보 탭

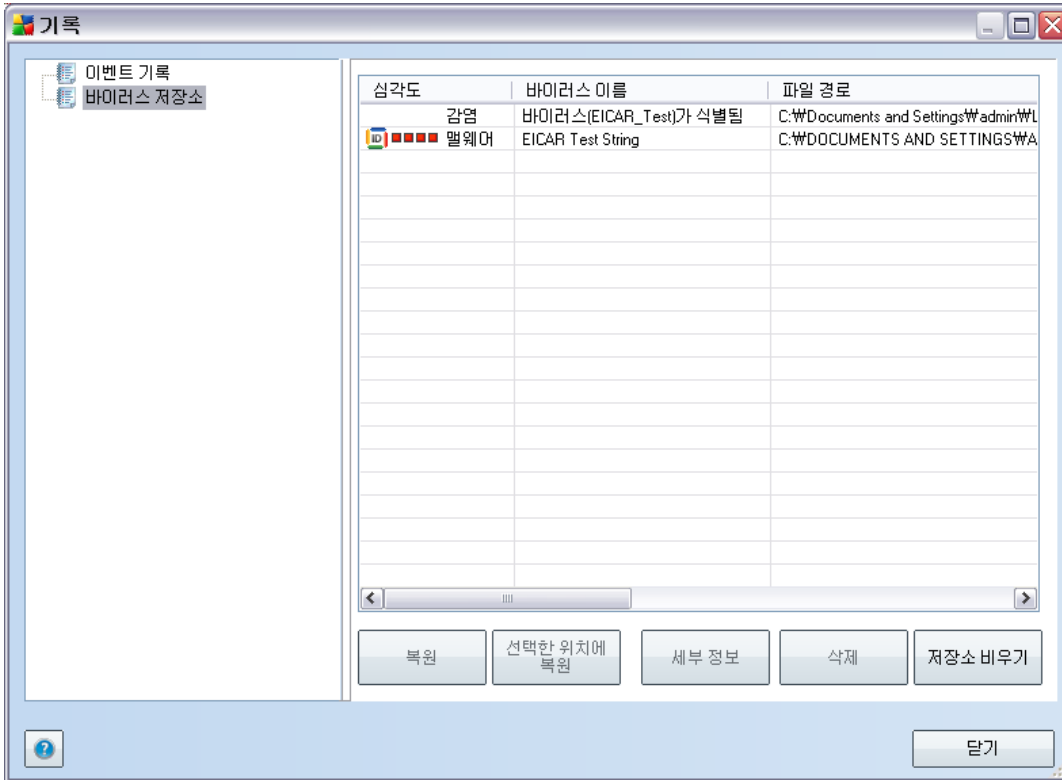
정보 탭에는 감염, 스파이웨어 등으로 분류할 수 없는 "검색 결과" 관련 데이터가 있습니다 . 이러한 데이터에는 위험한 요소로 레이블이 지정되지는 않지만 계속해서 주의를 기울이는 것이 좋습니다 . AVG 스캔에서는 감염 여부가 의심스러운 파일을 검색할 수 있습니다 . 이러한 파일은 [경고](#) 또는 **정보**로 보고됩니다 .

다음 이유 중 하나로 인해 심각도 **정보**가 보고될 수 있습니다 .

- **런타임에 압축됨** - 파일이 일반적이지 않은 런타임 압축 프로그램으로 압축되었습니다 . 이것은 파일의 스캔을 방해하려는 시도일 수 있습니다 . 하지만 이와 같은 파일의 보고가 모두 바이러스를 나타내는 것은 아닙니다 .
- **런타임에 재귀적으로 압축됨** - 위와 유사하지만 일반적인 소프트웨어에서는 거의 발생하지 않는 현상입니다 . 이와 같은 파일은 의심스러운 파일이므로 제거하거나 분석을 위해 제출하는 것을 고려해야 합니다 .

- **암호로 보호된 압축 파일 또는 문서** - 암호로 보호된 파일은 AVG 또는 일반적인 다른 모든 맬웨어 백신 프로그램으로 스캔할 수 없습니다 .
- **매크로 포함 문서** - 보고된 문서에 매크로가 포함되어 있으며 , 매크로가 악성일 수 있습니다 .
- **숨겨진 확장명** - 숨겨진 확장명이 있는 파일 , 예를 들어 *picture.jpg.exe*에서 *exe* 확장명을 숨기면 *파일이 사진인 것처럼 보일 수 있지만 사실은 실행 파일입니다* . Windows에서 두 번째 확장명은 기본적으로 보이지 않지만 AVG는 그와 같은 파일을 보고하여 실수로 여는 것을 방지해 줍니다 .
- **잘못된 파일 경로** - 중요한 시스템 파일이 기본 경로와 다른 경로에서 실행되는 경우 (예: *winlogon.exe*가 *Windows* 폴더가 아닌 폴더에서 실행되는 경우) AVG는 그러한 불일치를 보고합니다 . 바이러스가 시스템에서 자신의 존재를 숨기기 위해 표준 시스템 프로세스의 이름을 사용하는 경우가 있습니다 .
- **잠긴 파일** - 보고된 파일이 잠겨 있어 AVG에서 스캔할 수 없습니다 . 이것은 대개 해당 파일이 시스템에서 지속적으로 사용되고 있다는 의미입니다 (예: *스왑 파일*) .

12.8. 바이러스 저장소



바이러스 저장소 는 AVG 테스트 중에 발견된 의심스럽거나 감염된 개체를 관리할 수 있는 안전한 환경입니다 . 일단 스캔 중에 감염된 개체가 발견되고 AVG가 이를 자동으로 치료할 수 없는 경우 의심스러운 개체에 대한 조치를 결정하도록 사용자에게 요청합니다 . 바람직한 해결책은 추가적인 처리를 위해 **바이러스 저장소** 로 이동하는 것입니다 . **바이러스 저장소** 는 주로 삭제된 파일이 원래 위치에서 더 이상 필요하지 않다는 확신이 들 때까지 해당 파일을 일정 기간 동안 유지하는 데 사용됩니다 . 파일 부재로 인해 문제가 발생하는 경우라면 해당 파일을 분석을 위해 보내거나 원래 위치로 복원할 수 있습니다 .

바이러스 저장소 인터페이스는 별도의 창으로 열리며 검역소로 이동된 감염된 개체에 대한 정보의 개요를 제공합니다 .

- **심각도** - **Identity Protection** 구성 요소를 **AVG 9 Internet Security** 내에 설치하기로 결정한 경우 이 섹션에서는 유해하지 않은 수준 (■□□□)부터 매우 위험한 수준 (■■■■)에 이르기까지 네 단계로 관련 항목의 심각도가 그래픽으로 표시되며, 감염 유형에 대한 정보 (감염 수준 기준 - 나열된 모든 개체는 명시적으로 또는 잠재적으로 감염되었을 수 있음)도 제공됩니다 .

- **바이러스 이름** - [바이러스 백과 사전](#) (온라인)에 따라 발견된 감염의 이름을 지정합니다 .
- **파일 경로** - 발견된 감염 파일의 원래 위치에 대한 전체 경로입니다 .
- **원본 개체 이름** - 차트에 나열된 모든 검색 개체에는 스캔 과정에서 AVG가 지정한 표준 이름의 레이블이 지정되어 있습니다 . 개체의 이름이 원래 알려진 이름인 경우 (예: 전자 메일 첨부 파일의 이름이 첨부 파일의 실제 내용에 부합하지 않음) 그 이름이 이 열에 표시됩니다 .
- **저장소 날짜** - 의심스러운 파일이 발견되어 **바이러스 저장소로 이동한 날짜 및 시간**입니다 .

제어 단추

바이러스 저장소 인터페이스에서 다음 제어 단추에 액세스할 수 있습니다 .

- **복원** - 감염된 파일을 디스크의 원래 위치로 되돌려 보냅니다 .
- **선택한 위치에 복원** - 발견된 감염 개체를 **바이러스 저장소**에서 선택한 폴더로 이동하는 경우에 이 단추를 사용합니다 . 발견된 의심스러운 개체는 원래 이름으로 저장됩니다 . 원래 이름이 알려지지 않은 경우 표준 이름이 사용됩니다 .
- **세부 정보** - 이 단추는 [Identity Protection](#)에서 발견된 위협 요소에만 적용됩니다 . 이 단추를 클릭하면 *영향을 받은 파일/프로세스 , 프로세스의 특징 등 위협 요소 세부 정보에 대한 간략한 개요가 표시됩니다 .* IDP에서 발견된 것 이외의 다른 모든 항목에 대해서는 이 단추가 회색으로 표시되고 비활성화됩니다 !
- **삭제** - 감염된 파일을 **바이러스 저장소**에서 완전히 제거합니다 .
- **저장소 비우기** - 모든 **바이러스 저장소**의 내용을 완전히 제거합니다 . 바이러스 저장소에서 파일을 제거하면 해당 파일이 휴지통으로 이동되지 않고 디스크에서 영구적으로 제거됩니다 .

13. AVG 업데이트

새로 발견된 바이러스를 최대한 빨리 감지할 수 있도록 AVG를 최신 상태로 유지하는 것이 중요합니다 .

AVG 설치 프로세스 동안 AVG 업데이트 빈도를 지정하는 옵션이 제공됩니다 . 사용 가능한 옵션으로는 **4시간마다** 또는 **매일** 이 있습니다 (정기적인 스캔 및 업데이트 예약 대화 상자 참조). AVG 업데이트는 정해진 일정에 따르는 것이 아니라 새로운 위협 요소의 양과 심각도에 대응하는 방식으로 릴리스되기 때문에 적어도 하루에 한 번은 새 업데이트를 확인하는 것이 좋습니다 . 하루 중에도 **AVG 9 Internet Security**을(를) 최신 상태로 유지하고 싶다면 4시간마다 한 번씩 업데이트를 확인하십시오 .

13.1. 업데이트 수준

다음 두 가지 업데이트 수준 중에서 선택할 수 있습니다 .

- **정의 업데이트**에는 신뢰할 수 있는 바이러스 백신, 스팸 방지 및 맬웨어 백신 보호에 필요한 변경 내용이 포함됩니다 . 일반적으로 여기에는 코드에 대한 변경 내용이 포함되지 않으며 단지 정의 데이터베이스만 업데이트됩니다 . 이 업데이트는 가능한 한 빨리 적용되어야 합니다 .
- **프로그램 업데이트**에는 다양한 프로그램 변경 내용, 수정 사항 및 개선 사항이 포함됩니다 .

업데이트 예약 시 어떤 우선 순위 수준이 다운로드되고 적용될지 선택할 수 있습니다 .

참고 : 예약된 프로그램 업데이트와 예약된 스캔이 같은 시간에 수행될 경우 업데이트 프로세스의 우선 순위가 더 높으므로 스캔이 중단됩니다 .

13.2. 업데이트 유형

업데이트 유형은 다음 두 가지로 구분할 수 있습니다 .

- **요청 시 업데이트**는 필요할 때 언제든지 수행할 수 있는 즉각적인 AVG 업데이트입니다 .
- **예약된 업데이트** - AVG에서는 업데이트 계획을 미리 설정 할 수도 있습니다 . 그러면 구성 설정에 따라 계획된 업데이트가 주기적으로 수행됩니다 . 새 업데이트 파일이 지정된 위치에 있다면 해당 파일이 인터넷 또는 네트워크 디렉터리에서 직접 다운로드됩니다 . 새 업데이트가 없는 경우에는 아무 일도 일어나지 않습니다 .

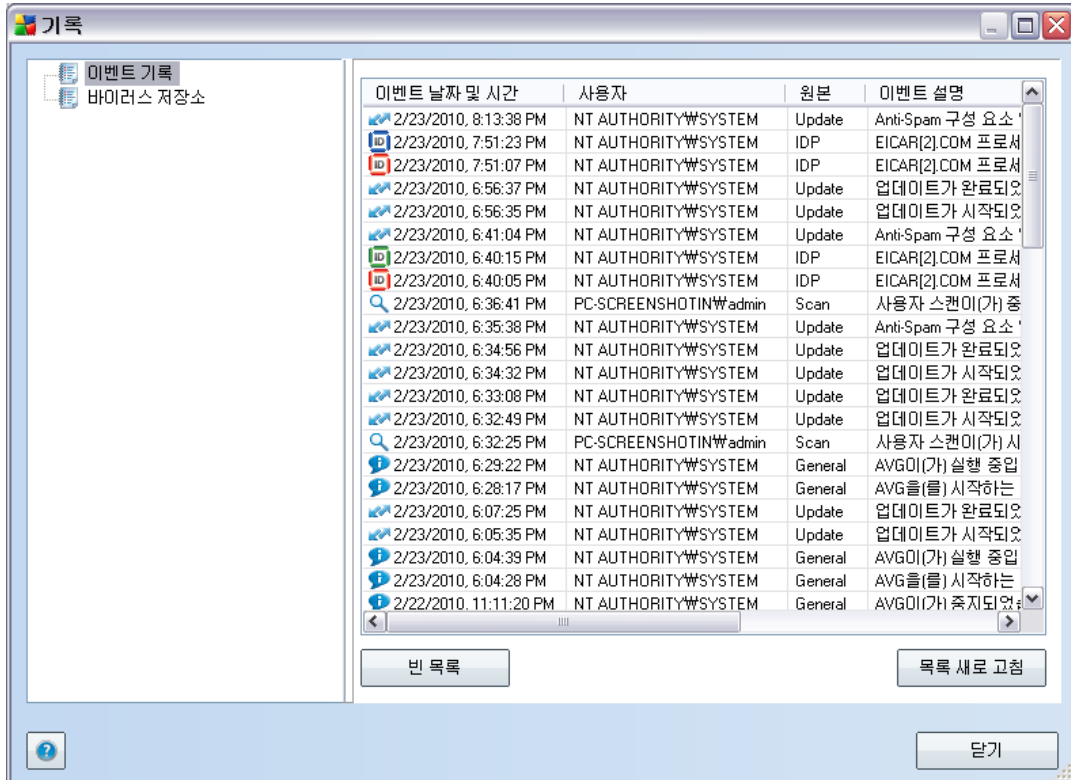
13.3. 업데이트 프로세스

업데이트 프로세스는 필요한 경우 **지금 업데이트 빠른 링크**를 사용하여 즉시 시작할 수 있습니다. 이 링크는 모든 **AVG 사용자 인터페이스** 대화 상자에서 언제든지 사용할 수 있습니다. 하지만 **업데이트 관리자** 구성 요소에서 편집할 수 있는 업데이트 일정에 명시된 대로 정기적인 업데이트를 수행하는 것이 좋습니다.

일단 업데이트를 시작하면 먼저 사용할 수 있는 새 업데이트 파일이 있는지 여부를 확인합니다. 새 업데이트 파일이 있는 경우 이를 다운로드하면서 업데이트 프로세스가 시작됩니다. 업데이트 프로세스 동안 **업데이트** 인터페이스로 리디렉션됩니다. 여기에서는 프로세스 진행 상황을 그래픽으로 확인할 수 있을 뿐 아니라 관련 통계 매개 변수의 개요 (업데이트 파일 크기, 받은 데이터, 다운로드 속도, 경과 시간 등)도 확인할 수 있습니다.

참고 : AVG 프로그램 업데이트를 시작하기 전에 시스템 복원 지점이 만들어집니다. 업데이트 프로세스가 실패하여 운영 체제가 중단되는 경우 언제든지 OS를 이 지점에서 원래 구성으로 복원할 수 있습니다. 이 옵션은 시작/모든 프로그램/보조 프로그램/시스템 도구/시스템 복원을 통해 액세스할 수 있지만 숙련된 사용자에게만 권장됩니다.

14. 이벤트 기록



이벤트 기록 대화 상자는 [기록 / 이벤트 기록 로그](#) 항목을 통해 **시스템 메뉴**에서 액세스할 수 있습니다. 이 대화 상자에서는 **AVG 9 Internet Security** 작업 중 발생한 중요한 이벤트에 대한 요약 내용을 확인할 수 있습니다. **이벤트 기록**은 다음과 같은 유형의 이벤트를 기록합니다.

- AVG 응용 프로그램의 업데이트에 대한 정보
- 스캔 시작, 종료 또는 중지 (자동 수행된 테스트 포함)
- [상주 보호](#) 또는 [스캔](#)에 의한 바이러스 검색과 연결된 이벤트 (발생 위치 포함)
- 기타 중요한 이벤트

제어 단추

- **목록 비우기** - 이벤트 목록에서 모든 항목을 삭제합니다.



- **목록 새로 고침** - 이벤트 목록에서 모든 항목을 업데이트합니다 .

15. FAQ 및 기술 지원

AVG 제품과 관련하여 업무적 또는 기술적인 문제가 발생한 경우에는 AVG 웹 사이트 (<http://www.avg.com/>)의 ***FAQ 섹션을 참조하십시오 .

이 방법으로 도움말을 찾을 수 없는 경우 전자 메일로 기술 지원 부서에 문의하십시오 .
도움말 / 온라인 도움말 보기 를 통해 시스템 메뉴에서 액세스할 수 있는 연락처 양식을
사용하시기 바랍니다 .