



AVG Internet Security 2012

사용자 설명서

문서 버전 2012.03 (29.11.2011)

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 1991를 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	7
2. AVG 설치 요구 사항	8
2.1 지원되는 운영 체제	8
2.2 최소/권장 하드웨어 요구 사항	8
3. AVG 설치 프로세스	9
3.1 시작	9
3.2 라이선스 활성화	11
3.3 설치 유형 선택	12
3.4 사용자 지정 옵션	13
3.5 AVG Security Toolbar 설치	14
3.6 설치 진행률	15
3.7 설치를 완료했습니다	16
4. 설치 후 작업	18
4.1 제품 등록	18
4.2 사용자 인터페이스 액세스	18
4.3 전체 컴퓨터 스캔	18
4.4 EICAR 테스트	18
4.5 AVG 기본 구성	19
5. AVG 사용자 인터페이스	20
5.1 시스템 메뉴	21
5.1.1 파일	21
5.1.2 구성 요소	21
5.1.3 기록	21
5.1.4 도구	21
5.1.5 도움말	21
5.1.6 지원	21
5.2 보안 상태 정보	28
5.3 빠른 링크	29
5.4 구성 요소 개요	30
5.5 시스템 트레이 아이콘	31
5.6 AVG 가젯	33
6. AVG 구성 요소	36



6.1 Anti- Virus	36
6.1.1 스캔 엔진	36
6.1.2 Resident Shield	36
6.1.3 Anti- Spyware 보호	36
6.1.4 Anti- Virus 인터페이스	36
6.1.5 Resident Shield 검색	36
6.2 LinkScanner	42
6.2.1 LinkScanner 인터페이스	42
6.2.2 Search- Shield 검색	42
6.2.3 Surf- Shield 검색	42
6.2.4 Online Shield 검색	42
6.3 전자 메일 보호	48
6.3.1 E- mail Scanner	48
6.3.2 Anti- Spam	48
6.3.3 전자 메일 보호 인터페이스	48
6.3.4 전자 메일 보호 검색	48
6.4 Firewall	52
6.4.1 Firewall 원리	52
6.4.2 Firewall 프로필	52
6.4.3 Firewall 인터페이스	52
6.5 Anti- Rootkit	56
6.5.1 Anti- Rootkit 인터페이스	56
6.6 시스템 도구	57
6.6.1 프로세스	57
6.6.2 네트워크 연결	57
6.6.3 자동 시작	57
6.6.4 브라우저 확장	57
6.6.5 LSP 뷰어	57
6.7 PC Analyzer	64
6.8 Identity Protection	65
6.8.1 Identity Protection 인터페이스	65
6.9 원격 관리	68
7. 내 응용 프로그램	69
7.1 LiveKive	69
7.2 Family Safety	70
7.3 PC Tuneup	70
8. AVG Security Toolbar	72



9. AVG 고급 설정	74
9.1 모양	74
9.2 사운드	77
9.3 일시적으로 AVG 보호 사용 안 함	78
9.4 Anti- Virus	79
9.4.1 Resident Shield	79
9.4.2 캐시 서버	79
9.5 전자 메일 보호	85
9.5.1 E- mail Scanner	85
9.5.2 Anti- Spam	85
9.6 LinkScanner	101
9.6.1 LinkScanner 설정	101
9.6.2 Online Shield	101
9.7 스캔	105
9.7.1 전체 컴퓨터 스캔	105
9.7.2 셀 확장 스캔	105
9.7.3 특정 파일 또는 폴더 스캔	105
9.7.4 이동식 장치 스캔	105
9.8 예약	111
9.8.1 예약된 스캔	111
9.8.2 정의 업데이트 일정	111
9.8.3 프로그램 업데이트 일정	111
9.8.4 Anti- Spam 업데이트 일정	111
9.9 업데이트	122
9.9.1 프록시	122
9.9.2 전화 접속	122
9.9.3 URL	122
9.9.4 관리	122
9.10 Anti- Rootkit	129
9.10.1 예외	129
9.11 Identity Protection	130
9.11.1 Identity Protection 설정	130
9.11.2 허용 목록	130
9.12 원치 않는 프로그램	133
9.13 바이러스 저장소	136
9.14 제품 개선 프로그램	136
9.15 오류 상태 무시	139



9.16 원격 관리	140
10. Firewall 설정	142
10.1 일반	142
10.2 보안	143
10.3 영역 및 어댑터 프로필	144
10.4 IDS	145
10.5 로그	147
10.6 프로필	148
10.6.1 프로필 정보	148
10.6.2 정의된 네트워크	148
10.6.3 응용 프로그램	148
10.6.4 시스템 서비스	148
11. AVG 스캔	159
11.1 스캔 인터페이스	159
11.2 미리 정의된 스캔	160
11.2.1 전체 컴퓨터 스캔	160
11.2.2 특정 파일 또는 폴더 스캔	160
11.2.3 Anti- Rootkit 스캔	160
11.3 Windows 탐색기에서 스캔	170
11.4 명령줄 스캔	171
11.4.1 CMD 스캔 매개 변수	171
11.5 스캔 일정	173
11.5.1 예약 설정	173
11.5.2 스캔 방법	173
11.5.3 스캔 대상	173
11.6 스캔 결과 개요	182
11.7 스캔 결과 세부 정보	183
11.7.1 결과 개요 탭	183
11.7.2 감염 탭	183
11.7.3 스파이웨어 탭	183
11.7.4 경고 탭	183
11.7.5 루트킷 탭	183
11.7.6 정보 탭	183
11.8 바이러스 저장소	190
12. AVG 업데이트	193
12.1 업데이트 시작	193



12.2 업데이트 진행률	193
12.3 업데이트 수준	194
13. 이벤트 기록	196
14. FAQ 및 기술 지원	198



1. 소개

이 사용자 설명서에는 **AVG Internet Security 2012**에 대한 포괄적인 내용이 포함되어 있습니다.

AVG Internet Security 2012는 사용자의 모든 온라인 작업에 대해 여러 계층의 방어 기능을 제공하므로 ID 도용이나 바이러스, 유해 사이트의 걱정 없이 편안하게 작업을 수행할 수 있습니다. AVG 보호 클라우드 기술 및 AVG 커뮤니티 보호 네트워크가 포함되어 있어 최신 위협 요소 정보를 수집한 다음 이를 커뮤니티와 공유하여 사용자는 최상의 보호를 받을 수 있습니다:

- AVG Firewall, Anti-Spam 및 Identity Protection을 사용하여 안전하게 온라인 쇼핑 및 बैंकिंग 이용
- AVG 소셜 네트워킹 보호를 통해 안전하게 소셜 네트워크 사용
- LinkScanner의 실시간 보호 기능으로 안전한 서핑 및 검색 가능



2. AVG 설치 요구 사항

2.1. 지원되는 운영 체제

AVG Internet Security 2012 제품은 다음 운영 체제가 실행되는 워크스테이션을 보호합니다.

- 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 XP x64 에서 지원되지 않습니다. 이러한 운영 체제에 AVG Internet Security 2012 제품을 설치할 수 있지만 IDP 구성 요소는 사용할 수 없습니다.

2.2. 최소/권장 하드웨어 요구 사항

AVG Internet Security 2012 의 최소 하드웨어 요구 사항:

- Intel Pentium CPU 1,5 GHz
- 512 MB 이상의 RAM 메모리
- 1000 MB의 사용 가능한 하드 드라이브 공간(설치용)

AVG Internet Security 2012 의 권장 하드웨어 요구 사항:

- Intel Pentium CPU 1,8 GHz
- 512 MB 이상의 RAM 메모리
- 1550 MB의 사용 가능한 하드 드라이브 공간(설치용)



3. AVG 설치 프로세스

설치 파일은 어디에서 구할 수 있습니까?

컴퓨터에 **AVG Internet Security 2012** 제품을 설치하려면 최신 설치 파일이 있어야 합니다. **AVG Internet Security 2012** 의 최신 버전을 설치하려면 AVG 웹 사이트 (<http://www.avg.com/>) 에서 설치 파일을 다운로드하는 것이 좋습니다. **지원 센터/다운로드** 섹션에는 각 AVG 버전의 설치 파일 개요가 체계적으로 나와 있습니다.

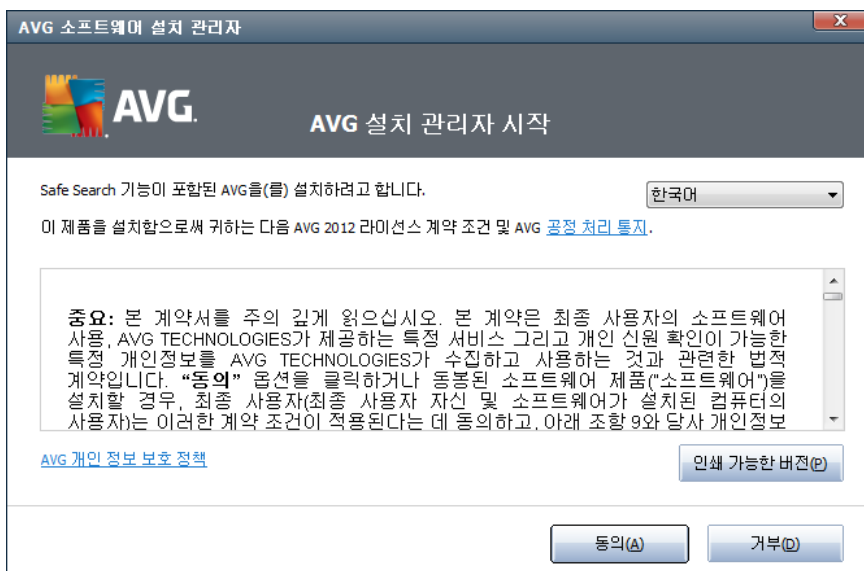
어느 파일을 다운로드하고 설치해야 하는지 잘 모르는 경우에는 웹 페이지 맨 아래에 있는 **제품 선택** 서비스를 사용할 수 있습니다. 이 서비스는 세 가지 간단한 질문을 통해 사용자에게 필요한 파일을 찾습니다. **계속** 단추를 누르면 사용자 개인의 필요에 맞게 사용자 지정된 다운로드 파일 목록 페이지로 연결됩니다.

설치 프로세스는 어떻게 진행됩니까?

하드 디스크에 설치 파일을 다운로드하여 저장하면 설치 프로세스를 시작할 수 있습니다. 설치하는 단순하고 이해하기 쉬운 일련의 대화 상자로 구성되며, 각 대화 상자에는 설치 프로세스의 각 단계에서 수행해야 하는 작업이 간략하게 설명되어 있습니다. 이제부터 각 대화 상자 창에 대한 자세한 설명이 이어집니다.

3.1. 시작

설치 프로세스는 **AVG 설치 관리자 시작** 대화 상자로 시작합니다.



설치 언어 선택

이 대화 상자에서는 설치 프로세스에 사용할 언어를 선택할 수 있습니다. 대화 상자에서



오른쪽 구석에 있는 콤보 상자를 클릭하여 언어 메뉴를 연 후 원하는 언어를 선택하면 해당 언어로 설치 프로세스가 진행됩니다.

주의: 이 시점에서는 설치 프로세스에 사용할 언어를 선택하는 것 뿐입니다. AVG Internet Security 2012 응용 프로그램은 선택한 언어 및 항상 자동으로 설치되는 영어로 설치됩니다. 그러나 원하는 경우 더 많은 언어를 설치하여 해당 언어로 AVG Internet Security 2012를 사용할 수도 있습니다. 설치 대화 상자 중 하나인 사용자 지정 옵션 대화 상자에서 대체 언어 전체를 선택 및 확인할 수 있습니다.

라이선스 계약

AVG 설치 관리자 시작 대화 상자에는 AVG 라이선스 계약 전문이 나와 있습니다. 계약 내용을 자세히 읽은 후 **동의** 단추를 눌러 계약 내용을 읽고 이해했으며 동의한다는 의사를 확인해 주십시오. 라이선스 계약에 동의하지 않을 경우 **거부** 단추를 누르면 설치 프로세스가 즉시 종료됩니다.

AVG 개인 정보 보호 정책

이 설치 대화 상자에는 라이선스 계약 이외에 AVG 개인 정보 보호 정책에 대한 자세한 설명도 제공됩니다. 대화 상자의 왼쪽 아래 구석에 있는 **AVG 개인 정보 보호 정책** 링크를 클릭하면 AVG Technologies 개인 정보 보호 원리 전체를 볼 수 있는 AVG 웹 사이트 (<http://www.avg.com/>)에 연결됩니다.

제어 단추

첫 번째 설치 대화 상자에는 다음과 같은 제어 단추 두 개만 있습니다.

- **동의** - 라이선스 계약을 읽고 이해했으며 동의함을 확인하려면 클릭합니다. 그러면 설치가 계속되어 다음 설치 대화 상자로 한 단계 진행합니다.
- **거부** - 라이선스 계약에 동의하지 않으면 클릭합니다. 그러면 설치 프로세스가 즉시 종료되고 **AVG Internet Security 2012**가 설치되지 않습니다.



3.2. 라이선스 활성화

라이선스 활성화 대화 상자에서는 제공된 텍스트 필드에 라이선스 번호를 입력하라는 메시지가 나타납니다.

AVG 소프트웨어 설치 관리자

라이선스 활성화

라이선스 번호:

예: IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

온라인으로 AVG 2012 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. 해당 번호를 올바르게 복사해야 합니다.

≤ 뒤로 다음 ≥ 취소

라이선스 번호 위치

판매 번호는 **AVG Internet Security 2012** 상자에 들어 있는 CD 패키지에서 확인할 수 있습니다. 라이선스 번호는 온라인에서 **AVG Internet Security 2012** 제품을 구매한 후에 받은 확인 전자 메일에 있습니다. 번호를 정확하게 입력해야 합니다. 라이선스 번호를 **전자 메일**을 통해 디지털 형식으로 제공받은 경우에는 직접 입력하지 말고 복사하여 붙여넣는 것이 좋습니다.

복사하여 붙여넣기 사용 방법

복사하여 붙여넣기 방법으로 **AVG Internet Security 2012** 라이선스 번호를 프로그램에 입력하면 번호를 잘못 입력할 염려가 없습니다. 다음 단계를 수행합니다.

- 라이선스 번호가 들어 있는 전자 메일을 엽니다.
- 라이선스 번호의 시작 부분에서 마우스 왼쪽 단추를 클릭한 채로 번호 끝까지 마우스를 끈 후 놓습니다. 이렇게 하면 번호가 강조 표시됩니다.
- **Ctrl** 키를 누른 채로 **C** 키를 누릅니다. 이렇게 하면 번호가 복사됩니다.
- 복사한 번호를 붙여 넣을 위치를 찾아 클릭합니다.
- **Ctrl** 키를 누른 채로 **V** 키를 누릅니다. 이렇게 하면 번호를 선택한 위치에 붙여 넣을 수 있습니다.

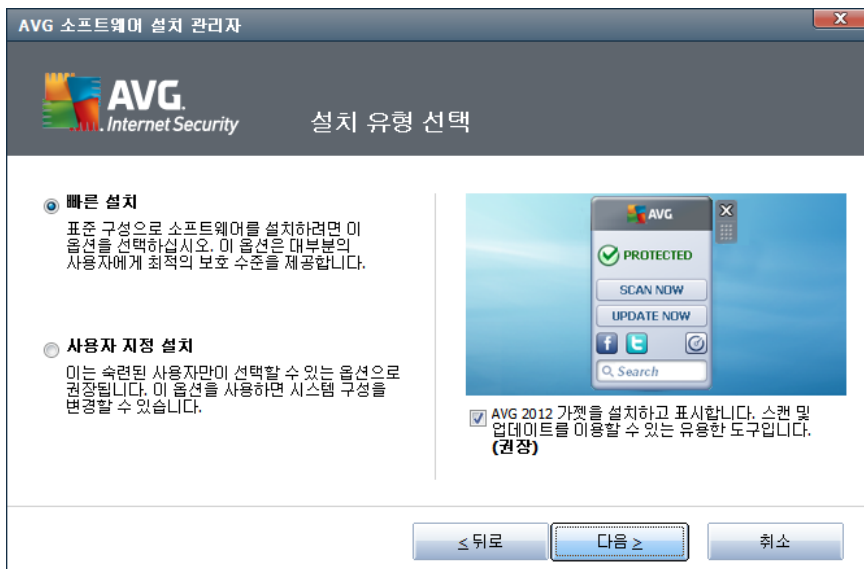


제 어 단 추

대부분의 설치 대화 상자에서는 다음 3가지 제어 단추를 사용할 수 있습니다.

- **뒤로** - 한 단계 뒤의 이전 설치 대화 상자로 되돌아가려는 경우 클릭합니다.
- **다음** - 설치를 계속하면서 한 단계 앞으로 진행하려는 경우 클릭합니다.
- **취소** - 설치 프로세스를 즉시 종료하려는 경우 클릭합니다. **AVG Internet Security 2012**가 설치되지 않습니다.

3.3. 설치 유형 선택



설치 유형

설치 유형 선택 대화 상자에는 **빠른 설치** 및 **사용자 지정 설치**의 두 가지 설치 옵션이 있습니다.

대부분의 사용자는 프로그램 공급업체에서 미리 정의한 설정을 사용하여 완전 자동 모드로 **AVG Internet Security 2012** 프로그램을 설치하는 표준 빠른 설치 옵션을 유지하는 것이 좋습니다. 이 구성은 최적의 리소스 사용률과 최상의 보안 수준을 제공합니다. 나중에 구성을 변경할 필요가 있는 경우에는 언제든지 **AVG Internet Security 2012** 응용 프로그램에서 직접 변경할 수 있습니다. **빠른 설치** 옵션을 선택한 경우 **다음** 단추를 눌러 [AVG Security Toolbar 설치](#) 대화 상자로 이동합니다.

사용자 지정 설치의 **AVG Internet Security 2012** 프로그램을 비표준 설정으로 설치해야 할 타당한 이유가 있는 숙련된 사용자만 사용해야 합니다. 예를 들면 특정한 시스템 요구 사항에 맞추기 위한 경우가 이에 해당합니다. 이 옵션을 선택한 경우 **다음** 단추를 눌러 [사용자 지정 옵션](#) 대화 상자로 이동합니다.



AVG 가젯 설치

대화 상자의 오른쪽 섹션에는 [AVG 가젯](#) (Windows Vista/Windows 7 에서 지원 됨)과 관련된 확인란이 있습니다. 이 가젯을 설치하려면 해당 확인란을 선택합니다. 그런 다음 **AVG Internet Security 2012** 제품의 가장 중요한 기능(예: [스캔](#) 및 [업데이트](#))에 즉시 액세스할 수 있게 해주는 Windows 사이드바를 통해 [AVG 가젯](#)에 액세스할 수 있습니다.

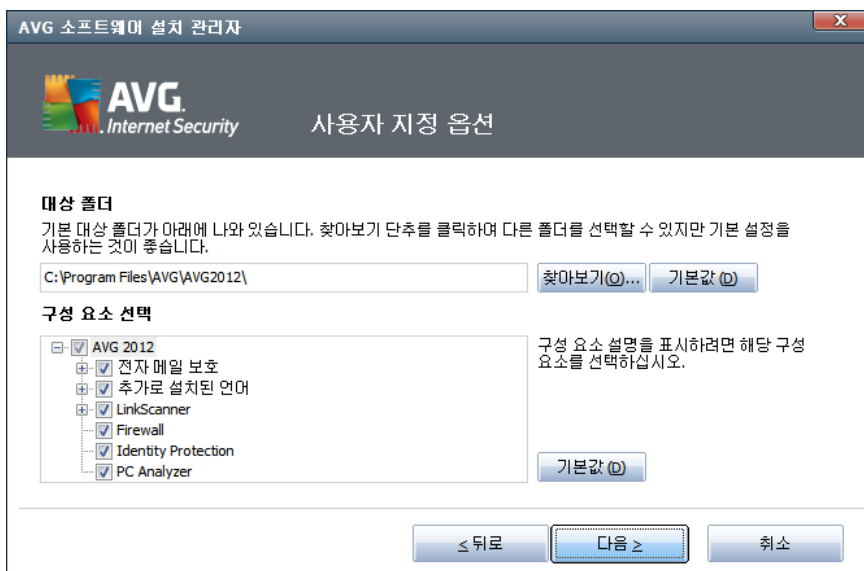
제어 단추

대부분의 설치 대화 상자에서는 다음 3가지 제어 단추를 사용할 수 있습니다.

- **뒤로** - 한 단계 뒤의 이전 설치 대화 상자로 되돌아가려는 경우 클릭합니다.
- **다음** - 설치를 계속하면서 한 단계 앞으로 진행하려는 경우 클릭합니다.
- **취소** - 설치 프로세스를 즉시 종료하려는 경우 클릭합니다. **AVG Internet Security 2012**가 설치되지 않습니다.

3.4. 사용자 지정 옵션

사용자 지정 옵션 대화 상자를 사용하면 두 가지 설치 매개 변수를 설정할 수 있습니다.



대상 폴더

이 대화 상자의 **대상 폴더** 섹션에서는 **AVG Internet Security 2012** 구성 요소를 설치할 위치를 지정해야 합니다. 기본적으로 **AVG Internet Security 2012** 제품은 드라이브 C:의 프로그램 파일 폴더에 설치됩니다. 이 위치를 변경하려면 **찾아보기** 단추를 사용하여 드라이브 구조를 표시한 다음 해당 폴더를 선택합니다.



구성 요소 선택

구성 요소 선택 섹션에서는 설치할 수 있는 모든 **AVG Internet Security 2012** 구성 요소에 대한 개요를 제공합니다. 기본 설정이 사용자에게 맞지 않으면 특정 구성 요소를 제거하거나 추가할 수 있습니다.

그러나 구입한 AVG 버전에 포함된 구성 요소에서만 선택할 수 있습니다!

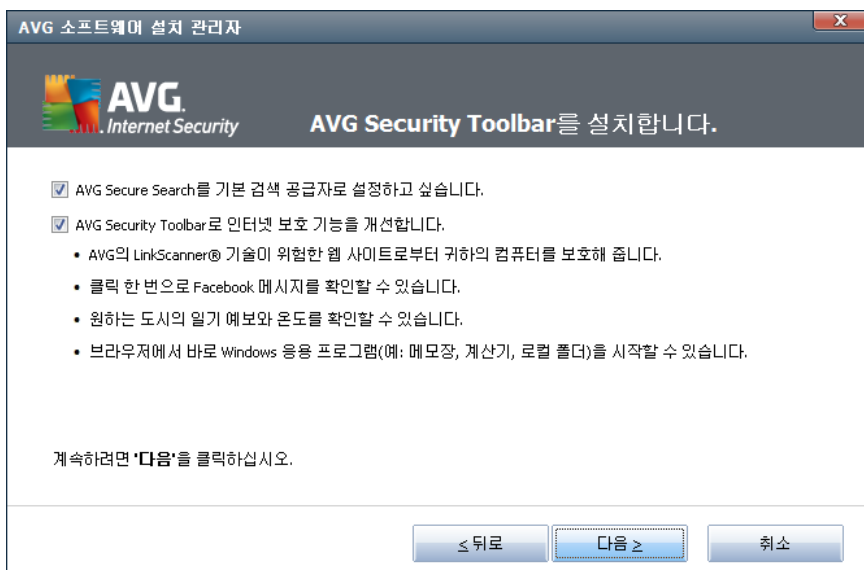
구성 요소 선택 목록에서 원하는 항목을 강조 표시합니다. 그러면 해당 구성 요소에 대한 간략한 설명이 이 섹션의 오른쪽에 표시됩니다. 각 구성 요소의 기능에 대한 자세한 정보는 이 설명서의 [구성 요소 개요](#) 장을 참조하십시오. 소프트웨어 공급업체에서 사전 설정한 기본 구성으로 되돌리려면 **기본값** 단추를 사용하십시오.

제어 단추

대부분의 설치 대화 상자에서는 다음 3가지 제어 단추를 사용할 수 있습니다.

- **뒤로** - 한 단계 뒤의 이전 설치 대화 상자로 되돌아가려는 경우 클릭합니다.
- **다음** - 설치를 계속하면서 한 단계 앞으로 진행하려는 경우 클릭합니다.
- **취소** - 설치 프로세스를 즉시 종료하려는 경우 클릭합니다. **AVG Internet Security 2012**가 설치되지 않습니다.

3.5. AVG Security Toolbar 설치



AVG Security Toolbar 설치 대화 상자에서 [AVG Security Toolbar](#)를 설치할지 여부를 결정합니다. 기본 설정을 변경하지 않으면 이 구성 요소가 인터넷 브라우저(**현재 지원되는 브라우저: Microsoft Internet Explorer 6.0 버전 이상 및 Mozilla Firefox 3.0 버전 이상**)에 자동으로 설



치되어 인터넷을 서핑하는 동안 포괄적인 온라인 보호 기능을 사용할 수 있게 됩니다.

또한 AVG Secure Search (powered by Google) 를 기본 검색 공급자로 선택할지 여부를 결정할 수 있습니다. 기본 검색 공급자로 선택하려면 해당 확인란을 선택된 상태로 유지합니다.

3.6. 설치 진행률

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



설치 프로세스가 완료되면 자동으로 다음 대화 상자로 이동합니다.

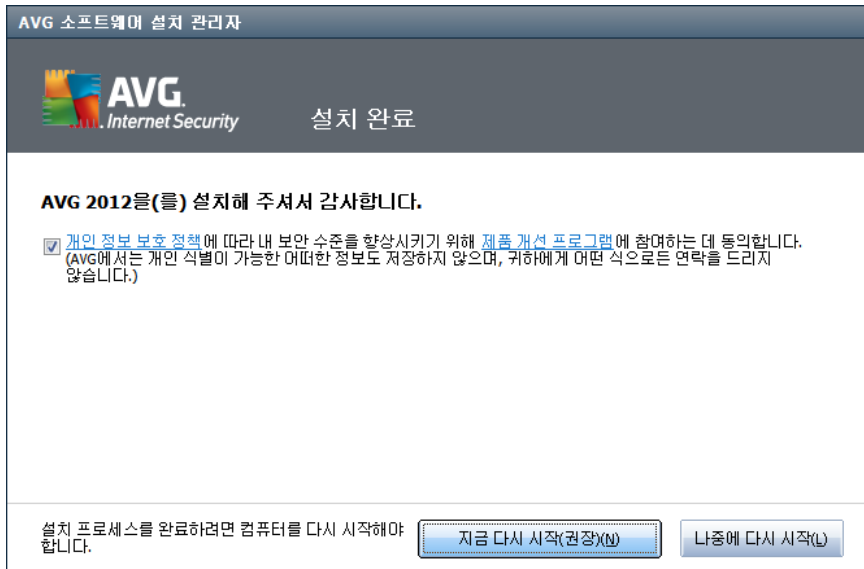
제어 단추

이 대화 상자에는 **취소** 제어 단추 하나만 있습니다. 이 단추는 실행 중인 설치 프로세스를 중지하려는 경우에만 사용해야 합니다. 설치 프로세스를 중지하면 **AVG Internet Security 2012** 가 설치되지 않습니다.



3.7. 설치를 완료했습니다

설치 완료 대화 상자는 AVG Internet Security 2012 제품이 성공적으로 설치 및 구성되었음을 알려 줍니다.



제품 개선 프로그램

이 대화 상자에서는 전반적인 인터넷 보안 수준을 높이기 위해 발견된 위협 요소에 대한 정보를 익명으로 수집하는 제품 개선 프로그램 ([AVG 고급 설정/제품 개선 프로그램](#) 참조)에 참여할지 여부를 결정할 수 있습니다. 여기에 동의하면 **AVG 2012 웹 보안 및 제품 개선 프로그램에 참여하는 데 동의합니다...** 옵션을 선택된 상태로 두십시오. 이 옵션은 기본적으로 선택되어 있습니다.

컴퓨터 다시 시작

설치 프로세스를 마치려면 컴퓨터를 다시 시작해야 합니다. **지금 다시 시작**을 선택하거나, 이 작업을 연기하려면 **나중에 다시 시작**을 선택하십시오.

비즈니스 라이선스 설치

AVG 비즈니스 라이선스를 사용하는 경우 원격 관리 항목을 설치하도록 이전에 선택한 경우 ([사용자 지정 옵션](#) 참조) 설치 완료 대화 상자에 다음과 같은 인터페이스가 표시됩니다.



AVG 소프트웨어 설치 관리자

설치 완료

AVG 2012을(를) 설치해 주셔서 감사합니다.

AVG Data Center 지정:

☒ [개인 정보 보호 정책](#)에 따라 내 보안 수준을 향상시키기 위해 [제품 개선 프로그램](#)에 참여하는 데 동의합니다.
(AVG에서는 개인 식별이 가능한 어떠한 정보도 저장하지 않으며, 귀하에게 어떤 식으로든 연락을 드리지 않습니다.)

설치 프로세스를 완료하려면 컴퓨터를 다시 시작해야 합니다.

[지금 다시 시작\(권장\)\(N\)](#) [나중에 다시 시작\(N\)](#)

AVG DataCenter 매개 변수를 지정해야 합니다. AVG DataCenter에 연결 문자열을 서버:포트 형식으로 입력하십시오. 아직 이 정보를 모르는 경우에는 필드를 비워두고 나중에 [고급 설정/원격 관리](#) 대화 상자에서 구성을 설정할 수 있습니다. AVG 원격 관리에 대한 자세한 내용은 AVG Business Edition 사용자 설명서를 참조하십시오. 이 설명서는 AVG 웹 사이트 (<http://www.avg.com/>)에서 다운로드할 수 있습니다.

이 설명서에서 [구성 요소 개요](#) 장을 참조하십시오. 소프트웨어 공급업체에서 사전 설정한 기본 구성으로 되돌리려면 [기본값](#) 단추를 사용하십시오.

제어 단추

이 대화 상자에서는 다음과 같은 제어 단추를 사용할 수 있습니다.

- **지금 다시 시작(권장)** - AVG Internet Security 2012 설치 프로세스를 완료하려면 컴퓨터를 다시 시작해야 합니다. 즉시 컴퓨터를 다시 시작하는 것이 좋습니다. 컴퓨터를 다시 시작해야만 **AVG Internet Security 2012**가 완전하게 설치되어 안전하게 보호를 받을 수 있습니다.
- **나중에 다시 시작** - 특별한 이유로 즉시 컴퓨터를 다시 시작할 수 없는 경우, 나중에 다시 시작하도록 연기할 수 있습니다. 그러나 컴퓨터를 즉시 다시 시작하는 것이 좋습니다. 컴퓨터를 다시 시작해야만 **AVG Internet Security 2012**를 사용하여 컴퓨터를 완전하게 보호할 수 있습니다.



4. 설치 후 작업

4.1. 제품 등록

AVG Internet Security 2012 설치를 마친 후에는 AVG 웹 사이트 (<http://www.avg.com/>) 에서 제품을 온라인으로 등록하십시오. 등록이 끝나면 AVG 사용자 계정, AVG 업데이트 뉴스레터 및 등록된 사용자에게만 제공되는 기타 서비스를 모두 이용할 수 있습니다.

AVG Internet Security 2012 사용자 인터페이스에서 직접 등록하는 방법이 가장 간단합니다. 기본 메뉴에서 [도움말/지금 등록](#) 항목을 선택하십시오. AVG 웹 사이트 (<http://www.avg.com/>) 의 [등록](#) 페이지로 이동합니다. 이 페이지의 지침을 따르십시오.

4.2. 사용자 인터페이스 액세스

[AVG 기본 대화 상자](#)는 다음과 같은 여러 가지 방법으로 액세스할 수 있습니다.

- [AVG 시스템 트레이 아이콘](#) 두 번 클릭
- 바탕 화면에서 AVG 아이콘 두 번 클릭
- [AVG 가젯](#) ([설치되어 있는 경우](#), Windows Vista/Windows 7 에서 지원됨)의 하단 섹션에 있는 상태 표시줄 두 번 클릭
- **시작/프로그램/AVG 2012/AVG 사용자 인터페이스 메뉴에서 액세스**

4.3. 전체 컴퓨터 스캔

AVG Internet Security 2012 설치 전에 컴퓨터 바이러스가 이미 사용자 컴퓨터에 전송되었을 위험이 있습니다. 따라서 [전체 컴퓨터 스캔](#)을 실행하여 사용자 PC가 감염되지 않았는지 확인해야 합니다.

[전체 컴퓨터 스캔](#) 실행 지침은 [AVG 스캔](#) 장을 참조하십시오.

4.4. EICAR 테스트

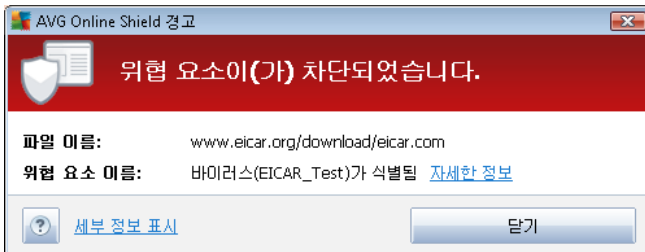
EICAR 테스트를 실행하면 AVG Internet Security 2012 제품이 올바르게 설치되었는지 확인할 수 있습니다.

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.

eicar.com 파일을 다운로드하고 로컬 디스크에 저장합니다. 테스트 파일 다운로드를 확인하는 즉시 [Online Shield](#) ([Link Scanner](#) 구성 요소에 포함되어 있음)가 이에 반응하여 경고를 표시합니다. 이 알림은 AVG가 사용자 컴퓨터에 올바르게 설치되었는지 여부를 표시



합니다.



<http://www.eicar.com> 웹 사이트에서 압축된 버전의 EICAR '바이러스'(예: *eicar_com.zip* 형식)를 다운로드할 수도 있습니다. [Online Shield](#) 를 사용하면 이 파일을 다운로드하여 로컬 디스크에 저장할 수 있지만, 파일 압축을 풀려고 할 때 [Resident Shield](#) ([Anti-Virus](#) 구성 요소에 포함되어 있음)에서 해당 파일을 '바이러스'로 검색합니다.

AVG가 EICAR 테스트 파일을 바이러스로 식별하는 데 실패할 경우 프로그램 구성을 다시 확인해야 합니다.

4.5. AVG 기본 구성

AVG Internet Security 2012 의 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.

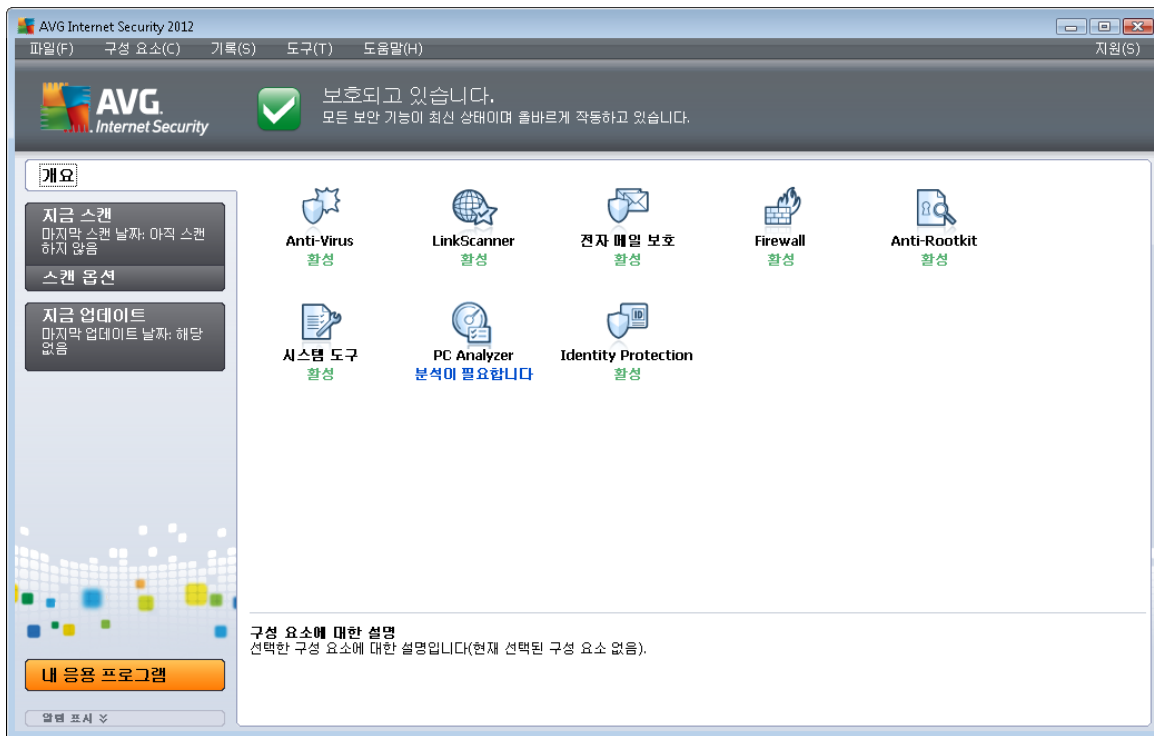
특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다.

[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.



5. AVG 사용자 인터페이스

AVG Internet Security 2012 는 기본 창으로 열립니다.



기본 창은 여러 섹션으로 나뉩니다.

- **시스템 메뉴**(창의 상단 시스템 줄)는 AVG Internet Security 2012의 모든 구성 요소, 서비스 및 기능에 액세스할 수 있는 표준 탐색 메뉴입니다. [세부 정보 >>](#)
- **보안 상태 정보**(창의 상단 섹션)에는 AVG Internet Security 2012의 현재 상태에 대한 정보가 나와 있습니다. [세부 정보 >>](#)
- **빠른 링크**(창의 왼쪽 섹션)에서는 AVG Internet Security 2012의 가장 중요하고 자주 사용하는 작업에 빠르게 액세스할 수 있습니다. [세부 정보 >>](#)
- **내 응용 프로그램**(창의 왼쪽 하단 섹션)은 AVG Internet Security 2012에 사용할 수 있는 추가적인 응용 프로그램인 [LiveKive](#), [Family Safety](#) 및 [PC Tuneup](#)
- **구성 요소 개요**(창의 중앙 섹션)에서는 AVG Internet Security 2012 내에 설치된 모든 구성 요소에 대한 개요를 제공합니다. [세부 정보 >>](#)
- **시스템 트레이 아이콘**(모니터의 오른쪽 아래 모서리, 시스템 트레이에 위치)은 AVG Internet Security 2012의 현재 상태를 보여 줍니다. [세부 정보 >>](#)
- **AVG 가젯**(Windows Vista/7 에서 지원되는 Windows 사이드바)을 사용하면 AVG Internet Security 2012 내에서 스캔 및 업데이트에 빠르게 액세스할 수 있습니다. [세부 정보 >>](#)



5.1. 시스템 메뉴

시스템 메뉴는 모든 Windows 응용 프로그램에서 사용되는 표준 탐색 메뉴입니다. **AVG Internet Security 2012** 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.

5.1.1. 파일

- **끝내기** - **AVG Internet Security 2012**의 사용자 인터페이스를 닫습니다. 그러나 AVG 응용 프로그램은 백그라운드에서 계속 실행되며 사용자 컴퓨터도 지속적으로 보호됩니다.

5.1.2. 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**는 시스템 내의 바이러스, 스파이웨어, 웜, 트로이 목마, 원치 않는 실행 파일 또는 라이브러리를 검색하여 악의적인 애드웨어로부터 사용자를 보호합니다. [세부 정보 >>](#)
- **LinkScanner**는 사용자가 인터넷을 검색 및 탐색하는 동안 웹 기반의 공격으로부터 사용자를 보호합니다. [세부 정보 >>](#)
- **전자 메일 보호**는 들어오는 전자 메일 메시지에서 스팸을 검사하고 바이러스, 피싱 공격 또는 기타 위협 요소를 차단합니다. [세부 정보 >>](#)
- **Firewall**은 각 네트워크 포트에서 모든 커뮤니케이션을 제어하여 악의적인 공격으로부터 사용자를 보호하고 모든 침입 시도를 차단합니다. [세부 정보 >>](#)
- **Anti-Rootkit**은 응용 프로그램, 드라이버 또는 라이브러리 내부에 숨어 있는 위험한 루트킷을 스캔합니다. [세부 정보 >>](#)
- **시스템 도구**는 AVG 환경에 대한 자세한 요약 정보와 운영 체제 정보를 제공합니다. [세부 정보 >>](#)
- **PC Analyzer** 분석기에서는 사용자 컴퓨터 상태에 대한 정보를 제공합니다. [세부 정보 >>](#)
- **Identity Protection**은 알려지지 않은 새로운 위협으로부터 사용자의 디지털 자산을 지속적으로 보호합니다. [세부 정보 >>](#)
- **Security Toolbar**는 인터넷 브라우저에서 선택한 AVG 기능을 바로 이용할 수 있도록 해줍니다. [세부 정보 >>](#)



- **원격 관리**는 [설치 프로세스](#)에서 이 구성 요소를 설치하도록 지정한 경우에 한해 AVG Business Edition에 표시됩니다.

5.1.3. 기록

- [스캔 결과](#) - AVG 테스트 인터페이스의 [스캔 결과 개요](#) 대화 상자로 전환합니다.
- [Resident Shield 검색](#) - [Resident Shield](#)에서 검색한 위협 요소에 대한 개요가 있는 대화 상자를 엽니다.
- [E-mail Scanner 검색](#) - [전자 메일 보호](#) 구성 요소에서 위협 요소로 검색한 전자 메일 메시지 첨부 파일에 대한 개요가 있는 대화 상자를 엽니다.
- [Online Shield 검색 결과](#) - [LinkScanner](#) 구성 요소 내의 [Online Shield](#) 서비스에서 검색한 위협 요소에 대한 개요가 있는 대화 상자를 엽니다.
- [바이러스 저장소](#) - 발견된 감염 중 자동으로 치료되지 않는 감염을 모두 제거하는 검역소 공간([바이러스 저장소](#))의 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 Internet Security 2012** 작업에 대한 개요가 있는 기록 로그 인터페이스를 엽니다.
- [Firewall](#) - 모든 Firewall 작업에 대한 상세한 개요가 있는 [로그](#) 탭에서 Firewall 설정 인터페이스를 엽니다.

5.1.4. 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 **AVG Internet Security 2012** 업데이트 프로세스를 실행합니다.
- [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 Internet Security 2012 구성을 편집할 수 있습니다. 일반적으로 소프트웨어 공급업체가 정의한 응용 프로그램의 기본 설정을 유지하는 것이 좋습니다.
- [Firewall 설정...](#) - [Firewall](#) 구성 요소의 고급 구성에 대한 독립 실행형 대화 상자가



열립니다.

5.1.5. 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 업그레이드 하는 경우)할 라이선스 번호를 입력할 수 있습니다.
- **지금 등록** - AVG 웹 사이트 (<http://www.avg.com/>)의 등록 페이지에 연결합니다. 등록 데이터를 입력하십시오. AVG 제품을 등록하는 고객만 무료 기술 지원을 받을 수 있습니다.

참고: AVG Internet Security 2012 평가판을 사용 중인 경우에는 마지막 두 항목이 **지금 구매** 및 **활성화**로 표시되기 때문에 프로그램의 정식 버전을 즉시 구매할 수 있습니다. 판매 번호를 사용하여 설치된 AVG Internet Security 2012의 경우에는 두 항목이 **등록** 및 **활성화**로 표시됩니다.

- **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.

5.1.6. 지원

지원 링크를 누르면 도움말 탐색 시 필요한 모든 정보 유형이 나와 있는 새로운 **정보** 대화 상자가 열립니다. 대화 상자에는 설치된 AVG 프로그램에 대한 기본 데이터 (**프로그램/데이터베이스 버전**), 라이선스 세부 정보 및 빠른 지원 링크 목록이 포함되어 있습니다.

정보 대화 상자는 다음과 같은 여섯 개의 탭으로 나뉩니다.



버전 탭은 다음과 같은 세 개의 섹션으로 나뉘어 있습니다.



- **지원 정보** - AVG Internet Security 2012 버전, 바이러스 데이터베이스 버전, [Anti-Spam](#) 데이터베이스 버전 및 [LinkScanner](#) 버전에 대한 정보를 제공합니다.
- **사용자 정보** - 라이선스가 있는 사용자 및 회사에 대한 정보를 제공합니다.
- **라이선스 세부 정보** - 라이선스에 대한 정보(제품 이름, 라이선스 유형, 라이선스 번호, 만료 날짜 및 허용된 사용자 수)를 제공합니다. 이 섹션에서는 [등록](#) 링크를 사용하여 온라인으로 **AVG Internet Security 2012** 프로그램을 등록할 수도 있으며, 이를 통해 [AVG 기술 지원](#)을 최대한 활용할 수 있습니다. 또한 [다시 활성화](#) 링크를 사용하여 **AVG 활성화** 대화 상자를 열 수도 있습니다. 이 대화 상자에서는 라이선스 번호를 해당 필드에 입력하여 판매 번호(AVG Internet Security 2012 설치 중에 사용된 판매 번호)를 바꾸거나 현재 라이선스 번호를 변경할 수 있습니다(예: 상위 AVG 제품으로 업그레이드할 경우).



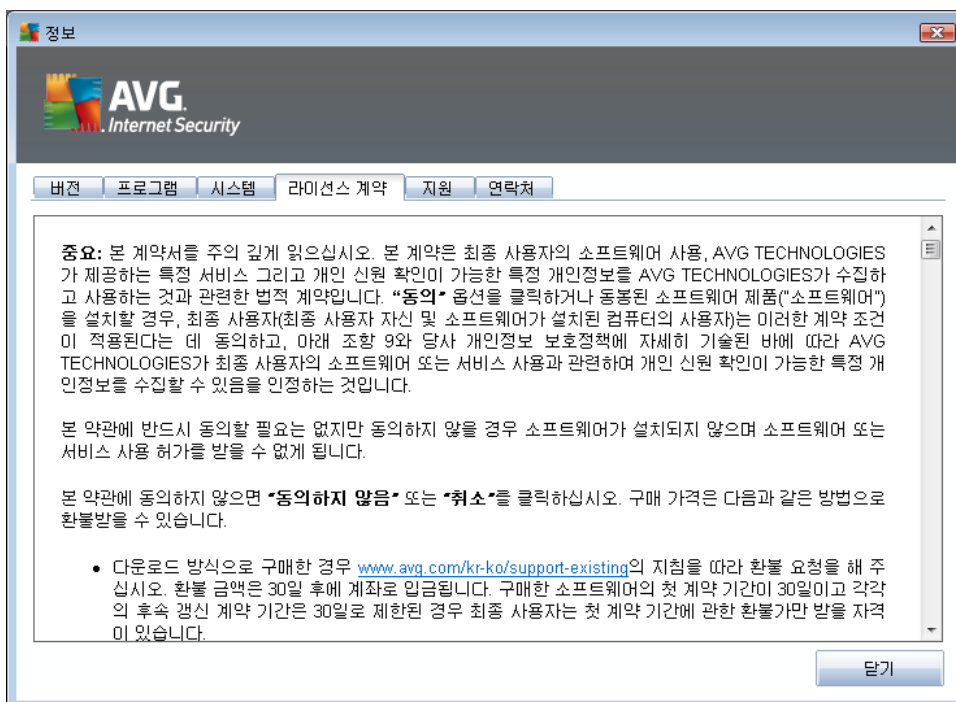
프로그램 탭에서는 **AVG Internet Security 2012** 프로그램 파일 버전 및 이 제품에 사용된 타사 코드에 대한 정보를 확인할 수 있습니다.



시스템 탭에는 운영 체제(프로세서 유형, 운영 체제 및 해당 버전, 빌드 번호, 사용된 서비스 팩, 총 메모리 크기 및 여유 메모리 크기)에 대한 매개 변수 목록이 포함되어 있습니다.



라이선스 계약 탭에서는 사용자와 AVG Technologies 사이의 라이선스 계약 전문을 읽을 수 있습니다.





지 원 탭에는 고객 지원에 문의할 수 있는 모든 옵션 목록이 표시됩니다. 또한 AVG 웹 사이트 (<http://www.avg.com/>), AVG 포럼, FAQ 등에 대한 링크를 제공하며, 고객 지원 팀에 문의할 때 사용할 수 있는 정보도 확인할 수 있습니다.





연락처 탭은 AVG Technologies 의 모든 연락처 목록과 AVG 지역 담당자 및 대리점에 대한 연락처를 제공합니다.



5.2. 보안 상태 정보

보안 상태 정보 섹션은 **AVG Internet Security 2012** 기본 창의 위쪽 부분에 있습니다. 이 섹션 내에서 사용자는 언제든지 **AVG Internet Security 2012** 의 현재 보안 상태에 대한 정보를 확인할 수 있습니다. 이 섹션에 표시되는 아이콘 및 그 의미에 대한 개괄적인 설명을 참조하십시오.



- 녹색 아이콘은 **AVG Internet Security 2012 프로그램이 완전하게 작동하고 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 살펴봐야 합니다. **AVG Internet Security 2012** 에 심각한 문제가 없으며 특별한 이유로 사용자가 일부 구성 요소의 설정을 해제했을 수 있습니다. 컴퓨터는 여전히 AVG 의 보호를 받습니다. 하지만 문제된 구성 요소의 설정을 살펴보기 바랍니다. 해당 구성 요소의 이름은 **보안 상태 정보** 섹션에서 확인할 수 있습니다.

주황색 아이콘은 어떤 이유로 사용자가 구성 요소의 오류 상태를 무시하기로 결정했을 때에도 나타날 수 있습니다. **구성 요소 상태 무시** 옵션은 **AVG Internet**



Security 2012 기본 창의 [구성 요소 개요](#)에 있는 해당 구성 요소의 아이콘을 마우스 오른쪽 단추로 클릭할 때 열리는 상황에 맞는 메뉴에서 사용할 수 있습니다. 이 옵션은 구성 요소 오류 상태를 알고 있지만 특정한 이유로 **AVG Internet Security 2012** 상태를 그대로 유지하고 [시스템 트레이 아이콘](#)으로 경고를 표시하지 않으려고 할 때 선택합니다. 이 옵션을 사용할 필요가 있는 경우가 있을 수 있지만 가능하면 빨리 **구성 요소 상태 무시** 옵션의 설정을 해제하는 것이 좋습니다.



- 빨간색 아이콘은 **AVG Internet Security 2012 프로그램이 심각한 상태에 있음을 나타냅니다**. 하나 이상의 구성 요소가 올바르게 작동하지 않으므로 **AVG Internet Security 2012** 프로그램이 컴퓨터를 보호할 수 없습니다. 보고된 문제의 해결 방법을 즉시 확인하시기 바랍니다. 오류를 스스로 해결할 수 없다면 [AVG 기술 지원](#) 팀에 문의하십시오.

AVG Internet Security 2012 프로그램이 최적의 성능으로 설정되어 있지 않은 경우 수정(또는 이러한 문제가 둘 이상의 구성 요소와 관련이 있는 경우 모두 수정)이라는 새로운 단추가 보안 상태 정보 옆에 표시됩니다. 이 단추를 누르면 자동으로 수행되는 프로그램 체크아웃 및 구성 프로세스가 시작됩니다. 이 방법을 사용하면 간편하게 AVG Internet Security 2012 프로그램의 성능을 최적화하고 보안 수준을 극대화할 수 있습니다.

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

참고: AVG Internet Security 2012 상태 정보는 [시스템 트레이 아이콘](#)에서도 언제든지 확인할 수 있습니다.

5.3. 빠른 링크

빠른 링크는 **AVG Internet Security 2012 사용자 인터페이스**의 왼쪽에 있습니다. 이 링크를 사용하면 가장 중요하고 자주 사용하는 응용 프로그램 기능(예: 스캔 및 업데이트)에 즉시 액세스할 수 있습니다. 빠른 링크는 다음과 같은 사용자 인터페이스의 모든 대화 상자에서 액세스할 수 있습니다.



빠른 링크는 그래픽상에서 다음과 같은 세 개의 섹션으로 나뉩니다.

- **개요** - 이 링크를 사용하면 현재 열려 있는 AVG 대화 상자가 [설치된 모든 구성 요소의 개요](#)가 표시된 기본 창으로 전환됩니다. 자세한 내용은 [구성 요소 개요](#) 장을 참조하십시오.



- **지금 스캔** - 기본적으로 이 단추는 마지막으로 실행된 스캔에 대한 정보(예: 스캔 유형, 마지막 실행일)를 제공합니다. **지금 스캔** 명령을 클릭하여 동일한 스캔을 다시 실행하십시오. 다른 스캔을 실행하려면 **스캔 옵션** 링크를 클릭하십시오. 이렇게 하면 [AVG 스캔 인터페이스](#)가 열려 스캔을 예약 및 실행하거나 해당 매개 변수를 편집할 수 있습니다. 자세한 내용은 [AVG 스캔](#) 장을 참조하십시오.
- **지금 업데이트** - 이 링크는 [업데이트](#)를 마지막으로 실행한 날짜와 시간을 제공합니다. 이 단추를 누르면 업데이트 프로세스가 즉시 실행되고 해당 프로세스의 진행률이 표시됩니다. 자세한 내용은 [AVG 업데이트](#) 장을 참조하십시오.

빠른 링크는 [AVG 사용자 인터페이스](#)에서 언제든지 액세스할 수 있습니다. 빠른 링크를 사용하여 스캔이나 업데이트 같은 특정 프로세스를 실행할 경우 새로운 대화 상자로 전환되지만 빠른 링크는 화면에 계속 표시됩니다. 또한 실행되는 프로세스가 탐색 패널에 그래픽으로 표시되므로 **AVG Internet Security 2012**에서 실행되는 모든 프로세스를 완전하게 제어할 수 있습니다.

5.4. 구성 요소 개요

구성 요소 개요 섹션

구성 요소 개요 섹션은 **AVG Internet Security 2012** [사용자 인터페이스](#)의 가운데 부분에 있습니다. 이 섹션은 다음 두 부분으로 나뉩니다.

- **설치된 모든 구성 요소에 대한 개요**에는 설치된 모든 구성 요소의 그래픽 패널이 나와 있습니다. 각 패널은 해당 구성 요소의 아이콘으로 레이블이 지정되어 있으며 각 구성 요소가 해당 시점에 활성 상태인지 비활성 상태인지에 대한 정보를 제공합니다.
- **구성 요소에 대한 설명**이 이 대화 상자의 아래쪽에 있습니다. 이 설명에는 구성 요소의 기본 기능이 간략하게 설명되어 있습니다. 또한 선택된 구성 요소의 현재 상태에 대한 정보가 제공됩니다.

설치된 구성 요소의 목록

AVG Internet Security 2012의 **구성 요소 개요** 섹션에는 다음 구성 요소에 대한 정보가 포함되어 있습니다.

- **Anti-Virus**는 시스템 내의 바이러스, 스파이웨어, 웜, 트로이 목마, 원치 않는 실행 파일 또는 라이브러리를 검색하여 악의적인 애드웨어로부터 사용자를 보호합니다. [세부 정보 >>](#)
- **LinkScanner**는 사용자가 인터넷을 검색 및 탐색하는 동안 웹 기반의 공격으로부터 사용자를 보호합니다. [세부 정보 >>](#)
- **전자 메일 보호**는 들어오는 전자 메일 메시지에서 스팸을 검사하고 바이러스, 피싱 공격 또는 기타 위협 요소를 차단합니다. [세부 정보 >>](#)
- **Firewall**은 각 네트워크 포트에서 모든 커뮤니케이션을 제어하여 악의적인 공격



으로부터 사용자를 보호하고 모든 침입 시도를 차단합니다. [세부 정보 >>](#)

- **Anti-Rootkit** 은 응용 프로그램, 드라이버 또는 라이브러리 내부에 숨어 있는 위험한 루트킷을 스캔합니다. [세부 정보 >>](#)
- **시스템 도구**는 AVG 환경에 대한 자세한 요약 정보와 운영 체제 정보를 제공합니다. [세부 정보 >>](#)
- **PC Analyzer** 분석기에서는 사용자 컴퓨터 상태에 대한 정보를 제공합니다. [세부 정보 >>](#)
- **Identity Protection** 은 알려지지 않은 새로운 위협으로부터 사용자의 디지털 자산을 지속적으로 보호합니다. [세부 정보 >>](#)
- **Security Toolbar** 는 인터넷 브라우저에서 선택한 AVG 기능을 바로 이용할 수 있도록 해줍니다. [세부 정보 >>](#)
- **원격 관리**는 [설치 프로세스](#)에서 이 구성 요소를 설치하도록 지정한 경우에 한해 AVG Business Edition에 표시됩니다.

액세스 가능한 작업

- **마우스를 구성 요소 아이콘으로 이동**하여 구성 요소 개요 내에서 해당 구성 요소를 강조 표시할 수 있습니다. 이와 동시에 구성 요소의 기본 기능 설명이 [사용자 인터페이스](#)의 아래쪽에 표시됩니다.
- **구성 요소의 아이콘을 한 번 클릭**하여 기본 통계 데이터 목록이 있는 구성 요소 자체의 인터페이스를 열 수 있습니다.
- **구성 요소의 아이콘을 마우스 오른쪽 단추로 클릭**하여 여러 옵션이 포함된 상황에 맞는 메뉴를 확장할 수 있습니다.
 - **열기** - 구성 요소 자체의 대화 상자를 열려면 이 옵션을 클릭합니다(구성 요소 아이콘을 한 번 클릭하는 것과 같음).
 - **이 구성 요소의 상태 무시** - [구성 요소의 오류 상태](#)를 알고 있지만 특정한 이유 때문에 이 상태를 유지하면서 [시스템 트레이 아이콘](#)으로 경고를 표시하지 않으려면 이 옵션을 선택합니다.
 - **고급 설정에서 열기...** - 이 옵션은 [고급 설정](#)이 가능한 일부 구성 요소에만 사용할 수 있습니다.

5.5. 시스템 트레이 아이콘

AVG 시스템 트레이 아이콘(Windows 작업 표시줄에서 모니터 오른쪽 아래에 위치)은 AVG Internet Security 2012의 현재 상태를 나타냅니다. **AVG Internet Security 2012의 사용자 인터페이스**가 열려 있을 때는 물론이고 닫혀 있더라도 시스템 트레이에 항상 표시됩니다.

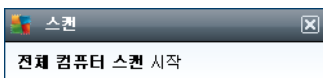


AVG 시스템 트레이 아이콘 표시

- 추가된 요소 없이 여러 가지 색으로 표시된 색상의 경우 아이콘은 모든 **AVG Internet Security 2012** 구성 요소가 활성 상태이며 완벽하게 작동하고 있음을 나타냅니다. 하지만 구성 요소 중 하나가 완벽하게 작동하지 않는데 사용자가 [구성 요소 상태를 무시하도록](#) 결정한 경우에도 이 아이콘이 표시될 수 있습니다. 구성 요소 상태 무시 옵션을 확인하면 사용자가 [구성 요소 오류 상태](#)를 파악하고 있지만 특정한 이유로 이 설정을 유지하여 이러한 상황에 대한 알림을 받지 않을 것임을 나타낼 수 있습니다.
- 느낌표가 있는 아이콘은 구성 요소가 [오류 상태](#)임을 나타냅니다. 항상 이러한 경고에 주의하여 제대로 설치되지 않은 구성 요소의 구성 문제를 제거하십시오. 구성 요소의 구성을 변경하려면 시스템 트레이 아이콘을 두 번 클릭하여 [응용 프로그램 사용자 인터페이스](#)를 엽니다. [오류 상태](#)의 구성 요소에 대한 자세한 내용은 [보안 상태 정보](#) 섹션을 참조하십시오.
- 또한 시스템 트레이 아이콘은 여러 가지 색으로 표시될 수 있으며 광선이 깜박이면서 회전합니다. 이 그래픽 버전은 현재 업데이트 프로세스가 시작되었음을 나타냅니다.
- 화살표가 있는 여러 가지 색으로 표시된 다른 표시 아이콘은 **AVG Internet Security 2012** 스캔이 실행 중임을 의미합니다.

AVG 시스템 트레이 아이콘 정보

AVG 시스템 트레이 아이콘은 **AVG Internet Security 2012**의 현재 작업에 대한 정보와 프로그램의 상태 변경 현황(예: 예약된 스캔 또는 업데이트의 자동 시작, Firewall 프로파일 전환, 구성 요소의 상태 변화, 오류 상태 발생 등)을 시스템 트레이 아이콘에서 열리는 팝업창을 통해 상세하게 알려 줍니다.



AVG 시스템 트레이 아이콘에서 액세스할 수 있는 작업



또한 아이콘을 두 번 클릭하면 **AVG 시스템 트레이 아이콘**을 통해 **AVG Internet Security 2012**의 [사용자 인터페이스](#)에 빠르게 액세스할 수 있습니다. 아이콘을 마우스 오른쪽 단추로 클릭하면 다음과 같은 옵션이 있는 간략한 상황에 맞는 메뉴가 열립니다.

- **AVG 사용자 인터페이스 열기** - 클릭하면 **AVG Internet Security 2012**의 [사용자 인터페이스](#)가 열립니다.
- **스캔** - 클릭하면 [미리 정의된 스캔](#)([전체 컴퓨터 스캔](#), [특정 파일 또는 폴더 스캔](#), [Anti-Rootkit 스캔](#))의 상황에 맞는 메뉴가 열리고, 필요한 스캔을 선택하면 즉시 시작됩니다.
- **Firewall** - [Firewall](#) 설정 옵션의 상황에 맞는 메뉴를 열려면 클릭합니다. 여기에서 [Firewall 상태](#)([Firewall 사용](#)/[Firewall 사용 안 함](#)/[긴급 모드](#)), [게임 모드 전환](#) 및 [Firewall 프로필](#)과 같은 주요 매개 변수를 편집할 수 있습니다.
- **PC Analyzer 실행** - 클릭하면 [PC Analyzer](#) 구성 요소가 시작됩니다.
- **스캔 실행 중** - 현재 컴퓨터에서 스캔이 실행되고 있는 경우에만 이 항목이 표시됩니다. 이러한 스캔의 경우 스캔 우선 순위를 설정하거나 실행 중인 스캔을 중지 또는 일시 중지할 수 있습니다. 또한 [모든 스캔에 대한 우선 순위 설정](#), [모든 스캔 일시 중지](#) 또는 [모든 스캔 중지](#) 등의 작업에도 액세스할 수 있습니다.
- **지금 업데이트** - 즉시 [업데이트](#)를 시작합니다.
- **도움말** - 시작 페이지에서 도움말 파일을 엽니다.

5.6. AVG 가젯

AVG 가젯은 Windows 바탕 화면(*Windows 사이드바*)에 표시됩니다. 이 응용 프로그램은 Windows Vista 및 Windows 7 운영 체제에서만 지원됩니다. **AVG 가젯**은 가장 중요한 **AVG Internet Security 2012** 기능(예: [스캔](#) 및 [업데이트](#))에 대한 즉각적인 액세스를 제공합니다.



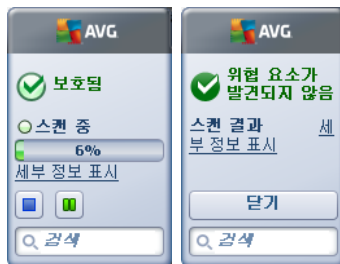
스캔 및 업데이트에 대한 빠른 액세스

필요한 경우 **AVG 가젯**에서는 스캔 또는 업데이트를 즉시 시작할 수 있습니다.

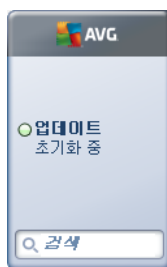
- **지금 스캔** - **지금 스캔** 링크를 클릭하여 [전체 컴퓨터 스캔](#)을 바로 시작할 수 있습니다. 가젯의 대체 사용자 인터페이스를 사용하는 경우 해당 인터페이스에서 스캔 프로세스의 진행률을 확인할 수 있습니다. 간략한 통계 개요에 스캔된 개체, 검색된 위협 요소 및 치료된 위협 요소의 수에 대한 정보가 표시됩니다. 스캔하는



동안 언제든지 스캔 프로세스를 일시 중지() 또는 중지()할 수 있습니다. 스캔 결과와 관련된 자세한 데이터를 보려면 표준 [스캔 결과 개요](#) 대화 상자를 확인하십시오. 이 대화 상자는 **세부 정보 표시** 옵션을 통해 가젯에서 바로 열 수 있습니다. 해당 스캔 결과는 사이드바 가젯 스캔 아래에 표시됩니다.



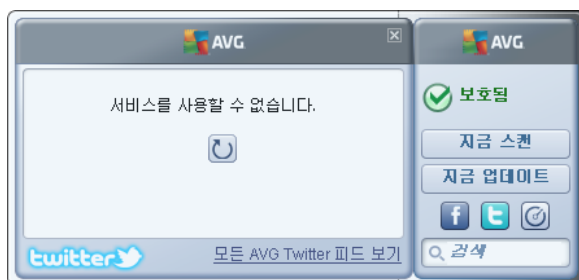
- **지금 업데이트 - 지금 업데이트** AVG Internet Security 2012 링크를 클릭하여 가젯에서 바로 업데이트를 실행할 수 있습니다.



소셜 네트워크 액세스

AVG 가젯에서는 또한 사용자를 주요 소셜 네트워크에 연결하는 빠른 링크를 제공합니다. 각 단추를 사용하여 Twitter, Facebook 또는 LinkedIn의 AVG 커뮤니티에 연결할 수 있습니다.

- **Twitter 링크** - Twitter에 게시된 최신 AVG 피드에 대한 개요를 제공하는 **AVG 가젯**을 새로 엽니다. 새 창에서 인터넷 브라우저를 열려면 **모든 AVG Twitter 피드 보기** 링크를 따르십시오. 그러면 Twitter 웹 사이트에서 AVG 관련 뉴스가 표시되는 페이지로 바로 리디렉션됩니다.



- **Facebook 링크** - 인터넷 브라우저에서 Facebook 웹 사이트의 **AVG 커뮤니티**



페이지를 엽니다.

- **LinkedIn**  - 이 옵션은 네트워크 설치(즉, *AVG Business Edition 라이선스 중 하나를 사용하여 AVG를 설치한 경우*)에서만 사용할 수 있으며 LinkedIn 소셜 네트워크의 **AVG SMB Community** 웹 사이트에서 인터넷 브라우저를 엽니다.

가젯을 통해 액세스할 수 있는 기타 기능

- **PC Analyzer**  - [PC Analyzer](#) 구성 요소의 사용자 인터페이스를 엽니다.
- **검색 상자** - 키워드를 입력하면 기본 웹 브라우저에서 새로 열리는 창으로 검색 결과를 즉시 확인할 수 있습니다.



6. AVG 구성 요소

6.1. Anti-Virus

Anti-Virus 구성 요소는 **AVG Internet Security 2012**의 기초가 되며 보안 프로그램의 여러 기본 기능을 결합하여 사용합니다.

- [스캔 엔진](#)
- [Resident Shield](#)
- [Anti-Spyware 보호](#)

6.1.1. 스캔 엔진

Anti-Virus 구성 요소의 기반이 되는 스캔 엔진은 모든 파일 및 파일 활동(*파일 열기/닫기* 등)에서 알려진 바이러스를 스캔합니다. 발견된 모든 바이러스는 활동할 수 없도록 차단한 후 치료하거나 [바이러스 저장소](#)에 격리합니다.

AVG Internet Security 2012 보호의 중요한 기능은 알려진 바이러스가 컴퓨터에서 실행되지 못하게 하는 것입니다.

검색 방법

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. **Anti-Virus**는 다음과 같은 검색 방법을 사용합니다.

- **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.

단일 기술만으로는 바이러스를 검색하거나 식별하기 어려운 경우 **Anti-Virus**는 다음과 같은 여러 기술을 함께 사용하여 사용자의 컴퓨터를 바이러스로부터 보호합니다. **AVG Internet Security 2012** 프로그램은 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 **AVG Internet Security 2012** 프로그램은 시스템 레지스트리에서 의심스러운 항목, 임시 인터넷 파일 및 추적 쿠키를 스캔하여 다른 감염과 같은 방법으로 잠재적으로 해로운 항목을 모두 처리할 수 있도록 합니다.

AVG Internet Security 2012 프로그램은 컴퓨터를 지속적으로 보호합니다.



6.1.2. Resident Shield

AVG Internet Security 2012에서는 Resident Shield라는 방식으로 지속적인 보호 기능을 제공합니다. **Anti-Virus** 구성 요소는 열려 있거나 저장 또는 복사된 모든 단일 파일을 스캔합니다(특정 확장명의 파일이나 확장명에 상관없이 파일 스캔). 또한 컴퓨터의 시스템 영역과 플래시 디스크와 같은 이동식 미디어를 보호합니다. 액세스한 파일에서 바이러스가 발견되면 현재 수행 중인 작업을 중단하여 해당 바이러스가 활성화되지 않도록 합니다. Resident Shield 기능은 "백그라운드"로 실행되므로 사용자는 대개 프로세스를 인지하지 못하며 위협 요소가 발견될 경우에만 알림을 받게 됩니다. 이때 **Anti-Virus**를 통해 위협 요소의 활성화가 차단되고 위협 요소가 제거됩니다.

Resident Shield는 컴퓨터가 시작되는 동안 메모리에 로드되고 항상 실행됩니다.

6.1.3. Anti-Spyware 보호

Anti-Spyware는 알려진 유형의 스파이웨어 정의를 식별하는 데 사용되는 스파이웨어 데이터베이스로 구성됩니다. AVG 스파이웨어 전문가들은 최신 스파이웨어 패턴이 출현하면 이를 바로 식별하여 기술한 다음 이에 대한 정의를 이 데이터베이스에 추가합니다. 업데이트 프로세스를 통해 이러한 새 정의가 사용자 컴퓨터에 다운로드되므로 사용자는 최신 스파이웨어 유형으로부터 항상 신뢰할 만한 보호를 받을 수 있습니다. **Anti-Spyware**를 사용하면 사용자 컴퓨터에 맬웨어/스파이웨어가 있는지 완전하게 스캔할 수 있습니다. 또한 다운로드되었으나 아직 활성화되지 않은 맬웨어와 같이 대기 중인 비활성 맬웨어도 검색할 수 있습니다.

스파이웨어란?

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 효과적으로 보호할 수 있는 방법은 항상 켜져 있는 백그라운드 스캐너인 **Anti-Spyware**를 사용하는 것입니다. Anti-Spyware는 Resident Shield처럼 작동하여 실행되는 응용 프로그램을 백그라운드에서 스캔합니다.



6.1.4. Anti-Virus 인터페이스

Anti-Virus 구성 요소의 인터페이스는 구성 요소의 기능에 대한 간략한 정보, 구성 요소의 현재 상태(활성)에 대한 정보 및 구성 요소의 기본 구성 옵션을 제공합니다.



구성 옵션

이 대화 상자에서는 **Anti-Virus** 구성 요소 내에서 사용할 수 있는 기능의 몇 가지 기본 구성 옵션을 제공합니다. 다음은 이러한 옵션에 대한 간략한 설명입니다.

- **AVG 에서 보호를 적용한 방식에 대한 온라인 보고서 보기** - 이 링크는 사용자를 AVG 웹 사이트 (<http://www.avg.com/>)의 특정 페이지로 리디렉션합니다. 이 페이지에는 지정된 기간 동안 사용자 컴퓨터에서 수행된 모든 **AVG Internet Security 2012** 활동에 대한 상세한 통계 개요가 포괄적으로 표시됩니다.
- **Resident Shield 사용** - 이 옵션을 사용하면 Resident Shield 를 간편하게 설정하거나 해제할 수 있습니다. Resident Shield 는 파일을 복사하거나 열거나 저장할 때 파일을 스캔합니다. 바이러스나 다른 종류의 위협 요소가 발견되는 즉시 경고가 표시됩니다. 기본적으로 이 기능은 설정되어 있으며 이를 그대로 유지하는 것이 좋습니다. Resident Shield 를 설정한 상태에서 발견될 감염의 처리 방법을 결정할 수 있습니다.
 - **모든 위협 요소 자동 제거/위협 요소 제거 전 확인** - 이들 옵션 중 하나를 선택합니다. 이 옵션은 보안 수준에 영향을 미치지 않으며 사용자의 선호도만을 반영합니다.

- **추적 쿠키 스캔** - 이전 옵션과는 독립적으로 추적 쿠키를 스캔할 것인지를 결정할 수 있습니다. (쿠키는 서버가 웹 브라우저로 전송한 후 다시 브라우저가 해당 서버에 액세스할 때마다 변경되지 않은 상태 그대로 반환하는 텍스트 꾸러미입니다. HTTP 쿠키는 사이트 기본 설정이나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 정보를 인증하고, 추적하고, 유지 관리하는 데 사용됩니다.) 이 옵션은 기본적으로 해제되어 있지만 특별한 경우에는 설정하여 보안 수준을 극대화할 수 있습니다.
- **인스턴트 메시징 보호 사용** - 인스턴트 메시징 커뮤니케이션(예: ICQ, MSN Messenger 등)에 바이러스가 없는지 확인하려면 이 항목을 선택합니다.
- **고급 설정...** - AVG Internet Security 2012의 [고급 설정](#) 내에 있는 각 대화 상자로 리디렉션하려면 이 링크를 클릭합니다. 해당 대화 상자에서 구성 요소의 구성을 세부적으로 편집할 수 있습니다. 하지만 모든 구성 요소의 기본 구성이 **AVG Internet Security 2012**의 성능을 최적화하고 보안을 극대화하도록 설정되어 있다는 점에 유의하십시오. 따라서 이러한 구성을 변경해야 할 특별한 이유가 없다면 기본 구성을 그대로 유지하는 것이 좋습니다.

제어 단추

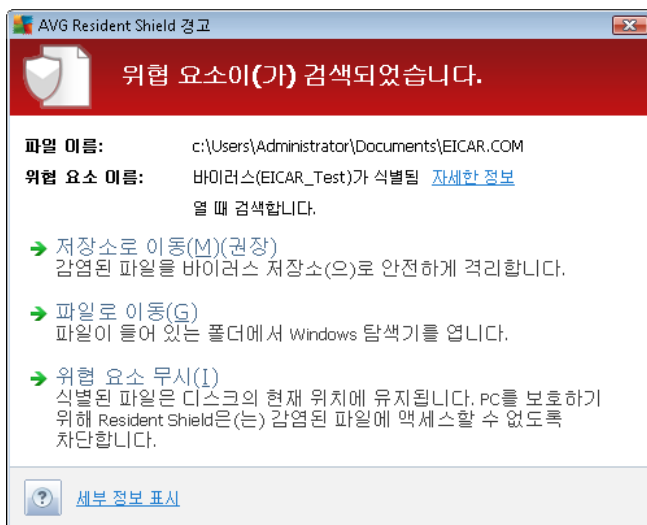
대화 상자 내에서 다음과 같은 제어 단추를 사용할 수 있습니다.

- **예외 관리** - 이름이 [Resident Shield - 예외](#)인 새 대화 상자를 엽니다. 이 대화 상자는 기본 메뉴에서 [고급 설정/Anti-Virus/Resident Shield/예외](#)를 차례로 선택하여 액세스할 수도 있습니다(자세한 설명은 해당 장 참조). 이 대화 상자 내에서 Resident Shield 스캔에서 제외할 파일 및 폴더를 지정할 수 있습니다. 반드시 제외해야 하는 경우가 아니라면 어떠한 항목도 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.
 - **파일 추가** - 로컬 디스크 탐색 트리에서 파일을 하나씩 선택하여 스캔에서 제외할 파일을 지정할 수 있습니다.
 - **항목 편집** - 선택한 파일 또는 폴더에 대해 지정된 경로를 편집할 수 있습니다.
 - **항목 제거** - 목록에서 선택한 항목의 경로를 삭제할 수 있습니다.
- **변경 사항 저장** - 이 대화 상자에서 수행된 구성 요소의 설정 변경 사항을 모두 저장하고 AVG Internet Security 2012의 기본 [사용자 인터페이스](#)(구성 요소 개요)로 돌아갑니다.
- **취소** - 이 대화 상자에서 수행된 구성 요소의 설정에 대한 모든 변경 사항을 취소합니다. 변경 사항이 저장되지 않습니다. AVG Internet Security 2012의 기본 [사용자 인터페이스](#)(구성 요소 개요)로 돌아갑니다.

6.1.5. Resident Shield 검색

위험 요소 탐지!

Resident Shield 는 파일을 복사하거나 열거나 저장할 때 파일을 스캔합니다. 바이러스나 다른 종류의 위험 요소가 발견되면 즉각 다음과 같은 대화 상자를 통해 경고가 표시됩니다.



이 경고 대화 상자에는 감염된 항목으로 검색 및 지정된 파일에 대한 데이터(*파일 이름*), 인식된 감염의 이름(*위험 요소 이름*) 및 [바이러스 백과 사전](#)에 대한 링크가 있습니다. 여기서 검색된 감염에 대한 자세한 정보(알려진 경우)를 확인할 수 있습니다(*자세한 정보*).

또한 지금 취해야 할 조치를 결정해야 합니다. 사용 가능한 옵션은 다음과 같습니다. **감염된 파일의 종류와 위치 등 특정 조건에 따라 일부 옵션을 사용하지 못할 수 있습니다.**

- **고급 사용자 권한으로 위험 요소 제거** - 일반 사용자로는 위험 요소를 제거할 수 있는 충분한 권한이 없다고 판단되면 이 상자를 선택합니다. 고급 사용자는 광범위한 액세스 권한이 있으며 위험 요소가 특정 시스템 폴더에 있으면 이 확인란을 선택해야 성공적으로 제거할 수 있습니다.
- **치료** - 검색된 감염을 치료할 수 있는 경우에만 이 단추가 표시됩니다. 그런 다음 검색된 감염을 파일에서 제거하고 해당 파일을 원래의 상태로 복원합니다. 파일 자체가 바이러스인 경우에는 이 기능을 사용하여 해당 파일을 삭제(즉, [바이러스 저장소로 이동](#))합니다.
- **저장소로 이동** - 바이러스를 [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.

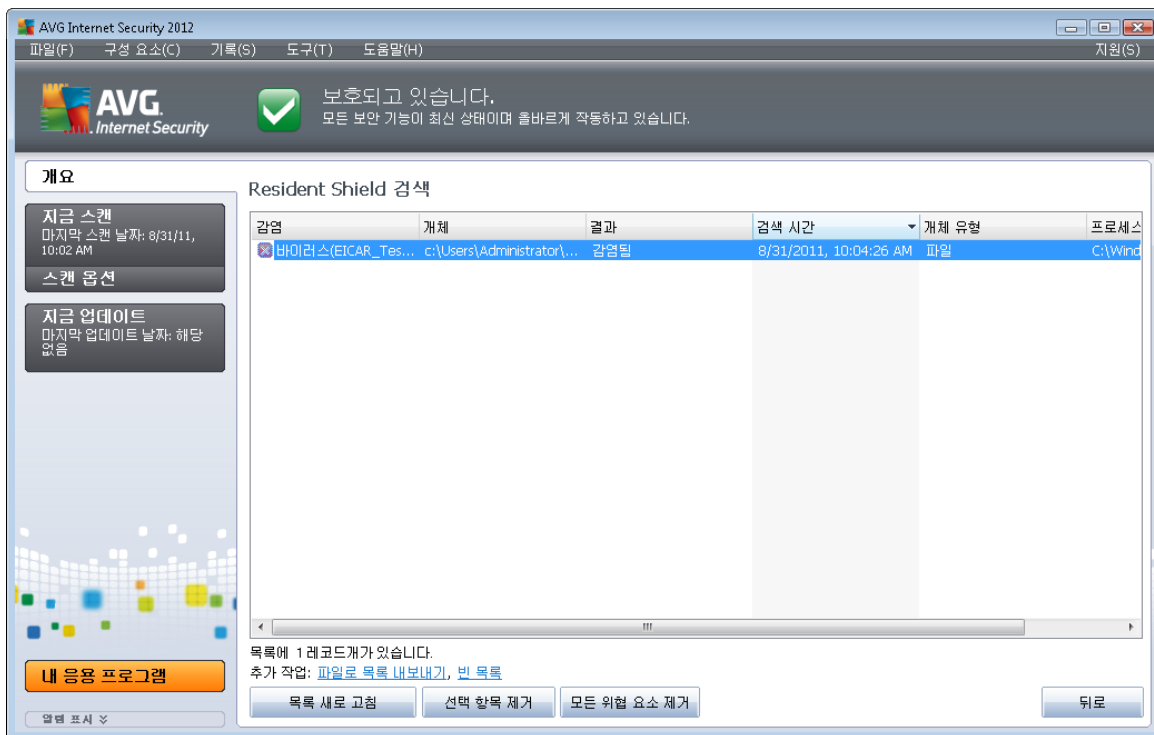


참고: 발견된 개체의 크기가 바이러스 저장소의 여유 공간 제한을 초과할 수도 있습니다. 이 경우 감염된 개체를 바이러스 저장소로 옮기려고 시도하면 해당 문제에 대해 알려 주는 경고 메시지가 표시됩니다. 하지만 바이러스 저장소 크기는 편집할 수 있습니다. 이 크기는 하드 디스크의 실제 크기에서 조정 가능한 부분을 백분율로 정의합니다. 바이러스 저장소의 크기를 늘리려면 [AVG 고급 설정](#)에 있는 [바이러스 저장소](#) 대화 상자로 이동하여 '바이러스 저장소 크기 제한' 옵션을 통해 변경합니다.

대화 상자의 아래쪽 섹션에는 **세부 정보 표시** 링크가 있습니다. 이 링크를 클릭하면 감염 요소를 검색하는 동안 실행되는 프로세스에 대한 자세한 정보 및 해당 프로세스의 ID가 표시된 팝업 창이 열립니다.

Resident Shield 검색 개요

[Resident Shield](#)에서 검색된 모든 위협 요소에 대한 전체적인 개요는 시스템 메뉴 옵션 **기록/Resident Shield 검색**에서 액세스할 수 있는 [Resident Shield 검색](#) 대화 상자에서 확인할 수 있습니다.



Resident Shield 검색에서는 [Resident Shield](#)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 하단의 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 **Resident Shield**에서 검색한 결과 목록을 업데이트합니다. **뒤로** 단추를 누르면 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

6.2. LinkScanner

LinkScanner는 웹에서 '새로 만들어져 바로 소멸되는' 위협으로부터 보호해 줍니다. 지속적으로 증가하고 있는 이러한 위협은 정부 기관과 잘 알려진 대기업은 물론 소규모 기업에 이르기까지 다양한 웹 사이트에서 숨겨진 형태로 존재할 수 있으며 대개는 24시간 이상 존속하지 않습니다. **LinkScanner**는 사용자가 방문하려는 웹 페이지의 링크에 연결된 페이지를 분석하여 해당 링크를 클릭하려고 하는 시점에 맞춰 해당 웹 페이지가 안전한지 알려줍니다.

LinkScanner는 서버 플랫폼 보호용이 아닙니다.

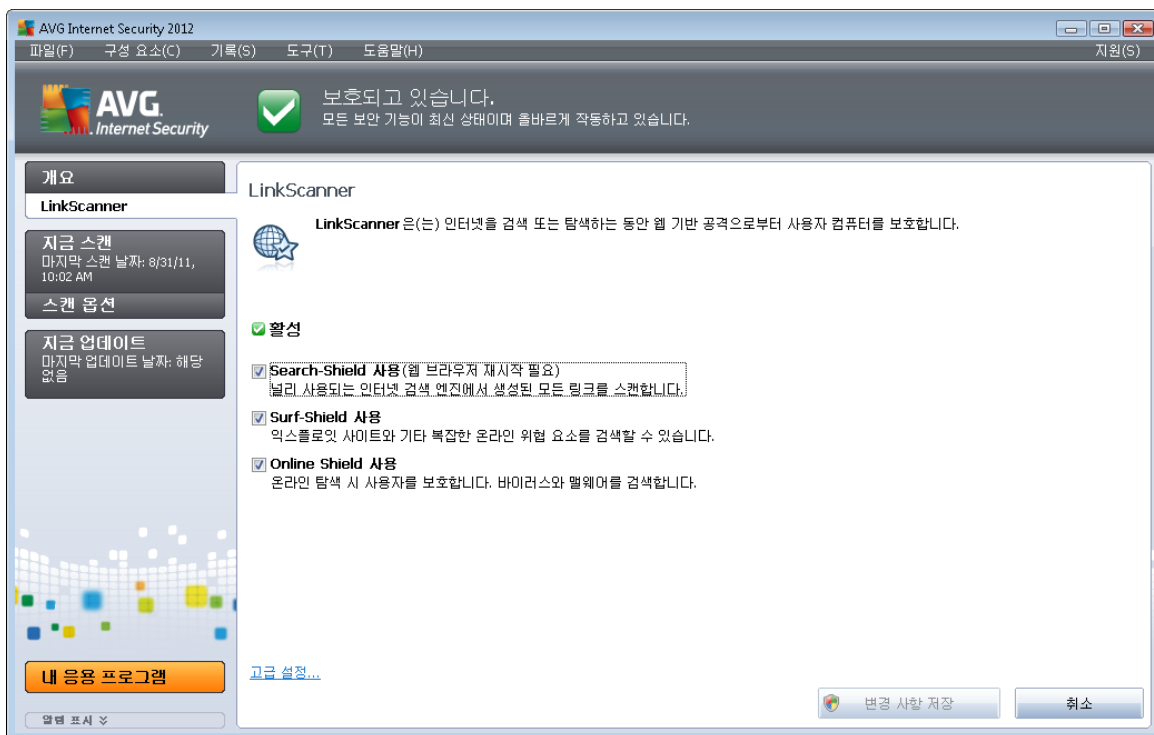
LinkScanner 기술은 다음과 같은 주요 기능으로 구성됩니다.

- **Search-Shield**에는 위험한 것으로 알려진 웹 사이트(URL 주소) 목록이 포함되어 있습니다. Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask 및 Seznam에서 검색할 때 이 목록을 기준으로 모든 검색 결과를 확인하여 판정 아이콘을 표시합니다(Yahoo! 검색 결과의 경우 "익스플로잇된 웹 사이트" 판정 아이콘만 표시됨).
- **Surf-Shield**는 웹 사이트의 주소에 관계없이 방문하는 모든 웹 사이트의 내용을 스캔합니다. 일부 웹 사이트가 **Search-Shield**에서 검색되지 않는 경우(예: 악성 웹 사이트가 새로 만들어졌거나 깨끗했던 웹 사이트에 맬웨어가 포함된 경우)에도 사용자가 웹 사이트를 방문하면 **Surf-Shield**가 위협 요소를 검색하여 차단합니다.
- **Online Shield**는 인터넷 서핑을 할 때 실시간으로 보호합니다. Online Shield는 방문한 웹 페이지의 콘텐츠 및 페이지에 포함된 파일을 웹 브라우저에 표시되거나 컴퓨터에 다운로드되기 전에 스캔합니다. **Online Shield**는 방문하려는 페이지에 포함된 바이러스와 스파이웨어를 검색하여 다운로드를 즉시 중지함으로써 위협 요소가 컴퓨터에 아예 침입하지 못하도록 합니다.
- **AVG Accelerator**는 온라인 비디오를 원활하게 재생하고 추가적인 다운로드가 쉽도록 도와줍니다. 비디오 가속이 진행 중이면 시스템 트레이 팝업 창을 통해 알림이 표시됩니다.



6.2.1. LinkScanner 인터페이스

[LinkScanner](#) 구성 요소 기본 대화 상자에는 구성 요소의 기능에 대한 간략한 설명과 구성 요소의 현재 상태(활성)에 대한 정보가 제공됩니다.



대화 상자의 아래쪽에는 구성 요소에 대한 기본적인 구성을 설정할 수 있습니다.

- **Search-Shield** 사용 - (기본적으로 설정됨): Search Shield 기능을 해제할 수 있는 타당한 이유가 있는 경우에만 이 상자를 선택 취소하십시오.
- **Surf-Shield** 사용 - (기본적으로 설정됨): 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.
- **Online Shield** 사용 - (기본적으로 설정됨): 방문하려는 웹 페이지에서 바이러스나 스파이웨어를 실시간으로 스캔합니다. 바이러스나 스파이웨어가 발견되면 해당 바이러스나 스파이웨어가 컴퓨터에 침입하지 못하도록 다운로드가 즉시 중지됩니다.

6.2.2. Search- Shield 검색

Search-Shield를 실행한 상태에서 인터넷을 검색하는 경우 *Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg 및 SlashDot* 등 가장 많이 사용하는 검색 엔진에서 반환되는 모든 결과는 위험한 링크인지 또는 의심스러운 링크인지 평가됩니다. [LinkScanner](#)에서는 이러한 링크를 확인하고 부적절한 링크를 표시함으로써 사용자가 위험하거나 의심스러운 링크를 클릭하기 전에 사용자에게 이를 경고하여 안전한 웹 사이트로만 연결되도록 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(*안전한 Yahoo! JP 검색 결과*).

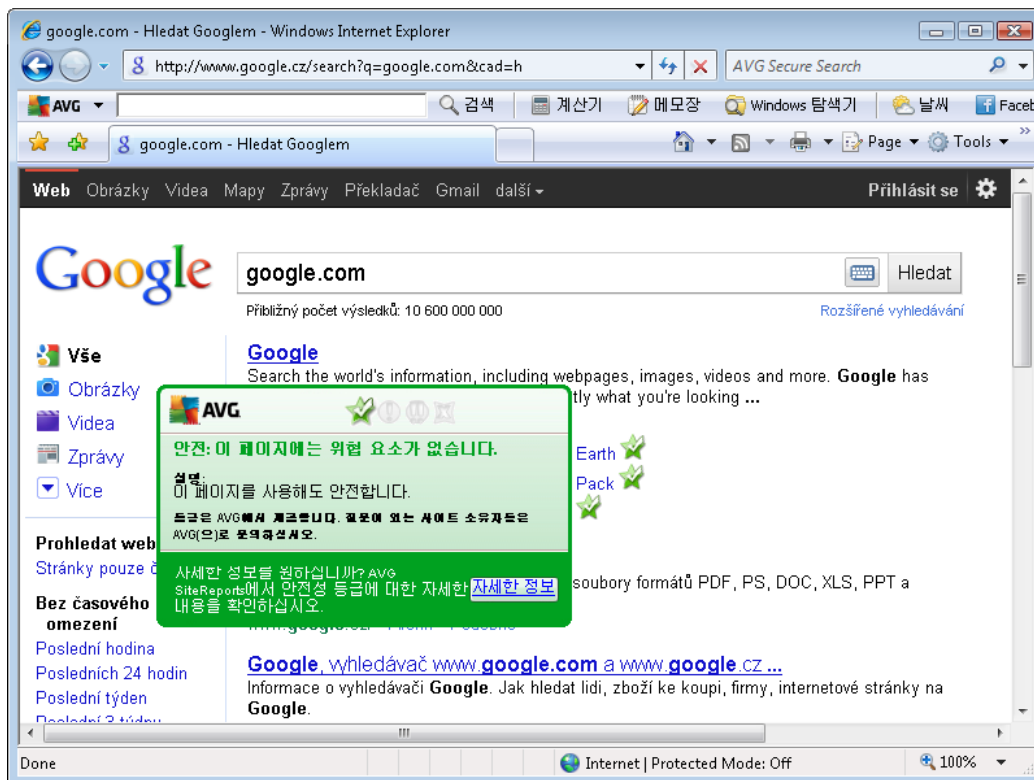
 연결된 페이지가 위협 요소를 포함하고 있지 않지만 다소 의심스럽습니다(*그 출처나 의도가 불확실해 보이므로 이러한 페이지에서 인터넷 쇼핑과 같은 활동은 하지 않는 것이 좋습니다*).

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

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

 액세스할 수 없는 연결된 페이지이므로 스캔하지 못했습니다.

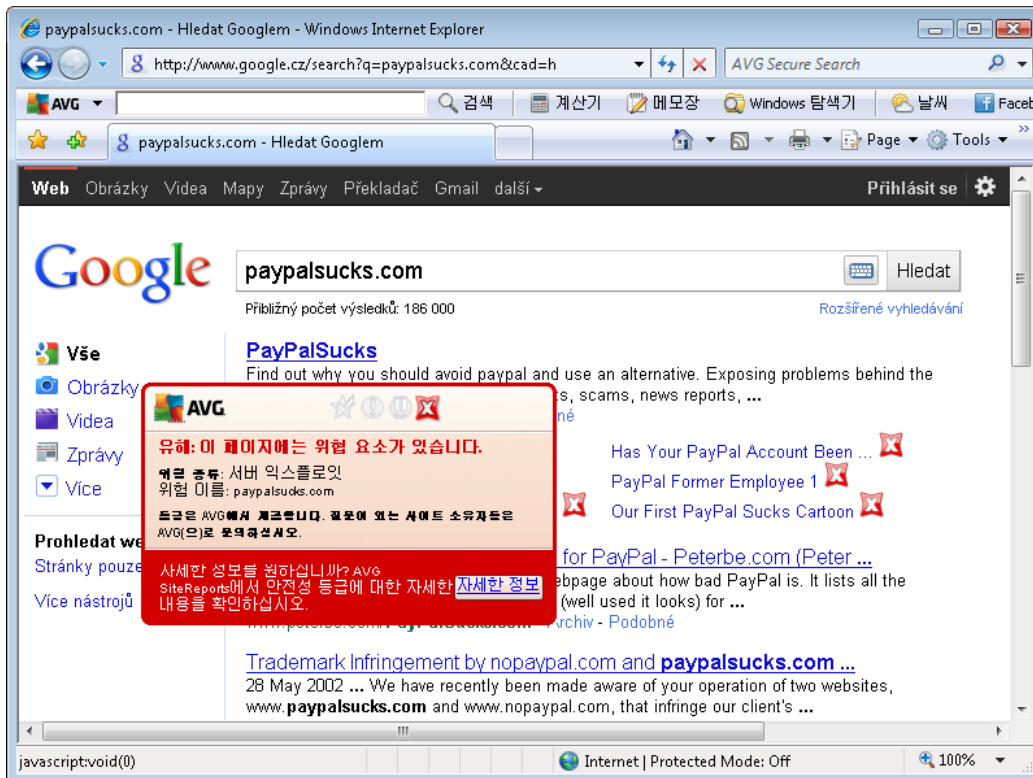
각 등급 아이콘 위에 마우스 포인터를 올려 놓으면 특정 링크에 대한 자세한 정보가 표시됩니다. 이러한 정보에는 위협 요소에 대한 자세한 정보(있는 경우)가 포함됩니다.



6.2.3. Surf- Shield 검색

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 [LinkScanner](#)에서 브라우저에 해당 웹 페이지가 표시되지 않도록 제한합니다.

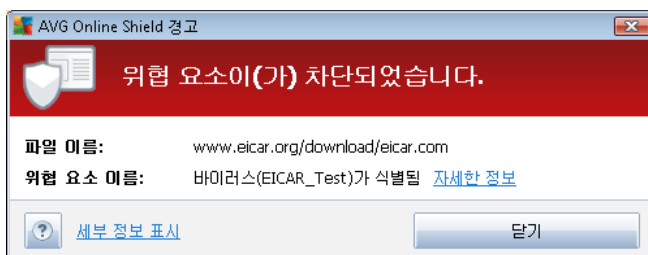
웹 브라우저에서 악의적인 웹 사이트가 열리면 [LinkScanner](#)에서 화면에 다음과 같은 경고 메시지를 표시합니다.



이 웹 사이트를 방문하는 것은 매우 위험하며 권장되지 않습니다!

6.2.4. Online Shield 검색

Online Shield 는 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.



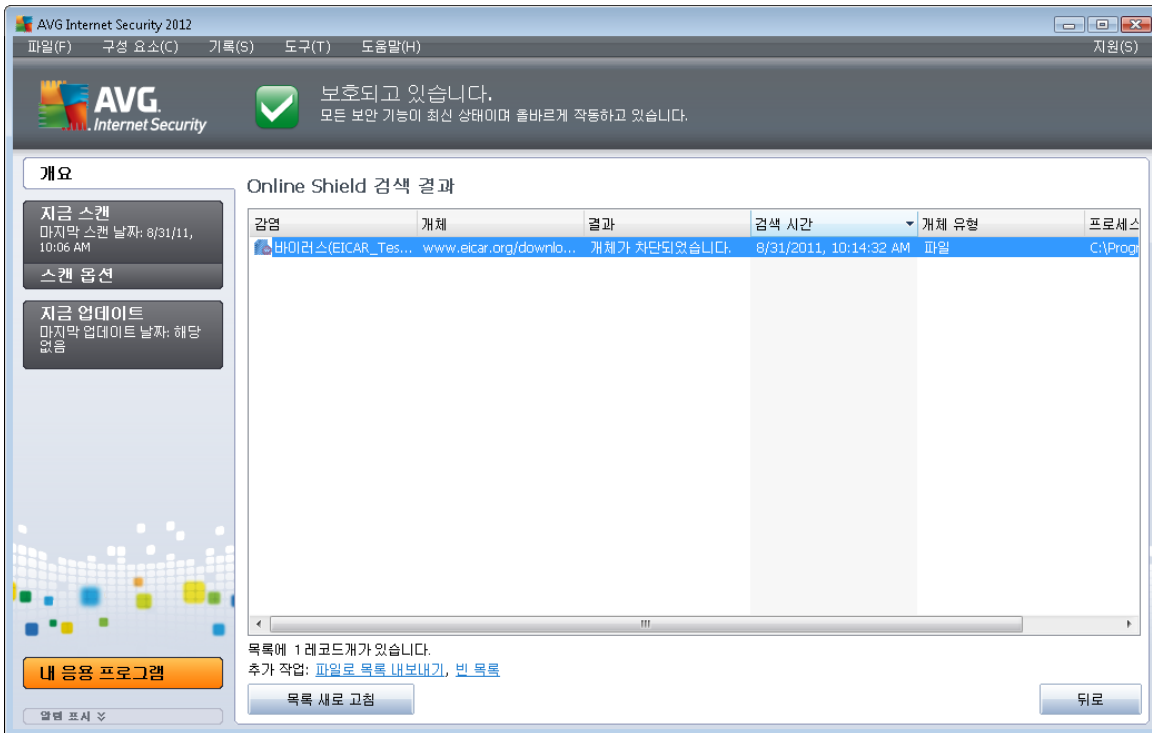
이 경고 대화 상자에는 감염된 항목으로 검색 및 지정된 파일에 대한 데이터(**파일 이름**), 인식된 감염의 이름(**위험 요소 이름**) 및 **바이러스 백과 사전**에 대한 링크가 있습니다. 바이러스 백과 사전에서는 검색된 감염에 대한 자세한 정보(**알려진 경우**)를 확인할 수 있습니다. 이 대화 상자에는 다음과 같은 단추가 있습니다.

- **세부 정보 표시 - 세부 정보 표시** 단추를 클릭하면 새로운 팝업 창이 열립니다. 이 창에서 감염 요소 검색 시 실행 중이던 프로세스에 대한 정보 및 해당 프로세스의 ID를 확인할 수 있습니다.



- **닫기** - 경고 대화 상자를 닫으려면 이 단추를 클릭합니다.

의심스러운 웹 페이지는 열리지 않으며 위험 요소 검색은 **Online Shield 검색 결과**에 기록됩니다. 발견된 위험 요소에 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** - 위험 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 하단의 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.

제어 단추



- **목록 새로 고침** - *Online Shield* 에서 발견한 결과 목록을 업데이트합니다.
- **뒤로** - [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

6.3. 전자 메일 보호

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 입력하는 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.

전자 메일 보호 구성 요소는 보내거나 받는 모든 전자 메일 메시지의 스캔을 담당합니다. 전자 메일에서 바이러스가 발견될 경우 해당 바이러스는 즉시 [바이러스 저장소](#)로 이동합니다. 또한 이 구성 요소는 특정 유형의 전자 메일 첨부 파일을 필터링하며 감염되지 않은 메시지에 인증 텍스트를 추가합니다. **전자 메일 보호**는 다음 두 가지 기본 기능으로 이루어져 있습니다.

- [E-mail Scanner](#)
- [Anti-Spam](#)

6.3.1. E-mail Scanner

개인용 전자 메일 스캐너에서는 들어오고 나가는 전자 메일을 자동으로 스캔합니다. 이 기능은 AVG에서 자체 플러그인이 없는 전자 메일 클라이언트를 사용하는 경우 함께 사용할 수 있습니다. 하지만 *Microsoft Outlook* 및 *The Bat* 와 같이 AVG 에서 지원하는 특정 플러그인이 있는 전자 메일 클라이언트에 대한 전자 메일 메시지를 스캔하는 데 사용할 수도 있습니다. 주로, Outlook Express, Mozilla, Incredimail 등의 전자 메일 응용 프로그램과 함께 사용합니다.

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.

E-mail Scanner 는 인터넷에서 전자 메일 클라이언트와 전자 메일 서버 간의 인터페이스로 작동합니다.

- **들어오는 메일:** 서버에서 메시지를 받는 동안 **E-mail Scanner** 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 E-mail Scanner 로 전송됩니다. E-mail Scanner 는 메시지와 첨부 파일에 바이러스가 있는지 테스트한 후 메시지를 SMTP 서버로 전송합니다(나가는 전자 메일의 스캔은 기본적으로 비활성화되어 있으며 수동으로 설정할 수 있음).



E-mail Scanner 는 서버 플랫폼용 이 아닙니다.

6.3.2. Anti- Spam

Anti-Spam 작동 방식

Anti-Spam에서는 들어오는 모든 전자 메일 메시지를 검사하고 원치 않는 전자 메일을 스팸 메일로 표시합니다. **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. **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. **Anti-Spam**에서는 스팸을 검색하기 위해 정기적으로 업데이트되는 데이터베이스를 사용합니다. [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.

스팸이란?

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

6.3.3. 전자 메일 보호 인터페이스





전자 메일 보호 대화 상자에서는 구성 요소의 기능을 설명하는 간단한 텍스트와 현재 상태(활성)에 대한 정보를 볼 수 있습니다. **AVG에서 보호를 적용한 방식에 대한 온라인 보고서 보기** 링크를 사용하여 AVG 웹 사이트 (<http://www.avg.com/>) 의 전용 페이지에서 **AVG Internet Security 2012** 활동 및 검색에 대한 자세한 통계를 검토할 수 있습니다.

기본 전자 메일 보호 설정

전자 메일 보호 대화 상자에서는 구성 요소의 기능에 대한 몇 가지 기본 기능을 추가로 편집할 수 있습니다.

- **수신 메시지 스캔**(기본적으로 설정되어 있음) - 사용자 계정에 수신된 모든 전자 메일에서 바이러스를 스캔하도록 지정하려면 이 항목을 선택합니다.
- **발신 메시지 스캔**(기본적으로 해제되어 있음) - 사용자 계정이 보내는 모든 전자 메일에서 바이러스를 스캔하도록 지정하려면 이 항목을 선택합니다.
- **전자 메일을 스캔하는 동안 알림 창 표시**(기본적으로 설정되어 있음) - 전자 메일을 스캔하는 동안 [시스템 트레이의 AVG 아이콘](#) 위에 표시되는 알림 대화 상자에서 알림을 받으려면 이 항목을 선택합니다.
- **Anti-Spam** 사용(기본적으로 설정되어 있음) - 들어오는 메일에서 원치 않는 메일을 필터링하도록 지정하려면 이 항목을 선택합니다.

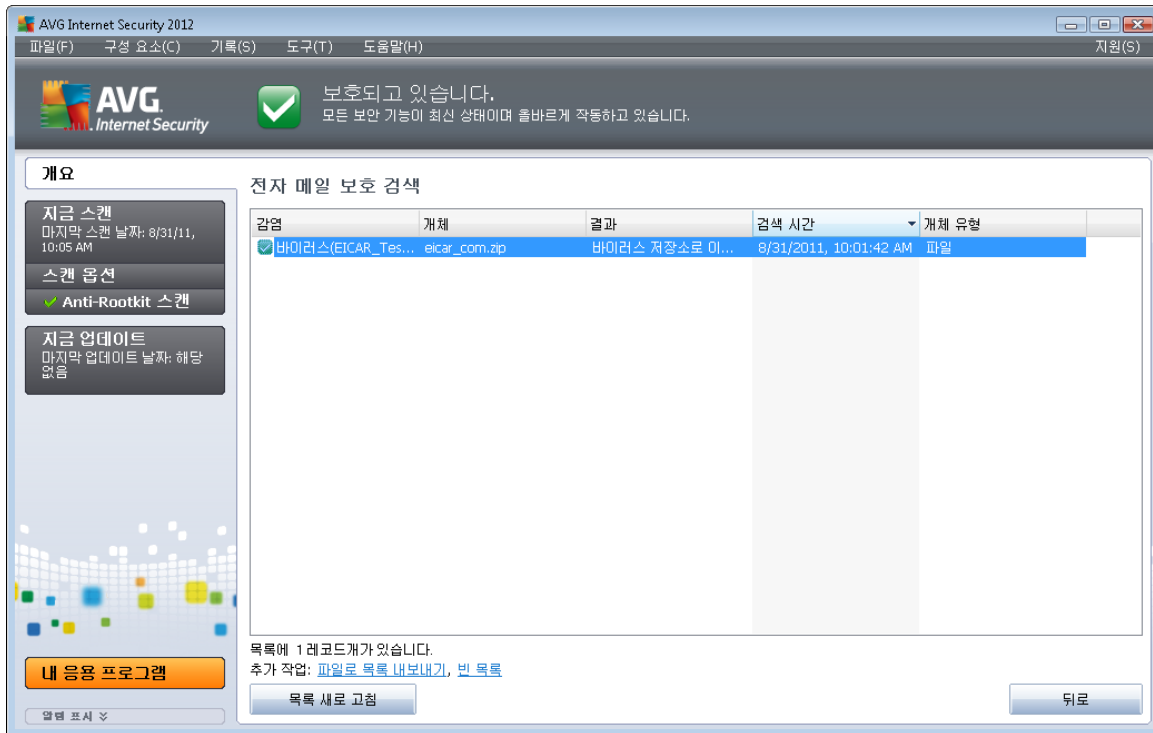
소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 모든 AVG 구성 요소를 설정합니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다. AVG 구성을 변경해야 하는 경우 시스템 메뉴 항목도 구/고급 설정을 선택하고 새로 열린 [AVG 고급 설정](#) 대화 상자에서 AVG 구성을 편집합니다.

제어 단추

전자 메일 보호 대화 상자에서 사용할 수 있는 제어 단추는 다음과 같습니다.

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

6.3.4. 전자 메일 보호 검색



E-mail Scanner 검색 대화 상자(시스템 메뉴 옵션인 기록/E-mail Scanner 검색을 통해 액세스 가능)에서는 [전자 메일 보호](#) 구성 요소에서 검색된 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 하단의 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.

제어 단추

E-mail Scanner 검색 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다.

- **목록 새로 고침** - 검색된 위협 요소 목록을 업데이트합니다.



- **뒤로** - 이전에 표시된 대화 상자로 돌아갑니다.

6.4. Firewall

Firewall은 트래픽을 차단/허용하는 방법으로 두 개 이상의 네트워크 간에 액세스 제어 정책을 적용하는 시스템입니다. **Firewall** 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. **Firewall**에서 침입 시도를 인지한 경우 이러한 시도를 "차단"하며 침입자가 컴퓨터에 액세스하지 못하도록 합니다.

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

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

Firewall을 통해 보호되지 않는 컴퓨터는 컴퓨터 해커나 데이터 도난의 대상이 되기 쉽습니다.

권장 사항: 한 컴퓨터에서 여러 개의 **Firewall**을 사용하는 것은 권장되지 않습니다. **Firewall**을 여러 개 설치해도 컴퓨터의 보안이 향상되지 않으며, 두 응용 프로그램 간에 충돌이 발생할 가능성이 더 높아집니다. 따라서 컴퓨터에서 **Firewall** 하나만 사용하고 나머지 **Firewall**은 비활성화하여 충돌 가능성 및 다른 관련 문제를 방지하는 것이 좋습니다.

6.4.1. Firewall 원리

AVG Internet Security 2012에서 **Firewall**은 컴퓨터에 있는 모든 네트워크 포트의 트래픽을 제어합니다. 정의된 규칙을 기반으로 **Firewall**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 **Firewall**은 네트워크 포트에서의 커뮤니케이션을 허용하거나 차단합니다. 응용 프로그램이 알려져 있지 않은 경우, 즉 정의된 **Firewall** 규칙이 없는 경우, **Firewall**은 해당 커뮤니케이션 시도를 허용할지 차단할지를 사용자에게 묻습니다.

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 [프로필](#)을 사용합니다.
- [다양한 네트워크에 연결하거나 다양한 네트워크 어댑터를 사용할 때 자동으로](#)

[프로필을 전환](#)합니다.

6.4.2. Firewall 프로필

[Firewall](#)을 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 [Firewall](#) 프로필은 [Firewall](#) 구성 요소의 특정 구성이며 이러한 미리 정의된 구성을 많이 사용할 수 있습니다.

사용 가능한 프로필

- **모두 허용** - 제조업체에서 미리 설정한 [Firewall](#) 시스템 프로필이며 항상 존재합니다. 이 프로필이 활성화되면 [Firewall](#) 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 Firewall을 사용하지 않도록 설정해야 합니다. 이 시스템 프로필은 복제하거나 삭제할 수 없으며 해당 설정을 수정할 수 없습니다.
- **모두 차단** - 제조업체에서 미리 설정한 [Firewall](#) 시스템 프로필이며 항상 존재합니다. 이 프로필이 활성화되면 모든 네트워크 커뮤니케이션이 차단되므로 외부 네트워크에서 컴퓨터에 액세스할 수 없으며 컴퓨터가 외부와 커뮤니케이션할 수 없습니다. 이 시스템 프로필은 복제하거나 삭제할 수 없으며 해당 설정을 수정할 수 없습니다.
- **사용자 지정 프로필** - 사용자 지정 프로필을 사용하면 다양한 네트워크에 자주 연결하는 경우(예: 노트북 사용 시)에 특히 유용한 자동 프로필 전환 기능을 활용할 수 있습니다. 사용자 지정 프로필은 **AVG Internet Security 2012** 설치 후에 자동으로 생성되며 [Firewall](#) 정책 규칙에 필요한 모든 개별 요구 사항을 처리할 수 있습니다. 사용할 수 있는 사용자 지정 프로필은 다음과 같습니다.
 - **인터넷에 직접 연결** - 추가적인 보호 기능 없이 인터넷에 직접 연결되어 있는 일반 가정용 데스크톱 컴퓨터나 노트북에 적합합니다. 이 옵션은 알 수 없는 안전하지 않은 여러 네트워크에 노트북을 연결하는 경우에도 사용하는 것이 좋습니다(예: 인터넷 카페, 호텔방 등). 이 프로필이 제공하는 가장 엄격한 [Firewall](#) 정책 규칙을 사용하면 이러한 컴퓨터를 적절하게 보호할 수 있습니다.
 - **도메인의 컴퓨터** - 학교나 직장 및 같이 로컬 네트워크에 속해 있는 컴퓨터에 적합합니다. 이 경우 네트워크가 전문적으로 관리되고 있으며 추가적인 보안 수단으로 보호되고 있다고 간주되기 때문에, 공유 폴더, 디스크 장치 등에 액세스할 수 있도록 위에서 설명한 경우들보다 낮은 보안 수준이 설정될 수 있습니다.
 - **소규모 가정용 또는 사무실 네트워크** - 가정이나 소규모 사무실과 같은 소규모 네트워크에 속해 있는 컴퓨터에 적합합니다. 대개 이 유형의 네트워크에는 "중앙" 관리자가 없으며 몇 대의 컴퓨터가 서로 연결되어 프린터, 스캐너 등과 같은 장치를 공유하는 경우가 많으므로 [Firewall](#) 규칙에서 이를 반영해야 합니다.

프로필 전환

프로필 전환 기능을 사용하면 특정 네트워크 어댑터를 사용하거나 특정 유형의 네트워크에 연결될 때 [Firewall](#) 이 자동으로 정의된 프로필로 전환됩니다. 네트워크 영역에 프로필이 할당되어 있지 않으면 다음 번에 해당 영역에 연결할 때 [Firewall](#) 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.

6.4.3. Firewall 인터페이스



Firewall 구성 요소라는 이름의 기본 대화 상자에는 이 구성 요소의 기능에 대한 기본적인 정보, 상태(활성) 및 구성 요소의 통계에 대한 간략한 개요가 표시됩니다.

- **Firewall 실행 기간** - [Firewall](#)을 마지막으로 시작한 후 경과된 시간입니다.
- **차단된 패킷** - 확인된 전체 패킷 중 차단된 패킷의 수입입니다.
- **전체 패킷** - [Firewall](#)을 실행하는 동안 검사된 총 패킷 수입입니다.



기본 Firewall 설정

- **Firewall 프로파일 선택** - 정의되어 있는 프로파일 중 하나를 롤다운 메뉴에서 선택합니다. 각 프로파일에 대한 자세한 설명 및 권장 사용은 [Firewall 프로파일](#) 장을 참조하십시오.
- **게임 모드 사용** - 전체 화면 응용 프로그램(게임, 프레젠테이션, 영화 등)이 실행 중일 때 [Firewall](#)에서 알 수 없는 응용 프로그램과의 커뮤니케이션을 허용할지 아니면 차단할지를 묻는 대화 상자를 표시하지 않게 하려면 이 옵션을 선택합니다. 그 시점에 알 수 없는 응용 프로그램이 네트워크를 통해 커뮤니케이션하려고 시도하면 [Firewall](#)에서 현재 프로파일의 설정에 따라 그러한 시도를 자동으로 허용하거나 차단합니다. **참고:** 게임 모드가 설정되어 있는 경우 예약된 모든 작업(스캔, 업데이트)은 응용 프로그램이 닫힐 때까지 연기됩니다.
- 또한 이 기본 설정 섹션에서는 [Firewall](#) 구성 요소의 현재 상태를 정의하는 다음의 세 가지 옵션 중에서 선택할 수 있습니다.
 - **Firewall 사용(기본값)** - 이 옵션을 선택하면 선택한 [Firewall](#) 프로파일에 정의된 규칙 집합에서 "허용"으로 지정된 응용 프로그램과 커뮤니케이션할 수 있습니다.
 - **Firewall 사용 안 함** - 이 옵션은 [Firewall](#)을 완전히 사용하지 않도록 설정하여 모든 네트워크 트래픽이 허용되거나 검사되지 않습니다.
 - **긴급 모드(모든 인터넷 트래픽 차단)** - 이 옵션을 선택하면 각 단일 네트워크 포트의 트래픽이 모두 차단됩니다. [Firewall](#)은 계속 실행되지만 모든 네트워크 트래픽은 중지됩니다.

참고: 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG Internet Security 2012 구성 요소를 설정해 놓았습니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다. Firewall 구성을 변경해야 하는 경우 시스템 메뉴 항목 **도구/Firewall 설정**을 선택하고 새로 열린 [Firewall 설정](#) 대화 상자에서 Firewall 구성을 편집합니다.

제어 단추

- **구성 다시 생성** - 이 단추를 누르면 현재 [Firewall](#) 구성을 덮어쓰고 자동 검색을 기반으로 한 기본 구성으로 되돌릴 수 있습니다.
- **변경 내용 저장** - 이 단추를 누르면 이 대화 상자에서 변경한 모든 내용이 저장 및 적용됩니다.
- **취소** - 이 단추를 누르면 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

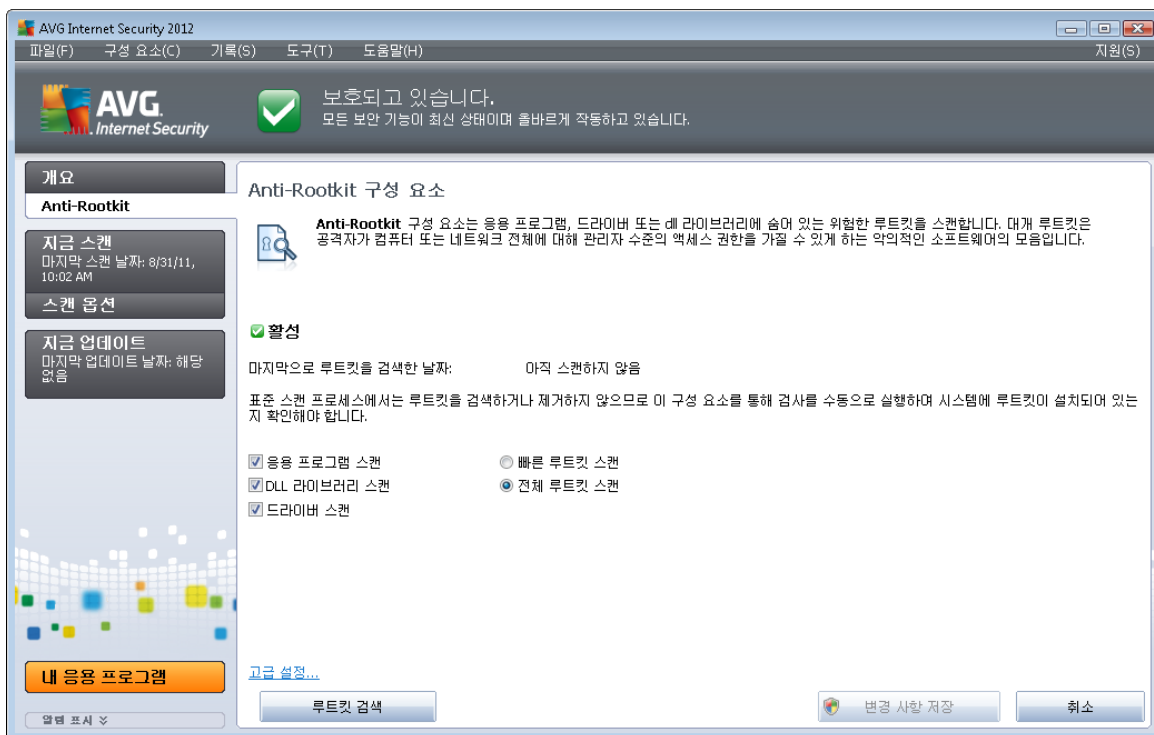
6.5. Anti- Rootkit

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

루트킷이란?

루트킷이란 시스템 소유자 및 합법적인 관리자의 승인 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. 대부분 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.

6.5.1. Anti- Rootkit 인터페이스



Anti-Rootkit 대화 상자는 구성 요소의 기능에 대한 간략한 설명을 제공하고 구성 요소의 현재 상태(활성)를 알려줄 뿐 아니라 **Anti-Rootkit** 테스트가 시작된 마지막 시간(**마지막으로 루트킷을 검색한 날짜**)에 대한 정보를 제공합니다. **Anti-Rootkit** 대화 상자에서는 [도구/고급 설정](#) 링크도 제공합니다. 이 링크를 사용하여 **Anti-Rootkit** 구성 요소의 고급 구성



을 지정할 수 있는 환경으로 리디렉션할 수 있습니다.

소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 모든 AVG 구성 요소를 설정합니다. 특별한 이유가 없다면 AVG 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자가 수행해야 합니다.

기본 Anti-Rootkit 설정

대화 상자의 아래쪽 부분에서 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, 시스템 폴더(일반적으로 c:\Windows)와 모든 로컬 디스크(플래시 디스크는 포함하지만 플로피 디스크/CD 드라이브는 제외)를 스캔합니다.

제어 단추

- 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 변경된 모든 내용을 저장하고 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갈 수 있습니다.
- 취소 - 이 단추를 누르면 변경한 내용을 저장하지 않고 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갈 수 있습니다.

6.6. 시스템 도구

시스템 도구는 **AVG Internet Security 2012** 환경 및 운영 체제에 대한 자세한 요약 정보를 제공하는 도구입니다. 구성 요소에 다음 개요가 표시됩니다.

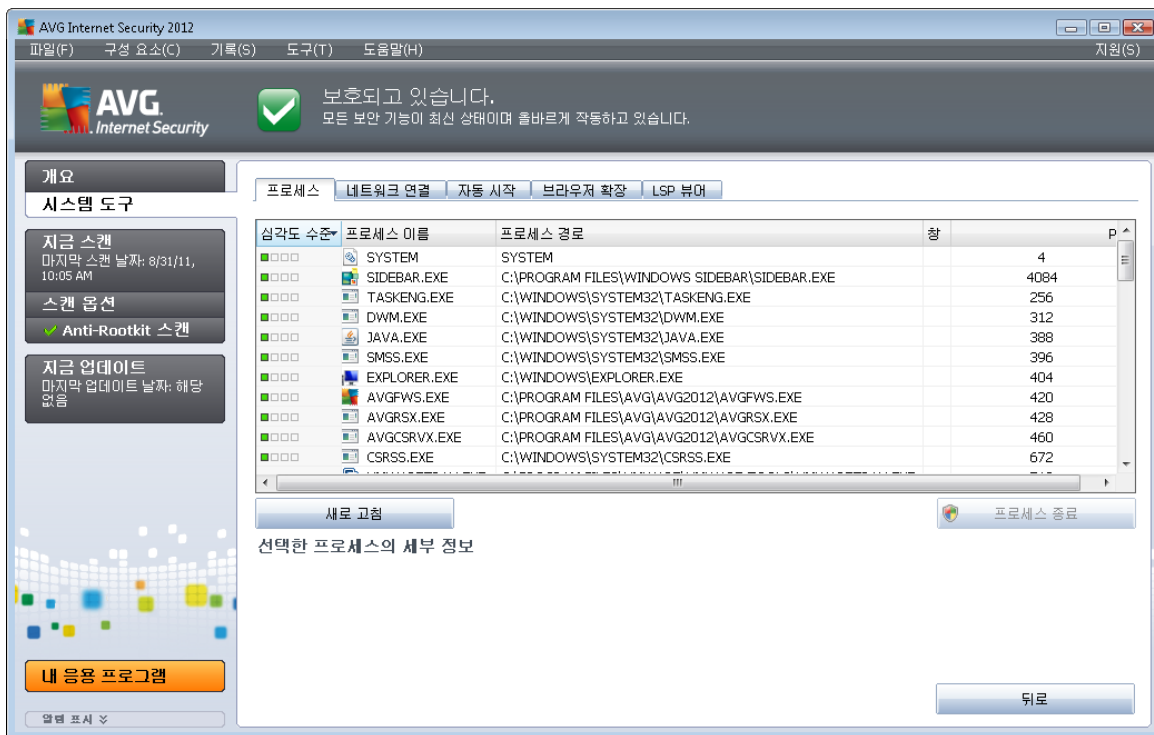
- [프로세스](#) - 현재 컴퓨터에서 활성 상태인 프로세스(예: 실행 중인 응용 프로그램)의 목록
- [네트워크 연결](#) - 현재 활성 연결의 목록



- [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 숙련된 사용자만 사용하는 것이 좋습니다.

6.6.1. 프로세스



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

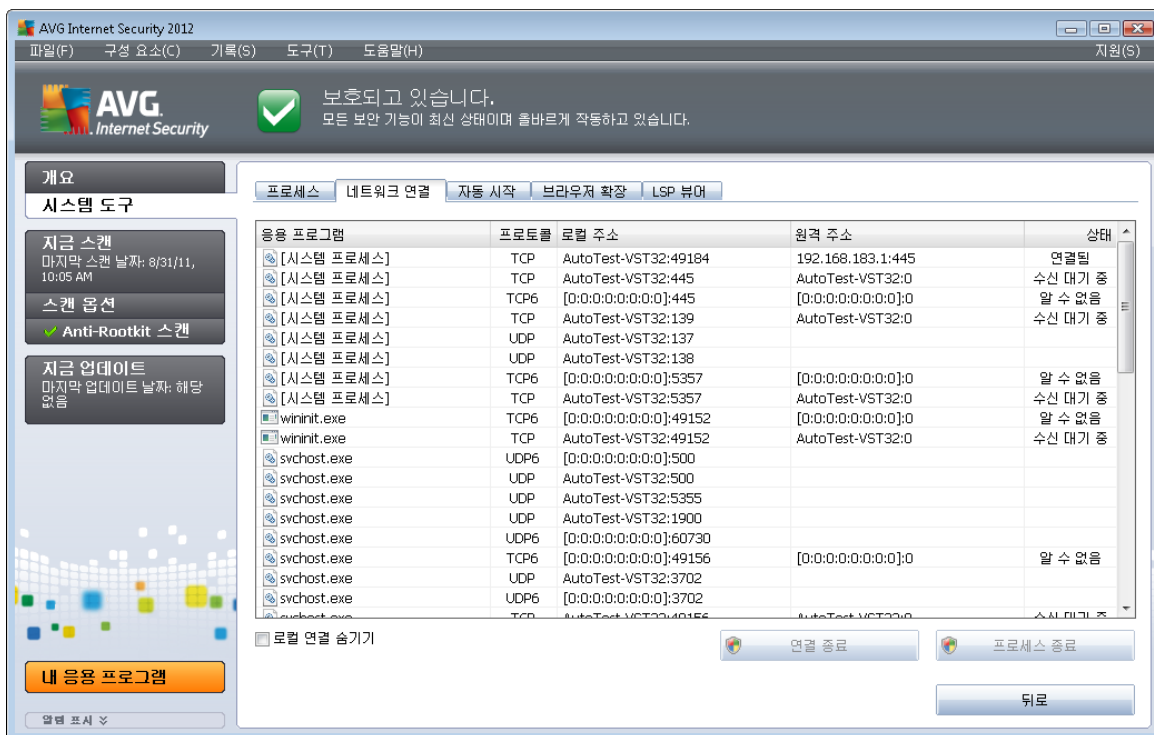
- **심각도 수준** - 관련 프로세스의 심각도를 유해하지 않은 수준 (■□□□)부터 심각한 수준 (■□□□)에 이르기까지 네 단계로 나타내는 그래픽 표시
- **프로세스 이름** - 실행 중인 프로세스의 이름
- **프로세스 경로** - 실행 중인 프로세스의 실제 경로
- **창** - 해당되는 경우 응용 프로그램 창 이름을 나타냅니다.
- **PID** - PID (프로세스 식별 번호)는 고유한 Windows 내부 프로세스 ID입니다.

제 어 단 추

프로세스 탭 내에서 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 위협 요소를 나타내는 경우가 아니라면 응용 프로그램을 종료하지 않는 것이 좋습니다.**
- **뒤로** - [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

6.6.2. 네트워크 연결



The screenshot shows the AVG Internet Security 2012 interface. The 'Network Connection' tab is selected, displaying a table of active network connections. The table has five columns: '응용 프로그램' (Application), '프로토콜' (Protocol), '로컬 주소' (Local Address), '원격 주소' (Remote Address), and '상태' (Status). The table lists various system processes and services, including wininit.exe, svchost.exe, and AutoTest-VST32.*. The status column shows various connection states like '연결됨' (Connected), '수신 대기 중' (Waiting for data), and '알 수 없음' (Unknown).

응용 프로그램	프로토콜	로컬 주소	원격 주소	상태
[시스템 프로세스]	TCP	AutoTest-VST32:49184	192.168.183.1:445	연결됨
[시스템 프로세스]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	수신 대기 중
[시스템 프로세스]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	알 수 없음
[시스템 프로세스]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	수신 대기 중
[시스템 프로세스]	UDP	AutoTest-VST32:137		
[시스템 프로세스]	UDP	AutoTest-VST32:138		
[시스템 프로세스]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	알 수 없음
[시스템 프로세스]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	수신 대기 중
[시스템 프로세스]	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	알 수 없음
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	수신 대기 중
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:60730		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	알 수 없음
svchost.exe	UDP	AutoTest-VST32:3702		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:3702		

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.

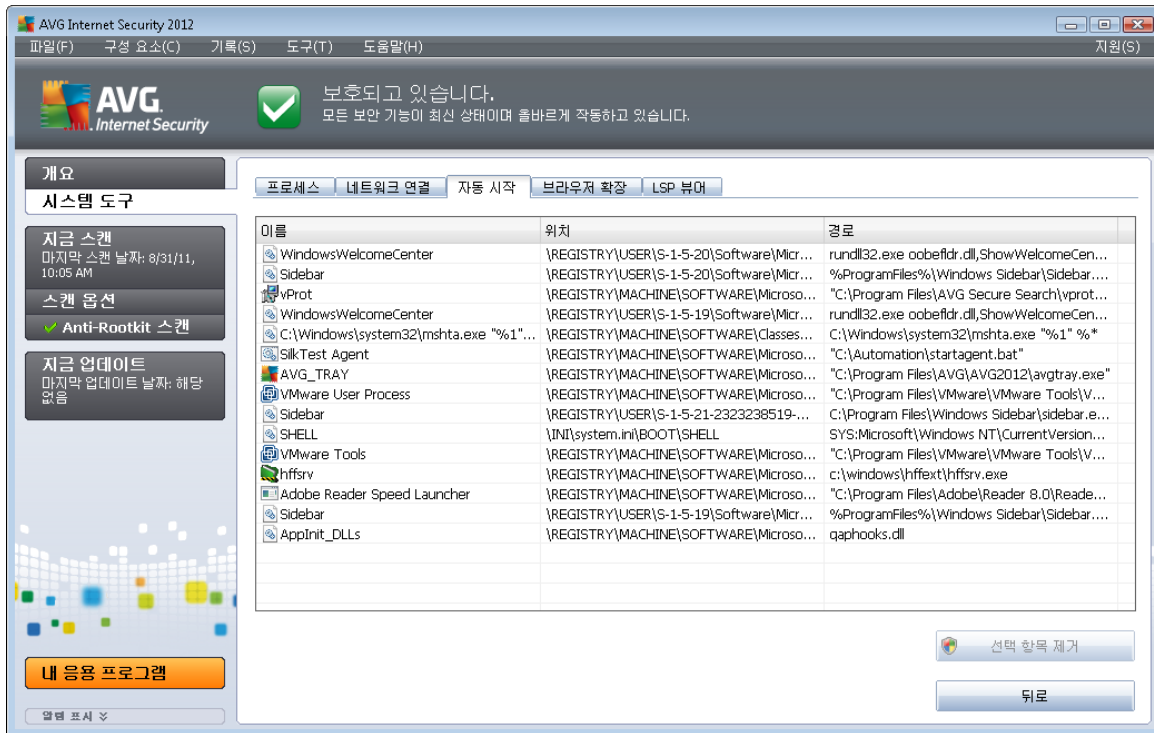
제어 단추

네트워크 연결 탭에서 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** - [AVG 기본 대화 상자](#)(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.

6.6.3. 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.

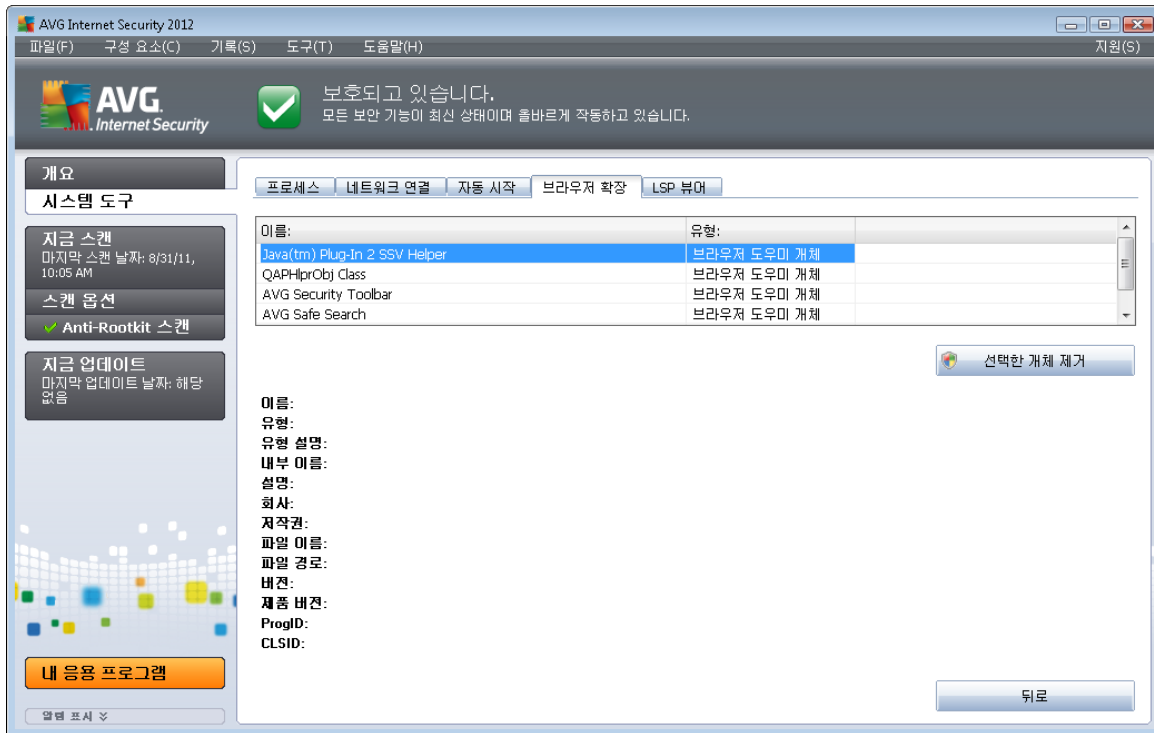
제어 단추

자동 시작 탭에서 사용할 수 있는 제어 단추는 다음과 같습니다.

- **선택 항목 제거** - 선택한 하나 이상의 항목을 삭제하려면 이 단추를 누릅니다.
- **뒤로** - [AVG 기본 대화 상자](#) (구성 요소 개요)로 돌아갑니다.

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

6.6.4. 브라우저 확장



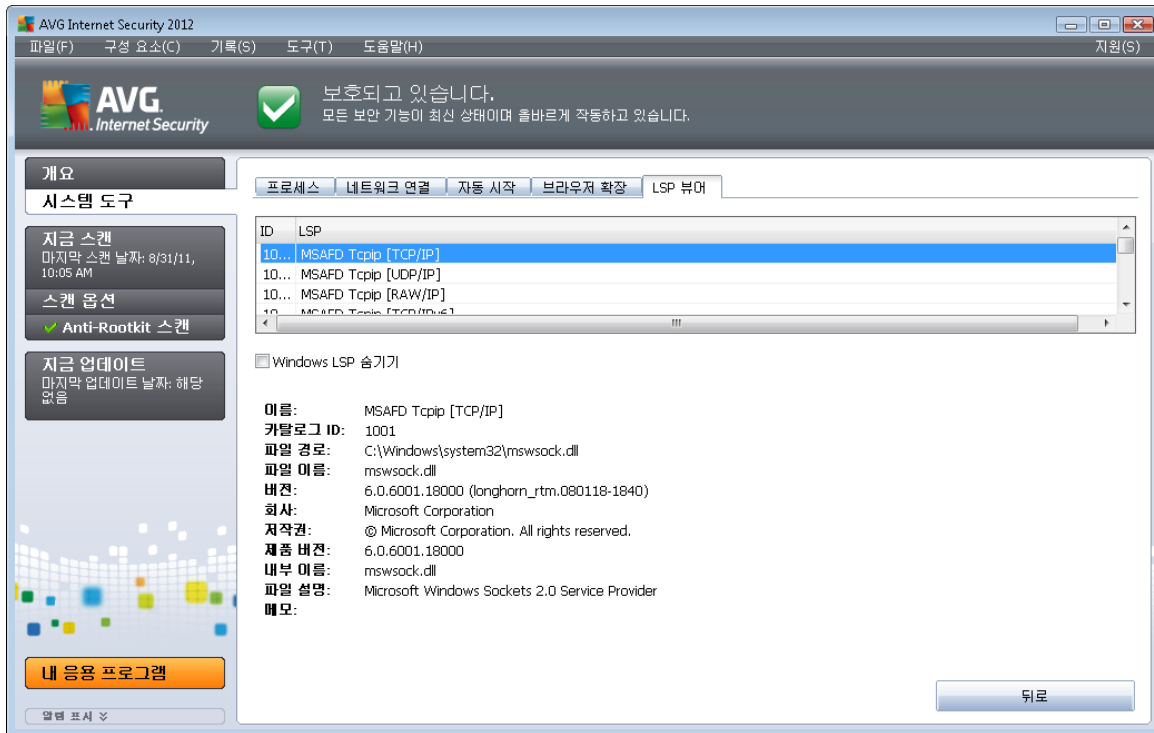
브라우저 확장 대화 상자에는 인터넷 브라우저 내에 설치되어 있는 플러그인(예: 응용 프로그램) 목록이 포함되어 있습니다. 이 목록에는 정규 응용 프로그램 플러그인뿐 아니라 잠재적인 맬웨어 프로그램이 포함되어 있을 수 있습니다. 목록에서 개체를 클릭하면 대화 상자 하단 섹션에 선택한 플러그인에 대한 자세한 정보가 표시됩니다.

제어 단추

브라우저 확장 탭에서 사용할 수 있는 제어 단추는 다음과 같습니다.

- **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** - [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

6.6.5. 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.

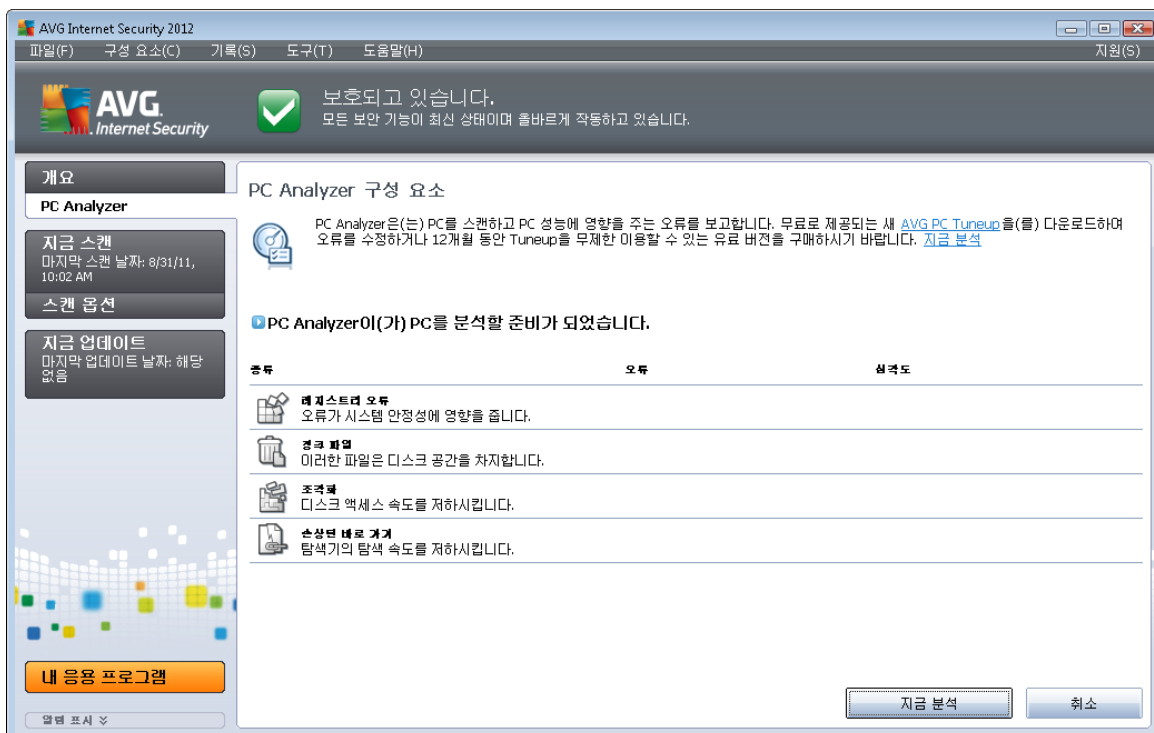
제어 단추

LSP 뷰어 탭에서 사용할 수 있는 제어 단추는 다음과 같습니다.

- **Windows LSP 숨기기** - 목록에 Windows LSP를 포함하려면 이 항목을 선택 취소합니다.
- **뒤로** - [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

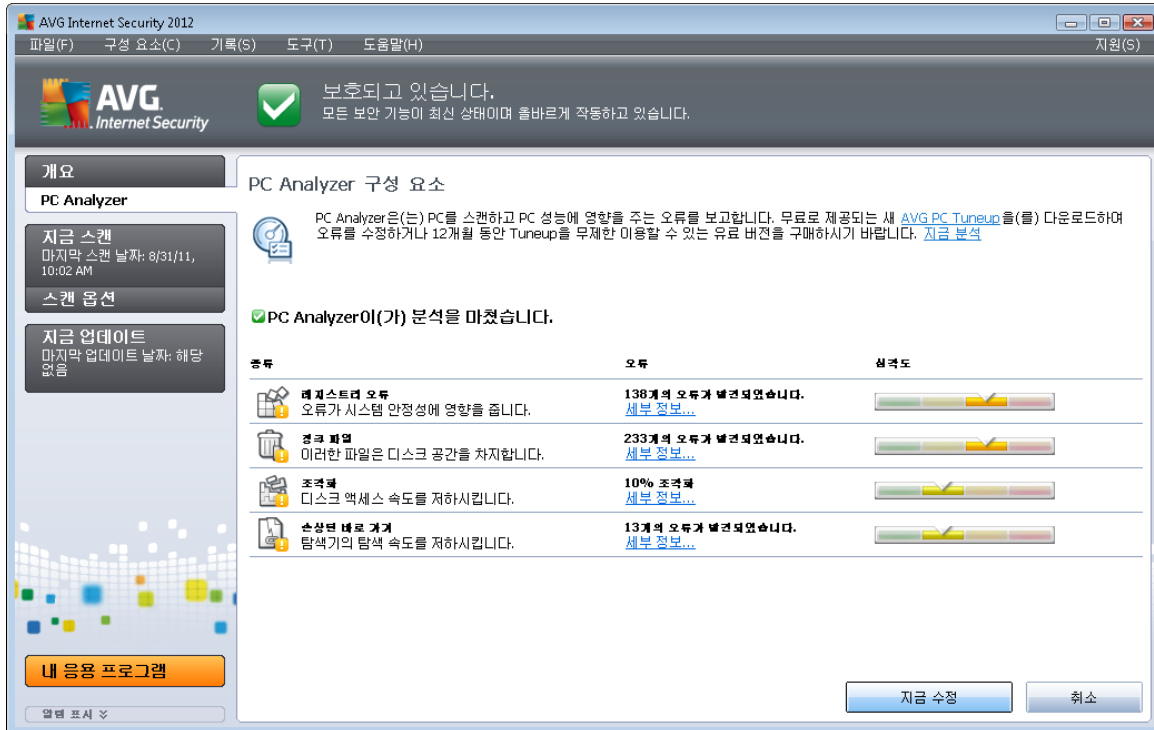
6.7. PC Analyzer

PC Analyzer 구성 요소는 사용자 컴퓨터에서 시스템 문제를 스캔하고 사용자에게 컴퓨터의 전반적인 성능을 저하시킬 수 있는 항목에 대한 명확한 개요를 제공할 수 있습니다. 이 구성 요소의 사용자 인터페이스에서는 레지스트리 오류, 정크 파일, 조각화 및 손상된 바로 가기 등 각 범주를 나타내는 네 줄로 나뉜 차트를 확인할 수 있습니다.



- **레지스트리 오류**는 Windows 레지스트리의 오류 개수를 알려 줍니다. 레지스트리를 수정하는 데에는 상당한 고급 지식이 필요하므로 사용자가 직접 레지스트리를 수정하는 것은 권장되지 않습니다.
- **정크 파일**은 없어도 작업에 문제가 되지 않는 파일의 수를 알려 줍니다. 대개 여러 가지 종류의 임시 파일, 휴지통에 있는 파일 등이 여기에 포함됩니다.
- **조각화**에서는 하드 디스크가 조각난 수준을 백분율로 계산하여 보여 줍니다. 하드 디스크를 오래 사용하게 되면 많은 파일이 실제 디스크의 여러 부분에 분산됩니다. 일부 조각 모음 도구를 사용하여 이러한 문제를 해결할 수 있습니다.
- **손상된 바로 가기**는 없는 위치로 연결되는 등 더 이상 작동하지 않는 바로 가기를 알려 줍니다.

시스템 분석을 시작하려면 **지금 분석** 단추를 누릅니다. 그런 다음 차트에서 바로 분석 진행률 및 그 결과를 확인할 수 있습니다.



결과 개요에는 테스트되는 각 범주를 기준으로 분류되어 검색된 시스템 문제(**오류**)의 개수가 나와 있습니다. 또한 분석 결과는 **심각도** 열의 측에 그래픽으로도 표시됩니다.

제어 단추

- **지금 분석**(분석이 시작되기 전에 표시됨) - 이 단추를 누르면 컴퓨터 분석이 즉시 시작됩니다.
- **지금 수정**(분석이 완료된 후에 표시됨) - 이 단추를 누르면 AVG 웹 사이트 (<http://www.avg.com/>)에서 **PC Analyzer** 구성 요소와 관련된 자세한 최신 정보를 제공하는 페이지로 이동합니다.
- **취소** - 이 단추를 누르면 실행 중인 분석을 중지하거나, 분석이 완료된 후 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.

6.8. Identity Protection

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. **Identity Protection**은 ID 도용자가 PC를 대상으로 하는 모든 종류의 악의적인 소프트웨어(맬웨어)를 통해 사용자의 암호, 은행 계좌 정보, 신용카드 번호 및 기타 개인 디지털 자산을 훔치지 못하도록 방지하는 데 주력합니다. 또한, PC에서 실행되는 모든 프로그램이 올바르게 작동하도록 보호합니다. **Identity Protection**은 지속적으로 의심스러운 동작을 검색하고 차단하며 컴퓨터를 새로운 모든 맬웨어로부터 보호합니다.



Identity Protection 구성 요소는 컴퓨터에서 새로운 위협 요소와 알려지지 않은 위협 요소에 대한 실시간 보호 기능을 제공합니다. 이 구성 요소는 숨겨진 프로세스를 포함한 모든 프로세스와 285 가지 이상의 다양한 동작 패턴을 모니터링하여 시스템 내에서 악의적인 동작이 발생하는지 확인합니다. 따라서 이 구성 요소는 바이러스 데이터베이스에 정의되지 않은 위협 요소를 발견할 수 있습니다. 이 구성 요소는 컴퓨터에 알려지지 않은 코드가 유입될 때마다 즉시 해당 코드가 악의적인 동작을 일으키는 지 감시하고 추적합니다. 파일이 악의적인 파일로 판단되는 경우 **Identity Protection**은 코드를 [바이러스 저장소](#)로 이동하고 시스템의 모든 변경 사항(코드 삽입, 레지스트리 변경, 포트 열기 등)을 취소합니다.. 사용자는 스캔을 시작하지 않아도 보호를 받습니다. 이 기술은 업데이트가 거의 필요하지 않고 항상 보호 기능을 수행한다는 점에서 사전 예방적인 측면이 돋보인다고 할 수 있습니다.

Identity Protection은 [Anti-Virus](#)를 보완하는 보호 기능입니다. PC를 완벽하게 보호하려면 두 구성 요소를 모두 설치하는 것이 좋습니다.

6.8.1. Identity Protection 인터페이스



Identity Protection 대화 상자에서는 구성 요소의 기본 기능, 해당 상태(활성) 및 몇 가지 통계 데이터에 대한 간략한 설명을 제공합니다.

- **제거된 위협 항목 수** - 맬웨어로 검색되어 제거된 응용 프로그램 수를 표시합니다.
- **모니터링되는 프로세스** - IDP에서 모니터링되고 있는 현재 실행 중인 응용 프로그램의 수
- **모니터링되는 동작** - 모니터링되는 응용 프로그램 내에서 실행되고 있는 특정 동작의 수



아래쪽에서는 [모니터링되는 프로세스 및 활동 모니터 표시](#) 링크를 찾을 수 있습니다. 이 링크는 모니터링되는 모든 프로세스에 대한 상세한 개요를 확인할 수 있는 [시스템 도구](#) 구성 요소의 사용자 인터페이스로 연결됩니다.

기본 Identity Protection 설정

대화 상자의 아래쪽에서는 구성 요소의 기능에 대한 기본적인 기능을 편집할 수 있습니다.

- **Identity Protection 활성화** - (기본적으로 설정되어 있음): IDP 구성 요소를 활성화하고 추가 편집 옵션을 열려면 선택합니다.

Identity Protection 에서 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.

- o **항상 묻기** - 응용 프로그램이 맬웨어로 발견된 경우 항상 사용자에게 차단 여부를 묻습니다(이 옵션은 기본적으로 설정되어 있으며 특별한 이유가 없다면 변경하지 않는 것이 좋음).
- o **발견된 위협 요소 자동 검역** - 맬웨어로 발견된 모든 응용 프로그램을 자동으로 차단합니다.
- o **알려진 위협 요소 자동 검역** - 발견된 응용 프로그램이 맬웨어라고 확인되는 경우에만 해당 응용 프로그램을 차단합니다.

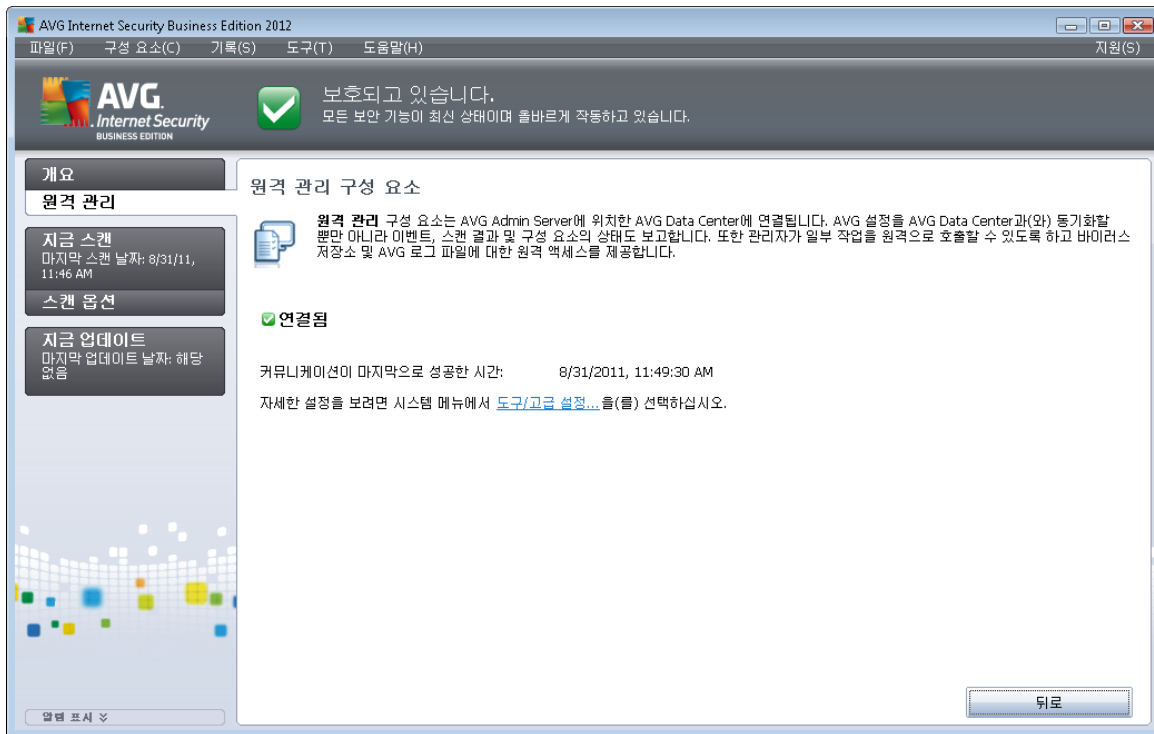
제어 단추

Identity Protection 인터페이스에서 사용할 수 있는 제어 단추는 다음과 같습니다.

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



6.9. 원격 관리



원격 관리 구성 요소는 **AVG Internet Security 2012** 프로그램의 Business Edition을 설치한 경우에만 해당 제품의 사용자 인터페이스에 표시됩니다. **설치에 사용된 라이선스에 대한 내용은 [지원](#) 시스템 메뉴 항목에서 열 수 있는 [정보](#) 대화 상자의 [버전](#) 탭을 참조하십시오**. **원격 관리 구성 요소** 대화 상자에서는 구성 요소가 활성 상태인지와 해당 구성 요소가 서버에 연결되어 있는지 여부를 확인할 수 있습니다. **원격 관리** 구성 요소의 모든 설정은 **고급 설정/원격 관리**에서 수행됩니다.

구성 요소 옵션 및 AVG 원격 관리 시스템의 기능에 대한 자세한 설명은 이 항목과 관련된 특정 설명서를 참조하십시오. 이 설명서는 AVG 웹 사이트 (<http://www.avg.com/>) 의 **지원 센터/다운로드/설명서** 섹션에서 다운로드할 수 있습니다.

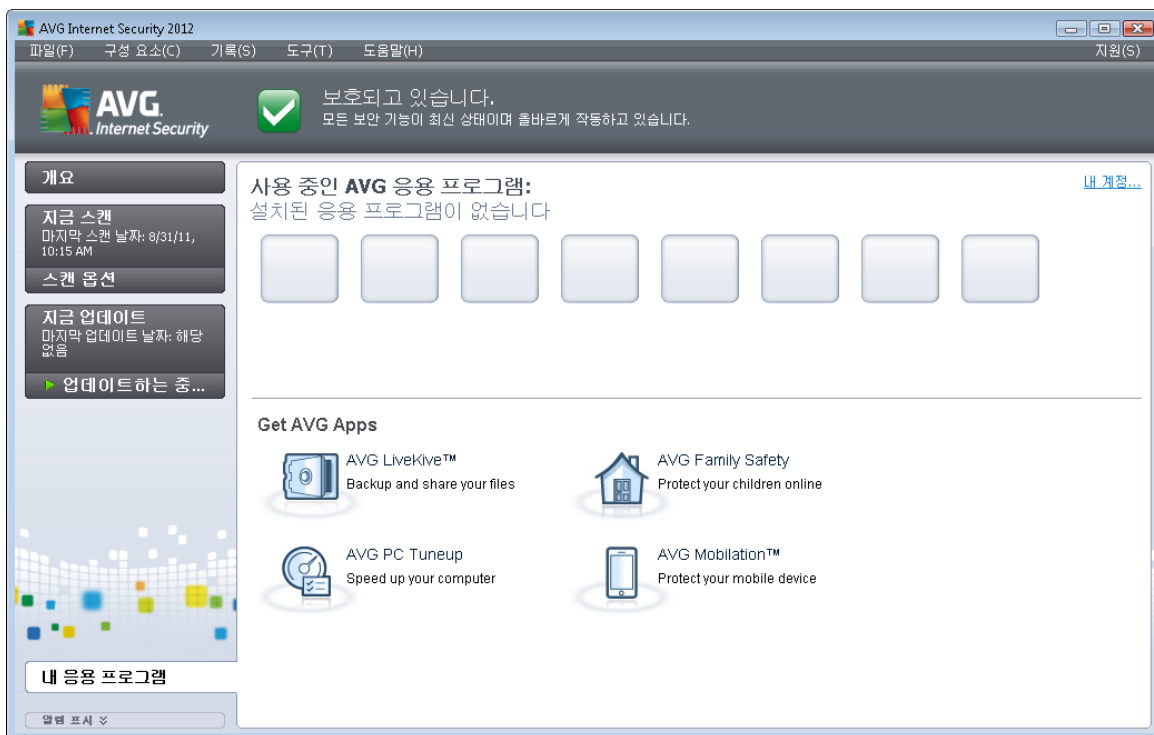
제어 단추

- **뒤로** - 이 단추를 누르면 [AVG 기본 대화 상자](#)(구성 요소 개요)로 돌아갑니다.



7. 내 응용 프로그램

다음의 세 가지 응용 프로그램인 [LiveKive](#), [Family Safety](#) 및 [PC Tuneup](#) 각각은 독립 실행형 AVG 제품으로 사용할 수 있으며 **AVG Internet Security 2012** 설치의 옵션 항목입니다. AVG 기본 대화 상자의 **내 응용 프로그램** 단추를 통해 직접 액세스할 수 있는 **사용 중인 AVG 응용 프로그램** 대화 상자에서는 이미 설치되어 있는 응용 프로그램 및 선택적으로 설치할 준비가 되어 있는 응용 프로그램에 대한 개요를 볼 수 있습니다.



7.1. LiveKive

LiveKive는 보안이 유지되는 서버에서 온라인 데이터 백업에만 사용됩니다. **LiveKive**는 모든 사용자 파일, 사진 및 음악을 자동으로 안전한 장소에 백업하기 때문에 사용자는 이러한 콘텐츠를 가족 및 친구와 공유하고, iPhone 및 Android 장치를 비롯한 모든 웹 사용 기기에서 액세스할 수 있습니다. **LiveKive**에는 다음과 같은 기능이 포함됩니다.

- 사용자 컴퓨터 및/또는 하드 디스크가 손상된 경우를 대비한 안전 장치 제공
- 인터넷에 연결된 장치에서 사용자 데이터에 액세스 지원
- 간편한 구성
- 사용자가 인증한 다른 사람과 공유 가능

자세한 내용을 보려면 이 구성 요소를 즉시 다운로드할 수 있는 전용 AVG 웹 페이지를 방문하십시오. 이 웹 페이지는 [내 응용 프로그램](#) 대화 상자의 LiveKive 링크를 통해 볼 수 있습니다.



7.2. Family Safety

Family Safety를 사용하면 부적절한 웹 사이트, 미디어 콘텐츠 및 온라인 검색으로부터 자녀를 보호하며 자녀의 온라인 활동 내용을 보고서로 알려 줍니다. 각 자녀에게 적합한 보호 수준을 설정하고 고유 로그인을 통해 자녀를 개별적으로 모니터링할 수 있습니다.

자세한 내용을 보려면 이 구성 요소를 즉시 다운로드할 수 있는 전용 AVG 웹 페이지를 방문하십시오. 이 웹 페이지는 [내 응용 프로그램 대화 상자](#)의 Family Safety 링크를 통해 볼 수 있습니다.

7.3. PC Tuneup

PC Tuneup 응용 프로그램은 세부적인 시스템 분석 및 수정을 위한 고급 도구로, 이를 이용하면 컴퓨터의 속도와 전반적인 성능을 향상시키는 방법을 알 수 있습니다. **PC Tuneup**에는 다음과 같은 기능이 포함됩니다.

- 디스크 정리 도구 - 컴퓨터 속도를 저하시키는 정크 파일을 제거합니다.
- 디스크 조각 모음 - 디스크 드라이브에 대해 조각 모음을 실행하여 시스템 파일 배치를 최적화합니다.
- 레지스트리 정리 도구 - 레지스트리 오류를 복구하여 PC 안정성을 높입니다.
- 레지스트리 조각 모음 - 레지스트리를 압축하여 메모리를 차지하는 공간을 제거합니다.
- 디스크 닥터 - 불량 섹터, 손실된 클러스터 및 디렉터리 오류를 찾아서 수정합니다.
- 인터넷 최적화 도구 - 공통적으로 사용되는 설정을 특정 인터넷 연결에 맞게 구성합니다.
- 추적 정보 제거 도구 - 컴퓨터 및 인터넷 사용 기록을 제거합니다.
- 디스크 청소 도구 - 중요한 데이터를 복구하지 못하도록 디스크의 사용 가능한 공간을 청소합니다.
- 파일 분쇄기 - 디스크나 USB 스틱에서 선택한 파일을 복구 불가능하도록 삭제합니다.
- 파일 복구 - 디스크, USB 스틱 또는 카메라에서 실수로 삭제한 파일을 복구합니다.
- 중복 파일 검색 도구 - 디스크 공간을 차지하는 중복 파일을 찾아서 제거하는 데 도움을 줍니다.
- 서비스 관리자 - 불필요한 서비스로 인해 컴퓨터 속도가 느려지지 않도록 방지합니다.
- 시작 관리자 - Windows 부팅 시 자동으로 시작되는 프로그램을 사용자가 관리할 수 있게 도와줍니다.



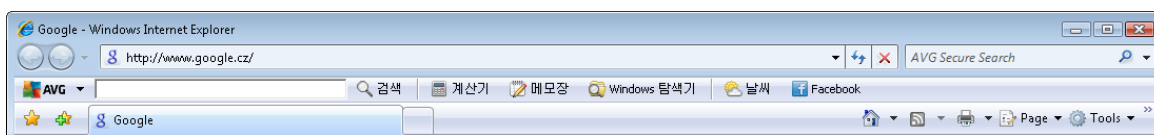
- 제거 관리자 - 더 이상 필요하지 않은 소프트웨어 프로그램을 완전히 제거합니다.
- 조정 관리자 - 수백 개의 숨겨진 Windows 설정을 사용자가 조정할 수 있도록 도와줍니다.
- 작업 관리자 - 실행 중인 모든 프로세스, 서비스 및 잠겨진 파일을 나열합니다.
- 디스크 탐색기 - 컴퓨터에서 가장 많은 공간을 차지하는 파일을 보여줍니다.
- 시스템 정보 - 설치되어 있는 하드웨어와 소프트웨어에 대한 자세한 정보를 제공합니다.

자세한 내용을 보려면 이 구성 요소를 즉시 다운로드할 수 있는 전용 AVG 웹 페이지를 방문하십시오. 이 웹 페이지는 [내 응용 프로그램](#) 대화 상자의 PC Tuneup 링크를 통해 볼 수 있습니다.



8. AVG Security Toolbar

AVG Security Toolbar는 [LinkScanner](#) 구성 요소와 함께 사용되는 도구로, 인터넷을 검색하는 동안 최대한의 보안을 제공합니다. **AVG Internet Security 2012**에서는 **AVG Security Toolbar** 설치가 선택 사항이며 [설치 프로세스](#) 동안 구성 요소를 설치할 것인지 여부를 결정하게 됩니다. **AVG Security Toolbar**는 인터넷 브라우저에서 직접 사용할 수 있습니다. 현재 지원되는 인터넷 브라우저는 Internet Explorer (**버전 6.0 이상**) 및/또는 Mozilla Firefox (**버전 3.0 이상**)입니다. 다른 브라우저는 지원되지 않습니다(*Avant Browser와 같은 대체 인터넷 브라우저를 사용하는 경우에는 예기치 않은 동작이 발생할 수 있음*).



AVG Security Toolbar는 다음과 같은 항목으로 구성됩니다.

- **다음과 같은 드롭다운 메뉴가 있는 AVG 로고:**

- **AVG Secure Search 사용** - **AVG Security Toolbar**에서 **AVG Secure Search** 엔진을 사용하여 직접 검색할 수 있습니다. 모든 검색 결과가 [Search-Shield](#) 서비스에 의해 지속적으로 검사되므로 절대적인 온라인 보안을 유지할 수 있습니다.
- **현재 위험 수준** - 웹의 현재 위험 수준을 그래픽으로 보여 주는 바이러스 연구실 웹 페이지를 엽니다.
- **AVG Threat Labs** - 이름별로 특정 위험 요소를 검색하고 각각의 위험 요소에 대한 자세한 정보를 볼 수 있는 AVG 웹 사이트(<http://www.avg.com/>)의 **사이트 보고서** 페이지를 엽니다.
- **도구 모음 도움말** - 모든 **AVG Security Toolbar** 기능에 대한 설명이 포함된 온라인 도움말을 엽니다.
- **제품 피드백 제출** - **AVG Security Toolbar**에 대한 피드백을 입력할 수 있는 양식이 포함된 웹 페이지를 엽니다.
- **정보...** - 현재 설치된 **AVG Security Toolbar** 버전에 대한 정보가 들어 있는 새 창을 엽니다.
- **검색 필드** - **AVG Security Toolbar**를 사용하여 표시된 모든 검색 결과는 완전히 안전한 것으로 간주할 수 있으므로 인터넷 검색을 간편하고 안전하게 수행할 수 있습니다. 검색 필드에 키워드나 구를 입력하고 **검색** 단추(또는 Enter 키)를 누릅니다. 모든 검색 결과는 [Search-Shield](#) 서비스([LinkScanner](#) 구성 요소에 포함됨)에 의해 지속적으로 검사됩니다.
- 다음 응용 프로그램에 빠르게 액세스할 수 있는 바로 가기 단추: **계산기**, **메모장**, **Windows 탐색기**
- **날씨** - 이 단추는 사용자 지역의 현재 날씨에 대한 정보와 앞으로 이틀 동안의 일기 예보를 제공하는 새 대화 상자를 엽니다. 이 정보는 3-6 시간마다 정기적으로

업데이트됩니다. 이 대화 상자에서는 원하는 지역으로 직접 변경할 수 있으며 온도를 섭씨로 표시할지 아니면 화씨로 표시할지 결정할 수 있습니다.



- **Facebook** - 이 단추를 사용하면 **AVG Security Toolbar** 에서 직접 [Facebook](#) 소셜 네트워크에 연결할 수 있습니다.

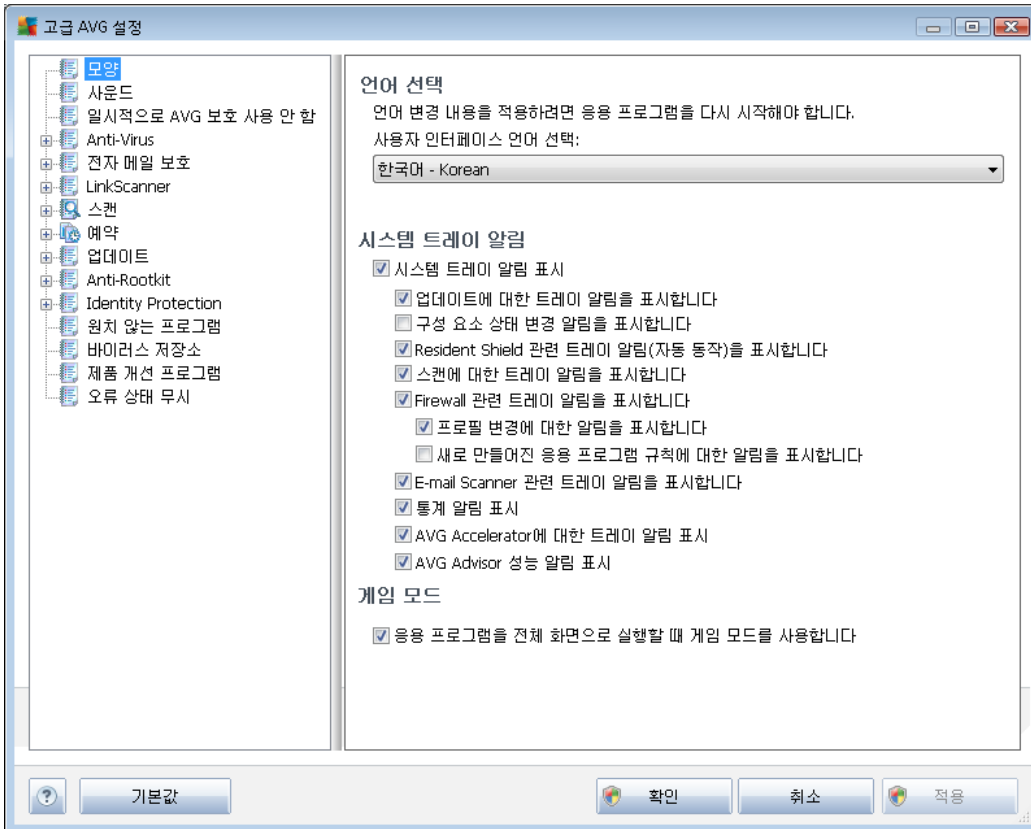


9. AVG 고급 설정

AVG Internet Security 2012의 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.

9.1. 모양

탐색 트리의 첫 번째 항목인 **모양**은 AVG Internet Security 2012 [사용자 인터페이스](#)의 일반 설정을 나타내며 응용 프로그램 동작의 몇 가지 기본 옵션을 제공합니다.

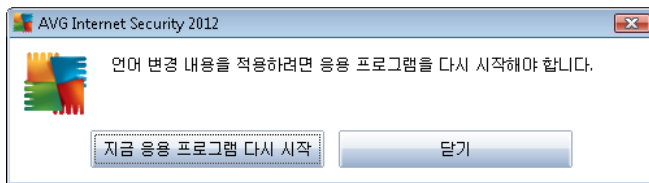


언어 선택

언어 선택 섹션의 드롭다운 메뉴에서 원하는 언어를 선택할 수 있습니다. 선택된 언어는 전체 **AVG Internet Security 2012 사용자 인터페이스**에 사용됩니다. 이 드롭다운 메뉴에서는 이전에 **설치 프로세스**에서 설치하도록 선택한 언어([사용자 지정 옵션](#) 장 참조)와 영어(영어는 항상 자동으로 기본 설치됨)만 제공합니다. **AVG Internet Security 2012**를 다른 언어로 전환하는 작업을 완료하려면 응용 프로그램을 다시 시작해야 합니다. 다음 단계를 수행합니다.

- 드롭다운 메뉴에서 응용 프로그램에 사용할 언어를 선택합니다.

- **적용** 단추(대화 상자의 오른쪽 하단 모서리에 있음)를 눌러 선택을 확인합니다.
- **확인** 단추를 눌러 확인합니다.
- 새 대화 상자에서 응용 프로그램의 언어를 변경하려면 **AVG Internet Security 2012**
- **지금 응용 프로그램 다시 시작** 단추를 눌러 프로그램을 다시 시작하는 데 동의하고 언어 변경이 적용될 때까지 잠시 기다립니다.



시스템 트레이 알림

이 섹션에서는 **AVG Internet Security 2012** 응용 프로그램 상태에 대한 시스템 트레이 알림이 표시되지 않도록 설정할 수 있습니다. 기본적으로 시스템 알림은 표시되도록 설정됩니다. 이 구성을 유지하는 것이 좋습니다. 시스템 알림은 예를 들어 스캔 또는 업데이트 프로세스의 시작을 알려주거나 **AVG Internet Security 2012** 구성 요소의 상태 변경에 대해 알려 줍니다. 이러한 알림에는 반드시 주의를 기울여야 합니다.

하지만 특별한 이유로 이러한 방식으로 알림을 받지 않으려고 하거나 특정 알림(특정 **AVG Internet Security 2012** 구성 요소와 관련된 알림)만 표시되게 하려면 다음 옵션을 선택/선택 취소하여 원하는 설정을 정의하고 지정할 수 있습니다.

- **시스템 트레이 알림 표시(기본적으로 설정되어 있음)** - 기본적으로 모든 알림이 표시됩니다. 모든 시스템 알림의 표시를 해제하려면 이 항목의 선택을 취소합니다. 이 항목을 설정한 경우에는 표시하려는 특정 알림을 선택할 수 있습니다.
 - o **업데이트**에 대한 트레이 알림을 표시합니다.(기본적으로 설정되어 있음) - **AVG Internet Security 2012** 업데이트 프로세스 시작, 진행 상황 및 완료와 관련된 정보를 표시할지 여부를 결정합니다.
 - o **구성 요소 상태 변경 알림을 표시합니다.**(기본적으로 해제되어 있음) - 구성 요소의 활성화/비활성화 또는 그와 관련하여 발생 가능한 문제에 대한 정보를 표시할지 여부를 결정합니다. 구성 요소의 오류 상태를 보고할 때 이 옵션은 **AVG Internet Security 2012** 구성 요소의 문제를 보고하는 **시스템 트레이 아이콘**의 정보 기능과 같습니다.
 - o **Resident Shield 관련 트레이 알림(자동 동작)을 표시합니다.**(기본적으로 설정되어 있음) - 파일 저장, 복사 및 열기 프로세스 관련 정보를 표시하거나 표시하지 않을지를 결정합니다(이 구성은 Resident Shield의 **자동 치료** 옵션이 설정되어 있는 경우에만 표시됨).
 - o **스캔**에 대한 트레이 알림을 표시합니다.(기본적으로 설정되어 있음) - 예약된 스캔의 자동 시작, 진행 상황 및 결과에 대한 정보를 표시할지 여부를 결정합니다.

- o **Firewall** 관련 트레이 알림을 표시합니다.(기본적으로 설정되어 있음) - **Firewall** 상태 및 프로세스 관련 정보(예: 구성 요소의 활성화/비활성화 경고, 발생 가능한 트래픽 차단 등)를 표시할지 여부를 결정합니다. 이 항목은 다음 두 개의 세부적인 선택 옵션(이들 각 항목에 대한 자세한 내용은 이 문서의 **Firewall** 장 참조)을 제공합니다.
 - **프로필 변경에 대한 알림을 표시합니다.**(기본적으로 설정되어 있음) - **Firewall** 프로필의 자동 변경 사항에 대해 알려 줍니다.
 - **새로 만들어진 응용 프로그램 규칙에 대한 알림을 표시합니다.**(기본적으로 해제되어 있음) - 안전한 응용 프로그램 목록을 기반으로 새 응용 프로그램에 대한 **Firewall** 규칙의 자동 생성에 대해 알려 줍니다.
- o **E-mail Scanner** 관련 트레이 알림을 표시합니다.(기본적으로 설정되어 있음) - 들어오거나 나가는 모든 전자 메일 메시지에 대한 스캔 정보를 표시할지 여부를 결정합니다.
- o **통계 알림 표시**(기본적으로 설정되어 있음) - 이 옵션을 선택된 상태로 유지하면 정기적인 통계 검토 알림이 시스템 트레이에 표시됩니다.
- o **AVG Accelerator** 에 대한 트레이 알림 표시(기본적으로 설정되어 있음) - **AVG Accelerator** 활동에 대한 정보를 표시해야 하는지 여부를 결정합니다. **AVG Accelerator** 서비스는 온라인 비디오를 매끄럽게 재생하고 추가 다운로드를 간편하게 수행하도록 도와 줍니다.
- o **AVG Advice** 성능 알림 표시(기본적으로 설정되어 있음) - **AVG Advice** 는 지원되는 인터넷 브라우저 (*Internet Explorer, Chrome, Firefox, Opera, 및 Safari*)의 성능을 감시하고 해당 브라우저가 권장되는 메모리 양을 초과하여 사용하는 경우 이를 사용자에게 알려 줍니다. 이 경우 컴퓨터 성능이 상당히 느려질 수 있으므로 속도를 높이려면 인터넷 브라우저를 다시 시작하는 것이 좋습니다. 알림을 받으려면 **AVG Advice** 성능 알림 표시 항목이 설정되어 있는 채로 둡니다.



게임 모드

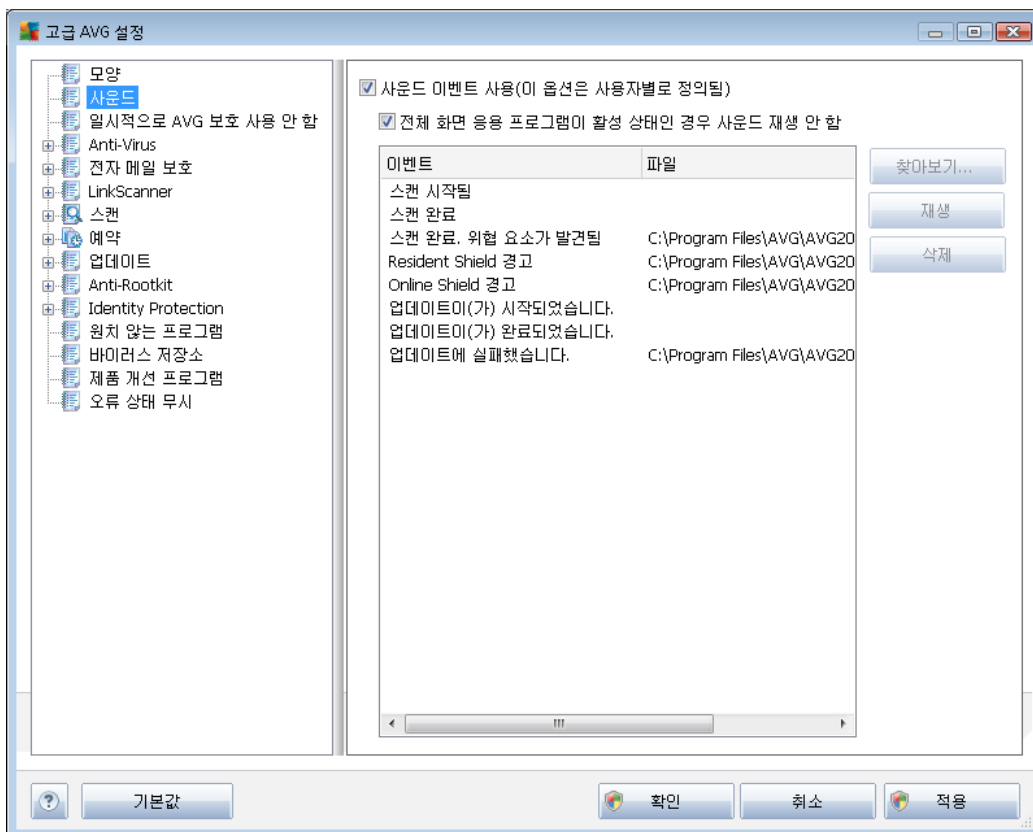
이 AVG 기능은 AVG 정보 풍선(예를 들어 예약된 스캔이 시작되는 경우에 표시)으로 인해 방해(응용 프로그램 최소화 또는 그래픽 손상)를 받을 수 있는 전체 화면 응용 프로그램에 적합하게 설계되었습니다. 이러한 상황을 방지하려면 **응용 프로그램을 전체 화면으**



로 실행할 때 게임 모드를 사용합니다. 옵션 확인란을 선택된 상태(기본 설정)로 두십시오.

9.2. 사운드

사운드 대화 상자 내에서 사운드 알림을 통해 특정 **AVG Internet Security 2012** 작업에 대한 알림을 받을지 여부를 지정할 수 있습니다.



이 설정은 현재 사용자 계정에 대해서만 유효하므로 컴퓨터의 각 사용자는 자신만의 사운드 설정을 지정할 수 있습니다. 사운드 알림을 받으려면 먼저 **사운드 이벤트 사용** 옵션(이 옵션은 기본적으로 설정되어 있음)을 선택하여 관련된 모든 작업 목록을 활성화해야 합니다. 또한 **전체 화면 응용 프로그램이 활성 상태인 경우 사운드 재생 안 함** 옵션을 선택하여 사운드 알림이 필요하지 않은 상황에서는 이를 해제할 수 있습니다. 자세한 내용은 이 문서의 [고급 설정/모양](#) 장에서 게임 모드 섹션을 참조하십시오.

제어 단추

- **찾아보기** - 목록에서 해당 이벤트를 선택한 경우 **찾아보기** 단추를 사용하여 할당하려는 사운드 파일에 사용할 디스크를 검색합니다. 참고: 현재 *.wav 사운드만 지원됩니다!
- **재생** - 선택한 사운드를 들어 보려면 목록에서 이벤트를 강조 표시하고 **재생** 단추를 누릅니다.

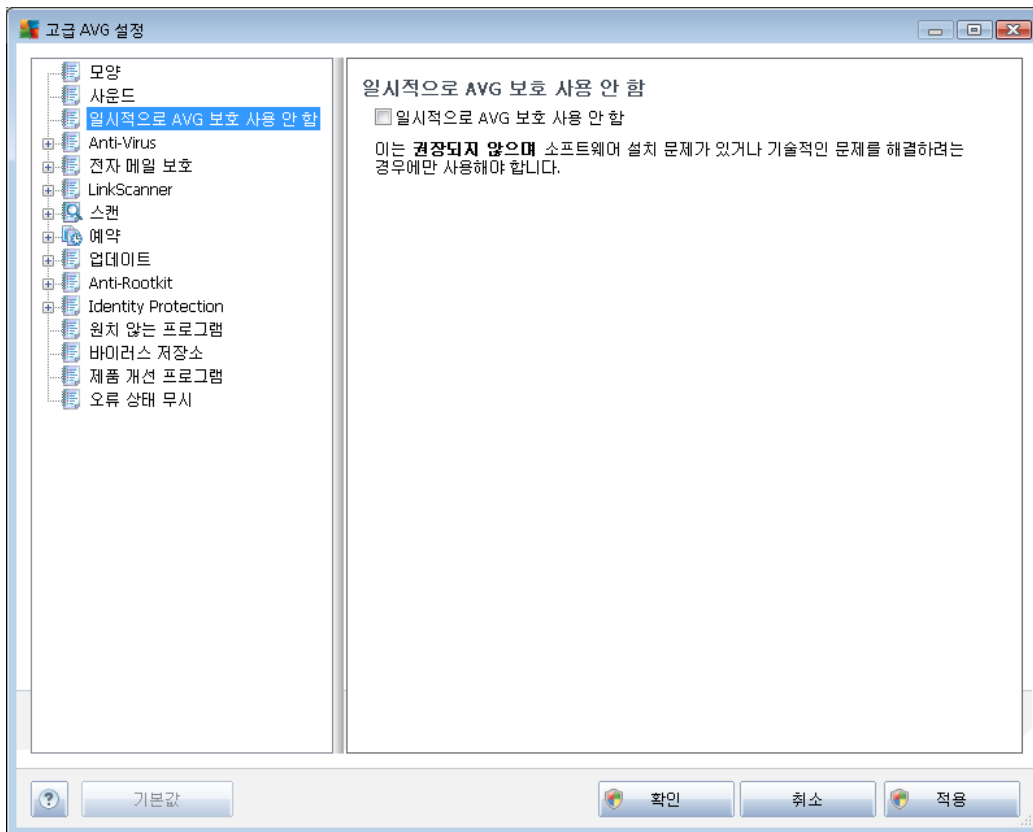


- **삭제** - 특정 이벤트에 할당된 사운드를 제거하려면 **삭제** 단추를 사용합니다.

9.3. 일시적으로 AVG 보호 사용 안 함

일시적으로 AVG 보호 사용 안 함 대화 상자에는 **AVG Internet Security 2012** 에서 제공하는 전체 보호 기능을 한 번에 해제하는 옵션이 있습니다.

반드시 필요한 경우가 아니면 이 옵션을 사용하지 마십시오.



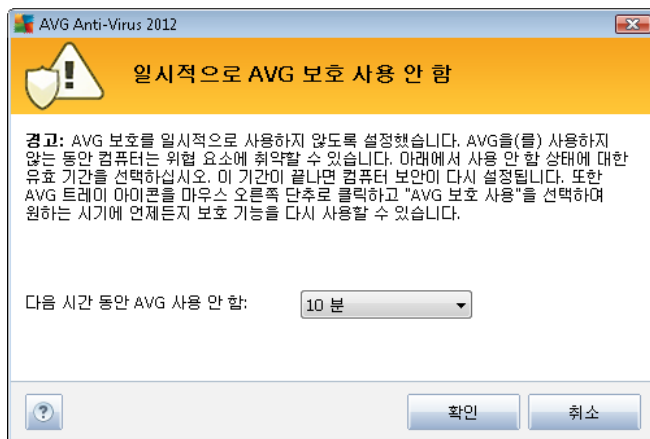
대부분의 경우 **AVG Internet Security 2012** 프로그램을 비활성화하지 않고도 새로운 소프트웨어나 드라이버를 설치할 수 있습니다. 설치 관리자나 소프트웨어 마법사에서 설치 프로세스 중에 중단되지 않도록 실행 중인 프로그램과 응용 프로그램을 종료하도록 요구하는 경우에도 마찬가지입니다. 설치 중에 문제가 발생하면 먼저 [Resident Shield](#) 를 **비활성화** (*Resident Shield* 사용)해 보십시오. 일시적으로 **AVG Internet Security 2012** 프로그램을 비활성화해야 하는 경우 해당 작업을 마치는 즉시 다시 활성화해야 합니다. 바이러스 백신 소프트웨어가 비활성화되어 있는 동안 인터넷이나 네트워크에 연결하면 컴퓨터가 공격에 취약해질 수 있습니다.

AVG 보호를 비활성화하는 방법

- **일시적으로 AVG 보호 사용 안 함** 확인란을 선택하고 **적용** 단추를 눌러 선택을 확인합니다.



- 새로 열린 **일시적으로 AVG 보호 사용 안 함** 대화 상자에서 **AVG Internet Security 2012** 프로그램을 비활성화할 기간을 지정할 수 있습니다. 기본적으로 10분 정도 보호 기능을 비활성화하면 새 소프트웨어를 설치하는 등의 작업을 충분히 수행할 수 있습니다. 초기 시간 제한은 15분으로 설정되어 있을 수 있으며 보안상의 이유 때문에 이 값은 재정의할 수 없다는 점에 유의해 주십시오. 지정된 기간이 경과하면 모든 비활성화된 구성 요소가 자동으로 다시 활성화됩니다.

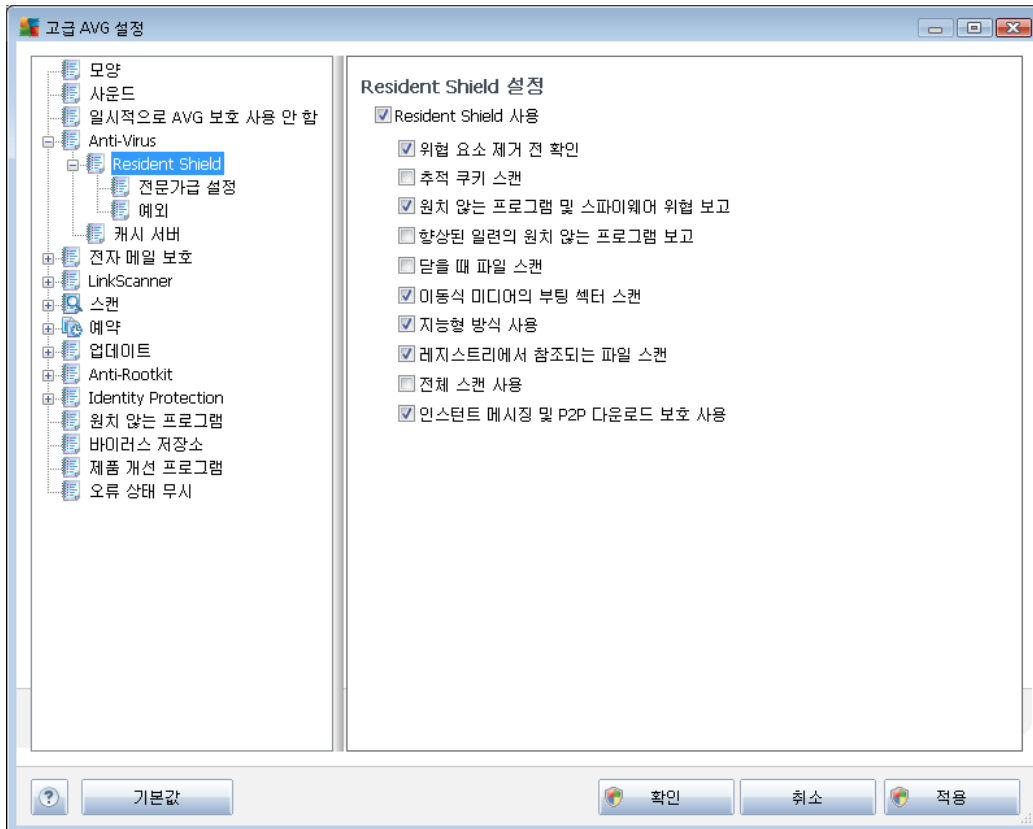


9.4. Anti- Virus

여기에 항목 텍스트를 입력하십시오.

9.4.1. Resident Shield

Resident Shield 는 파일 및 폴더를 바이러스, 스파이웨어 및 기타 맬웨어로부터 실시간으로 보호해 줍니다.



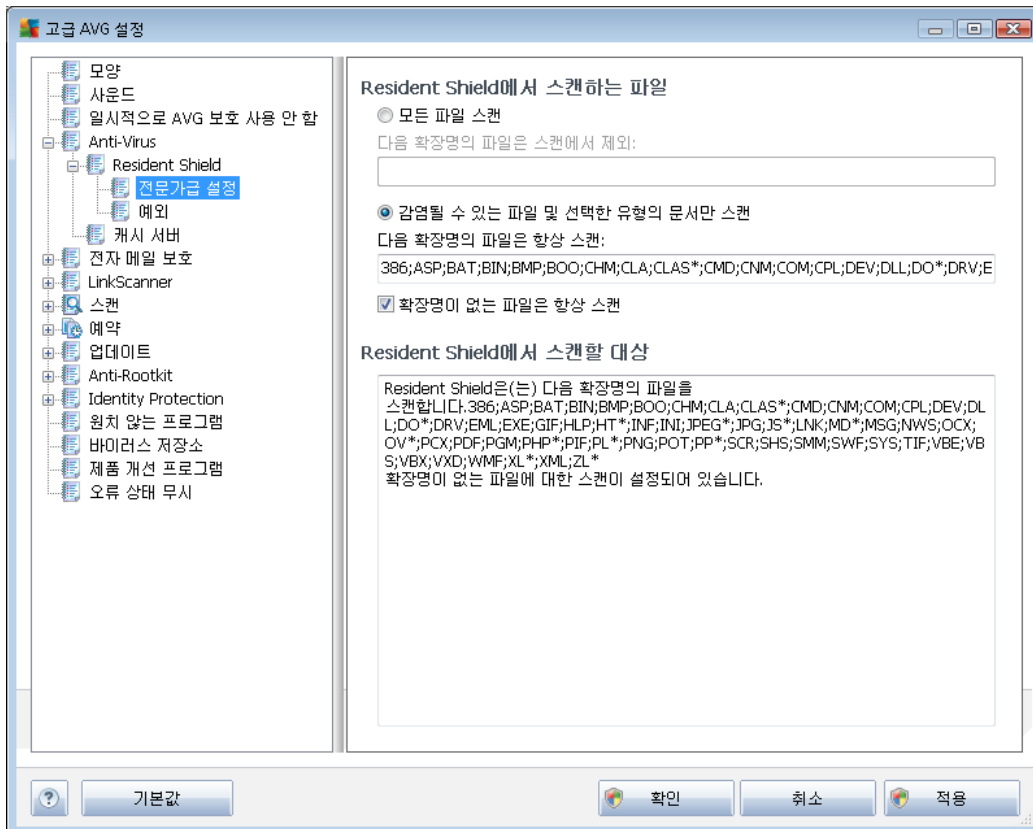
Resident Shield 설정 대화 상자에서 **Resident Shield 사용** 항목을 선택하거나 선택 취소하여 Resident Shield 기능을 완전히 활성화하거나 비활성화할 수 있습니다. 이 옵션은 기본적으로 설정되어 있습니다. 또한 다음과 같이 활성화해야 할 Resident Shield 기능을 선택할 수도 있습니다.

- **추적 쿠키 스캔**(기본적으로 해제되어 있음) - 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.
- **원치 않는 프로그램 및 스파이웨어 위협 보고**(기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스파이웨어](#)는 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**(기본적으로 해제되어 있음) - [스파이웨어](#)의 확장 패키지를 검색하려면 이 상자를 선택합니다. 스파이웨어 프로그램은 제조업체에서 바로 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 오용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되

지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.

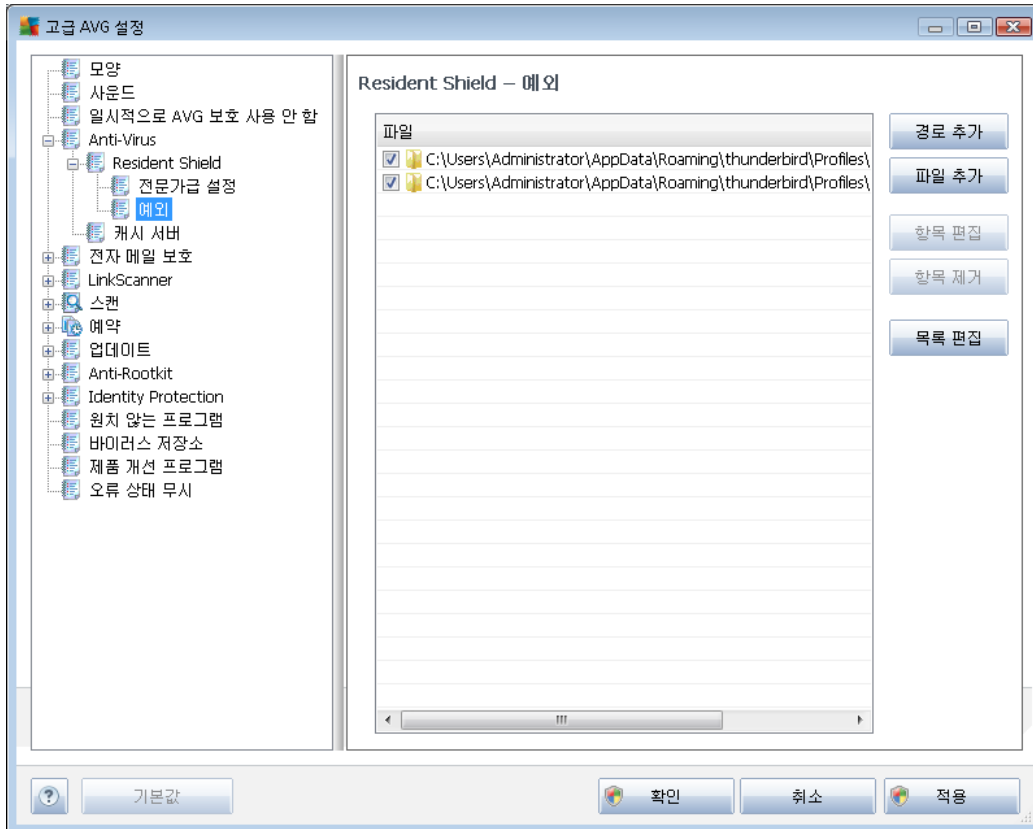
- **닫을 때 파일 스캔**(기본적으로 해제되어 있음) - 닫을 때 스캔 기능을 사용하면 활성 개체(예: 응용 프로그램, 문서)를 열 때는 물론 닫을 때도 해당 개체를 스캔할 수 있습니다. 이 기능은 일부 유형의 복잡한 바이러스로부터 사용자 컴퓨터를 보호하는 데 유용합니다.
- **이동식 미디어의 부팅 섹터 스캔**(기본적으로 설정되어 있음)
- **지능형 방식 사용**(기본적으로 설정되어 있음) - [지능형 분석](#)은 검색에 사용됩니다(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침).
- **모든 위험 요소 자동 제거**(기본적으로 해제되어 있음) - 발견된 모든 감염 요소는 치료가 가능한 경우 자동으로 치료되며, 치료할 수 없는 감염 요소는 모두 제거됩니다.
- **레지스트리에서 참조되는 파일 스캔**(기본적으로 설정되어 있음) - 이 매개 변수는 시작 레지스트리에 추가된 모든 실행 파일을 스캔하여 알려진 감염 요소가 다음에 컴퓨터를 시작할 때 실행되지 않도록 정의합니다.
- **전체 스캔 사용**(기본적으로 해제되어 있음) - 특정한 상황(매우 긴급한 상황)에서 이 옵션을 선택하면 위험이 될 수 있는 모든 개체를 세밀하게 검사하는 전체 스캔 알고리즘을 활성화할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- **인스턴트 메시징 및 P2P 다운로드 보호 사용**(기본적으로 설정되어 있음) - 인스턴트 메시징 커뮤니케이션(예: ICQ, MSN Messenger 등) 및 P2P 다운로드에 바이러스가 없는지 확인하려면 이 항목을 선택합니다.

Resident Shield 에서 스캔 하는 파일 대화 상자에서 스캔할 파일을 구성할 수 있습니다(특정 확장명 기준).



해당 확인란을 선택하여 **모든 파일을 스캔**할지 아니면 **감염될 수 있는 파일 및 선택한 유형의 문서만 스캔**할지 결정합니다. 후자의 경우 스캔에서 제외할 파일을 정의하는 확장명 목록을 추가로 지정할 수 있으며 어떤 상황에서든 스캔해야 하는 파일을 정의하는 파일 확장명 목록을 지정할 수도 있습니다.

아래쪽에 있는 **Resident Shield 에서 스캔할 대상** 섹션에는 현재 설정에 대한 요약과 함께 **Resident Shield** 에서 실제로 스캔하는 대상에 대한 상세한 개요가 표시됩니다.



Resident Shield - 예외 대화 상자에서는 **Resident Shield** 스캔에서 제외할 파일 및/또는 폴더를 정의할 수 있습니다.

반드시 제외해야 하는 경우가 아니라면 어떠한 항목도 제외하지 않는 것이 좋습니다.

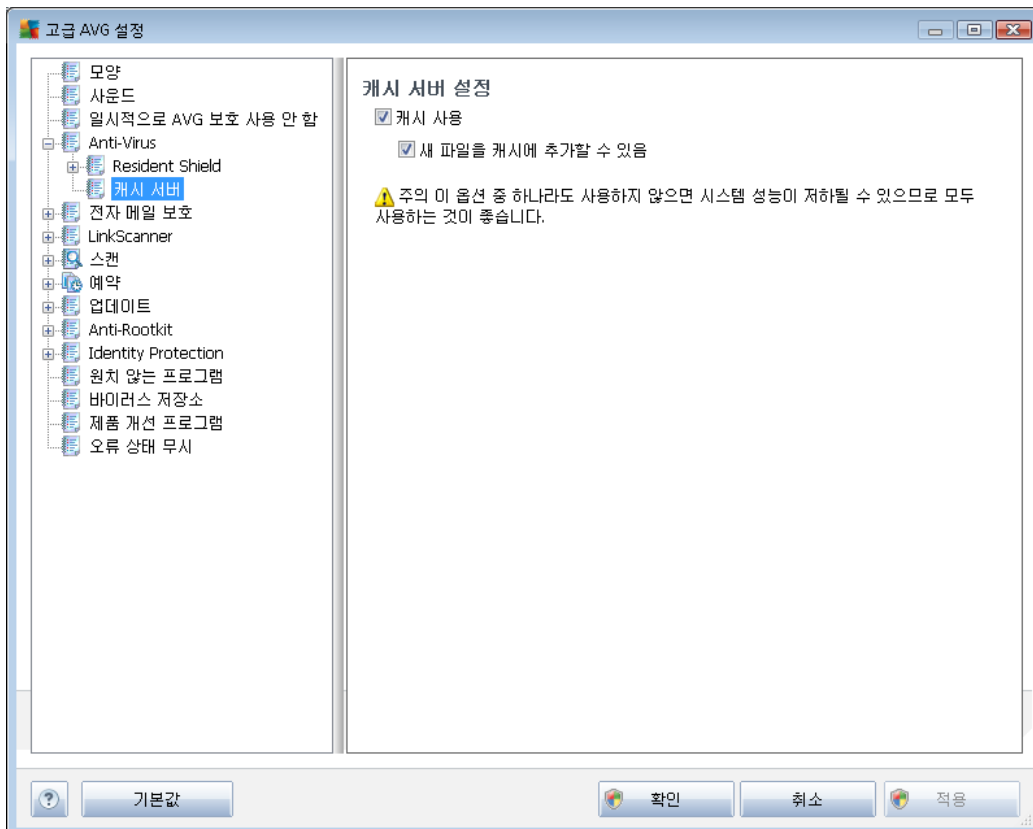
제어 단추

이 대화 상자에는 다음과 같은 제어 단추가 있습니다.

- **경로 추가** - 로컬 디스크 탐색 트리에서 디렉토리를 하나씩 선택하여 스캔에서 제외할 디렉토리를 지정할 수 있습니다.
- **파일 추가** - 로컬 디스크 탐색 트리에서 파일을 하나씩 선택하여 스캔에서 제외할 파일을 지정할 수 있습니다.
- **항목 편집** - 선택한 파일 또는 폴더에 대해 지정된 경로를 편집할 수 있습니다.
- **항목 제거** - 목록에서 선택한 항목의 경로를 삭제할 수 있습니다.
- **목록 편집** - 표준 텍스트 편집기처럼 작동하는 새 대화 상자에서 정의된 예외 목록 전체를 편집할 수 있습니다.

9.4.2. 캐시 서버

캐시 서버 설정 대화 상자는 모든 유형의 **AVG Internet Security 2012** 스캔 속도를 높이기 위해 설계된 캐시 서버 프로세스를 나타냅니다.



캐시 서버는 신뢰할 수 있는 파일(신뢰할 수 있는 원본의 디지털 서명으로 서명된 파일은 신뢰할 수 있는 것으로 간주됨)에 대한 정보를 수집하여 보관합니다. 이러한 파일은 자동으로 안전한 것으로 취급되어 다시 스캔되지 않으므로 스캔하는 동안 건너뛰집니다.

캐시 서버 설정 대화 상자는 다음 구성 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.

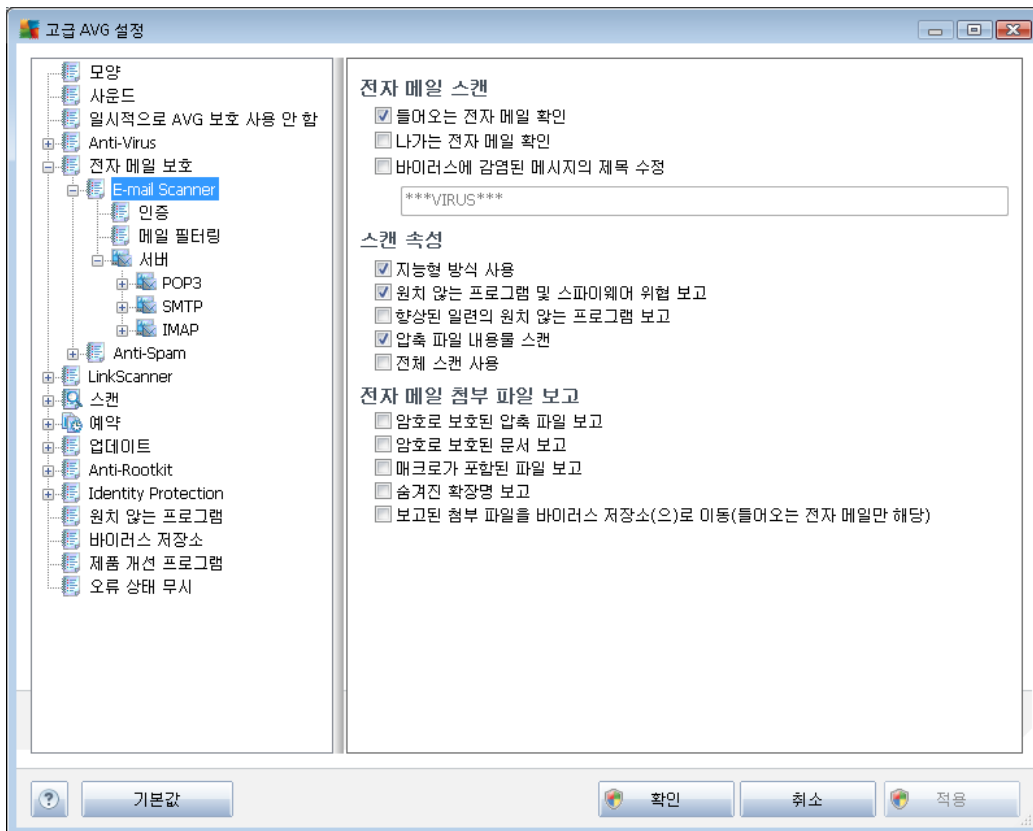
캐시 서버를 반드시 해제해야 할 경우가 아니라면 기본 설정을 유지하여 이 두 옵션을 모두 설정해 두는 것이 좋습니다. 그렇지 않으면 시스템 속도와 성능이 현저하게 저하될 수 있습니다.

9.5. 전자 메일 보호

전자 메일 보호 섹션에서는 [E-mail Scanner](#) 및 [Anti-Spam](#) 의 세부 구성을 편집할 수 있습니다.

9.5.1. E- mail Scanner

E-mail Scanner 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.

- **들어오는 전자 메일 확인**(기본적으로 설정되어 있음) - 전자 메일 클라이언트로 전송된 모든 전자 메일 메시지를 스캔하는 옵션을 설정/해제하려면 선택합니다.
- **나가는 전자 메일 확인**(기본적으로 해제되어 있음) - 사용자 계정에서 보낸 모든 전자 메일을 스캔하는 옵션을 설정/해제하려면 선택합니다.
- **바이러스에 감염된 메시지의 제목 수정**(기본적으로 해제되어 있음) - 스캔된 전자 메일 메시지가 감염된 것으로 검색된 경우 경고 메시지를 받으려면 이 항목을 선택하고 텍스트 필드에 원하는 텍스트를 입력합니다. 그러면 식별 및 필터링이 용이하도록 이 텍스트가 검색된 각 전자 메일 메시지의 "제목" 필드에 추가됩니다. 기본값은 ***VIRUS*** 이며 그대로 유지하는 것이 좋습니다.

스캔 속성

이 섹션에서는 전자 메일 메시지의 스캔 방법을 지정할 수 있습니다.

- **지능형 방식 사용** (기본적으로 설정되어 있음) - 전자 메일 메시지를 스캔할 때 지능형 검색 방식을 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 위험 보고** (기본적으로 설정되어 있음) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. [스파이웨어](#)는 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** (기본적으로 해제되어 있음) - [스파이웨어](#)의 확장 패키지를 검색하려면 선택합니다. 스파이웨어 프로그램은 제조업체에서 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 내용물 스캔** (기본적으로 설정되어 있음) - 전자 메일 메시지에 첨부된 압축 파일의 내용물을 스캔하려면 선택합니다.
- **전체 스캔 사용** (기본적으로 해제되어 있음) - 컴퓨터가 바이러스 또는 익스플로잇에 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.

전자 메일 첨부 파일 보고

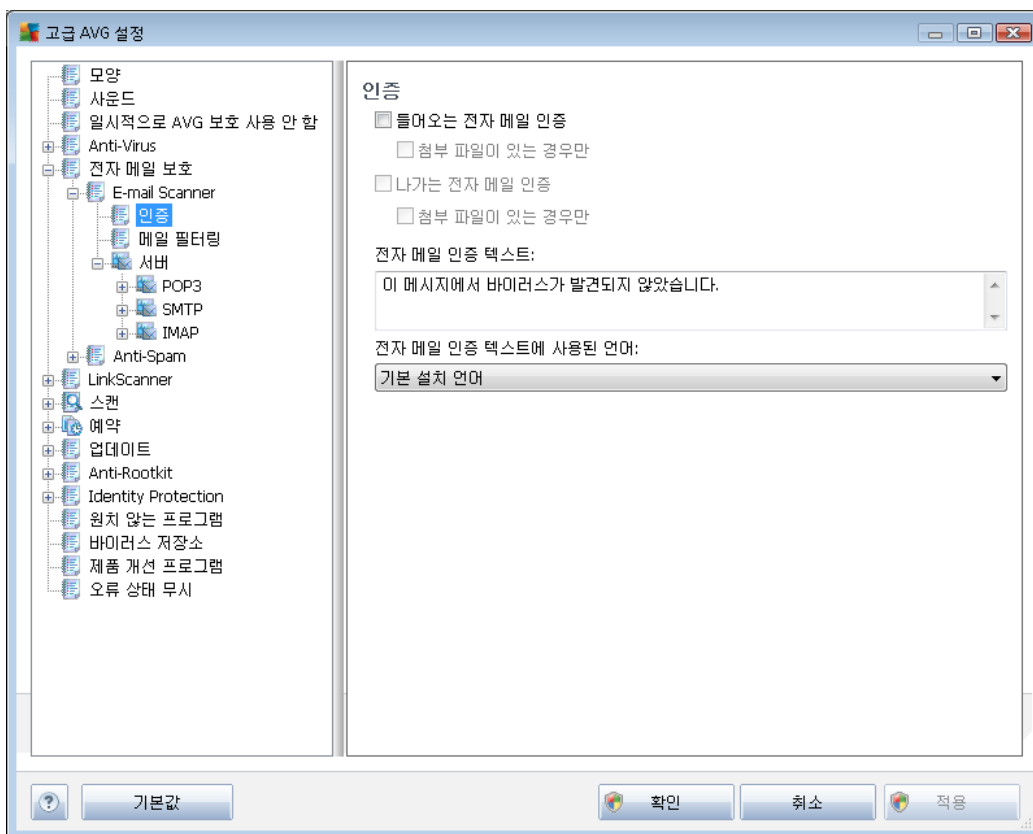
이 섹션에서는 잠재적으로 위험하거나 의심스러운 파일에 대한 추가 보고서를 설정할 수 있습니다. 전자 메일 메시지의 끝에 인증 텍스트가 추가되지만 하고 경고 대화 상자가 표시되지 않는다는 점에 주의해야 합니다. 이러한 모든 보고서는 [E-mail Scanner 검색](#) 대화 상자에 나열됩니다.

- **암호로 보호된 압축 파일 보고** - 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 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 하려면 상자를 선택합니다.
- **숨겨진 확장명 보고** - 예를 들면 의심스러운 실행 파일인 "something.txt.exe"가

확장명이 숨겨져 안전한 일반 텍스트 파일인 "something.txt" 로 표시될 수 있습니다. 이러한 파일을 잠재적으로 위험하다고 보고하려면 상자를 선택합니다.

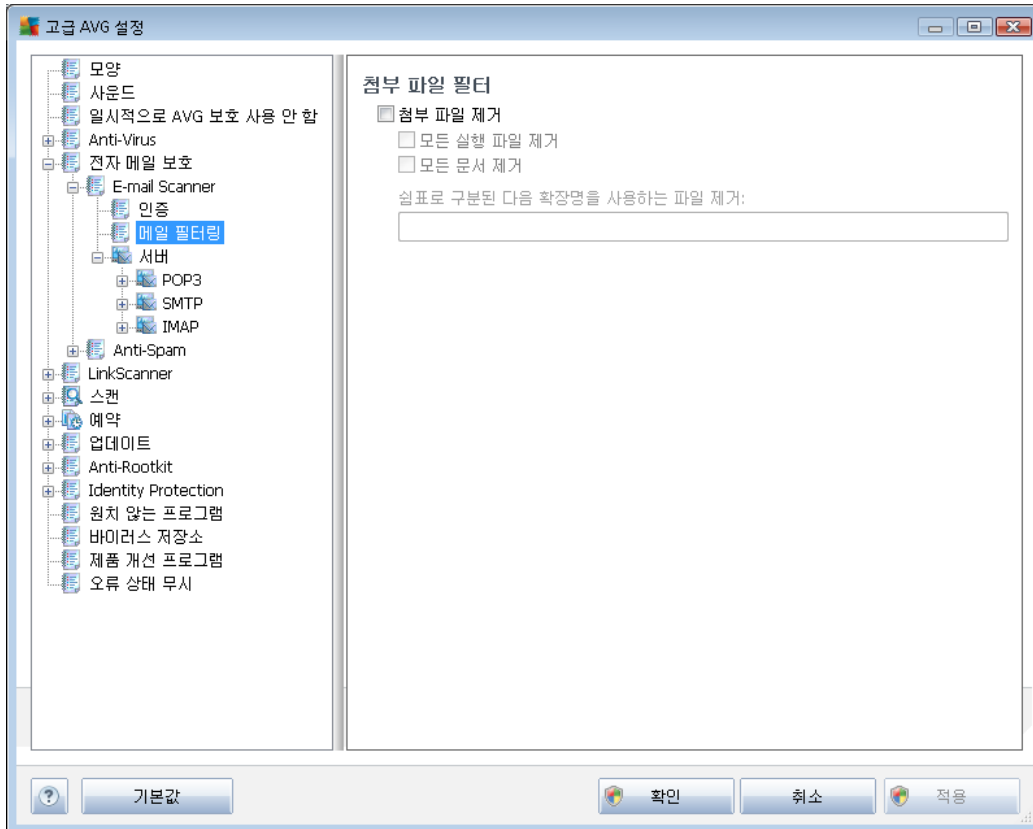
- **보고된 첨부 파일을 바이러스 저장소로 이동** - 암호로 보호된 압축 파일, 암호로 보호된 문서, 매크로가 포함된 파일 및/또는 스캔된 전자 메일 메시지의 첨부 파일로 발견된 확장명이 숨겨진 파일에 대한 전자 메일 알림을 받을지 여부를 지정합니다. 스캔 중 이러한 메시지가 확인될 경우 발견된 감염 개체를 [바이러스 저장소](#)로 이동할지 여부를 정의합니다.

인증 대화 상자에서 특정 확인란을 선택하여 들어오는 메일(**들어오는 전자 메일 인증**) 및/또는 나가는 메일(**나가는 전자 메일 인증**)을 인증할지 여부를 결정할 수 있습니다. 이들 각 옵션에 대해 첨부 파일이 있는 전자 메일 메시지에만 인증이 추가되도록 **첨부 파일이 있는 경우만** 매개 변수를 추가로 지정할 수 있습니다.



기본적으로 인증 텍스트는 **이 메시지에서 바이러스가 발견되지 않았습니다.** 라는 기본 정보로만 이루어져 있습니다. 하지만 이 정보는 사용자의 필요에 따라 확장하거나 변경할 수 있습니다. 즉, 원하는 인증 텍스트를 **전자 메일 인증 텍스트** 필드에 입력할 수 있습니다. **전자 메일 인증 텍스트에 사용된 언어** 섹션에서 자동으로 생성되는 인증 부분(**이 메시지에서 바이러스가 발견되지 않았습니다.**)을 어떤 언어로 표시할지 정의할 수 있습니다.

참고: 기본 텍스트만 요청한 언어로 표시되고 사용자가 지정한 텍스트는 자동으로 번역되지 않는다는 점에 유의하십시오.



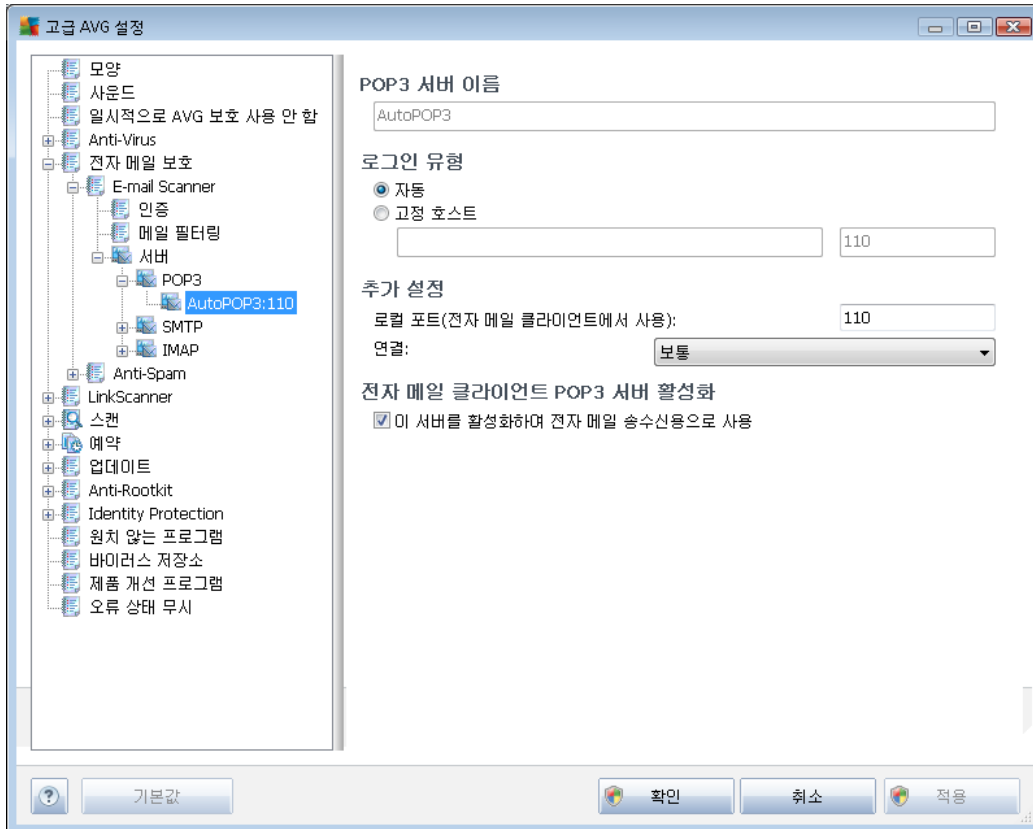
첨부 파일 필터 대화 상자에서는 전자 메일 메시지 첨부 파일 스캔을 위한 매개 변수를 설정할 수 있습니다. 기본적으로 **첨부 파일 제거** 옵션은 해제되어 있습니다. 이 옵션을 활성화하면 감염성이나 위험성이 있는 것으로 검색된 모든 전자 메일 메시지 첨부 파일이 자동으로 제거됩니다. 제거하려는 첨부 파일의 특정 유형을 정의하려면 해당 옵션을 선택하십시오.

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

서버 섹션에서는 [E-mail Scanner](#) 서버의 매개 변수를 편집할 수 있습니다.

- [POP3 서버](#)
- [SMTP 서버](#)
- [IMAP 서버](#)

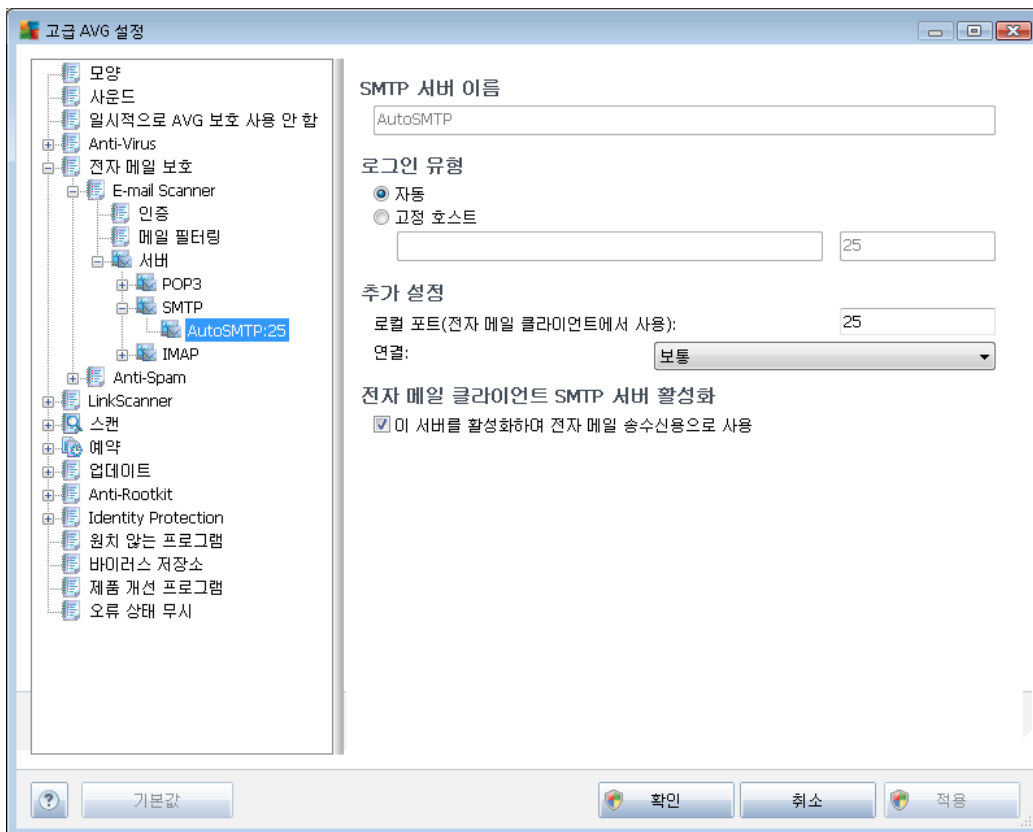
또한 **새 서버 추가** 단추를 사용하여 새 서버에서 수신 및 발신 메일을 정의할 수도 있습니다.



서버/POP3를 통해 열린 이 대화 상자에서 들어오는 전자 메일에 대해 POP3 프로토콜을 사용하는 새로운 **E-mail Scanner** 서버를 설정할 수 있습니다.

- **POP3 서버 이름** - 이 필드에서 새로 추가된 서버의 이름을 지정할 수 있습니다. POP3 서버를 추가하려면 왼쪽 탐색 메뉴의 POP3 항목을 마우스 오른쪽 단추로 클릭합니다. 자동으로 생성된 "AutoPOP3" 서버의 경우 이 필드는 비활성화됩니다.
- **로그인 유형** - 들어오는 메일에 사용되는 메일 서버를 결정하는 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. 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.

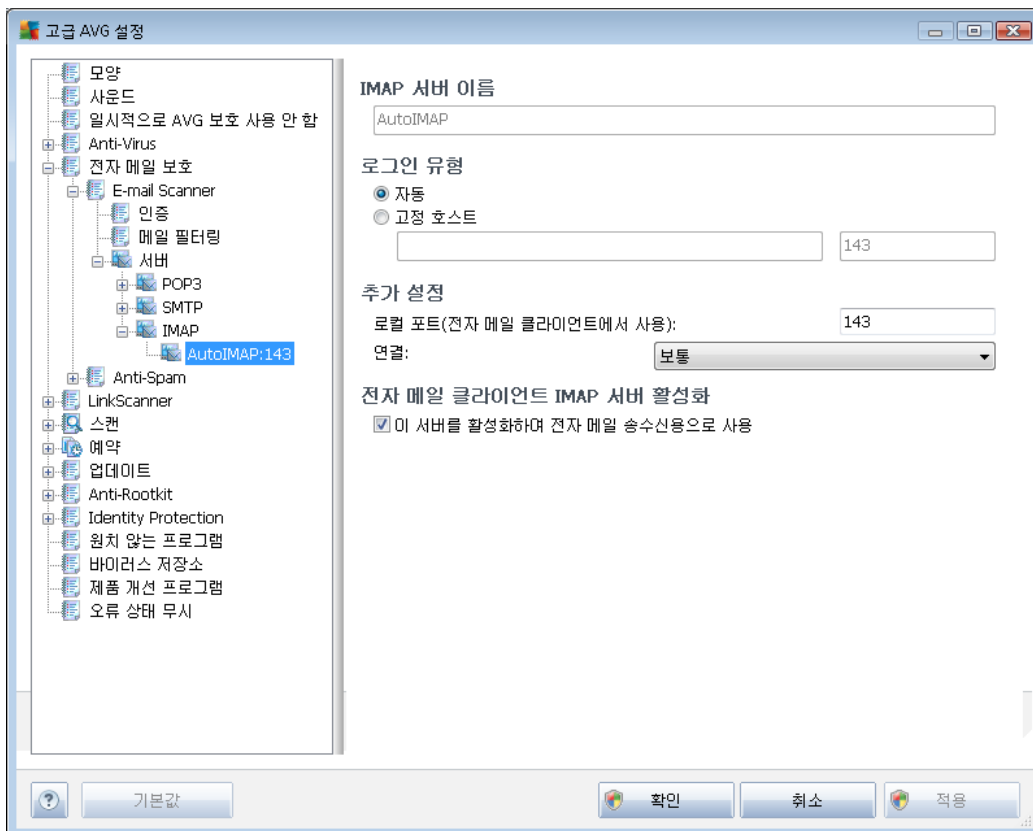
- **로컬 포트** - 메일 응용 프로그램의 커뮤니케이션이 전달되는 포트를 지정합니다. 그런 다음 메일 응용 프로그램에서 이 포트를 POP3 커뮤니케이션 포트로 지정해야 합니다.
- **연결** - 드롭다운 메뉴에서 사용할 연결 유형(**보통/SSL/SSL 기본값**)을 지정할 수 있습니다. SSL 연결을 선택한 경우 전송되는 데이터가 제3자에 의해 모니터링 또는 추적되지 않도록 암호화됩니다. 이 기능도 대상 메일 서버에서 이를 지원해야만 사용할 수 있습니다.
- **전자 메일 클라이언트 POP3 서버 활성화** - 지정된 POP3 서버를 활성화하거나 비활성화하려면 이 항목을 선택하거나 선택 취소합니다.



서버/SMTP를 통해 열리는 이 대화 상자에서는 나가는 메일에 SMTP 프로토콜을 사용하는 새로운 **E-mail Scanner** 서버를 설정할 수 있습니다.

- **SMTP 서버 이름** - 이 필드에서 새로 추가된 서버의 이름을 지정할 수 있습니다. SMTP 서버를 추가하려면 왼쪽 탐색 메뉴의 SMTP 항목을 마우스 오른쪽 단추로 클릭합니다. 자동으로 생성된 "AutoSMTP" 서버의 경우 이 필드는 비활성화됩니다.
- **로그인 유형** - 나가는 메일에 사용되는 메일 서버를 결정하는 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 과 같이 콜론을 구분 기호로 사용하여 서버 이름 뒤에 해당 포트를 입력할 수 있습니다. SMTP 커뮤니케이션의 표준 포트는 25 입니다.
- **추가 설정** - 보다 상세하게 매개 변수를 지정합니다.
 - **로컬 포트** - 메일 응용 프로그램의 커뮤니케이션이 전달되는 포트를 지정합니다. 그런 다음 메일 응용 프로그램에서 이 포트를 SMTP 커뮤니케이션 포트로 지정해야 합니다.
 - **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.
- **전자 메일 클라이언트 SMTP 서버 활성화** - 위에 지정된 SMTP 서버를 활성화 또는 비활성화하려면 이 확인란을 선택하거나 선택을 취소합니다.



서버/IMAP를 통해 열리는 이 대화 상자에서는 나가는 메일에 IMAP 프로토콜을 사용하는

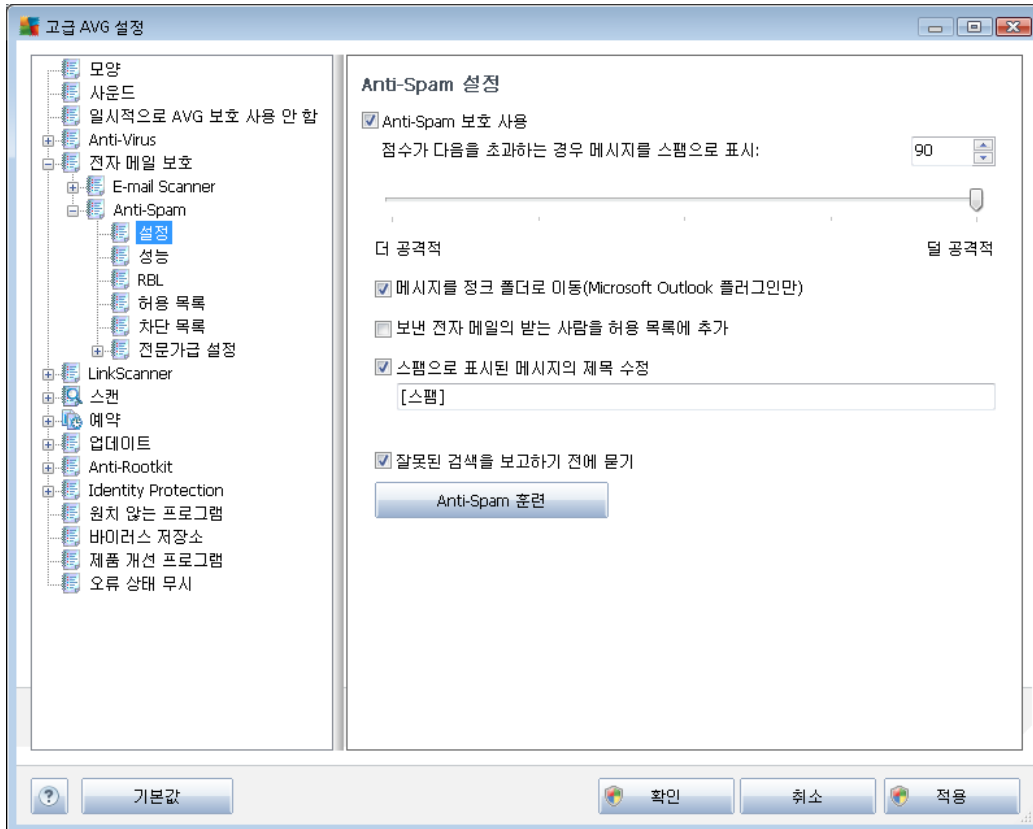


새로운 [E-mail Scanner](#) 서버를 설정할 수 있습니다.

- **IMAP 서버 이름** - 이 필드에서는 새로 추가하는 서버의 이름을 지정할 수 있습니다. IMAP 서버를 추가하려면 왼쪽 탐색 메뉴에서 IMAP 항목을 마우스 오른쪽 단추로 클릭합니다. 자동으로 생성되는 "AutoIMAP" 서버의 경우 이 필드는 비활성화됩니다.
- **로그인 유형** - 나가는 메일에 사용되는 메일 서버를 결정하는 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 사용하는 경우 콜론을 구분 기호로 사용하여 서버 이름 뒤에 해당 포트를 입력할 수 있습니다(예: imap.acme.com:8200). IMAP 커뮤니케이션의 표준 포트는 143입니다.
- **추가 설정** - 보다 상세하게 매개 변수를 지정합니다.
 - **로컬 포트** - 메일 응용 프로그램의 커뮤니케이션이 전달되는 포트를 지정합니다. 그런 다음 메일 응용 프로그램에서 이 포트를 IMAP 커뮤니케이션 포트로 지정해야 합니다.
 - **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.
- **전자 메일 클라이언트 IMAP 서버 활성화** - 위에 지정된 IMAP 서버를 활성화/비활성화하려면 이 확인란을 선택하거나 선택을 취소합니다.

9.5.2. Anti- Spam

여기에 항목 텍스트를 입력하십시오.



Anti-Spam 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 그대로 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. **점수가 다음을 초과하는 경우 메시지를 스팸으로 표시** 설정은 특정 값을 입력하거나 슬라이더를 왼쪽 또는 오른쪽으로 이동하여(값 범위는 50에서 90 사이로 제한됨) 조정할 수 있습니다.

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

- **80 ~ 90 값** - 스팸일 가능성이 있는 전자 메일 메시지가 필터링되며 스팸이 아닌 일부 메시지도 잘못 필터링될 수 있습니다.
- **60 ~ 79 값** - 어느 정도 공격적인 구성으로 간주됩니다. 스팸일 가능성이 있는 전자 메일 메시지가 필터링되며 스팸이 아닌 메시지도 필터링될 수 있습니다.
- **50 ~ 59 값** - 매우 공격적인 구성입니다. 스팸이 아닌 전자 메일 메시지도 실제 스팸 메시지로 필터링될 수 있습니다. 이 임계값 범위는 일반 사용자에게는 권장되지 않습니다.



Anti-Spam 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 목록에 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 스팸으로 발견된 모든 메시지의 전자 메일 제목 필드에 특정 단어나 문자를 표시하거나, 활성화된 텍스트 필드에 원하는 텍스트를 입력할 수 있습니다.
- **잘못된 검색을 보고하기 전에 묻기** - [설치 프로세스](#)에서 [제품 개선 프로그램](#)에 참여하는 데 동의한 경우 제공됩니다. 제품 개선 프로그램에 참여하는 데 동의한 경우 검색된 위험 요소를 AVG에 보고할 수 있습니다. 보고는 자동으로 수행됩니다. 그러나 검색된 스팸을 AVG에 보고하여 메시지를 스팸으로 분류하기 전에 이를 확인하는 메시지를 표시하려는 경우에도 이 확인란을 선택할 수 있습니다.

제어 단추

Anti-Spam 훈련 단추를 누르면 [다음 장](#)에 자세한 내용이 설명된 [Anti-Spam 훈련 마법사](#)가 열립니다.

Anti-spam 훈련 마법사의 첫 번째 대화 상자에서는 훈련에 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.



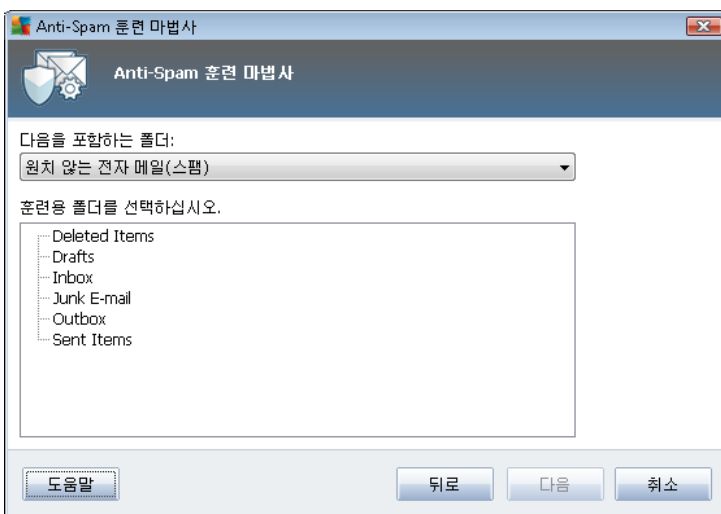
- **특정 전자 메일 클라이언트** - 나열된 전자 메일 클라이언트 (*MS Outlook, Outlook Express, The Bat!*) 중 하나를 사용하는 경우 해당 옵션을 선택하면 됩니다.
- **EML 파일이 있는 폴더** - 다른 전자 메일 프로그램을 사용하려면 우선 메시지를 특정 폴더에 .eml 형식으로 저장하거나 전자 메일 클라이언트 메시지 폴더의 위치를 알고 있어야 합니다. 그런 다음 **EML 파일이 있는 폴더**를 선택하면 다음 단계에서 원하는 폴더를 찾을 수 있습니다.

훈련 프로세스를 보다 빠르고 쉽게 진행하려면 먼저 폴더에서 전자 메일을 정렬하여 훈련에 사용할 폴더에 훈련 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 훈련에 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.

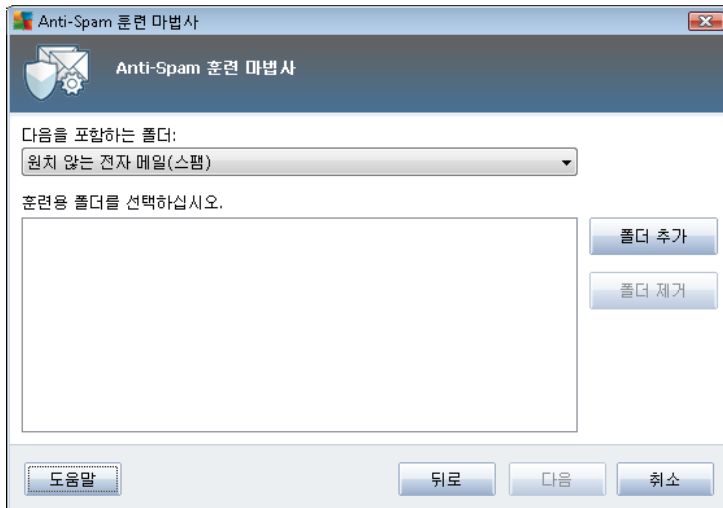
다음에 포함하는 폴더 드롭다운 메뉴에서 선택한 폴더에 원하는 메시지(**원**)가 포함되었음을 나타내는 옵션 또는 원치 않는 메시지(**스팸**)가 포함되었음을 나타내는 옵션 중 하나를 설정합니다. 다음 단계에서 메시지를 필터링할 수 있으므로 폴더에 훈련 전자 메일만 포함되지 않아도 됩니다. **폴더 제거** 단추를 클릭하면 선택된 원치 않는 폴더를 목록에서 제거할 수도 있습니다.

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



특정 전자 메일 클라이언트

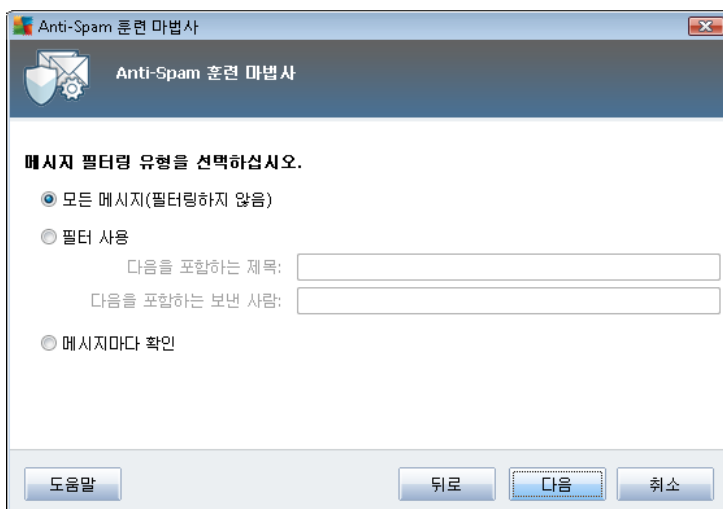
옵션 중 하나를 확인하면 새 대화 상자가 나타납니다.



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

다음에 포함하는 폴더 드롭다운 메뉴에서 선택한 폴더에 원하는 메시지(행)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 훈련 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.

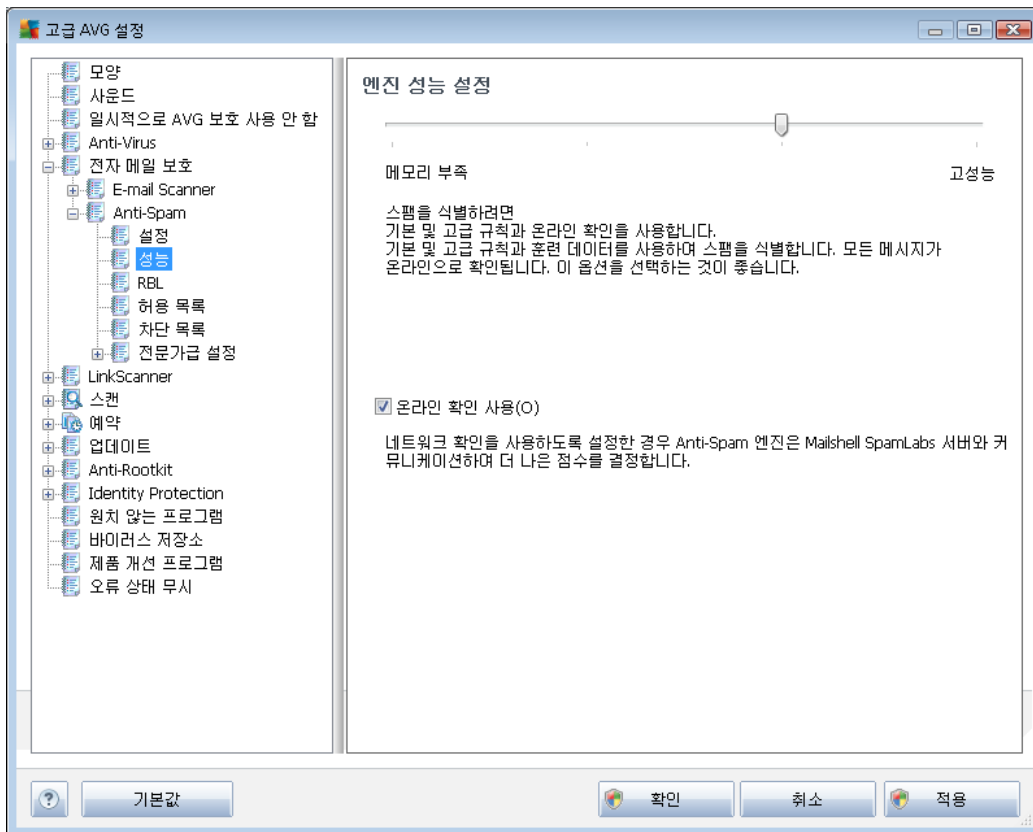


이 대화 상자에서는 전자 메일 메시지의 필터링을 설정할 수 있습니다.

- **모든 메시지(필터링하지 않음)** - 선택한 폴더에 훈련에 사용할 메시지만 있는 경우 **모든 메시지(필터링하지 않음)** 옵션을 선택합니다.
- **필터 사용** - 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 훈련에 사용됩니다. 두 텍스트 필드를 모두 입력하면 두 조건 중 하나와 일치하는 주소도 사용됩니다.
- **메시지마다 확인** - 폴더에 어떤 메시지가 포함되어 있는지 확실하지 않아 마법사로 메시지를 훈련에 사용할지 여부를 각 메시지별로 확인하려면 **메시지마다 확인** 옵션을 선택합니다.

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

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 성

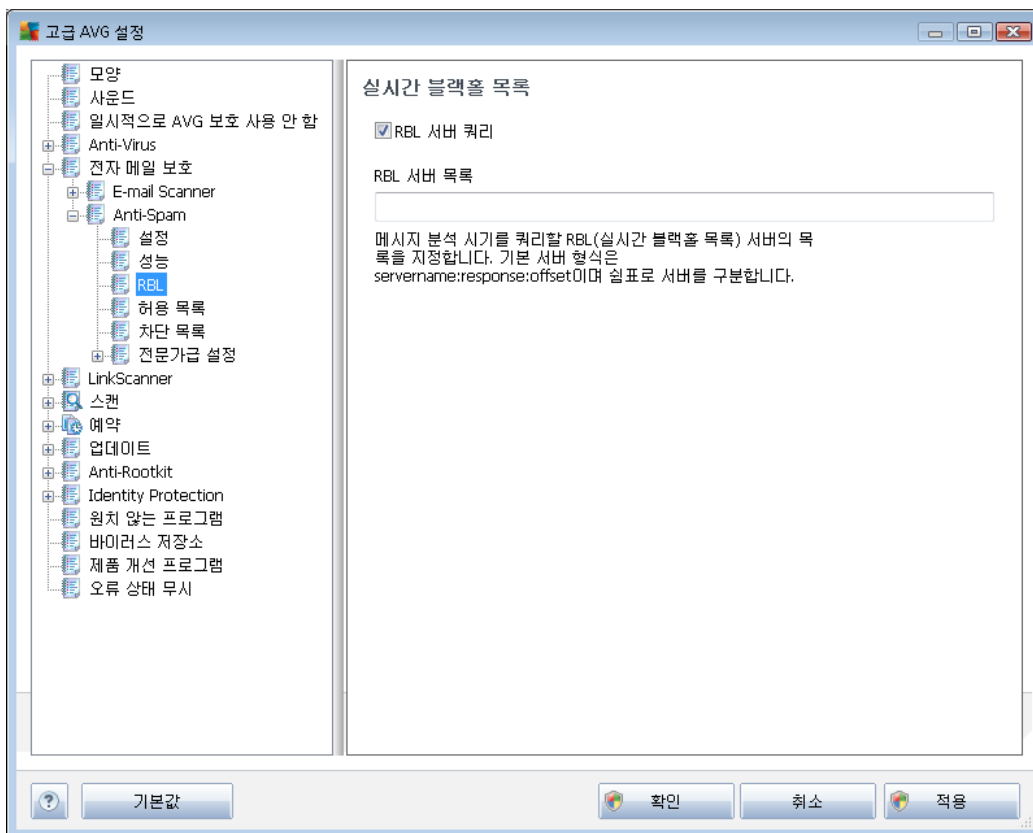
능 수준을 조정할 수 있습니다.

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

온라인 확인 사용 항목은 기본적으로 설정되어 있습니다. 이 옵션이 설정된 경우 Mailshell 서버와의 커뮤니케이션을 통해 보다 정확한 **스팸** 검색이 가능합니다. 즉, 스캔된 데이터는 온라인에서 [Mailshell](#) 데이터베이스와 비교됩니다.

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

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 데이터베이스가 있는 DNS 서버입니다. 이 기능이 설정된 경우 모든 전자 메일 메시지가 RBL 서버 데이터베이스에서 확인되고 데이터베이스에서 동일한 항목이 발견되면 스팸으로 표시됩니다.

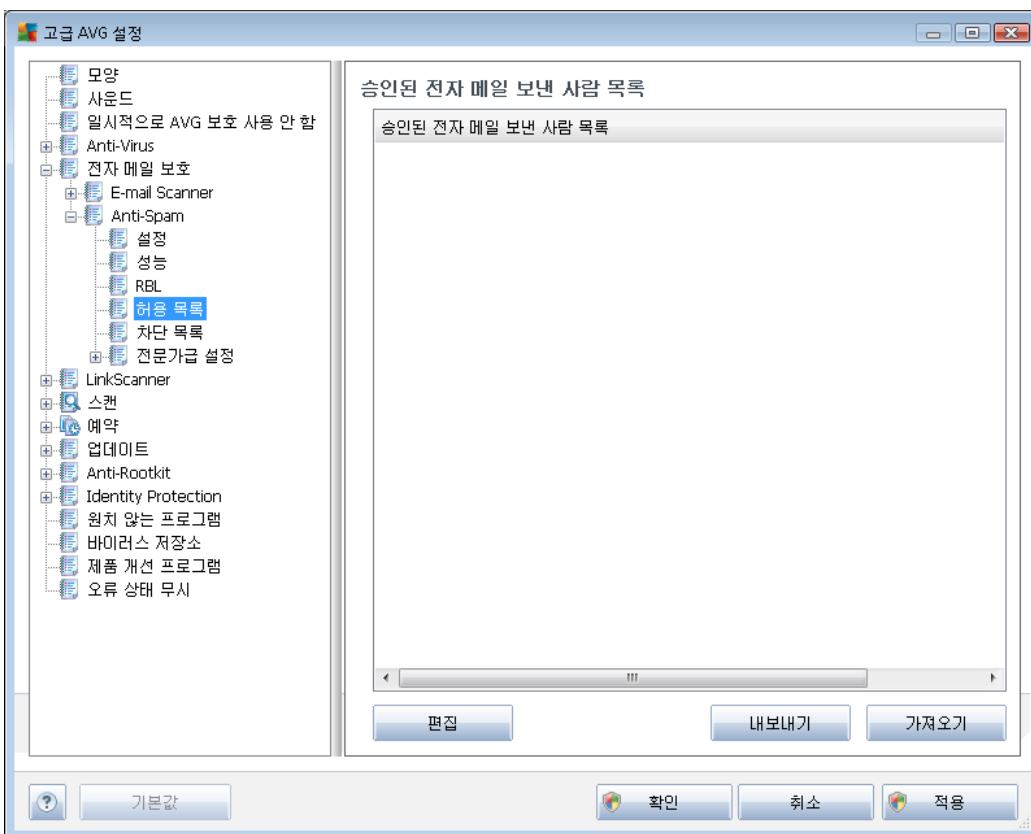


다. RBL 서버 데이터베이스에는 가장 최신의 스팸 자료가 포함되어 있으므로 가장 정확한 스팸 검색이 가능합니다. 이 기능은 보통 [Anti-Spam](#) 엔진으로 검색할 수 없는 스팸을 다량으로 받는 사용자에게 특히 유용합니다.

RBL 서버 목록에서 특정 RBL 서버 위치를 정의할 수 있습니다. 이 기능을 사용하면 모든 메시지를 하나씩 RBL 서버 데이터베이스와 비교하여 확인해야 하므로 일부 시스템 및 구성에서 전자 메일 수신 프로세스가 느려질 수 있습니다.

개인 데이터는 서버에 전송되지 않습니다.

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.



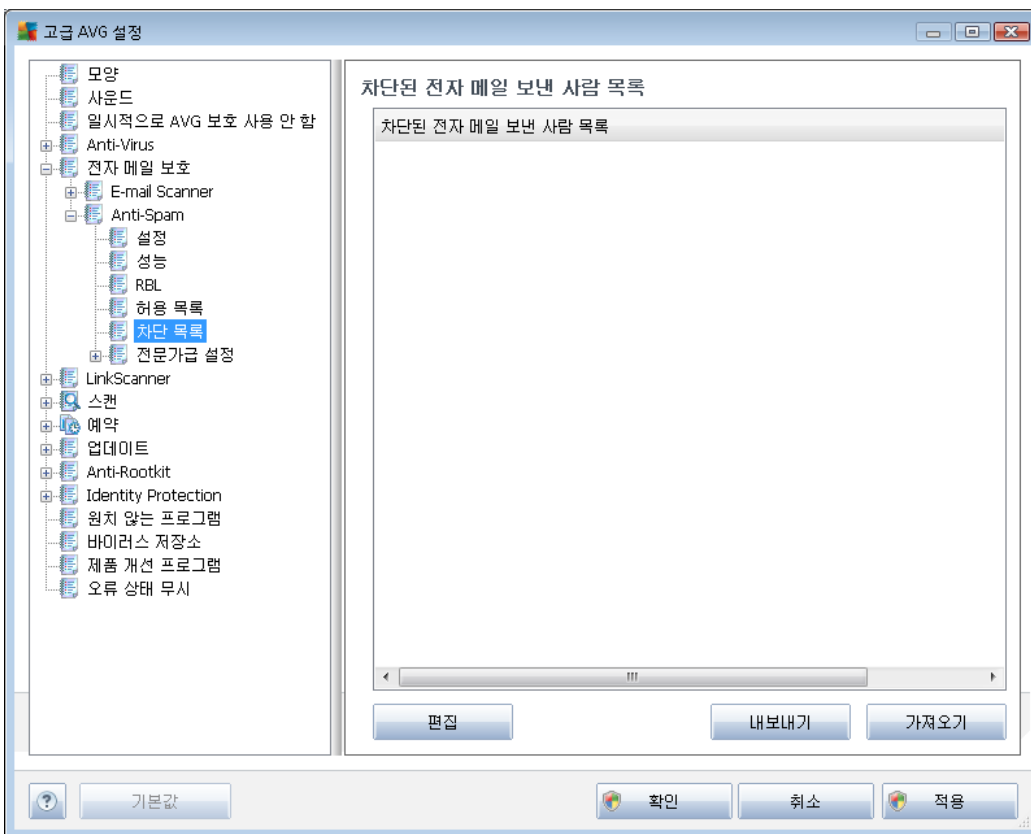
편집 인터페이스에서 사용자에게 원치 않는 메시지(스팸)를 보내지 않을 것으로 예상되는 보낸 사람 목록을 만들 수 있습니다. 또한 스팸 메시지를 만들지 않는다고 사용자가 알고 있는 전체 도메인 이름(예: avg.com)의 목록을 만들 수도 있습니다. 보낸 사람 및/또는 도메인 이름 목록을 준비했으면 각 전자 메일 주소를 직접 입력하거나 전체 주소 목록을 한꺼번에 가져오는 방법으로 이들 항목을 입력할 수 있습니다.

제어 단추

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 준비한 경우 이 단추를 선택하여 간단하게 파일의 항목을 가져올 수 있습니다. 파일 콘텐츠에는 한 줄에 한 항목(주소, 도메인 이름)만 있어야 합니다.

차단 목록 항목은 차단된 보낸 사람 전자 메일 주소 및 도메인 이름에 대한 전역 목록이 포함된 대화 상자를 엽니다. 이러한 주소로부터 온 메시지는 항상 스팸으로 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.

제어 단추

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 준비한 경우 이 단추를 선택하여 간단하게 파일의 항목을 가져올 수 있습니다.

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 사용자만을 위한 것입니다. 이러한 이유로 개별 대화 상자에는 추가 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.

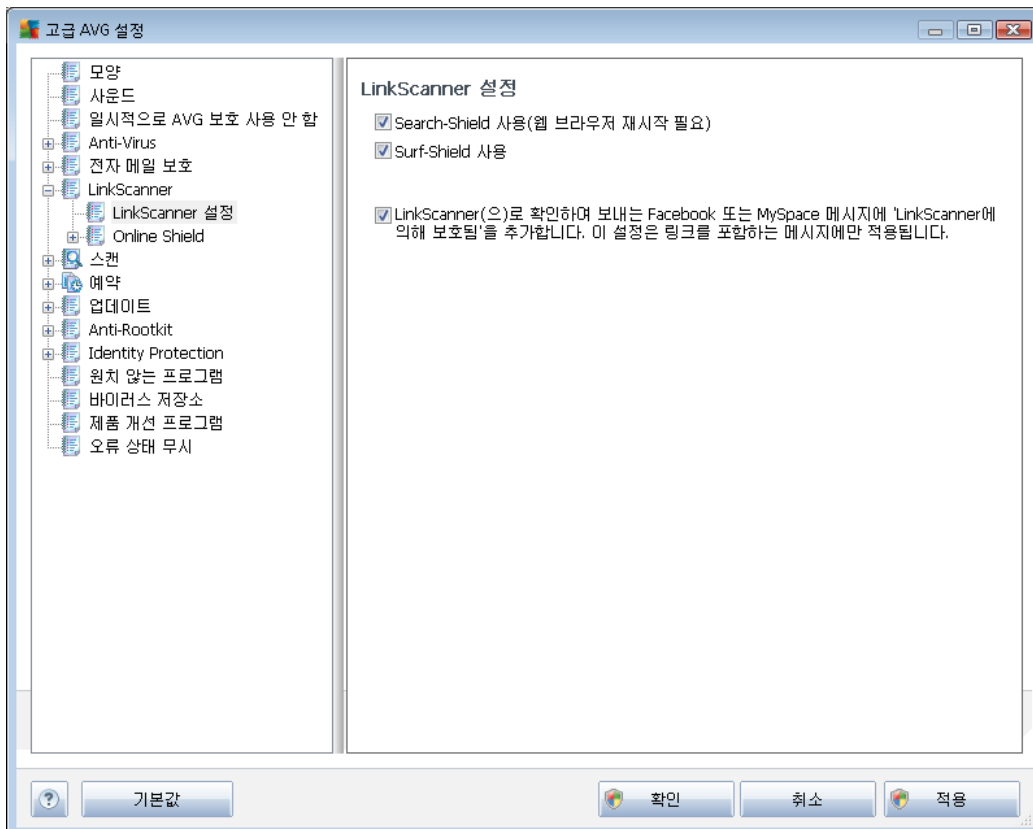
그래도 [Anti-Spam](#) 구성을 세부적으로 변경해야 한다면 사용자 인터페이스에서 직접 제공하는 지침을 따르십시오. 일반적으로 각 대화 상자는 하나의 특정한 기능을 제공하며 이를 편집할 수 있습니다. 각 대화 상자에는 항상 지원하는 기능에 대한 설명을 제공합니다.

- **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

9.6. LinkScanner

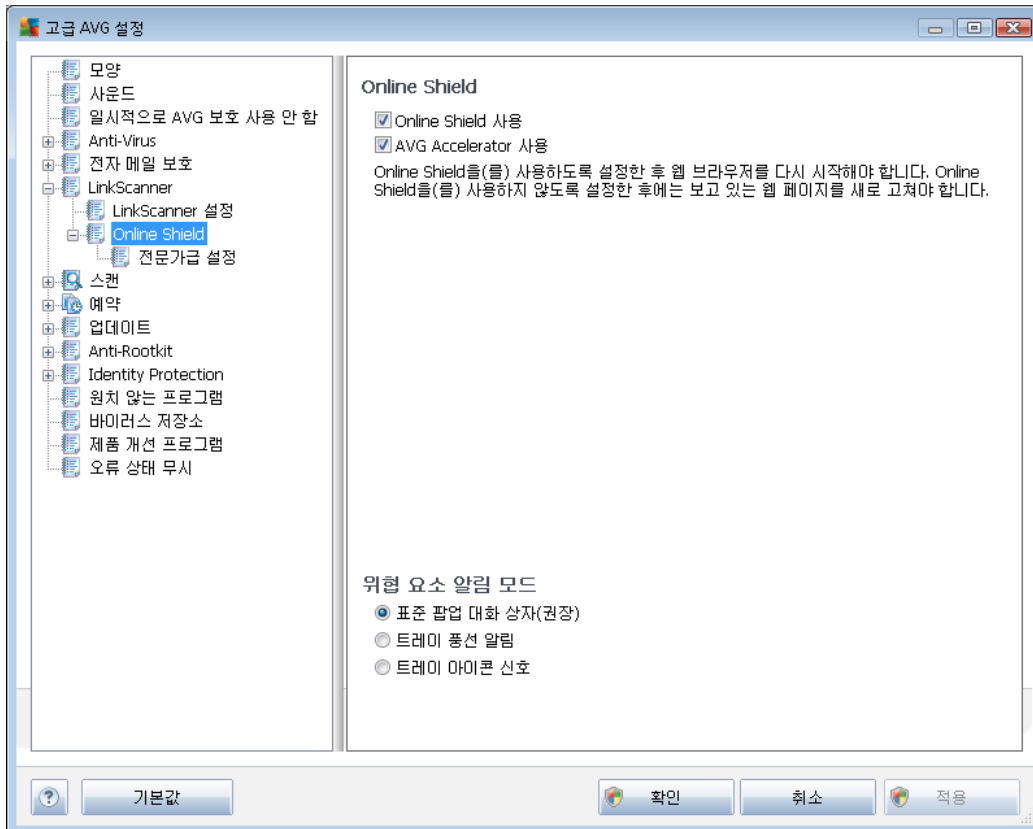
9.6.1. LinkScanner 설정

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



- **Search-Shield 사용** - (기본적으로 설정되어 있음): Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg 또는 SlashDot 검색 엔진에서 반환하는 사이트의 내용을 미리 검사하여 해당 검색 엔진에서 수행하는 검색에 대한 안전도를 알려주는 아이콘입니다.
- **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.
- **'LinkScanner에 의해 보호됨' 추가...** - (기본적으로 설정됨): Facebook 및 MySpace 소셜 네트워크에서 보낸 활성 하이퍼링크가 포함된 모든 메시지에 **LinkScanner** 검사에 대한 인증 텍스트를 입력하려면 이 항목을 선택합니다.

9.6.2. Online Shield

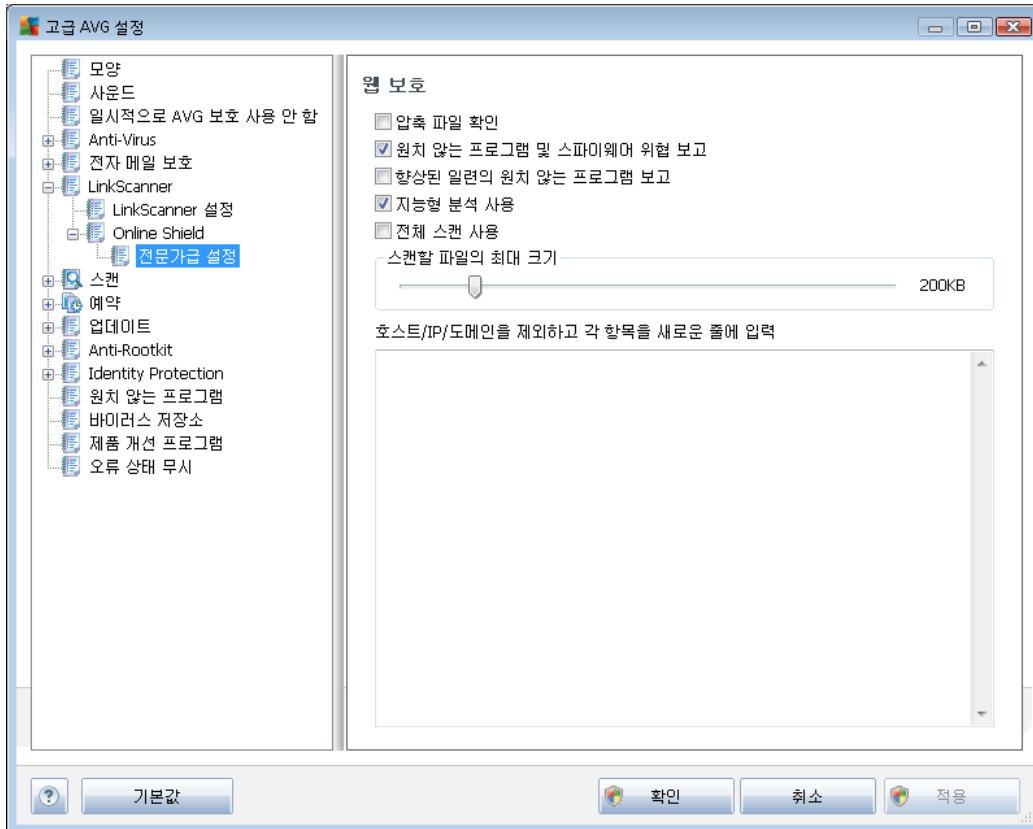


Online Shield 대화 상자에는 다음과 같은 옵션이 있습니다.

- **Online Shield 사용** (기본적으로 설정되어 있음) - 전체 **Online Shield** 서비스를 활성화 또는 비활성화합니다. **Online Shield**에 대한 추가 고급 설정은 [웹 보호](#)라는 이후의 대화 상자에서 계속할 수 있습니다.
- **AVG Accelerator 사용** (기본적으로 설정되어 있음) - **AVG Accelerator** 서비스를 활성화 또는 비활성화하며 이러한 서비스를 통해 온라인 비디오를 더욱 원활하게 재생하고 추가 다운로드를 쉽게 받을 수 있습니다.

위험 요소 알림 모드

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



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** - (기본적으로 해제되어 있음): 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. [스파이웨어](#)는 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** - (기본적으로 해제되어 있음): [스파이웨어](#)의 확장 패키지를 검색하려면 선택합니다. 스파이웨어 프로그램은 제조업체에서 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 기

본적으로 해제되어 있습니다.

- o **지능형 분석 사용** - (기본적으로 설정되어 있음): 표시할 페이지의 콘텐츠를 [지능형 분석](#) 방법(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)을 사용하여 스캔합니다.
- o **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- 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 Shield** 로 스캔할 파일의 최대 크기를 지정할 수 있습니다. 다운로드한 파일이 지정한 크기보다 커서 Online Shield 로 스캔할 수 없는 경우라도 하더라도 사용자의 컴퓨터는 여전히 보호됩니다. 파일이 감염된 경우에는 **Resident Shield** 가 즉시 이를 검색합니다.
- o **호스트/IP/도메인 제외** - 텍스트 필드에는 **Online Shield** 가 스캔하지 않아도 되는 서버(호스트, IP 주소, 마스크가 있는 IP 주소 또는 URL) 또는 서버의 정확한 이름을 입력할 수 있습니다. 따라서 위험한 웹 사이트 콘텐츠를 제공하지 않는다고 확신할 수 있는 호스트만 제외해야 합니다.

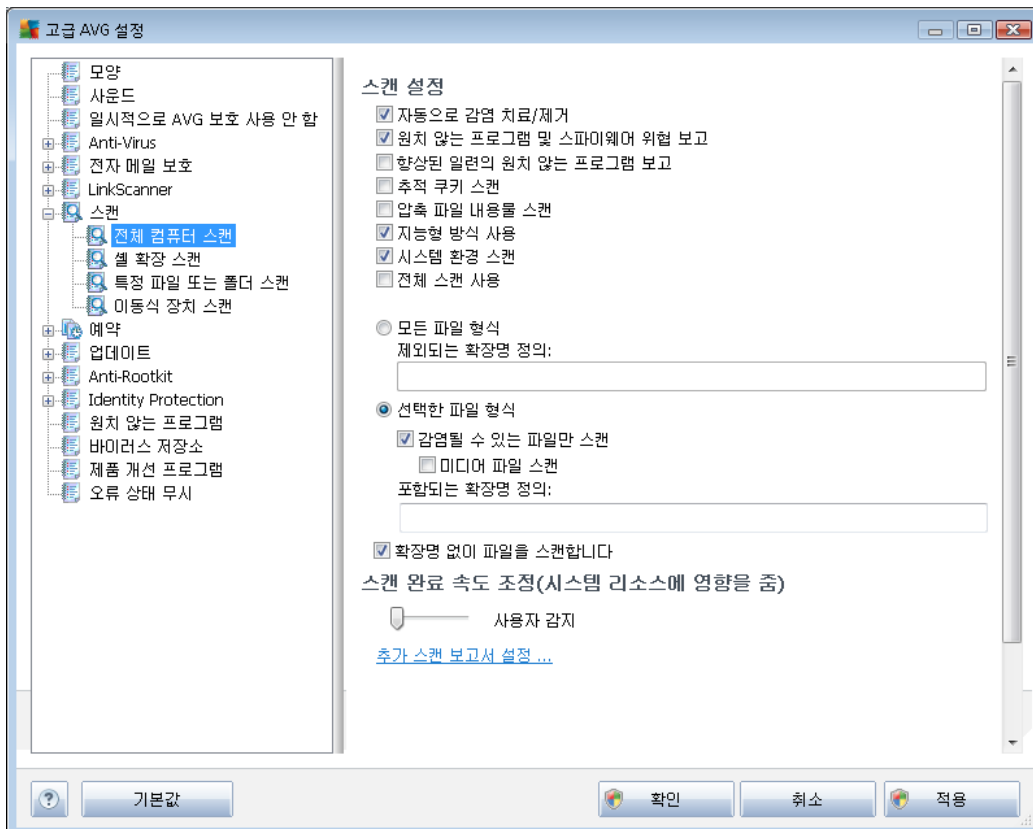
9.7. 스캔

고급 스캔 설정은 소프트웨어 공급 업체가 정의한 특정 스캔 유형과 관련하여 다음 네 가지 범주로 나뉩니다.

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

9.7.1. 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**(기본적으로 설정됨) - 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없으면 감염된 개체가 [바이러스 저장소](#)로 이동됩니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고**(기본적으로 설정됨) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 일반적으로 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**(기본적으로 해제되어 있음) - 스파이웨어의 확장 패키지를 검색하려는 경우 선택합니다. 스파이웨어 프로그램은 제조업체에서 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로

로 오용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.

- **추적 쿠키 스캔**(기본적으로 해제되어 있음) - [Anti-Spyware](#) 구성 요소의 이 매개 변수는 쿠키가 검색되도록 정의합니다. HTTP 쿠키는 사이트 기본 설정이나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 특정 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.
- **압축 파일 내용물 스캔**(기본적으로 해제되어 있음) - 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일에 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.
- **지능형 방식 사용**(기본적으로 설정됨) - 지능형 분석(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- **시스템 환경 스캔**(기본적으로 설정됨) - 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.

계속해서 스캔 여부를 결정해야 합니다.

- **모든 파일 형식**은 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 그대로 유지하는 것이 좋습니다. 확장명이 없는 파일은 다소 의심스럽기 때문에 항상 스캔해야 합니다.

스캔 완료 속도 조정

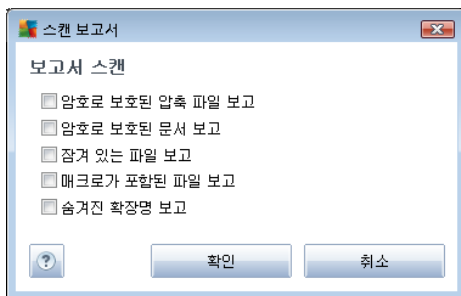
스캔 완료 속도 조정 섹션에서 시스템 리소스 사용량에 따라 원하는 스캔 속도를 추가로 지정할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 사용자 감지 수준으로 설정되어 있습니다. 스캔을 더 빠르게 실행하려고 하면 스캔 시간이 단축되기는 하지만 시스템의 리소스 사용량이 현저하게 증가하고 PC에서 실행 중인 다른 활동의 진행 속도가 느려지게 됩니다. 이 옵션은 컴퓨터가 켜져 있지만 아무도 컴퓨터에서 작업을



수행하고 있지 않은 경우에 사용할 수 있습니다. 반대로, 스캔 기간을 늘리면 시스템 리소스 사용량을 줄일 수 있습니다.

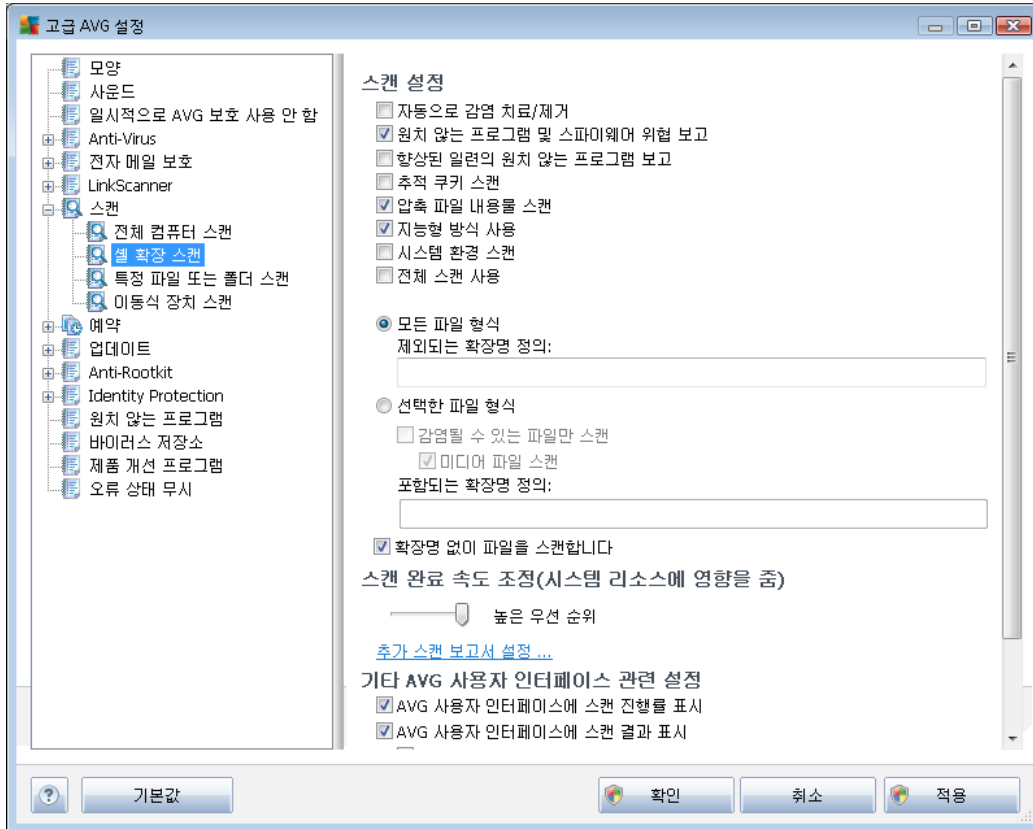
추가 스캔 보고서 설정 ...

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



9.7.2. 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.



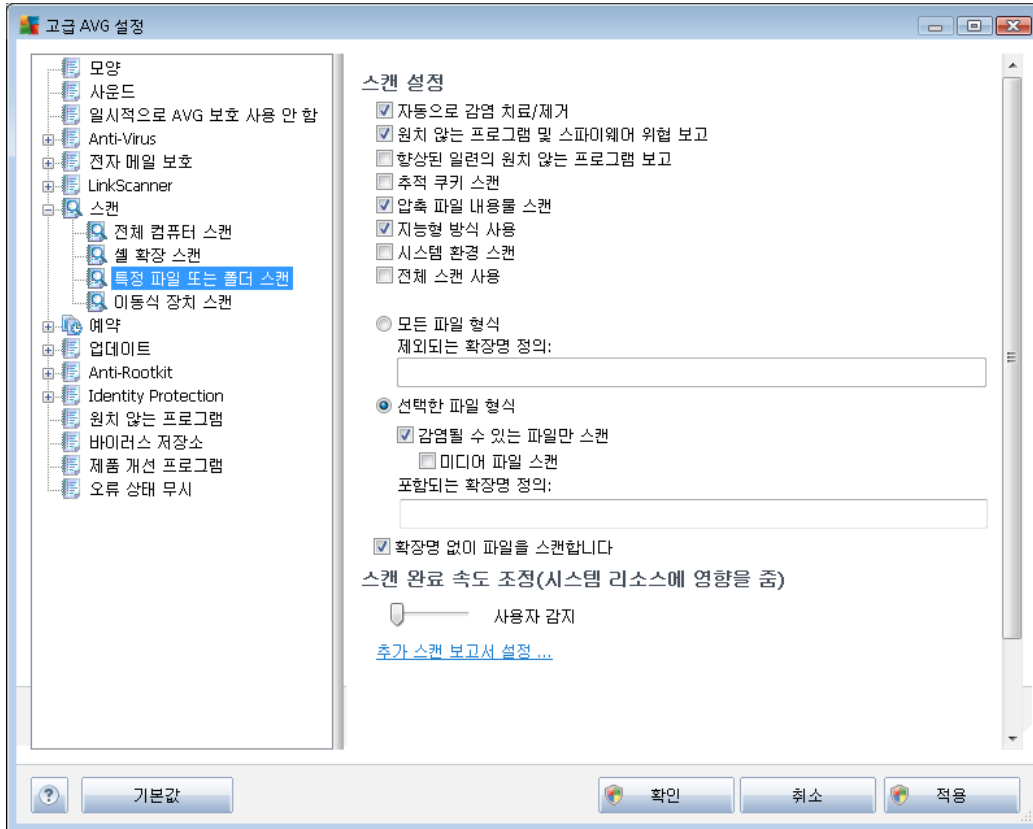
매개 변수의 목록은 [전체 컴퓨터 스캔](#)에서 제공되는 것과 같습니다. 그러나 기본 설정은 다릅니다. 예를 들어, 전체 컴퓨터 스캔은 기본적으로 시스템 환경은 스캔하지만 압축 파일은 검사하지 않습니다. 반면 셀 확장 스캔은 이와 다르게 작동합니다.

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

[전체 컴퓨터 스캔](#) 대화 상자와 비교해 보면 [셀 확장 스캔](#) 대화 상자에는 **기타 AVG 사용자 인터페이스 관련 설정** 섹션이 포함되어 있습니다. 여기서는 AVG 사용자 인터페이스에서 스캔 진행률 및 스캔 결과에 액세스할지 여부를 지정할 수 있습니다. 또한, 스캔 도중 감염이 검색되는 경우에만 스캔 결과를 표시하도록 정의할 수 있습니다.

9.7.3. 특정 파일 또는 폴더 스캔

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

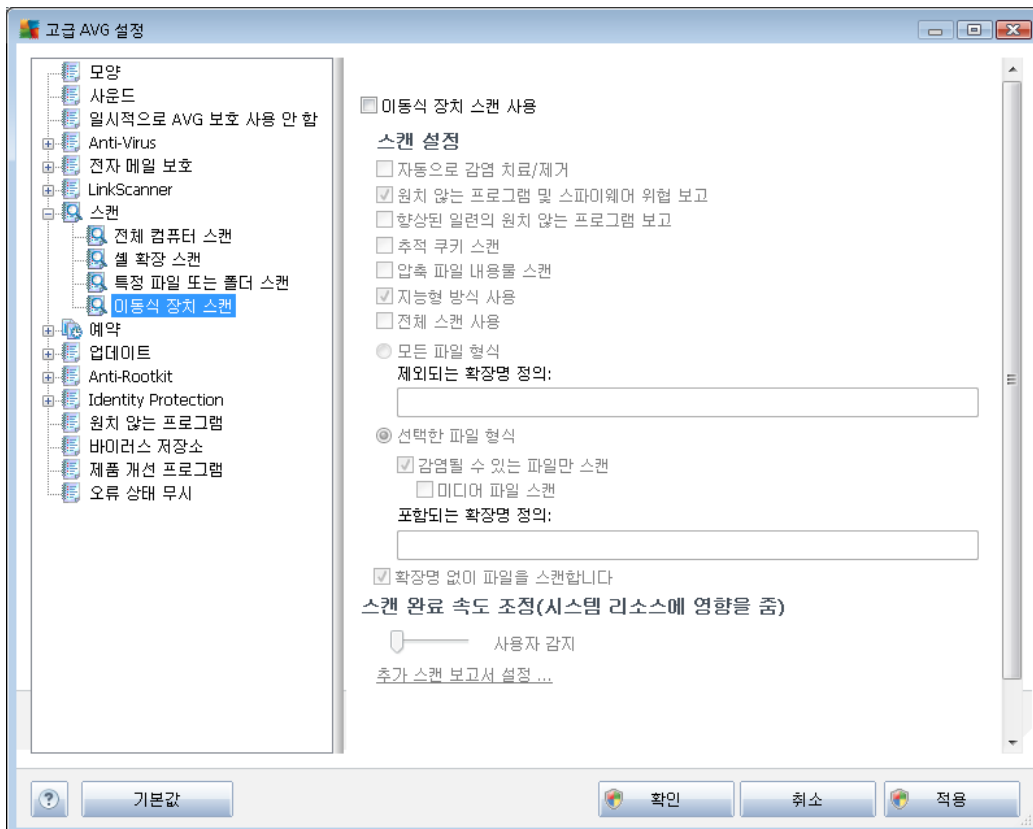


이 구성 대화 상자의 모든 매개 변수 설정은 오직 특정 파일 또는 폴더 스캔으로 스캔하기 위해 선택한 영역에만 적용됩니다.

참고: 특정 매개 변수에 대한 설명은 AVG 고급 설정/스캔/전체 컴퓨터 스캔 장을 참조하십시오.

9.7.4. 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.

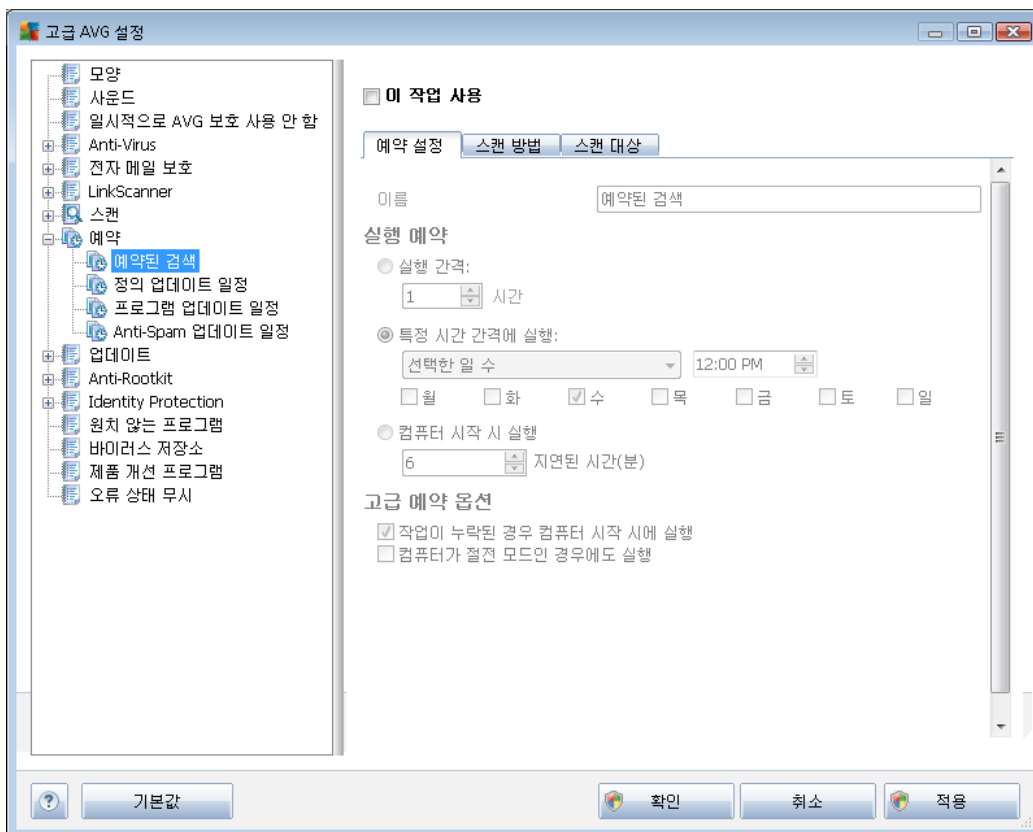
9.8. 예약

예약 섹션에서 다음 기본 설정을 편집할 수 있습니다.

- [예약된 검색](#)
- [정의 업데이트 일정](#)
- [프로그램 업데이트 일정](#)
- [Anti-Spam 업데이트 일정](#)

9.8.1. 예약된 스캔

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

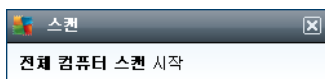


실행 예약

여기서 새로 예약된 스캔이 시작되는 시간 간격을 지정할 수 있습니다. 특정 시간이 지나면 스캔 실행이 반복되도록 정의하거나(**실행 간격...**) 정확한 날짜 및 시간을 정의하여 스캔이 실행되도록 정의(**특정 시간 간격에 실행...**)할 수 있습니다. 아니면 스캔이 특정 이벤트와 연관되어 실행(**컴퓨터 시작 시 실행**)되도록 지정할 수도 있습니다.

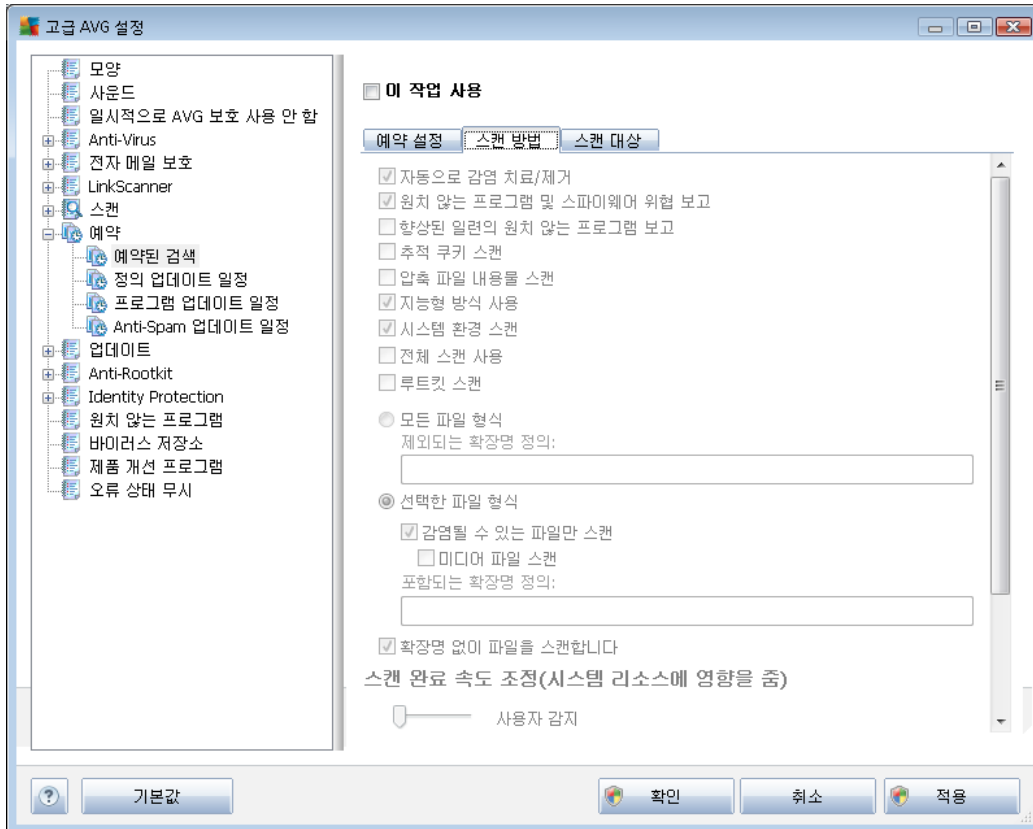
고급 예약 옵션

이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때와 같이 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.



그리고 예약된 스캔이 실행 중임을 알리는 새로운 [AVG 시스템 트레이 아이콘](#)(**컬러 표시 아이콘**)이 나타납니다. 실행 중인 스캔 AVG 아이콘을 마우스 오른쪽 단추로 클릭하여 상황에 맞는 메뉴를 열고 실행 중인 스캔을 중지 또는 일시 중지하고 현재 실행 중인 스캔의 우선 순위를 변경할 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**(기본적으로 설정되어 있음): 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없으면 감염된 개체가 [바이러스 저장소](#)로 이동됩니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고**(기본적으로 설정되어 있음): [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 일반적으로 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**(기본적으로 해제되어 있음): 스파이웨어의 확장 패키지를 검색하려면 선택합니다. 스파이웨어 프로그램은 제조업체에서 제공될 때는 무해하고 문제 없이 작동하지만, 나중에 악의적인 목적으로 오용될 수 있습니다. 이 방법을 사용하면 컴퓨터 보안이 크게 향상되지만, 합법적인 프로그램을 차단할 가능성이 있으므로 기본적으로 해제되어 있습니다.
- **추적 쿠키 스캔**(기본적으로 해제되어 있음): [Anti-Spyware](#) 구성 요소의 이 매개 변수는 스캔 중에 쿠키가 검색되도록 정의합니다. **HTTP 쿠키는 사이트 기본 설정이**

나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 특정 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.

- **압축 파일 내용물 스캔**(기본적으로 해제되어 있음): 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일 형식으로 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.
- **지능형 방식 사용**(기본적으로 설정됨): 지능형 분석(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- **시스템 환경 스캔**(기본적으로 설정됨): 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- **루트킷 스캔**(기본적으로 해제되어 있음): 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.

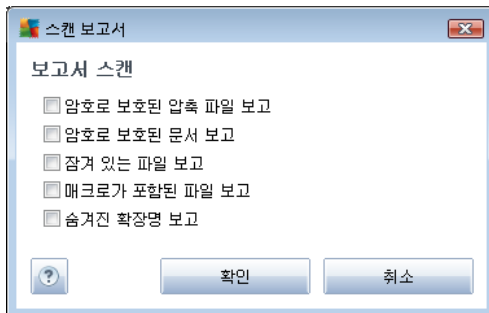
- **모든 파일 형식**은 스캔하지 않아야 할 파일의 확장명을 심표(저장하면 세미콜론으로 변경됨)로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.
- **선택한 파일 형식** - 감염 가능성이 있는 파일만 스캔(일반 텍스트 파일과 기타 비실행 파일 등 감염되지 않는 파일은 스캔 안 함)하도록 지정할 수 있으며, 이때 미디어 파일(비디오, 오디오 파일 - 이러한 파일은 대개 크기가 크고 바이러스 감염 가능성이 크지 않기 때문에 이 확인란을 선택 해제된 상태로 두면 스캔 시간을 크게 줄일 수 있음)도 포함하여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

스캔 완료 속도 조정

스캔 완료 속도 조정 섹션에서 시스템 리소스 사용량에 따라 원하는 스캔 속도를 추가로 지정할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 사용자 감지 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.

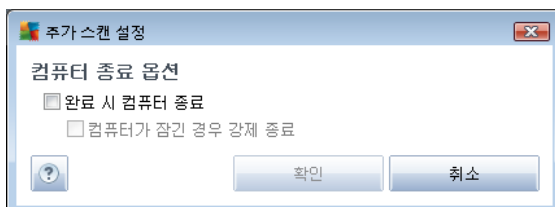
추가 스캔 보고서 설정

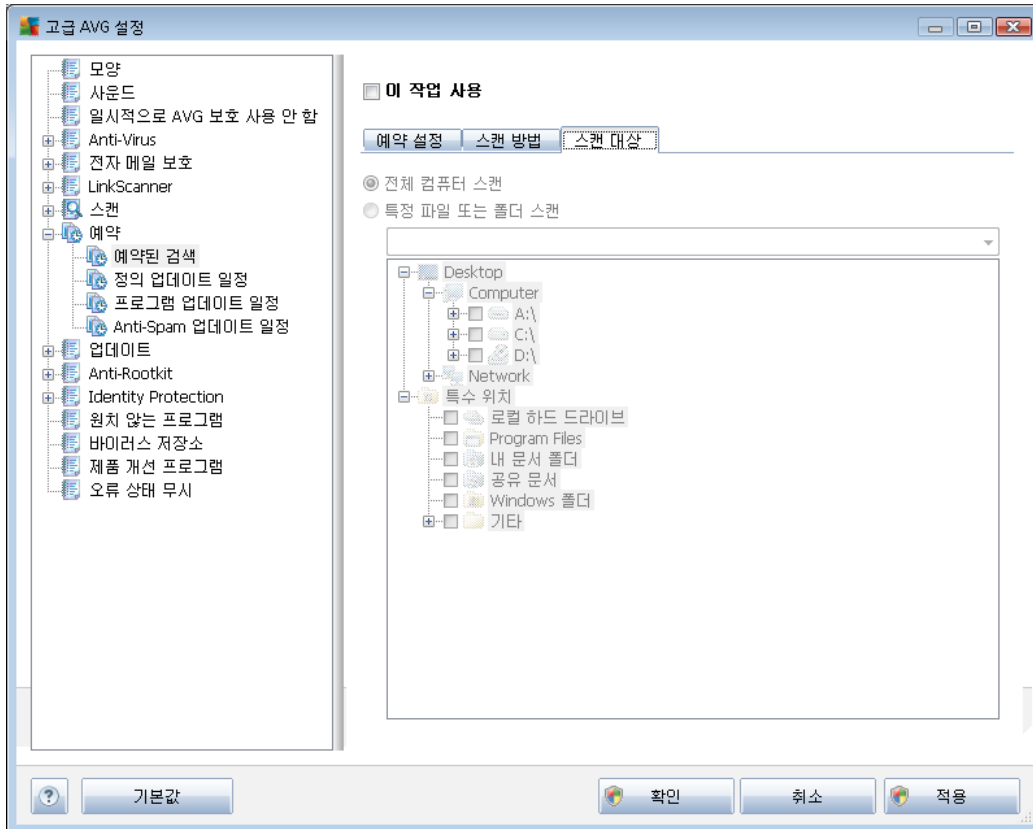
추가 스캔 보고서 설정... 링크를 클릭하여 **스캔 보고서**라는 독립 실행형 대화 상자 창을 열고 보고할 스캔 결과를 정의하는 몇 가지 항목을 선택할 수 있습니다.



추가 스캔 설정

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.

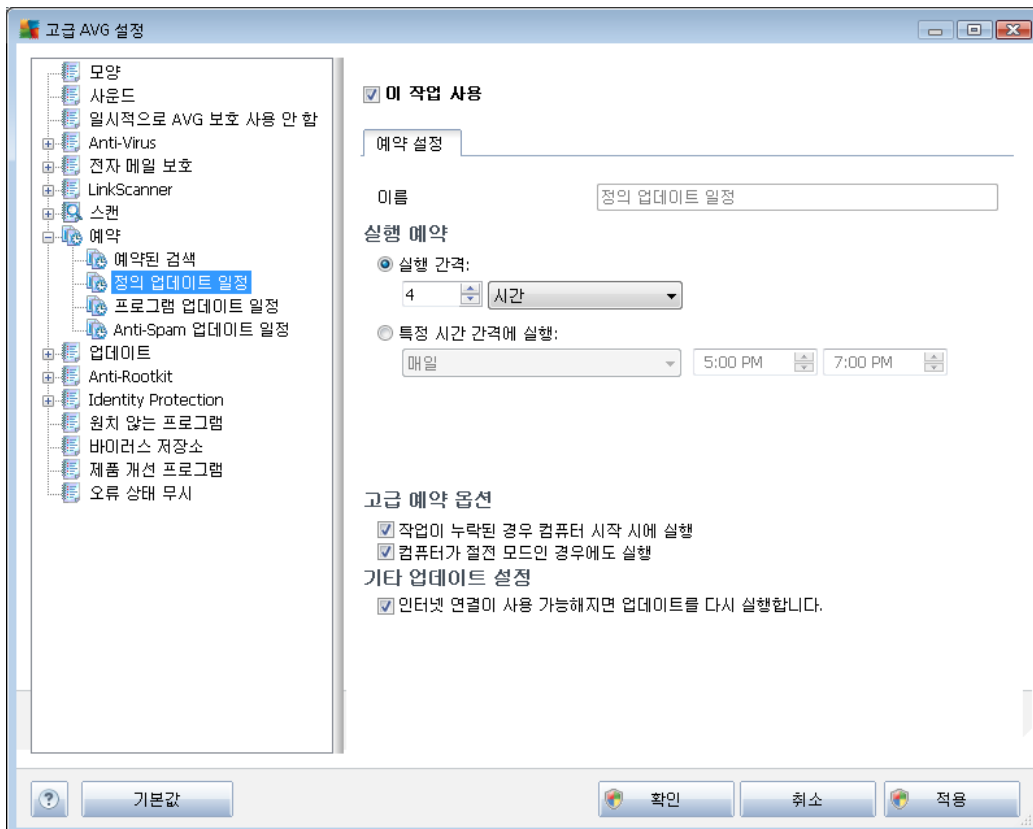




스캔 대상 탭에서 [전체 컴퓨터 스캔](#)을 예약할지 아니면 [특정 파일 또는 폴더 스캔](#)을 예약할지 여부를 정의할 수 있습니다. 특정 파일 또는 폴더 스캔을 선택한 경우 표시된 트리 구조가 이 대화 상자의 아래쪽 부분에서 활성화되며 여기서 스캔할 폴더를 지정할 수 있습니다.

9.8.2. 정의 업데이트 일정

반드시 필요한 경우, 이 작업 사용 항목을 선택 취소하여 예약된 정의 업데이트를 일시적으로 비활성화했다가 나중에 다시 설정할 수 있습니다.



이 대화 상자에서 정의 업데이트 일정의 세부적인 매개 변수 중 일부를 설정할 수 있습니다. **이름**(모든 기본 일정에 대해 비활성 상태로 표시됨) 텍스트 필드에는 프로그램 공급 업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

이 섹션에서는 새로 예약된 정의 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

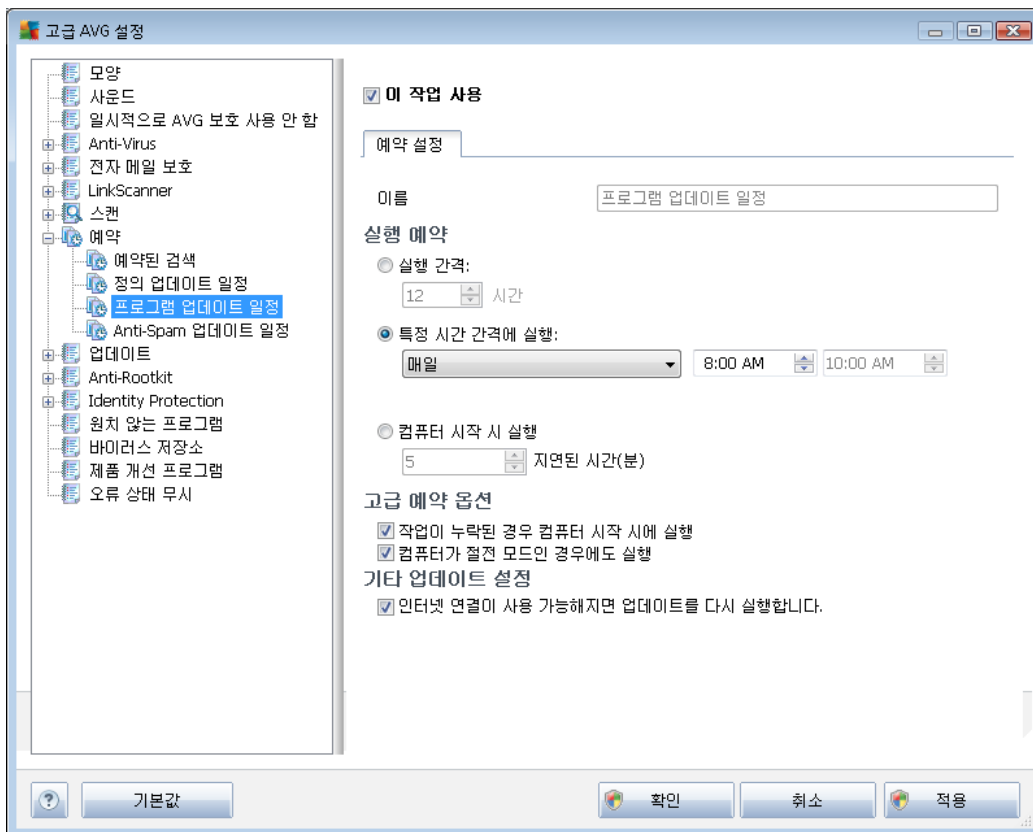
이 섹션에서는 컴퓨터가 절전 모드일 때나 완전히 꺼졌을 때 정의 업데이트가 실행 또는 실행되지 않아야 하는 조건을 정의할 수 있습니다.

기타 업데이트 설정

마지막으로, 인터넷 연결이 끊어져 업데이트 프로세스가 실패한 경우 인터넷 연결이 복구되는 즉시 업데이트가 다시 시작되게 하려면 **인터넷 연결이 사용 가능해지는 즉시 업데이트를 다시 실행** 옵션을 선택합니다. 예약된 업데이트가 지정한 시간에 시작되면 **AVG 시스템 트레이 아이콘(고급 설정/모양 대화 상자의 기본 구성을 유지한 경우)** 위로 팝업 창이 열려 해당 내용을 알립니다.

9.8.3. 프로그램 업데이트 일정

반드시 필요한 경우, 이 작업 사용 항목을 선택 취소하여 예약된 프로그램 업데이트를 일시적으로 비활성화했다가 나중에 다시 설정할 수 있습니다.



이름(모든 기본 일정에 대해 비활성 상태로 표시됨) 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

여기서 새로 예약된 프로그램 업데이트가 실행되는 주기를 지정합니다. 특정 기간이 지나면(**실행 간격...**) 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 수



도 있습니다.

고급 예약 옵션

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

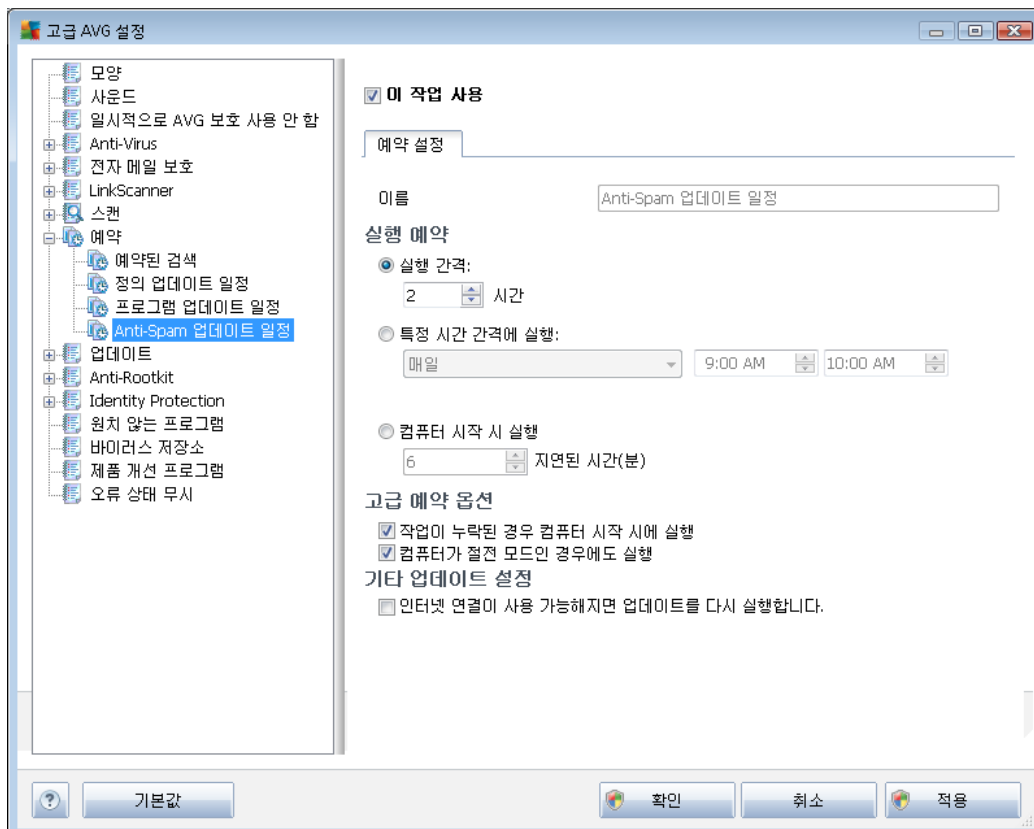
기타 업데이트 설정

인터넷 연결이 끊어져 업데이트 프로세스가 실패한 경우 인터넷 연결이 복구되는 즉시 업데이트가 다시 시작되게 하려면 **인터넷 연결이 사용 가능해지는 즉시 업데이트를 다시 실행** 옵션을 선택합니다. 예약된 업데이트가 지정한 시간에 시작되면 [AVG 시스템 트레이 아이콘](#) ([고급 설정/모양](#) 대화 상자의 기본 구성을 유지한 경우) 위로 팝업 창이 열려 해당 내용을 알립니다.

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

9.8.4. Anti-Spam 업데이트 일정

반드시 필요한 경우 **이 작업 사용** 항목을 선택 취소하여 예약된 [Anti-Spam](#) 업데이트를 일시적으로 비활성화했다가 나중에 다시 설정할 수 있습니다.





이 대화 상자에서 업데이트 일정의 세부적인 매개 변수 중 일부를 설정할 수 있습니다.
이름(모든 기본 일정에 대해 비활성 상태로 표시됨) 텍스트 필드에는 프로그램 공급업체에서 일정에 지정한 이름이 나타납니다.

실행 예약

여기에서 새로 예약된 [Anti-Spam](#) 업데이트가 실행되는 주기를 지정합니다. 특정 시간이 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.

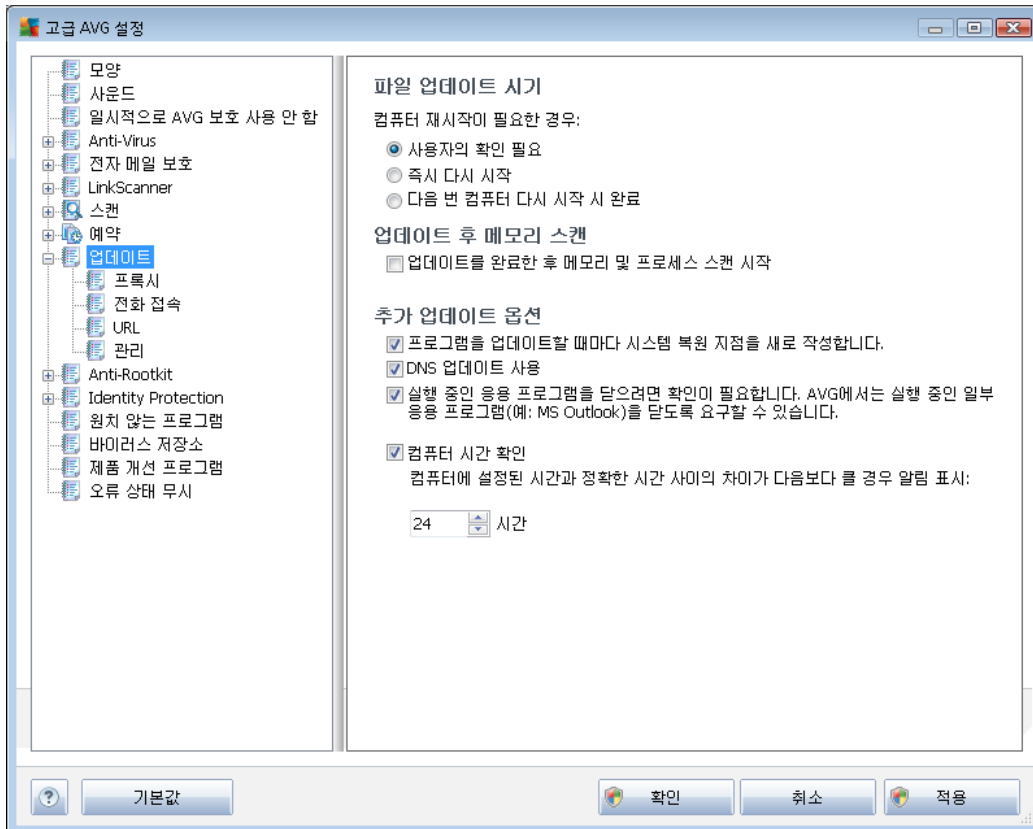
기타 업데이트 설정

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

지정한 시간에 예약된 스캔이 시작되면 [AVG 시스템 트레이 아이콘](#)([고급 설정/모양](#) 대화 상자에서 기본 구성을 유지한 경우) 위로 팝업 창이 표시되어 해당 내용을 알립니다.

9.9. 업데이트

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



파일 업데이트 시기

이 섹션에서는 업데이트 프로세스에서 PC를 다시 시작해야 하는 경우에 사용할 옵션을 세 가지 중에서 선택할 수 있습니다. 다음 PC 다시 시작 시에 업데이트가 완료되도록 예약하거나, PC를 즉시 다시 시작할 수 있습니다.

- **사용자의 확인 필요** (기본값) - [업데이트](#) 프로세스를 완료하기 위해 PC를 다시 시작할지 묻는 승인 메시지를 표시합니다.
- **즉시 다시 시작** - 컴퓨터는 [업데이트](#) 프로세스가 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 컴퓨터를 하루에 한 번 이상 정기적으로 다시 시작하는 경우에만 사용하는 것이 좋습니다.



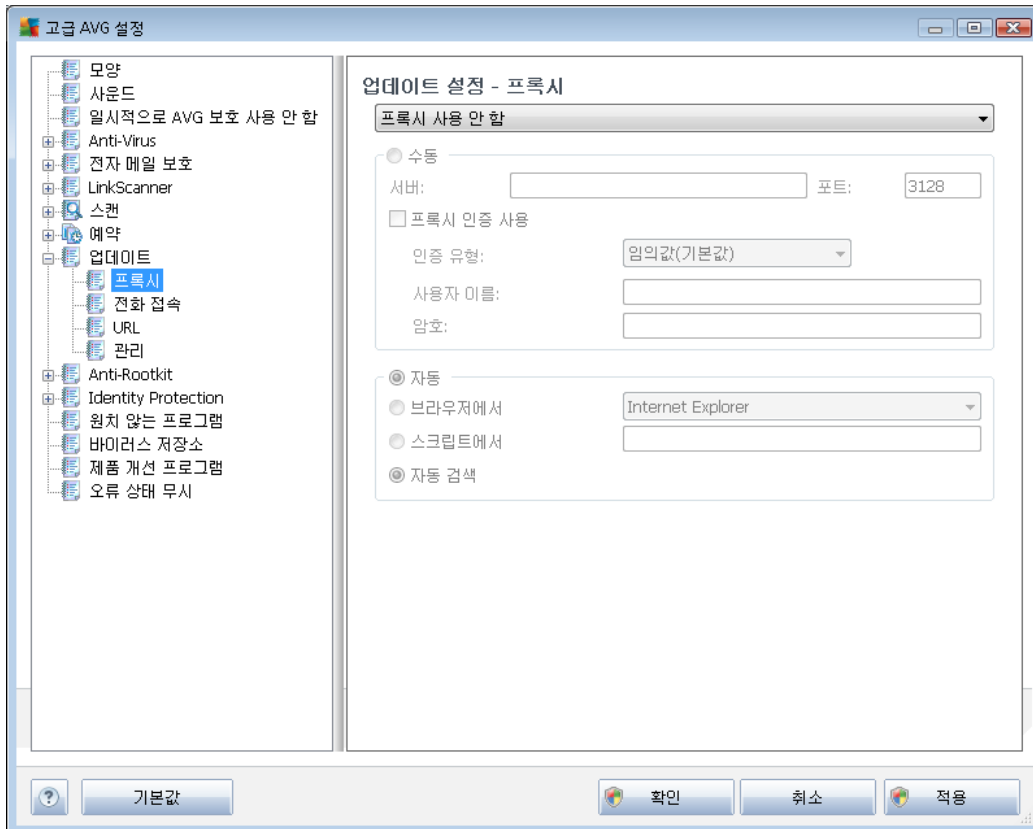
업데이트 후 메모리 스캔

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** (기본적으로 설정됨) - 이 항목을 선택하면 업데이트를 시작할 때 **AVG Internet Security 2012** 에서 DNS 서버에 있는 최신 바이러스 데이터베이스 버전 및 최신 프로그램 버전에 대한 정보를 검색합니다. 그런 다음 반드시 필요한 최소한의 업데이트 파일만 다운로드하여 적용합니다. 이러한 방법으로 다운로드할 전체 데이터의 양을 최소화하고 업데이트를 빠르게 처리합니다.
- **실행 중인 응용 프로그램을 닫으려면 확인이 필요합니다.** (기본적으로 설정되어 있음) 옵션을 설정하면 업데이트 프로세스를 완료하기 위해 현재 실행 중인 응용 프로그램을 닫아야 할 경우에 항상 사용자의 확인을 요구합니다.
- **컴퓨터 시간 확인** - 컴퓨터 시간과 정확한 시간 사이의 차이가, 정해진 값보다 큰 경우 알림이 표시되도록 하려면 이 옵션을 선택합니다.

9.9.1. 프록시



프록시 서버는 인터넷에 대한 보다 안전한 연결을 보장하기 위해 PC에서 실행되는 서비스 또는 독립 실행형 서버입니다. 지정된 네트워크 규칙에 따라 프록시 서버를 통하거나 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 사용 안 함** - 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 활성화하고 다음 항목을 지정해야 합니다.

- **서버** - 서버의 IP 주소 또는 서버 이름을 지정합니다.



- **포트** - 인터넷 액세스를 지원하는 포트 번호를 지정합니다. 기본적으로 이 번호는 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.

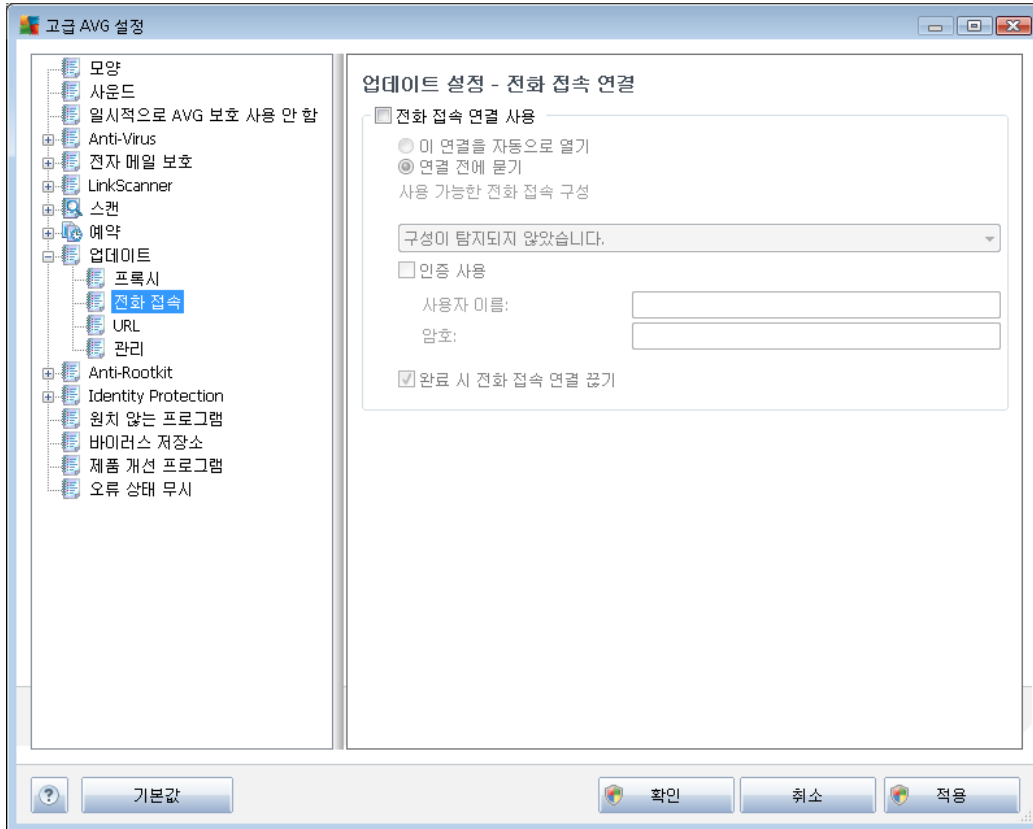
자동 구성

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

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

9.9.2. 전화 접속

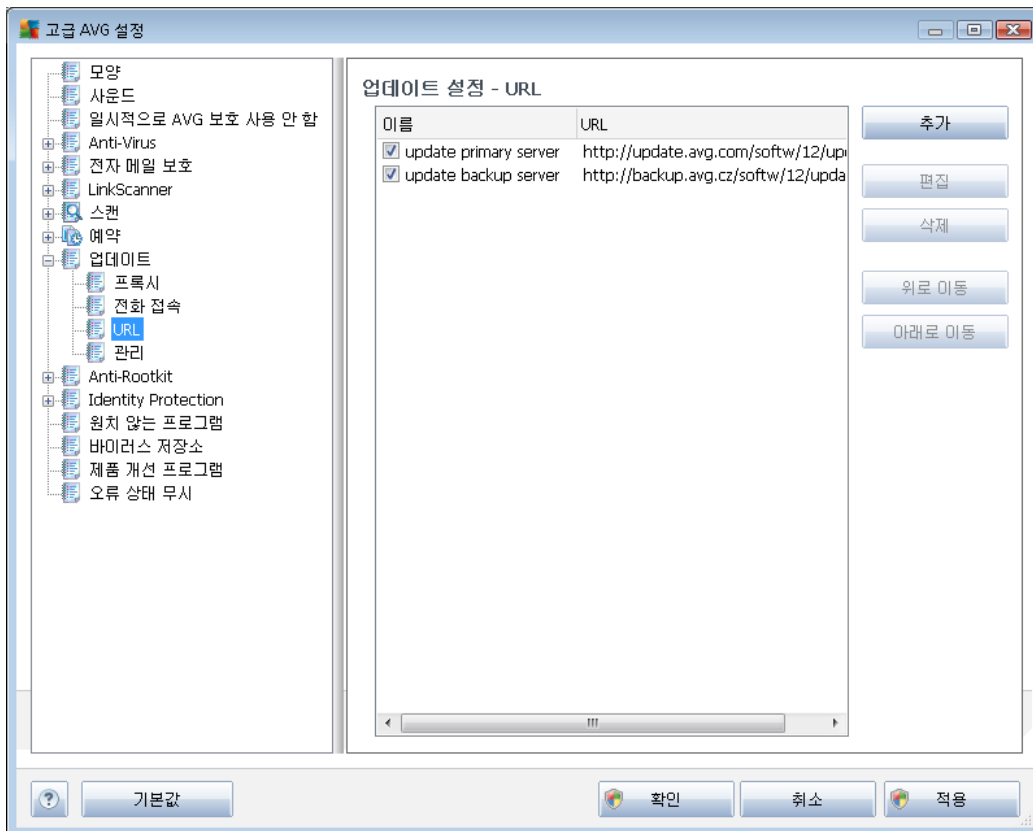
업데이트 설정 - 전화 접속 연결 대화 상자에서 선택적으로 정의된 모든 매개 변수는 인터넷에 대한 전화 접속 연결과 관련되어 있습니다. 이 대화 상자의 필드는 **전화 접속 연결 사용** 옵션을 선택하여 필드를 활성화할 때까지 비활성 상태를 유지합니다:



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**).

9.9.3. URL

URL 대화 상자에는 업데이트 파일을 다운로드할 수 있는 인터넷 주소의 목록이 제공됩니다:



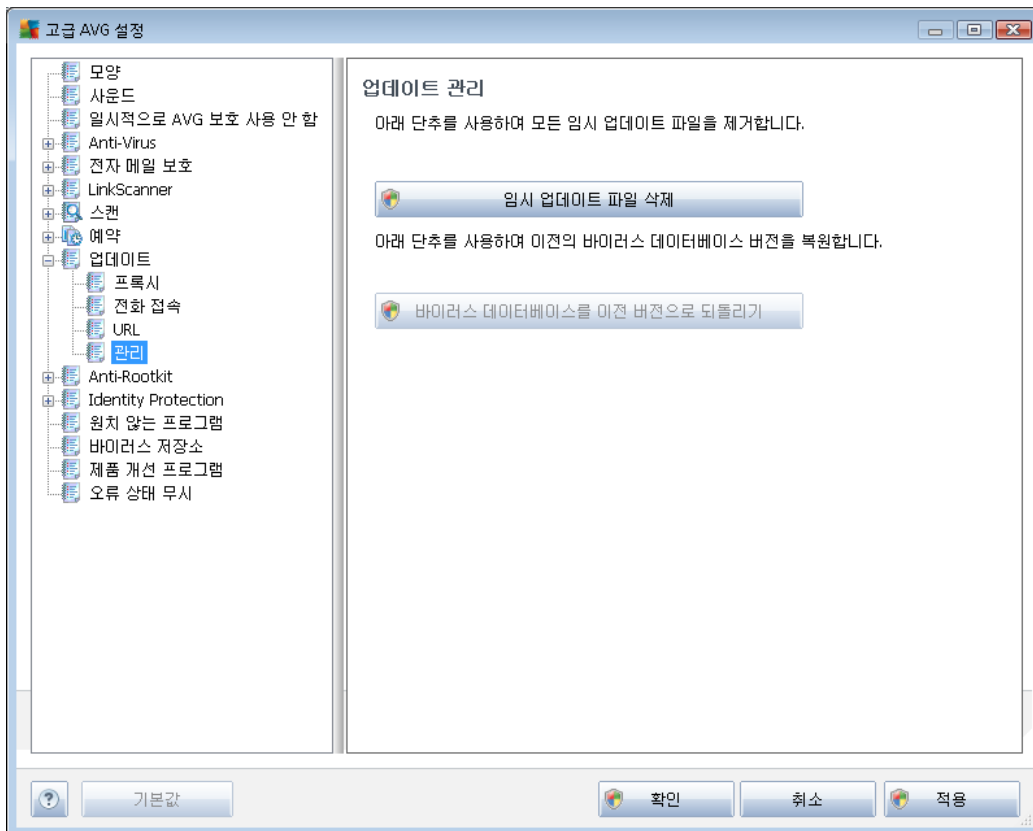
제어 단추

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.

9.9.4. 관리

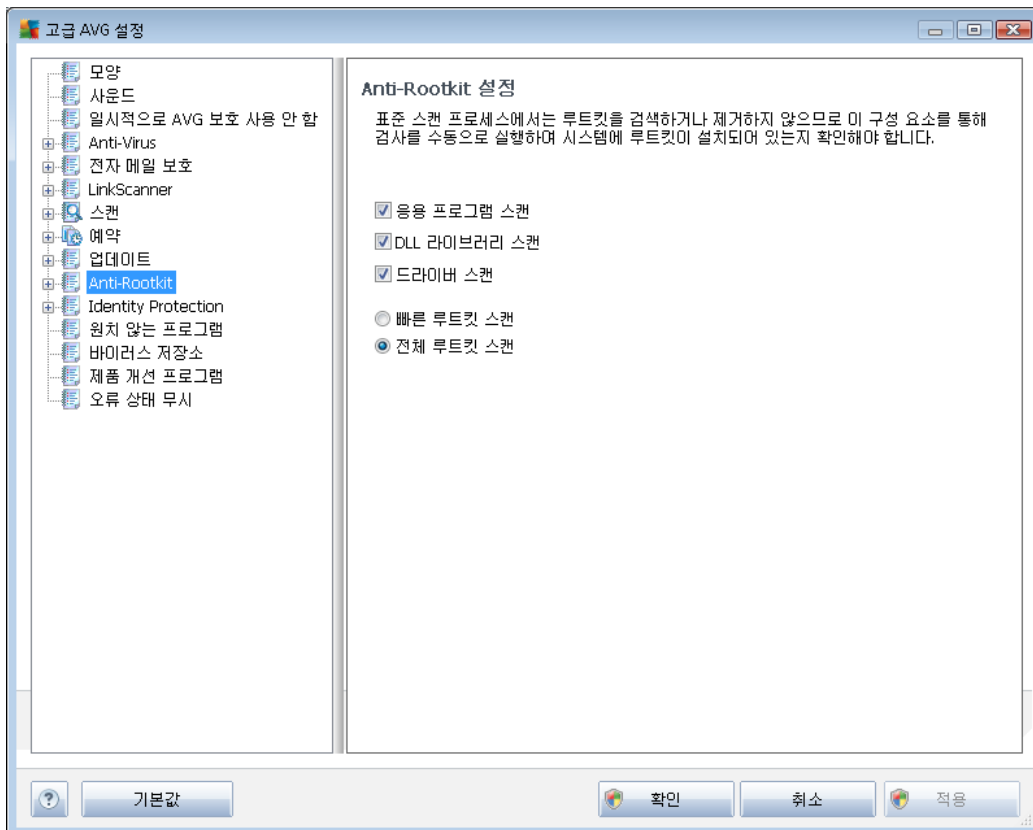
업데이트 관리 대화 상자에는 두 개의 단추를 통해 액세스할 수 있는 두 가지 옵션이 있습니다.



- **임시 업데이트 파일 삭제** - 하드 디스크에서 모든 중복 업데이트 파일을 삭제하려면 이 단추를 누릅니다. 기본적으로 이 파일은 30 일 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.

9.10. Anti- Rootkit

Anti-Rootkit 설정 대화 상자에서 [Anti-Rootkit](#) 구성 요소의 구성을 편집할 수 있습니다.



이 대화 상자에서 제공되는 [Anti-Rootkit](#) 구성 요소의 모든 기능은 [Anti-Rootkit 구성 요소의 인터페이스](#)에서도 직접 액세스하여 편집할 수 있습니다.

먼저 각 확인란을 선택하여 스캔할 개체를 지정합니다.

- **응용 프로그램 스캔**
- **DLL 라이브러리 스캔**
- **드라이버 스캔**

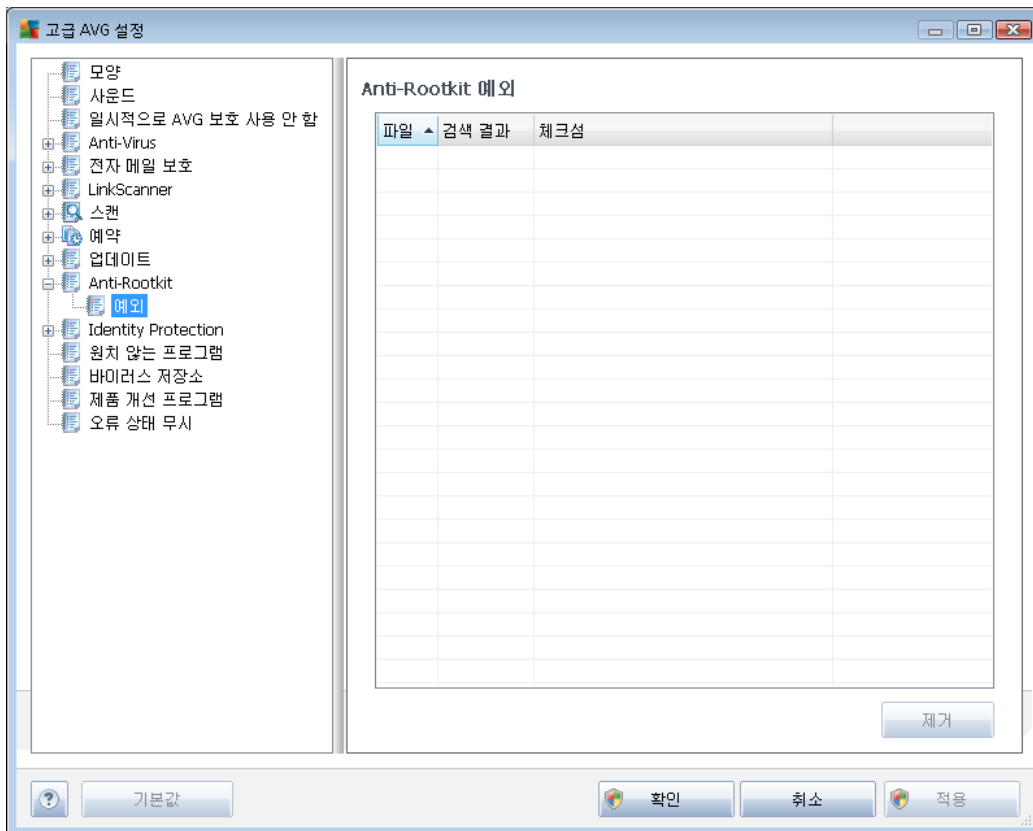
또한 루트킷 스캔 모드도 선택할 수 있습니다.

- **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.



9.10.1. 예외

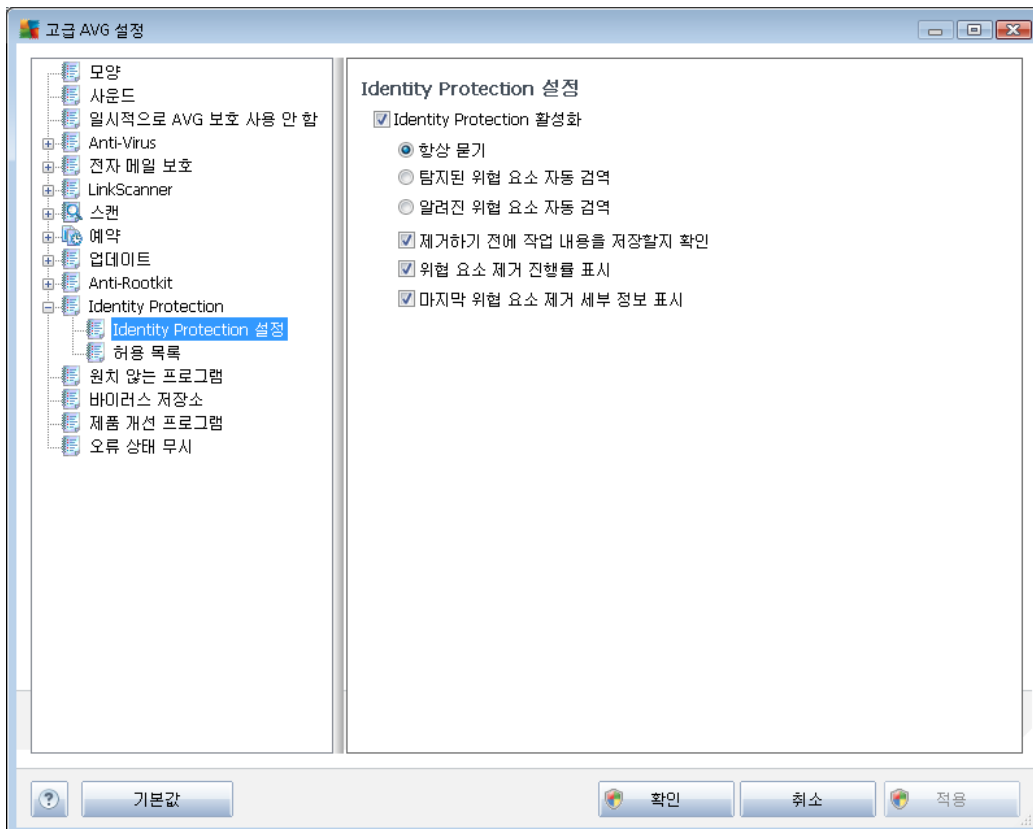
Anti-Rootkit 예외 대화 상자에서는 이 스캔에서 제외할 특정 파일(예: 양성 오류로 인해 루트킷으로 검색될 수 있는 드라이버)을 정의할 수 있습니다.



9.11. Identity Protection

9.11.1. Identity Protection 설정

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



Identity Protection 활성화(기본적으로 설정되어 있음) - [Identity Protection](#) 구성 요소를 해제하려면 선택을 취소합니다.

특별한 경우가 아니면 선택을 취소하지 않는 것이 좋습니다.

[Identity Protection](#) 이 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 [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 발견된 모든 응용 프로그램을 자동으로 즉시 [바이러스 저장소](#)로 이동하려면 이 항목을 선택한 상태로 유지합

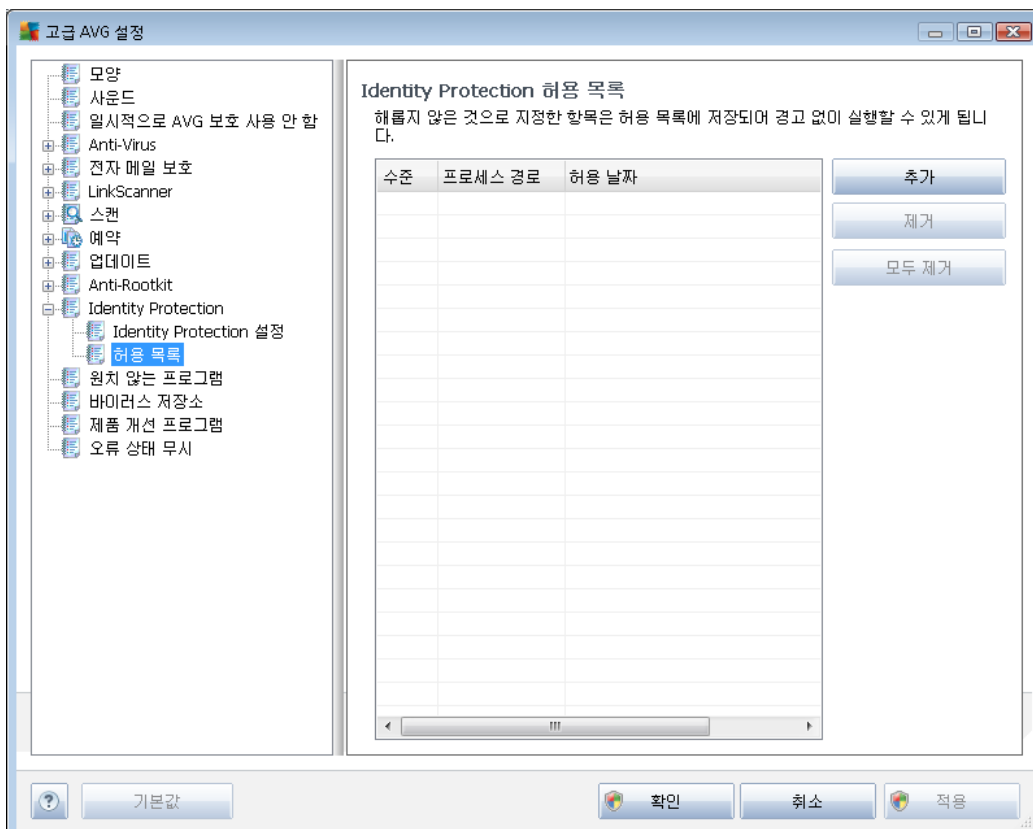
니다.

또한 특정 항목을 지정하여 [Identity Protection](#) 기능을 좀 더 활성화할 수도 있습니다.

- **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 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.

9.11.2. 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 유지되도록 확인하면 해당 응용 프로그램이 **Identity Protection** **허용 목록**에 추가되고 잠재적으로 위험한 응용 프로그램으로 다시 보고되지 않습니다.



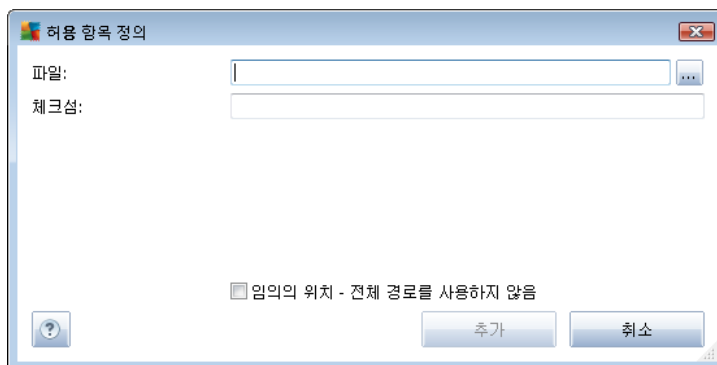
Identity Protection 허용 목록에는 각 응용 프로그램에 대해 다음과 같은 정보가 표시됩니다.

- **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

Identity Protection 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.

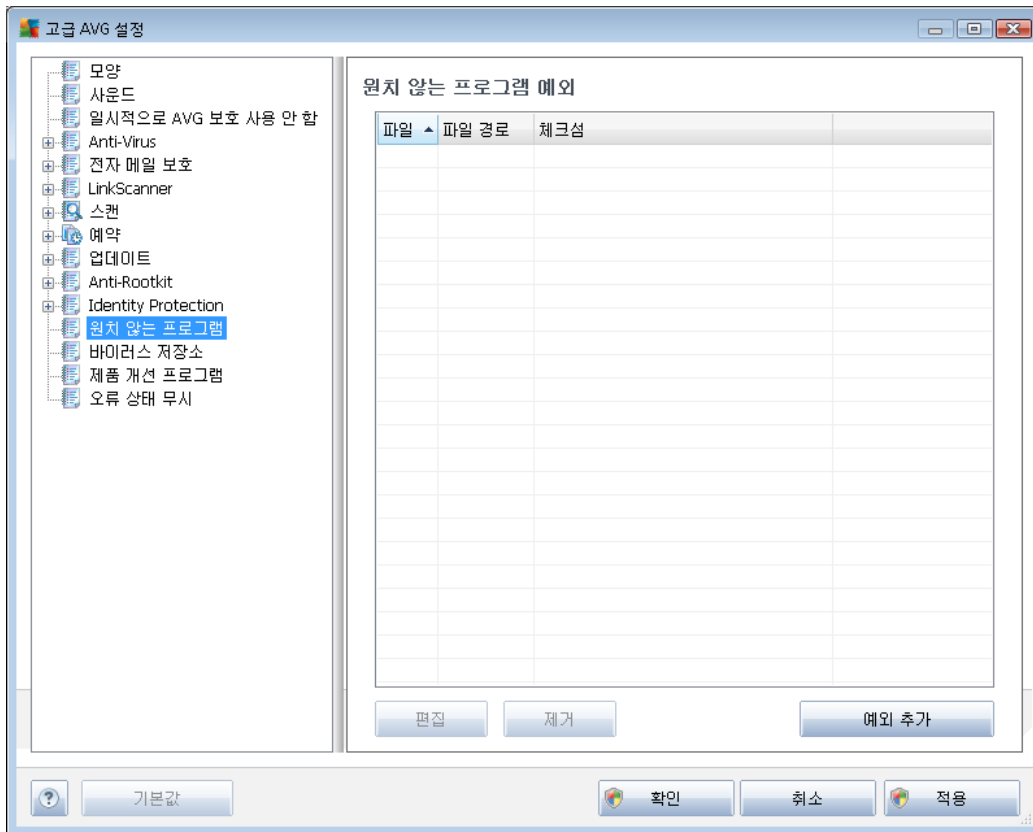


- **파일** - 예외로 표시할 파일(응용 프로그램)에 대한 전체 경로를 입력합니다.
- **체크섬** - 선택된 파일의 고유한 '서명'을 표시합니다. 이 체크섬은 자동으로 생성되는 문자열로, AVG에서는 체크섬을 통해 선택된 파일을 다른 파일과 구분합니다. 체크섬은 파일이 추가된 후에 생성되어 표시됩니다.
- **임의의 위치** - 전체 경로를 사용하지 않음 - 특정 위치에 있는 이 파일만을 예외로 정의하려는 경우에는 이 확인란을 선택 해제된 상태로 두십시오.
- **제거** - 선택한 응용 프로그램을 목록에서 제거하려면 누릅니다.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

9.12. 원치 않는 프로그램

AVG Internet Security 2012는 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(고의로 설치한 프로그램인 경우). 무료 프로그램 등의 일부 프로그램은 애드웨어일 수 있습니다. **AVG Internet Security 2012**에서

는 그러한 애드웨어를 **원치 않는 프로그램**으로 검색하여 보고합니다. 컴퓨터에서 그러한 프로그램을 그대로 유지하고자 할 때는 원치 않는 프로그램에 대한 예외로 정의할 수 있습니다.



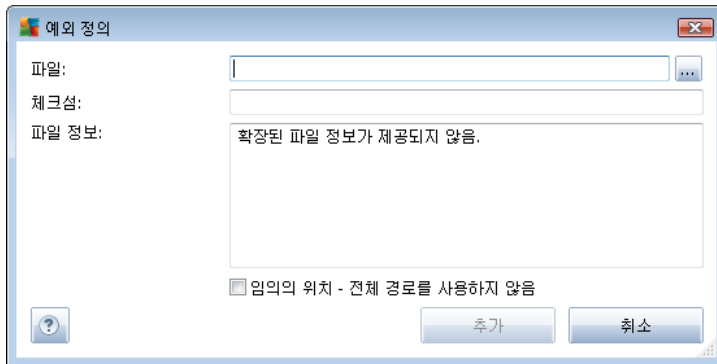
원치 않는 프로그램 예외 대화 상자에는 기존에 이미 원치 않는 프로그램에 대한 예외로 정의되어 현재 사용되고 있는 예외 목록이 표시됩니다. 목록을 편집하거나 기존 항목을 삭제하거나 새 예외를 추가할 수 있습니다. 각 예외에 대해 목록에서 다음 정보를 찾을 수 있습니다.

- **파일** - 해당 응용 프로그램의 정확한 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

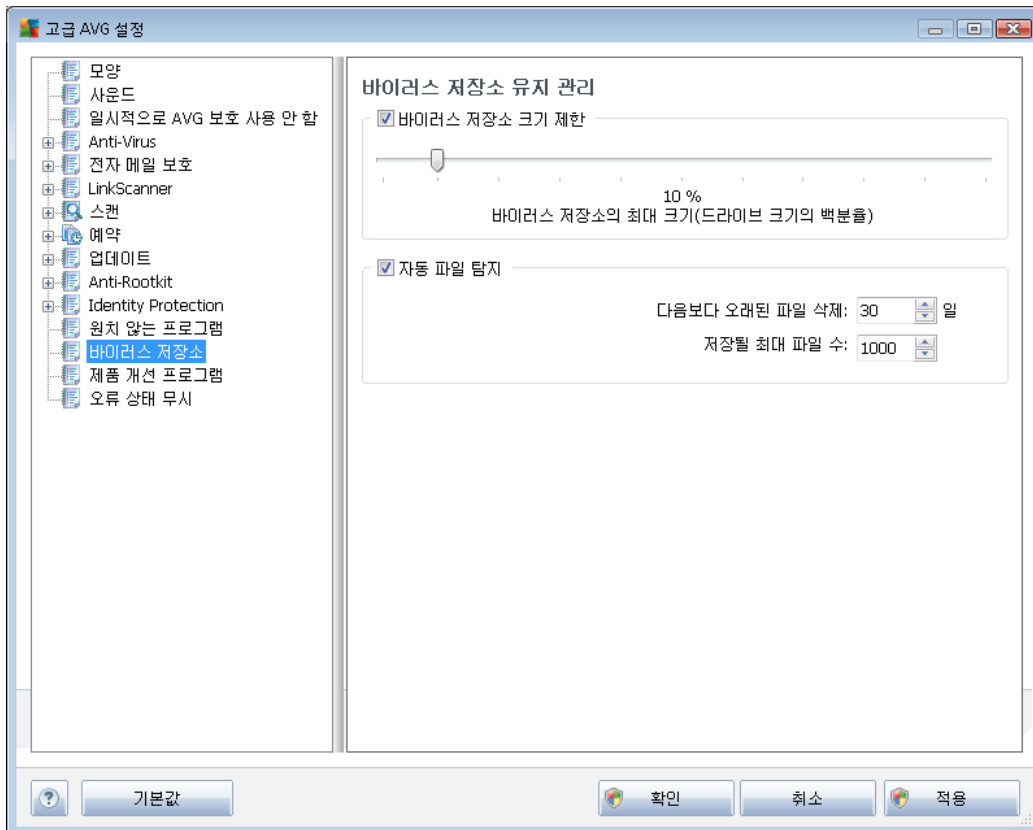
- **편집** - 이미 정의된 예외에 대한 편집 대화 상자를 엽니다(*아래의 새로운 예외 정의 대화 상자*와 동일). 여기서 예외 매개 변수를 변경할 수 있습니다.
- **제거** - 예외 목록에서 선택된 항목을 삭제합니다.

- **예외 추가** - 생성할 새로운 예외 매개 변수를 정의할 수 있는 편집 대화 상자를 엽니다.



- o **파일** - 예외로 지정할 파일에 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 **파일 정보** - 파일에 대한 추가적인 정보(라이선스/버전 정보 등)를 표시합니다.
- o **임의의 위치 - 전체 경로를 사용하지 않음** - 특정 위치에 있는 파일만을 예외로 정의하려는 경우에는 이 확인란을 선택 취소된 상태로 두십시오. 이 확인란이 선택되어 있으면 지정한 파일이 그 위치에 상관없이 예외로 정의됩니다. 하지만, 이 경우에도 해당 파일의 전체 경로를 입력해야 합니다. 그러면 시스템에 이름이 같은 두 개의 파일이 표시되는 경우 해당 파일을 고유한 예제로 사용할 수 있습니다.

9.13. 바이러스 저장소



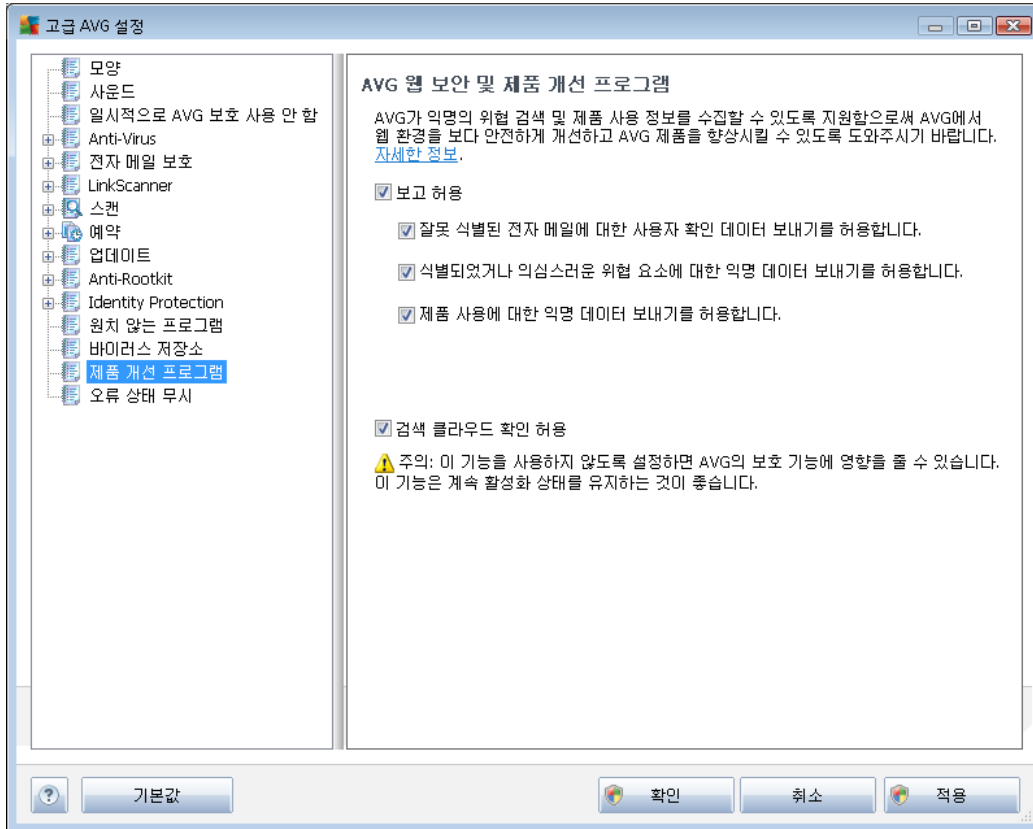
바이러스 저장소 유지 관리 대화 상자를 사용하여 [바이러스 저장소](#)에 저장된 개체를 관리하기 위한 몇 가지 매개 변수를 정의할 수 있습니다.

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

9.14. 제품 개선 프로그램

AVG 웹 보안 및 제품 개선 프로그램 대화 상자에서는 AVG 제품 개선 프로그램에 참여하고 전반적인 인터넷 보안 수준을 높일 수 있도록 안내합니다. **보고 허용** 옵션을 선택하면 검색된 위협 요소를 AVG 연구소에 보고할 수 있습니다. AVG에서는 이를 통해 전 세계의 사용자로부터 최신 위협 요소에 대한 정보를 수집하고, 수집된 정보를 활용하여 보호 기능을 개선할 수 있습니다.

보고 작업은 자동으로 이루어지므로 사용자에게 아무런 불편을 끼치지 않으며 개인 데이터는 보고서에 포함되지 않습니다. 검색된 위협 요소를 보고하는 것은 개인의 선택이지만 이 옵션을 설정하면 AVG에서 사용자를 위해 보호 기능을 개선하는 데 많은 도움이 될 것입니다.



요즘에는 일반 바이러스 외의 위협 요소가 더 많습니다. 악의적인 코드와 위험한 웹 사이트를 만드는 사람들은 매우 혁신적이어서 새로운 종류의 위협 요소가 빈번히 등장하게 되고 이들 대부분이 인터넷상에 존재합니다. 가장 일반적인 위협 요소로 다음과 같은 예를 들 수 있습니다.

- **바이러스**는 자체적으로 복사 및 전파되는 악의적인 코드로, 피해가 발생한 후에 발견되는 것이 대부분입니다. 어떤 바이러스는 매우 심각한 위협 요소로, 파일을 삭제하거나 고의적으로 변경하는 반면 어떤 바이러스는 음악을 재생하는 등 겉보기에 무해한 작업을 수행할 수 있습니다. 그러나 단순한 바이러스도 전체 컴퓨터 메모리를 한순간에 차지하여 작동을 중단시킬 수 있으므로 모든 바이러스는 기본적으로 위험합니다.
- **웜**은 바이러스의 일종으로, 일반적인 바이러스와 달리 "운반" 개체를 필요로 하지 않습니다. 대개 전자 메일을 통해 자체적으로 포함되어 다른 컴퓨터로 전송되며 감염되는 경우 전자 메일 서버와 네트워크 시스템에 과부하를 초래합니다.
- **일반적으로 스파이웨어**는 트로이 목마 등의 프로그램을 포함하는 맬웨어(*바이러스를 포함한 모든 악의적인 소프트웨어*) 범주로 정의됩니다. 컴퓨터 소유자의 인지도 없이 개인 정보, 암호, 신용 카드 번호를 훔치거나 컴퓨터에 침투하여 공격자가 원격으로 제어권을 획득하기 위한 목적으로 사용됩니다.
- **원치 않는 프로그램**은 일종의 스파이웨어로, 컴퓨터에 유해할 수도 있고 유해하지 않을 수도 있습니다. PUP의 예로 애드웨어를 들 수 있습니다. 애드웨어란 대개 광고 팝업을 표시하여 광고를 배포하도록 고안된 소프트웨어입니다. 귀찮기

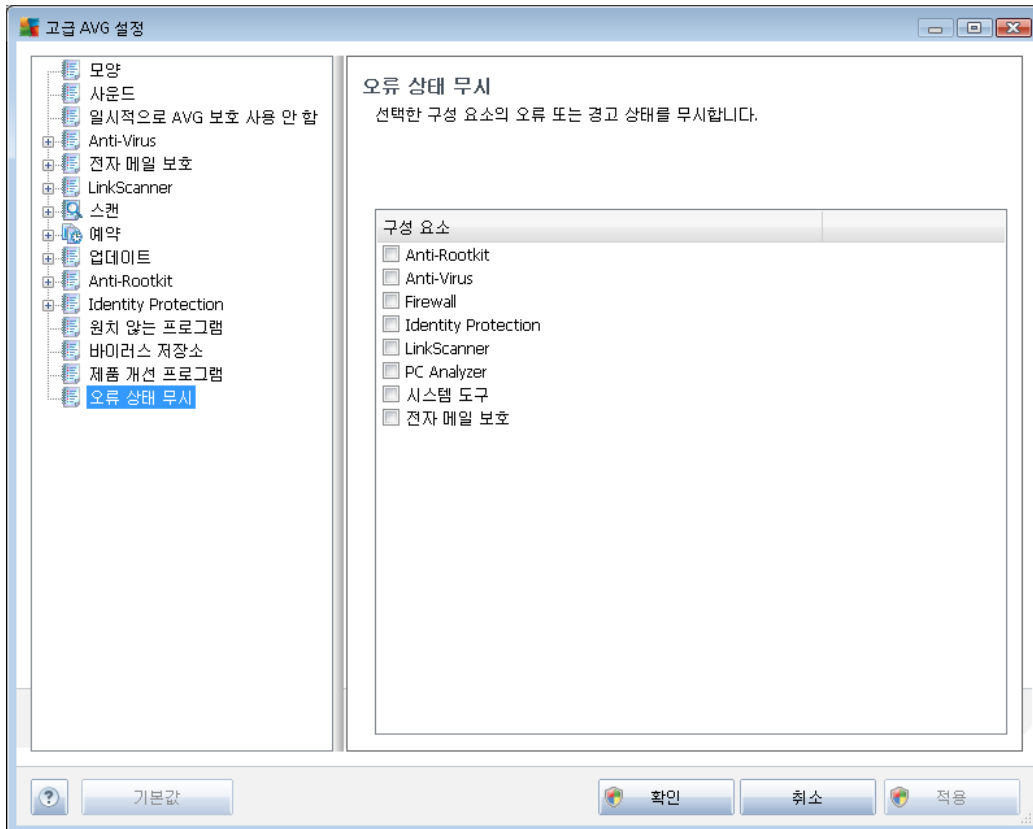
는 하지만 유해하지는 않습니다.

- **추적 쿠키**도 일종의 스파이웨어로 간주될 수 있습니다. 추적 쿠키란 웹 브라우저에 저장되는 작은 파일로, 사용자가 다시 방문할 때 "상위" 웹 사이트로 자동 전송됩니다. 여기에는 탐색 기록과 기타 유사한 정보 등의 데이터가 포함될 수 있습니다.
- **익스플로잇**은 운영 체제, 인터넷 브라우저 또는 다른 필수 프로그램의 결함이나 취약점을 이용하는 악의적인 코드입니다.
- **피싱**은 신뢰할 수 있고 잘 알려진 조직을 가장하여 중요한 개인 데이터를 얻으려는 시도를 말합니다. 일반적으로 은행 계좌 정보를 업데이트하라는 등의 대량 전자 메일을 받는 사람들이 피해를 당할 수 있습니다. 이들은 사용자로 하여금 제공된 링크를 따라가도록 만들어서 가짜 은행 웹 사이트로 유인합니다.
- **혹스**는 위험하거나 놀라게 하는 내용 또는 쓸데없고 귀찮기만 한 내용이 포함된 대량 전자 메일입니다. 위에서 설명한 위협 요소가 대부분 혹스 전자 메일 메시지를 통해 퍼집니다.
- **악의적인 웹 사이트**는 사용자의 컴퓨터에 악의적인 소프트웨어를 교묘하게 설치하며 해킹 사이트 역시 이와 같은 작업을 합니다. 단지 해킹 사이트는 침입자에 의해 감염된 합법적인 웹 사이트라는 점에서 다릅니다.

이러한 여러 가지 종류의 위협 요소로부터 보호할 수 있도록 AVG Internet Security 2012에는 다음과 같은 특수한 구성 요소가 포함되어 있습니다. 이러한 구성 요소에 대한 간략한 설명을 보려면 [구성 요소 개요](#) 장을 참조하십시오.

9.15. 오류 상태 무시

오류 상태 무시 대화 상자에서는 관련 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 아이콘이 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.

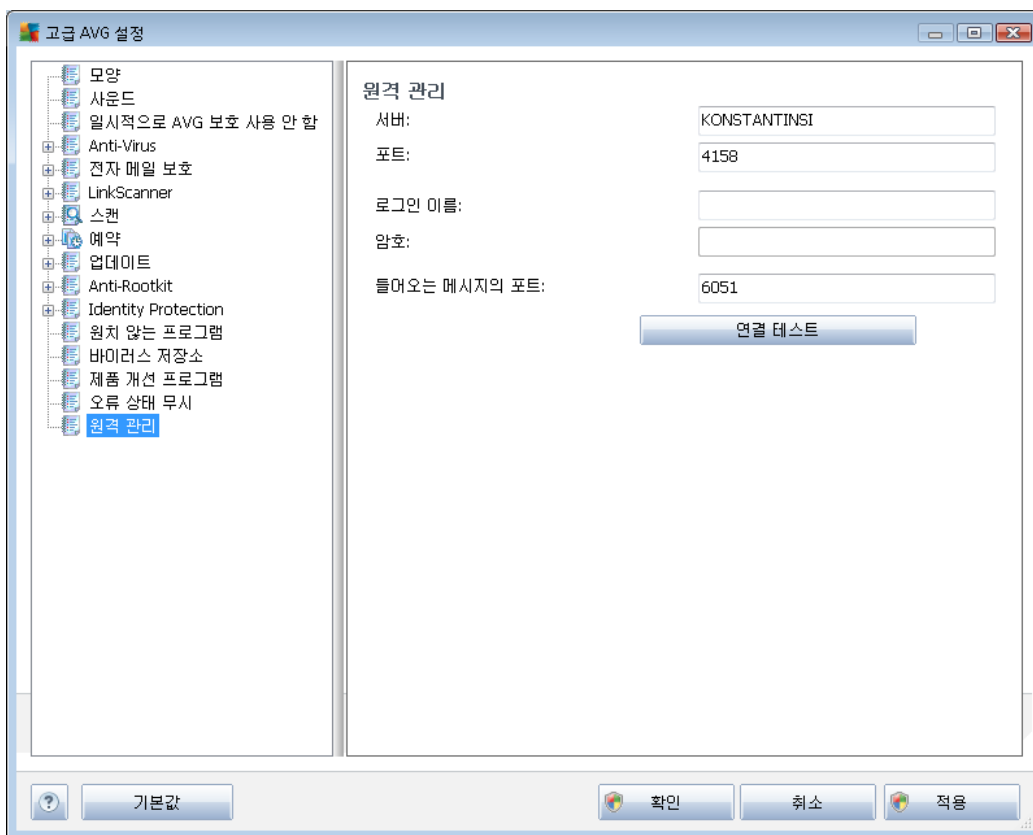
이 경우 위의 대화 상자에서 오류 상태(또는 *해제된 상태*)에 있지만 해당 상태에 대한 알림을 받지 않으려는 구성 요소를 선택할 수 있습니다. 같은 옵션인 [구성 요소 상태 무시](#)



도 [AVG 기본 창에 있는 구성 요소 개요](#)에서 특정 구성 요소에 바로 사용할 수 있습니다.

9.16. 원격 관리

AVG Business Edition 라이선스 중 하나를 사용하여 **AVG Internet Security 2012** 프로그램을 설치하고 설치 프로세스 중에 **원격 관리** 구성 요소가 설치되도록 지정한 경우에 탐색 트리에 **원격 관리** 항목 및 해당 대화 상자가 표시됩니다. 원격 관리 설치 및 구성에 대한 자세한 내용은 AVG 웹 사이트 (<http://www.avg.com/>)의 [지원 센터/다운로드](#) 섹션에서 다운로드할 수 있는 AVG Network Edition 설명서를 참조하십시오.



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.

제어 단추

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

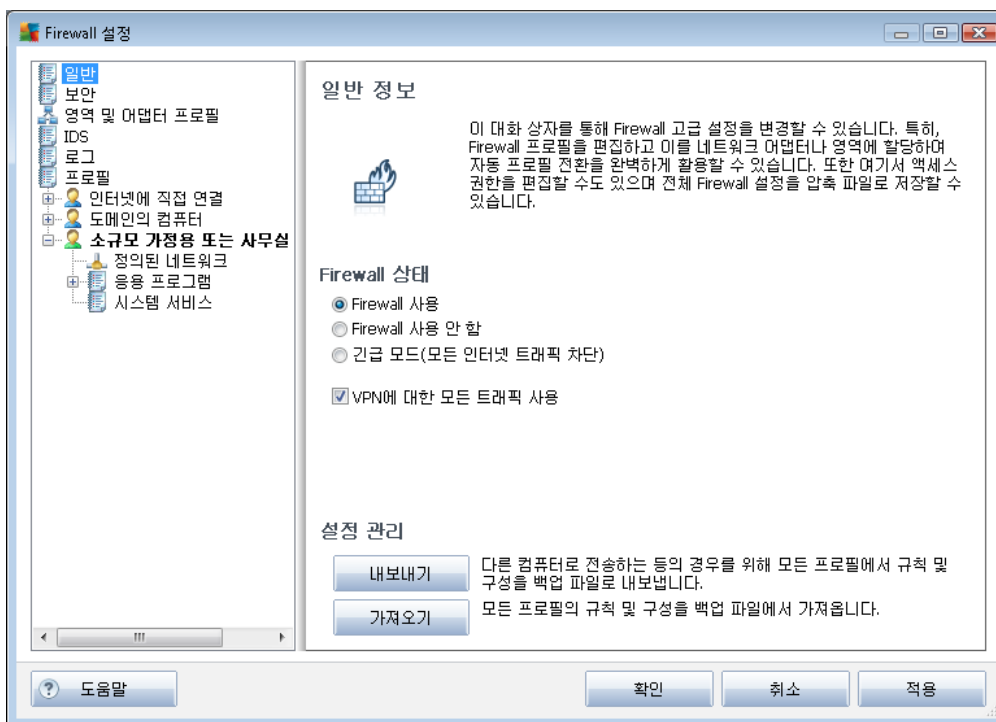
10. Firewall 설정

Firewall 구성은 구성 요소의 고급 매개 변수를 설정할 수 있는 여러 개의 대화 상자가 있는 새 창에서 열립니다.

그러나 소프트웨어 공급업체가 최적의 성능을 낼 수 있도록 이미 모든 AVG Internet Security 2012 구성 요소를 설정해 놓았습니다. 특별한 이유가 없다면 기본 구성을 변경하지 마십시오. 모든 설정 변경은 숙련된 사용자만 수행해야 합니다.

10.1. 일반

일반 정보 대화 상자는 다음 두 섹션으로 나뉩니다.



Firewall 상태

Firewall 상태 섹션에서는 필요한 경우 **Firewall** 상태를 전환할 수 있습니다.

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

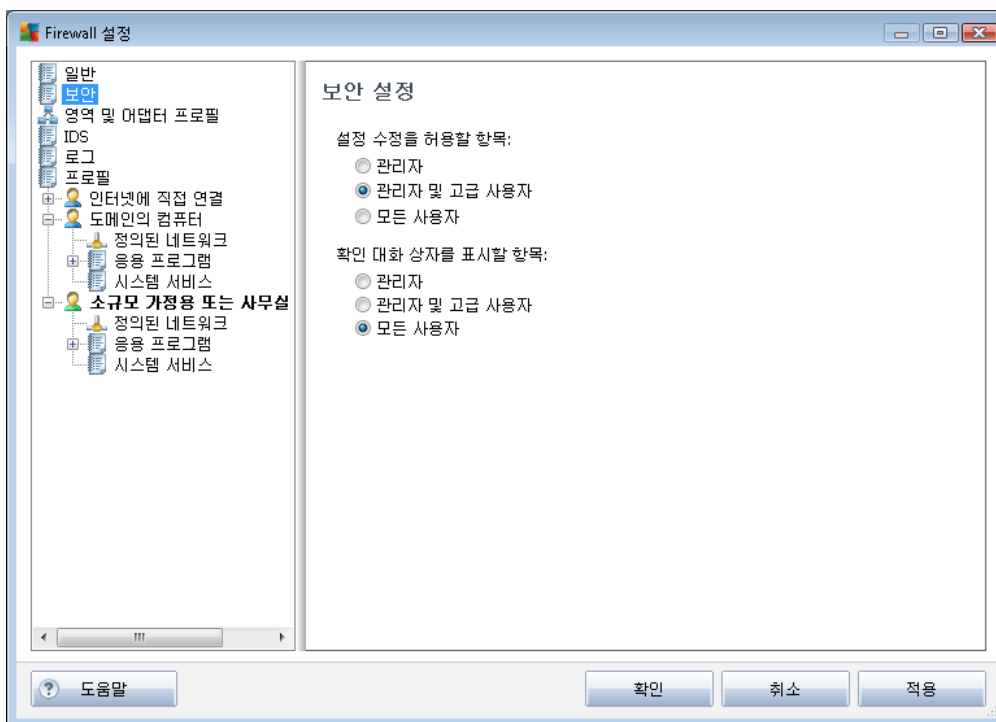
- **VPN에 대한 모든 트래픽 사용** (기본적으로 설정되어 있음) - VPN (가상 사설망) 연결을 사용하는 경우 (예: 집에서 사무실 연결) 이 상자를 선택하는 것이 좋습니다. **AVG Firewall**은 자동으로 네트워크 어댑터를 검색하여 VPN 연결에 사용되는 어댑터를 찾아 모든 응용 프로그램이 대상 네트워크에 연결되도록 해줍니다 (특정 Firewall 규칙이 할당되지 않은 응용 프로그램에만 적용됨). 일반 네트워크 어댑터가 있는 표준 시스템에서는 이러한 간단한 단계를 수행함으로써 VPN을 통해 사용해야 하는 각 응용 프로그램에 대해 세부 규칙을 설정하지 않아도 됩니다.

참고: VPN 연결을 활성화하려면 GRE, ESP, L2TP, PPTP 시스템 프로토콜에 대한 커뮤니케이션을 허용해야 합니다. 이 작업은 [시스템 서비스](#) 대화 상자에서 수행할 수 있습니다.

설정 관리

설정 관리 섹션에서는 [Firewall](#) 구성 **내보내기/가져오기**를 수행할 수 있습니다. 예를 들어, 정의된 [Firewall](#) 규칙 및 설정을 백업 파일로 내보내거나 전체 백업 파일을 가져올 수 있습니다.

10.2. 보안



보안 설정 대화 상자에서 [방화벽](#) 동작에 대한 일반 규칙을 선택된 프로필에 상관없이 정의할 수 있습니다.

- **설정 수정을 허용할 대상** - [Firewall](#) 구성을 변경할 수 있는 사용자를 지정합니다.
- **확인 대화 상자를 표시할 항목** - 확인 대화 상자 (정의된 [Firewall](#) 규칙이 적용되지

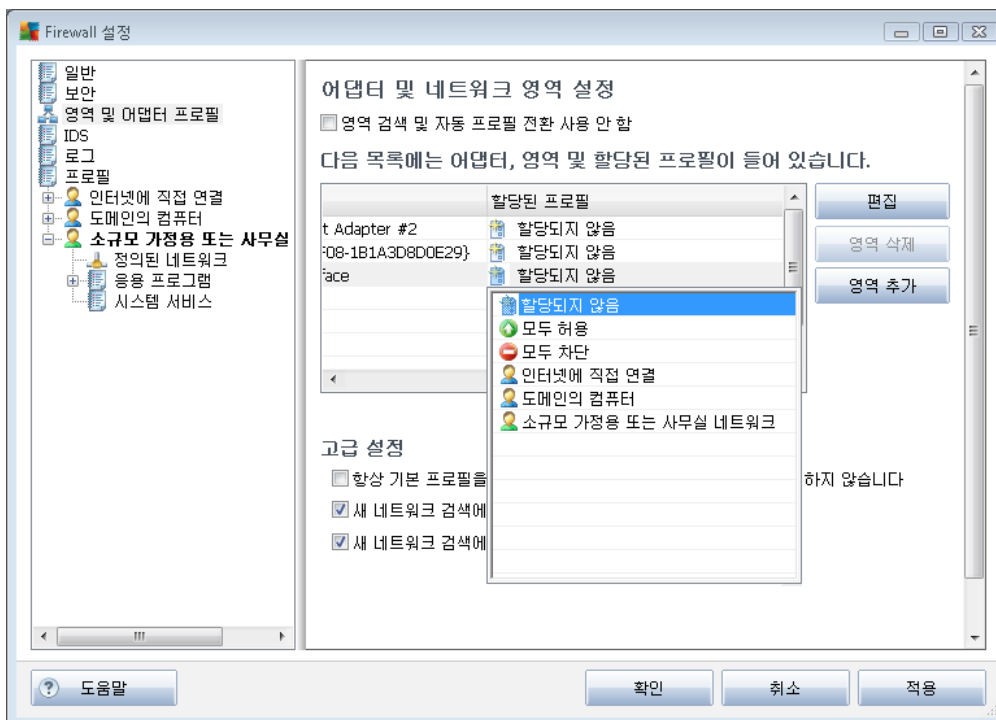
않는 상황에서 사용자의 결정 사항을 확인하는 대화 상자)를 표시해야 할 대상 사용자를 지정합니다.

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

- **관리자** - PC를 완전히 제어할 수 있으며 모든 사용자를 특별히 정의된 권한이 있는 그룹에 할당할 수 있습니다.
- **관리자 및 고급 사용자** - 관리자는 모든 사용자를 지정된 그룹(고급 사용자)에 할당하고 그룹 구성원의 권한을 정의할 수 있습니다.
- **모든 사용자** - 특정 그룹에 할당되지 않은 기타 사용자입니다.

10.3. 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**(기본적으로 해제되어 있음)- 정의된 프로필 중 하나를 각 네트워크 인터페이스 유형, 즉 각각의 영역에 할당할 수 있습니다. 특정 프로필을 정의하지 않는 경우 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.



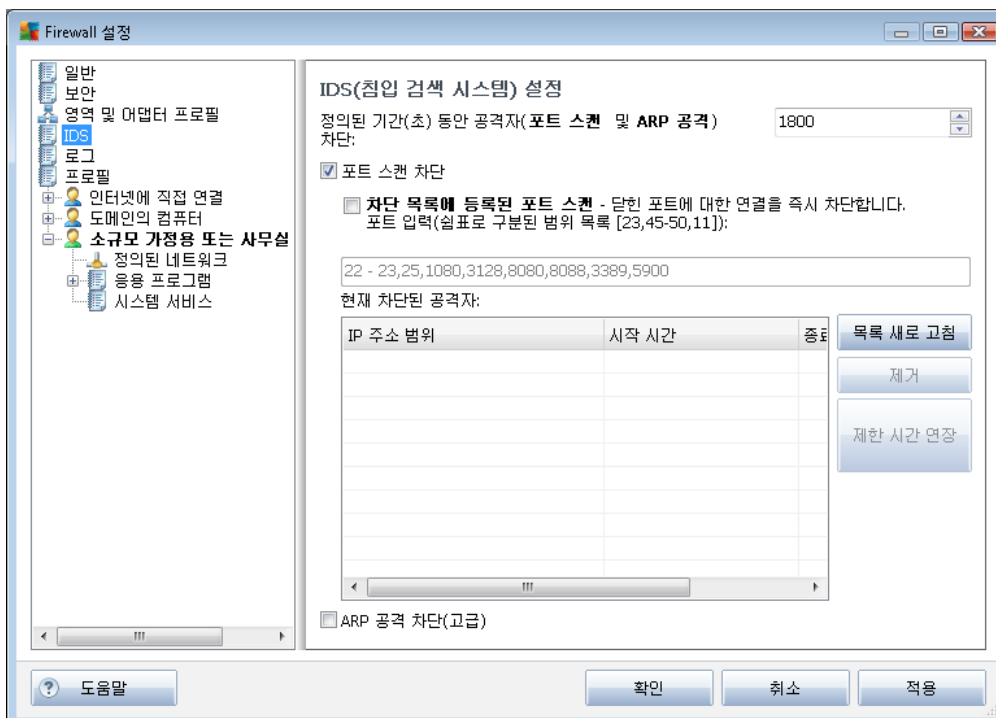
- **어댑터, 영역 및 할당된 프로필 목록** - 이 목록에서 검색된 어댑터 및 영역에 대한 개요를 찾을 수 있습니다. 그 각각에 대해 정의된 프로필 메뉴의 특정 프로필을 할당할 수 있습니다. 이 메뉴를 열려면 어댑터 목록(할당된 프로필 열)의 각 항목을 마우스 왼쪽 단추로 클릭하고 상황에 맞는 메뉴에서 프로필을 선택합니다.

고급 설정

- o **항상 기본 프로필을 사용하되 새 네트워크 검색 대화 상자를 표시하지 않음** - 사용자 컴퓨터가 새 네트워크에 연결될 때마다 [Firewall](#)에서는 사용자에게 경고 메시지를 표시하며 네트워크 연결 유형을 선택하고 이를 [Firewall 프로필](#)에 할당하라는 메시지가 포함된 대화 상자를 표시합니다. 이 대화 상자를 표시하지 않으려면 이 확인란을 선택하십시오.
- o **새 네트워크 검색에 AVG 지능형 검색 사용** - AVG의 고유한 메커니즘을 사용하여 새로 검색된 네트워크에 대한 정보를 수집할 수 있습니다(하지만 이 옵션은 VISTA OS 이상에서만 사용할 수 있음).
- o **새 네트워크 검색에 Microsoft 지능형 분석 사용** - Windows 서비스(이 옵션은 Windows Vista 이상 버전에서만 제공됨)에서 새로 검색된 네트워크에 대한 정보를 얻을 수 있습니다.

10.4. IDS

침입 검색 시스템은 컴퓨터의 특정 포트에서 발생하는 의심스러운 커뮤니케이션 시도를 식별하여 차단하도록 설계된 특수한 동작 분석 기능입니다. **IDS(침입 검색 시스템) 설정** 대화 상자 내에서 IDS 매개 변수를 구성할 수 있습니다.



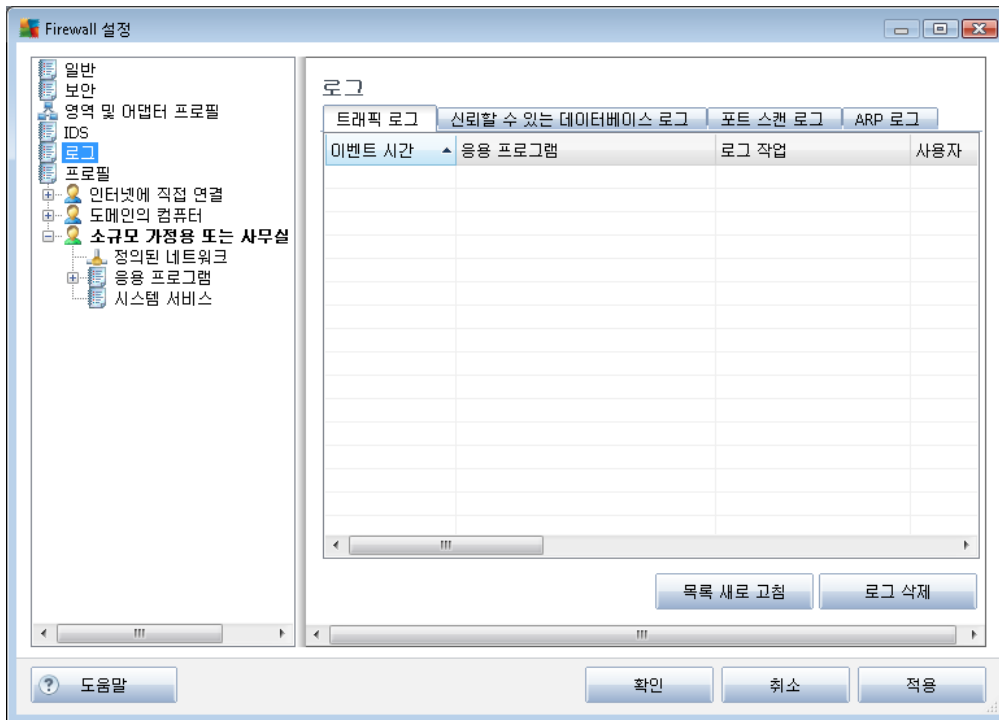
IDS (침입 검색 시스템) 설정 대화 상자에서는 다음 구성 옵션을 제공합니다.

- **정의된 기간 동안 공격자(포트 스캔 및 ARP 공격) 차단** - 여기서는 의심스러운 커뮤니케이션 시도가 검색될 경우 해당 포트를 차단할 시간(초)을 지정할 수 있습니다. 기본적으로 시간 간격은 1800 초(30 분)로 설정되어 있습니다.
- **포트 스캔 차단(기본으로 설정되어 있음)** - 외부에서 TCP 및 UDP 포트를 통해 컴퓨터로 들어오려는 모든 커뮤니케이션 시도를 차단하려면 이 상자를 선택합니다. 이와 같은 연결이 있는 경우 5 번까지 시도가 허용되고 그 이후부터는 차단됩니다. 이 항목은 기본으로 사용하도록 되어 있으며 이 설정은 그대로 유지하는 것이 좋습니다. **포트 스캔 차단** 옵션을 선택한 채로 두면 세부적인 추가 구성을 지정할 수 있습니다. *이 옵션을 선택하지 않으면 다음 항목은 비활성화됩니다.*
 - **차단 목록에 등록된 포트 스캔** - 아래의 텍스트 필드에 지정한 포트에서 발생하는 모든 커뮤니케이션 시도를 즉시 차단하려면 이 상자를 선택합니다. 각 포트나 포트 범위는 쉼표로 구분해야 합니다. 이 기능을 사용할 때 권장되는 포트 목록이 미리 정의되어 있습니다.
 - **현재 차단된 공격자** - 이 섹션에는 현재 [Firewall](#)에 의해 차단된 모든 커뮤니케이션 시도가 나열됩니다. 차단된 시도에 대한 전체 기록은 [로그](#) 대화 상자의 **포트 스캔 로그 탭**에서 볼 수 있습니다.
- **ARP 공격 차단(고급)(기본적으로 선택되지 않음)** - 로컬 네트워크 내부에서 발생하며 IDS에서 잠재적으로 위험한 것으로 검색되는 특수한 종류의 커뮤니케이션 시도를 차단하려면 이 옵션을 선택합니다. 이 경우 **정의된 기간 동안 공격자 차단에 설정된 기간이 적용됩니다.** 로컬 네트워크의 유형과 위험 수준에 대해 잘 알고 있는 고급 사용자만 이 기능을 사용하는 것이 좋습니다.

제 어 단 추

- **목록 새로 고침** - 목록을 업데이트하여 **최근에 차단된 시도를 모두 포함하려면** 이 단추를 누릅니다.
- **제거** - 선택된 차단을 취소하려면 누릅니다.
- **제한 시간 연장** - 선택한 시도를 차단할 기간을 연장하려면 누릅니다. 시간 연장 옵션이 있는 대화 상자가 나타납니다. 여기에서 특정 시간과 날짜를 설정하거나 기간을 무한정으로 설정할 수 있습니다.

10.5. 로그



로그 대화 상자에서는 네 개의 탭을 통해 기록된 모든 **Firewall** 작업 및 이벤트 목록은 물론 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)을 검토할 수 있습니다.

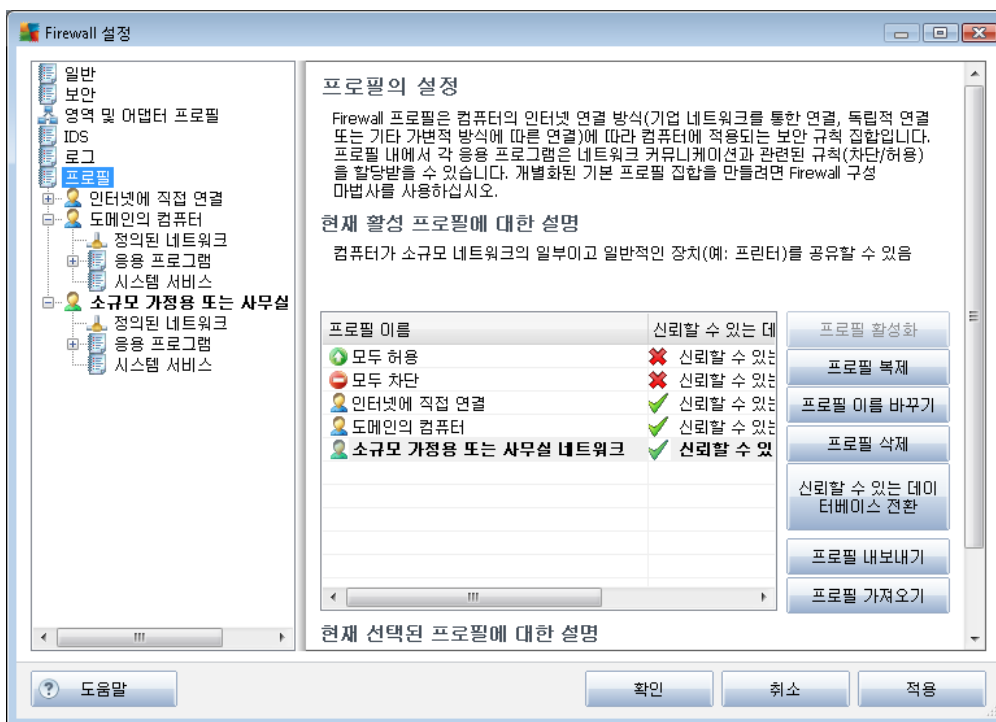
- **트래픽 로그** - 네트워크에 연결하려고 시도한 모든 응용 프로그램 활동에 대한 정보를 제공합니다.
- **신뢰할 수 있는 데이터베이스 로그** - 신뢰할 수 있는 데이터베이스는 온라인 커뮤니케이션이 항상 허용되는 인증되고 신뢰할 수 있는 응용 프로그램에 대해 AVG 내부에서 수집한 데이터베이스 정보입니다. 새 응용 프로그램을 처음 네트워크에 연결하려고 할 때(예: 해당 응용 프로그램에 대한 Firewall 규칙이 지정되지 않은 경우) 해당 응용 프로그램에 대한 네트워크 커뮤니케이션을 허용할지 여부를 판단해야 합니다. AVG는 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 표시합니다.
- **포트 스캔 로그** - 모든 **침입 검색 시스템** 활동을 기록합니다.
- **ARP 로그** - 로컬 네트워크 내부에서 발생하며 **침입 검색 시스템**에서 잠재적으로 위험한 것으로 검색된 특정 종류의 커뮤니케이션 시도의 차단(**ARP 공격 차단 옵션**)과 관련된 정보를 기록합니다.

제어 단추

- **목록 새로 고침** - 해당 열 머리글을 클릭하면 기록된 모든 매개 변수가 선택된 특성에 따라, 즉 발생 순서(날짜) 또는 알파벳순(기타 열)으로 정렬됩니다. **목록 새로 고침** 단추를 사용하면 현재 표시된 정보를 업데이트할 수 있습니다.
- **로그 삭제** - 이 단추를 누르면 차트에 있는 모든 항목이 삭제됩니다.

10.6. 프로필

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



시스템 프로필(**모두 허용**, **모두 차단**)은 편집할 수 없습니다. 하지만 모든 사용자 지정 **프로필**(**인터넷에 직접 연결**, **도메인의 컴퓨터**, **소규모 가정용 또는 사무실 네트워크**)은 다음 제어 단추를 사용하여 이 대화 상자에서 바로 편집할 수 있습니다.

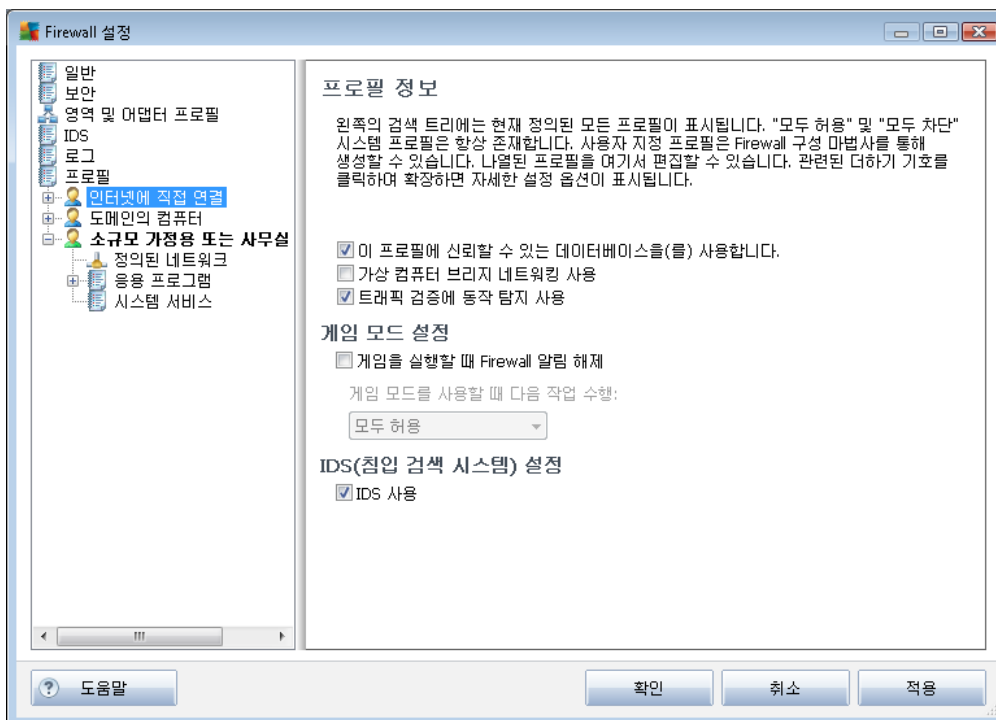
- **프로필 활성화** - 이 단추는 선택된 프로필을 활성 상태로 설정합니다. [Firewall](#) 에서는 선택된 프로필 구성을 사용하여 네트워크 트래픽을 제어합니다.
- **프로필 복제** - 선택된 프로필의 동일한 사본을 만듭니다. 이 사본을 편집하고 이름을 바꾸어 복제한 원본 프로필에 기반하는 새로운 프로필을 만들 수 있습니다.
- **프로필 이름 바꾸기** - 선택된 프로필에 대해 새로운 이름을 정의할 수 있습니다.
- **프로필 삭제** - 목록에서 선택된 프로필을 삭제합니다.

- **신뢰할 수 있는 데이터베이스 전환** - 선택한 프로필에 대해 신뢰할 수 있는 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.

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.

10.6.1. 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 데이터베이스 사용** (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 선택하십시오. 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 탐지 사용**(기본적으로 설정되어 있음) - [Firewall](#)에서 응용 프로그램을 평가할 때 [Identity Protection](#) 기능을 사용하도록 허용하려면 이 옵션을 선택합니다. [Identity Protection](#)은 응용 프로그램이 의심스러운 동작을 나타내는 지, 아니면 신뢰할 수 있으며 온라인에서 커뮤니케이션하도록 허용할 수 있는 응용 프로그램인지 여부를 알려 줄 수 있습니다.

게임 모드 설정

정보 메시지는 어느 정도 방해가 될 수 있으므로 **게임 모드 설정** 섹션에서 해당되는 항목을 선택하여 전체 화면 응용 프로그램이 컴퓨터에서 실행되고 있을 때 [Firewall](#) 정보 메시지가 표시되도록 할지 여부를 결정할 수 있습니다. 이 설정은 **게임**과 **PPT 프레젠테이션** 등 전체 화면으로 실행되는 모든 응용 프로그램에 적용됩니다.

게임을 실행할 때 Firewall 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.

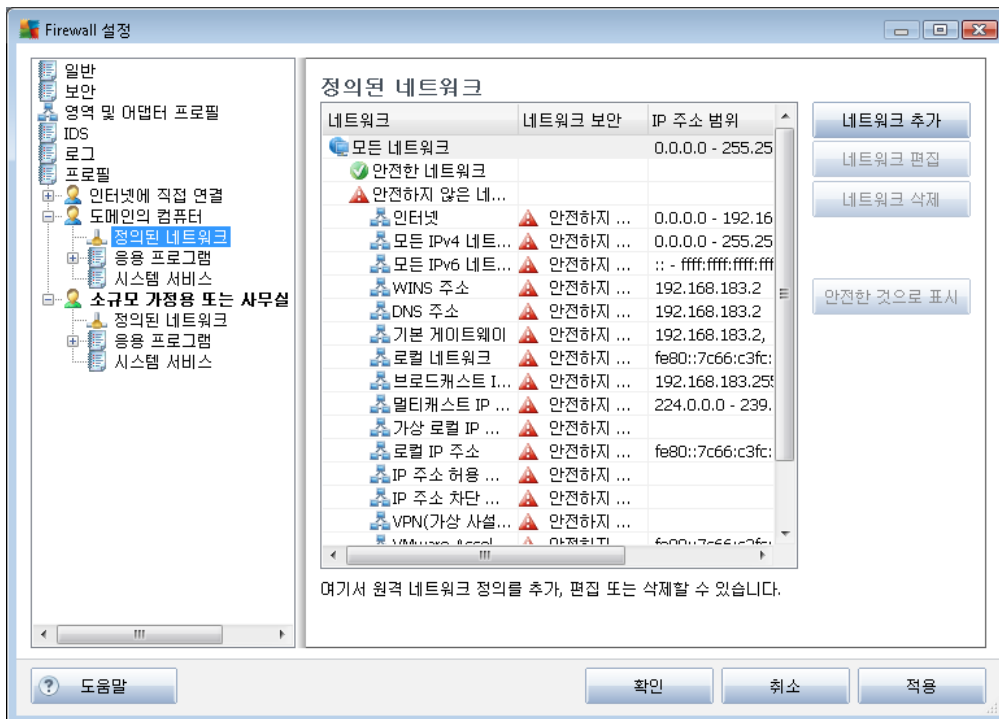
게임 모드가 설정되어 있는 경우 예약된 모든 작업(스캔, 업데이트)은 응용 프로그램이 닫힐 때까지 연기됩니다.

IDS(침입 검색 시스템) 설정

IDS 사용 확인란을 선택하여 컴퓨터의 특정 포트에서 발생하는 의심스러운 커뮤니케이션 시도를 식별하여 차단하도록 설계된 특수한 동작 분석 기능(이러한 기능 설정에 대한 자세한 내용은 이 설명서의 [IDS](#) 장 참조)를 활성화합니다.

10.6.2. 정의된 네트워크

정의된 네트워크 대화 상자에는 사용자 컴퓨터가 연결된 모든 네트워크 목록이 제공됩니다.

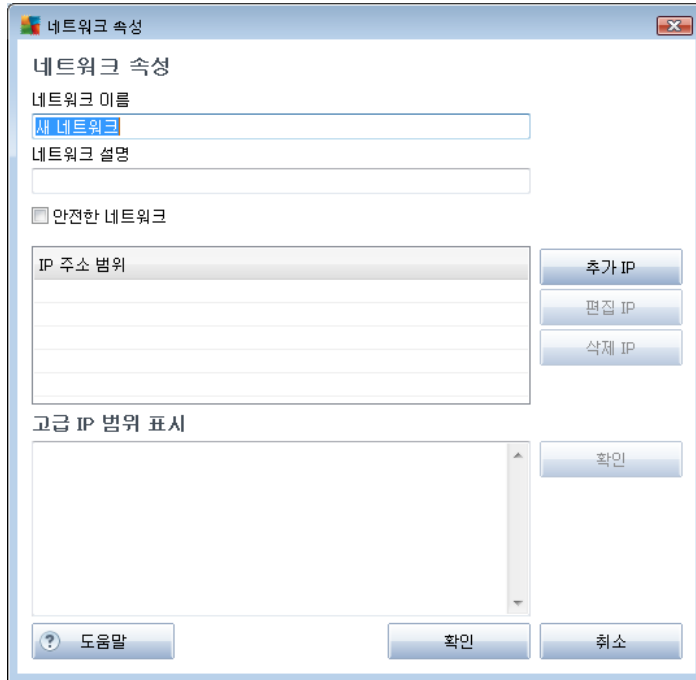


이 목록은 검색된 모든 네트워크에 대해 다음 정보를 제공합니다.

- **네트워크** - 해당 컴퓨터가 연결된 모든 네트워크의 이름 목록을 제공합니다.
- **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 네트워크가 자동으로 검색되며 IP 주소 범위 형태로 지정됩니다.

제어 단추

- **네트워크 추가** - 새로 정의된 네트워크의 매개 변수를 편집할 수 있는 **네트워크 속성** 대화 상자 창을 엽니다.

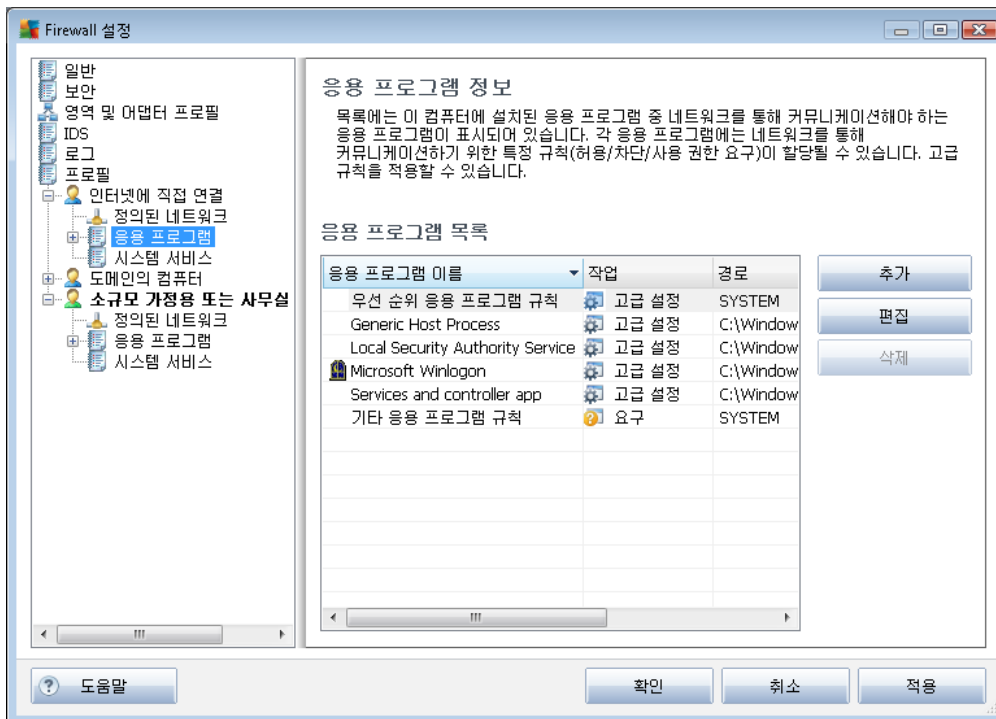


이 대화 상자에서 **네트워크 이름**을 지정하고 **네트워크 설명**을 제공할 수 있으며 네트워크를 안전한 것으로 지정할 수도 있습니다. **IP 추가** 단추(또는 **IP 편집/IP 삭제**)를 통해 독립 실행형 대화 상자에서 새 네트워크를 수동으로 정의하거나 이 대화 상자에서 IP 범위나 마스크를 제공하여 해당 네트워크를 지정할 수 있습니다. 새로 생성된 네트워크의 일부로 다수의 네트워크를 정의해야 하는 경우 **고급 IP 범위 표시** 옵션을 사용할 수 있습니다. 각 텍스트 필드에 모든 네트워크 목록을 입력하고(**모든 표준 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.
- **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.

10.6.3. 응용 프로그램

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



응용 프로그램 목록에 있는 응용 프로그램은 사용자 컴퓨터(및 할당된 각 작업)에서 검색된 응용 프로그램입니다. 다음 작업 유형을 사용할 수 있습니다.

-  - 모든 네트워크에 대한 커뮤니케이션 허용
-  - 안전한 것으로 정의된 네트워크만 커뮤니케이션 허용
-  - 커뮤니케이션 차단
-  - 요구 대화 상자 표시(응용 프로그램이 네트워크를 통해 커뮤니케이션을 시도할 때 사용자가 커뮤니케이션을 허용할지 아니면 차단할지를 결정할 수 있습니다)
-  - 고급 설정이 정의됨

이미 설치된 응용 프로그램만 검색할 수 있으므로 새 응용 프로그램을 나중에 설치한 경우 이에 대한 Firewall 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 대답을 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 **추**



가를 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.

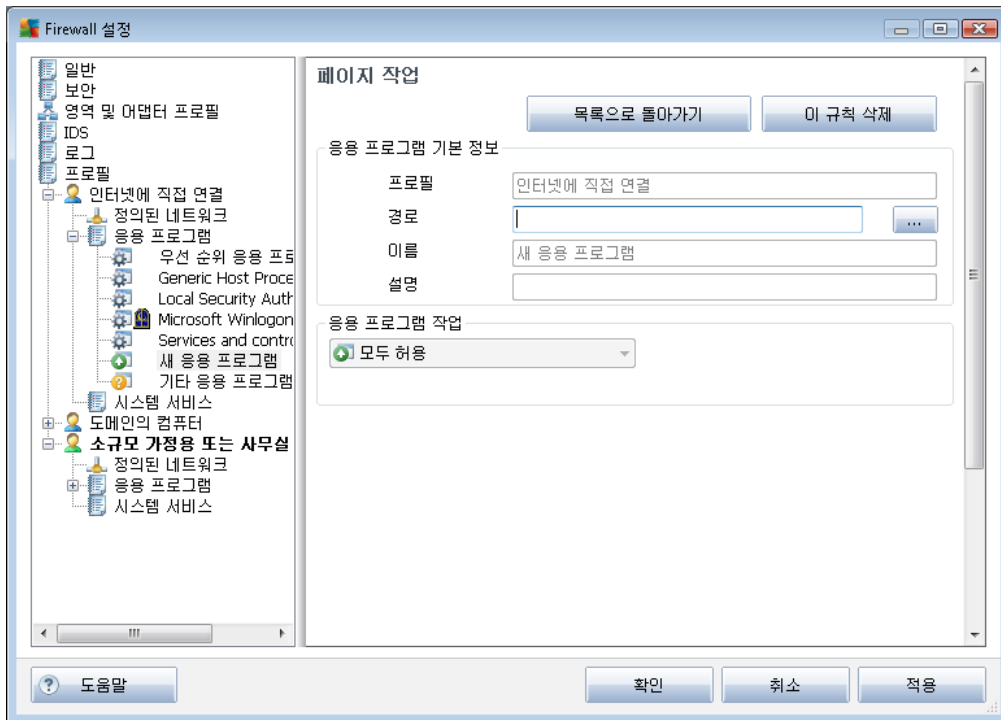
이러한 항목은 일반 응용 프로그램과는 다른 설정 옵션을 가지며 숙련된 사용자만 사용할 수 있습니다. 설정을 수정하지 않는 것을 적극 권장합니다.

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.

페이지 작업 대화 상자에서 각 응용 프로그램의 설정을 상세하게 정의할 수 있습니다.



제어 단추

대화 상자 상단에는 다음 두 개의 제어 단추가 있습니다.

- **목록으로 돌아가기** - 정의된 모든 응용 프로그램 규칙에 대한 개요를 표시하려면 이 단추를 누릅니다.
- **이 규칙 삭제** - 현재 표시된 응용 프로그램 규칙을 지우려면 이 단추를 누릅니다. **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 대한 전체 경로를 입력합니다. 또는 "..." 단추를 누른 다음 트리 구조에서 편리하게 응용 프로그램을 찾을 수도 있습니다.

응용 프로그램 작업

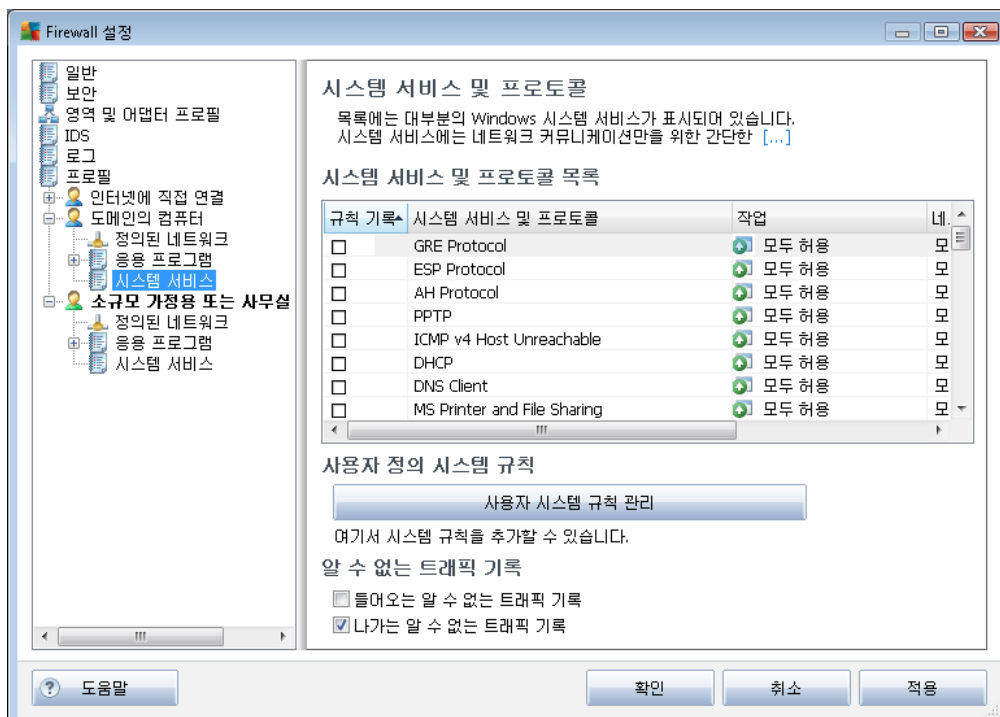
드롭다운 메뉴에서 응용 프로그램의 **Firewall** 규칙(즉, 응용 프로그램이 네트워크를 통해 커뮤니케이션할 때 **Firewall**에서 수행할 동작)을 선택할 수 있습니다.

- **모두 허용** - 응용 프로그램이 정의된 모든 네트워크 및 어댑터를 통해 제한 없이 커뮤니케이션하도록 허용합니다.
- **안전한 경우에만 허용** - 응용 프로그램이 안전(신뢰)하다고 정의된 네트워크를 통해서만 커뮤니케이션하도록 허용합니다.
- **차단** - 커뮤니케이션을 자동으로 차단하여 응용 프로그램이 네트워크에 연결되지 못하도록 합니다.
- **요구** - 해당 순간에 커뮤니케이션 시도를 허용할지 아니면 차단할지 결정할 수 있는 대화 상자를 표시합니다.
- **고급 설정 - 응용 프로그램 세부 규칙** 섹션의 대화 상자 아래쪽에 광범위한 세부 설정 옵션을 표시합니다. 세부 정보는 목록 순서대로 적용되므로 목록에서 규칙을 위로 이동 또는 아래로 이동하여 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.

10.6.4. 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.



시스템 서비스 및 프로토콜 목록

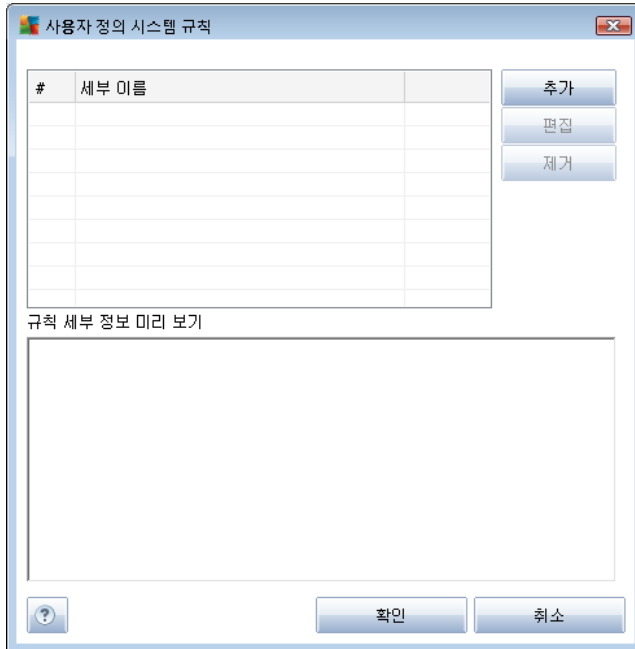
차트에는 다음과 같은 열이 있습니다.

- **로그 규칙 작업** - 이 상자를 사용하면 규칙이 적용될 때마다 [로그](#)에 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.

목록의 항목에 대한 설정(할당된 작업 포함)을 편집하려면 항목을 마우스 오른쪽 단추로 클릭하고 **편집**을 선택합니다. **하지만 시스템 규칙 편집은 고급 사용자만 수행해야 하며, 되도록 시스템 규칙을 편집하지 않는 것이 좋습니다.**

사용자 정의 시스템 규칙

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 Firewall 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.

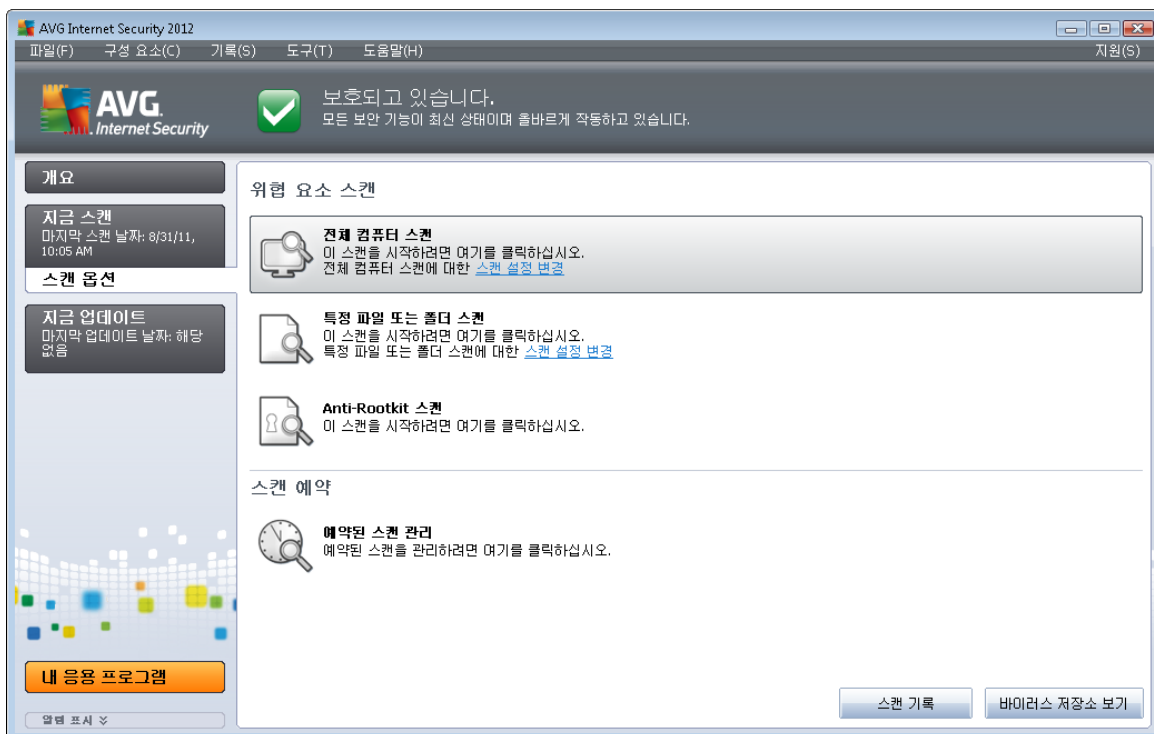
알 수 없는 트래픽 기록

- **들어오는 알 수 없는 트래픽 기록**(기본적으로 해제되어 있음) - 외부에서 컴퓨터에 연결하려는 알 수 없는 시도가 있을 때마다 [로그](#)에 기록하려면 이 상자를 선택합니다.
- **나가는 알 수 없는 트래픽 기록**(기본적으로 설정되어 있음) - 컴퓨터에서 외부 위치에 연결하려는 알 수 없는 시도가 있을 때마다 [로그](#)에 기록하려면 이 상자를 선택합니다.

11. AVG 스캔

기본적으로 **AVG Internet Security 2012**에서는 스캔을 실행하지 않습니다. 스캔을 처음 수행한 후에는 항상 보호 기능을 실행하여 악의적인 코드가 컴퓨터에 침입할 수 없도록 확실하게 차단하는 **AVG Internet Security 2012**의 상주 구성 요소에 의해 완벽하게 보호되기 때문입니다. 물론 정기적으로 스캔을 실행하도록 [스캔을 예약](#)하거나 필요한 경우 원하는 시간에 스캔을 직접 실행할 수도 있습니다.

11.1. 스캔 인터페이스



AVG 스캔 인터페이스는 [스캔 옵션 빠른 링크](#)를 통해 액세스할 수 있습니다. 이 링크를 클릭하여 **위협 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.
 - o [전체 컴퓨터 스캔](#)
 - o [특정 파일 또는 폴더 스캔](#)
 - o [Anti-Rootkit 스캔](#)
- [스캔 일정](#) 섹션 - 필요한 경우 새 테스트를 정의하고 새 일정을 만들 수 있습니다.

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.

11.2. 미리 정의된 스캔

AVG Internet Security 2012의 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.

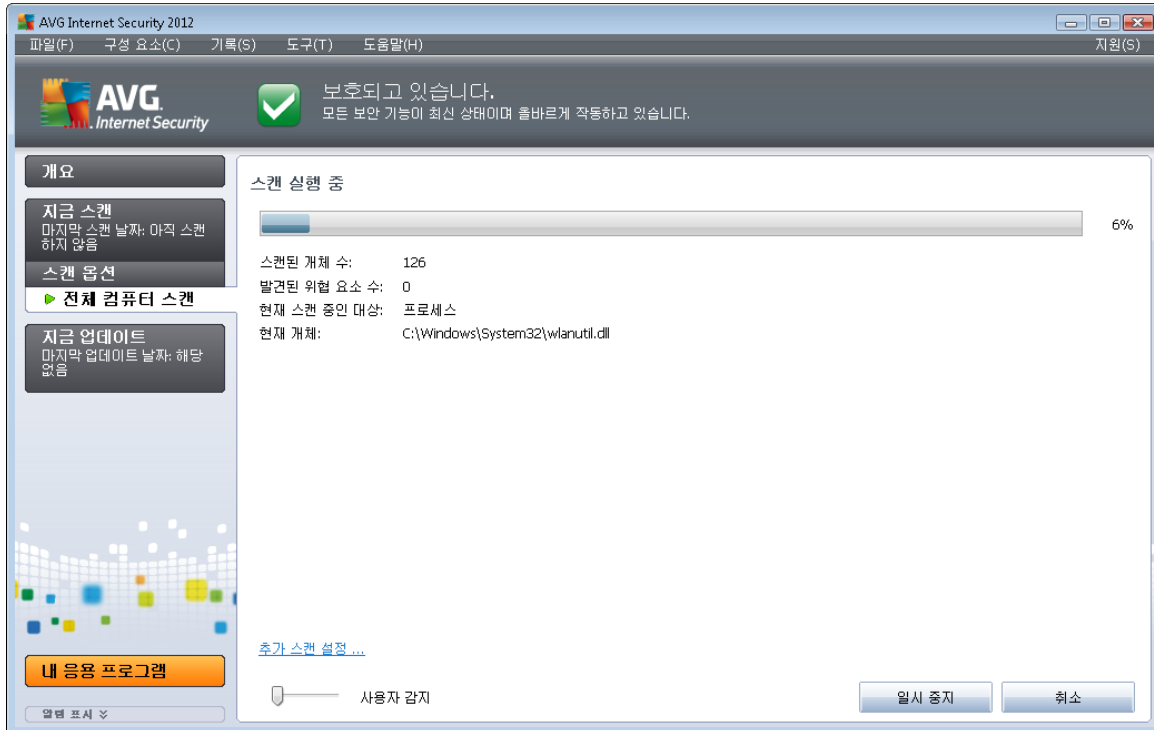
AVG Internet Security 2012에서는 소프트웨어 공급업체에서 미리 정의한 다음 스캔 유형이 제공됩니다.

11.2.1. 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..

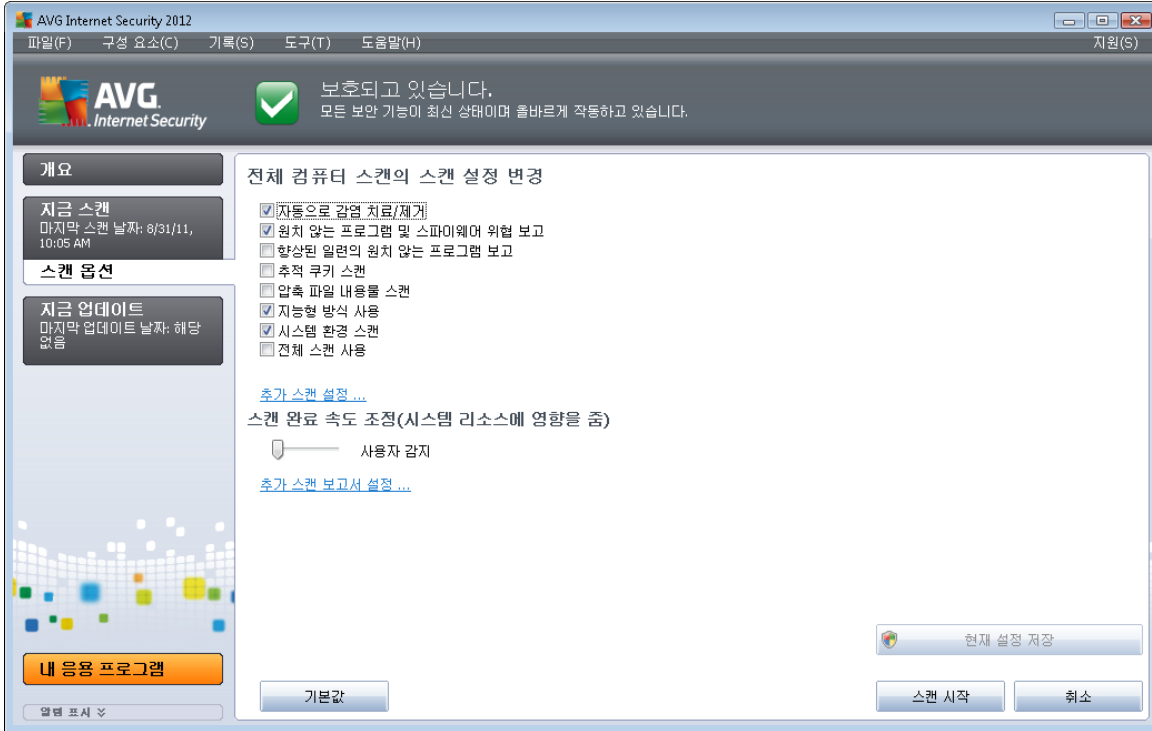
스캔 시작

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.



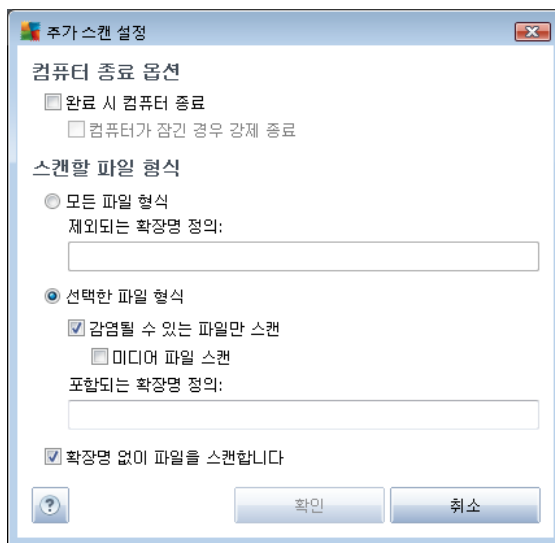
스캔 구성 편집

미리 정의된 **전체 컴퓨터 스캔**의 기본 설정을 편집하는 옵션이 있습니다. **스캔 설정 변경** 링크를 눌러 **전체 컴퓨터 스캔의 스캔 설정 변경** 대화 상자([전체 컴퓨터 스캔의 스캔 설정 변경 링크](#)를 통해 [스캔 인터페이스](#)에서 액세스할 수 있음)로 이동합니다. **기본 설정을 반드시 변경해야 하는 경우가 아니라면 해당 설정을 그대로 유지하는 것이 좋습니다.**



에서 ZIP, RAR 등의 압축 파일에 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.

- o **지능형 방식 사용**(기본적으로 설정됨) - 지능형 분석(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- o **시스템 환경 스캔**(기본적으로 설정됨) - 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- o **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- **추가 스캔 설정** - 이 링크는 다음 매개 변수를 지정할 수 있는 새 **추가 스캔 설정** 대화 상자를 엽니다.



- o **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.

- o **스캔할 파일 형식** - 스캔할 항목을 더 자세히 정의할 수 있습니다.

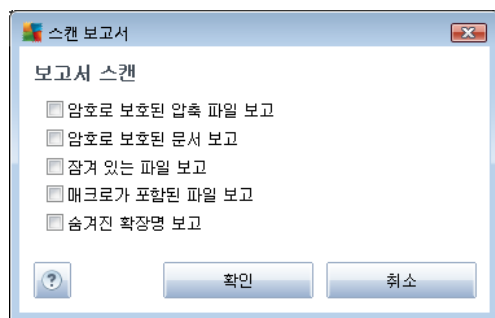
➤ **모든 파일 형식**은 스캔하지 않아야 할 파일의 확장명을 심표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.

➤ **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 지정

할 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 그대로 유지하는 것이 좋습니다. 확장명이 없는 파일은 다소 의심스럽기 때문에 항상 스캔해야 합니다.

- **스캔 완료 속도 조정** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 **사용자 감지** 수준으로 설정되어 있습니다. 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 실행합니다(예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우).
- **추가 스캔 보고서 설정** - 이 링크를 클릭하면 보고할 검색 결과 유형을 선택할 수 있는 새로운 **보고서 스캔** 대화 상자가 열립니다.



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.

11.2.2. 특정 파일 또는 폴더 스캔

특정 파일 또는 폴더 스캔 - 사용자가 스캔하려고 선택한 컴퓨터 영역(선택한 폴더, 하드 디스크, 플로피 디스크, CD 등)만 스캔합니다. 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

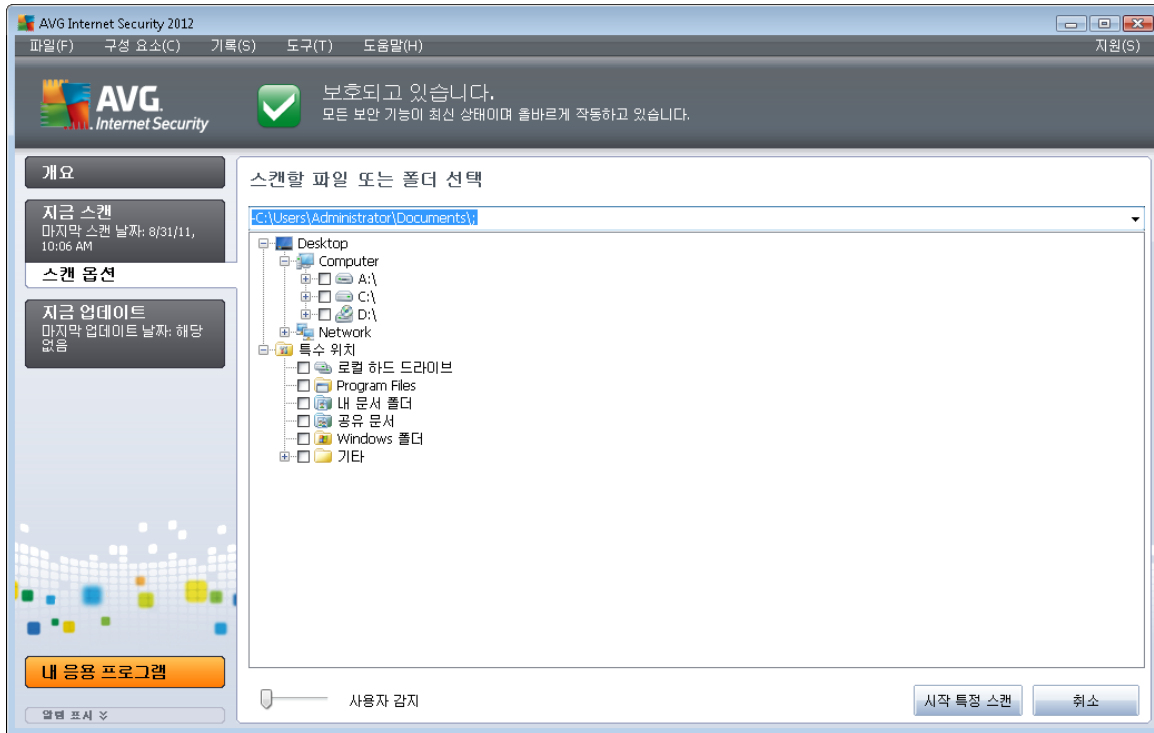
특정 파일 또는 폴더 스캔은 스캔 아이콘을 클릭하여 [스캔 인터페이스](#)에서 직접 시작할 수 있습니다. **스캔할 파일 또는 폴더 선택**이라는 새 대화 상자가 열립니다. 컴퓨터의 트리 구조에서 스캔하려는 폴더를 선택합니다. 선택한 각 폴더의 경로는 자동으로 생성되어 이 대화 상자 위쪽에 있는 텍스트 상자에 나타납니다.

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



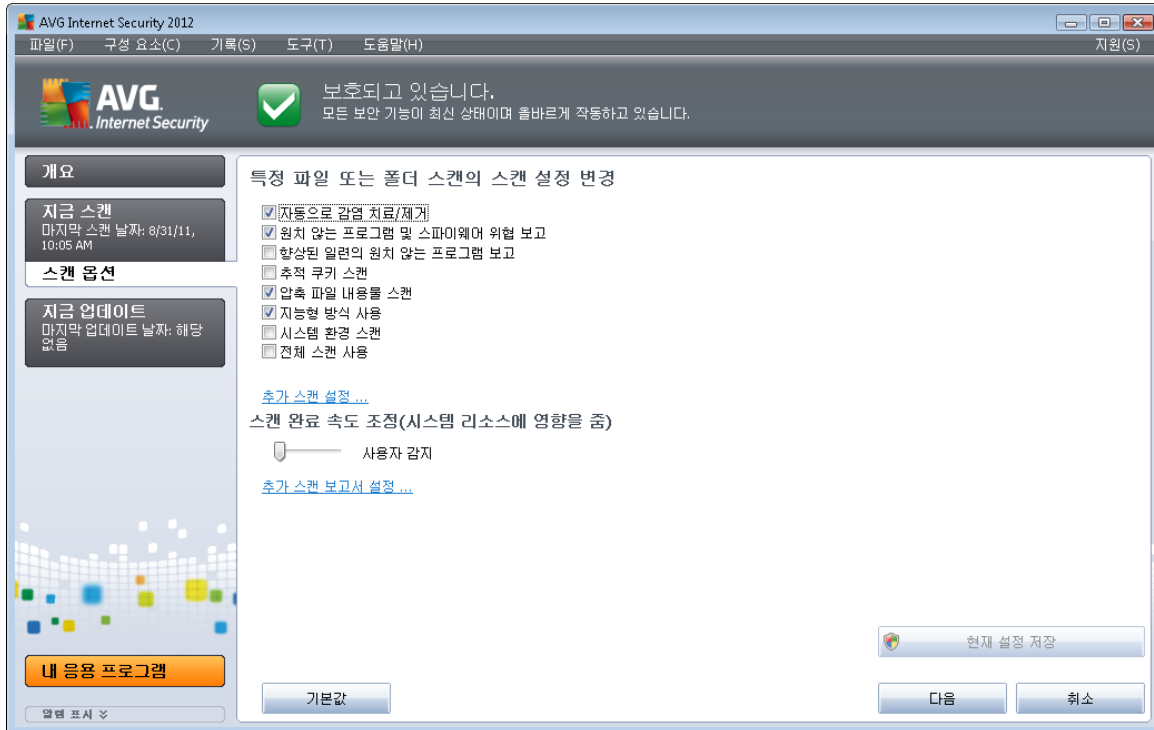
면 "!" 매개 변수를 사용합니다.

마지막으로, 스캔을 시작하려면 **스캔 시작** 단추를 누릅니다. 스캔 프로세스 자체는 기본적으로 전체 컴퓨터 스캔과 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.**

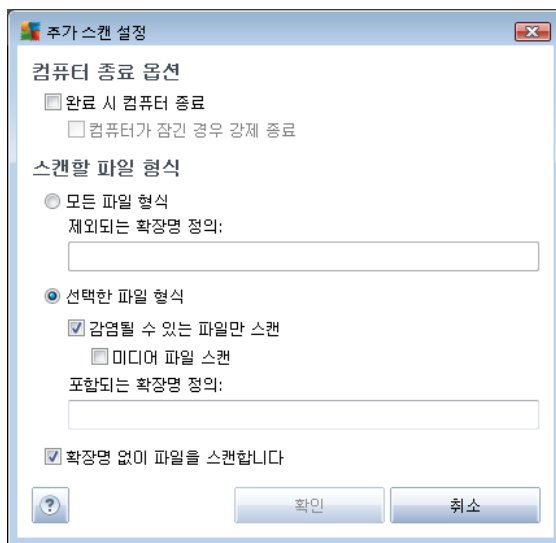


- **스캔 매개 변수** - 스캔 매개 변수 목록에서 필요한 특정 매개 변수를 설정/해제할 수 있습니다.

- **자동으로 감염 치료/제거**(기본적으로 설정됨) - 스캔하는 동안 바이러스가 식별되는 경우 치료가 가능하면 자동으로 치료됩니다. 감염된 파일을 자동으로 치료할 수 없으면 감염된 개체가 [바이러스 저장소](#)로 이동됩니다.
- **원치 않는 프로그램 및 스파이웨어 위협 보고**(기본적으로 설정됨) - [Anti-Spyware](#) 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 일반적으로 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**(기본적으로 해제되어 있음) - 스파이웨어의 확장 패키지를 검색하려면 선택합니다. 스파이웨어 프로그램은 제조업체에서 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 해제되어 있음) - [Anti-Spyware](#) 구성 요소의 이 매개 변수는 쿠키가 검색되도록 정의합니다. [HTTP 쿠키는 사이트 기본 설정이나 온라인 쇼핑 카트의 내용물과 같이 사용자와 관련된 특정 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.](#)
- **압축 파일 내용물 스캔**(기본적으로 설정됨) - 이 매개 변수는 스캔에서 ZIP,

RAR 등의 압축 파일에 저장된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.

- o **지능형 방식 사용**(기본적으로 해제되어 있음) - 지능형 분석(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- o **시스템 환경 스캔**(기본적으로 해제되어 있음) - 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- o **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- **추가 스캔 설정** - 이 링크는 다음 매개 변수를 지정할 수 있는 새 **추가 스캔 설정** 대화 상자를 엽니다.



- o **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.

- o **스캔할 파일 형식** - 스캔할 항목을 더 자세히 정의할 수 있습니다.

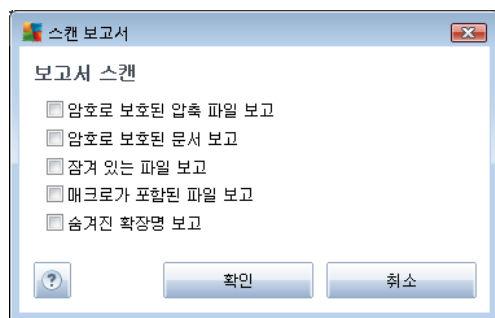
➤ **모든 파일 형식**은 스캔하지 않아야 할 파일의 확장명을 심표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.

➤ **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 지정

할 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 그대로 유지하는 것이 좋습니다. 확장명이 없는 파일은 다소 의심스럽기 때문에 항상 스캔해야 합니다.

- **스캔 프로세스 우선 순위** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 **사용자 감지** 수준으로 설정되어 있습니다. 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 실행합니다(**예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우**).
- **추가 스캔 보고서 설정** - 이 링크를 클릭하면 보고할 검색 결과 유형을 선택할 수 있는 새로운 **보고서 스캔** 대화 상자가 열립니다.



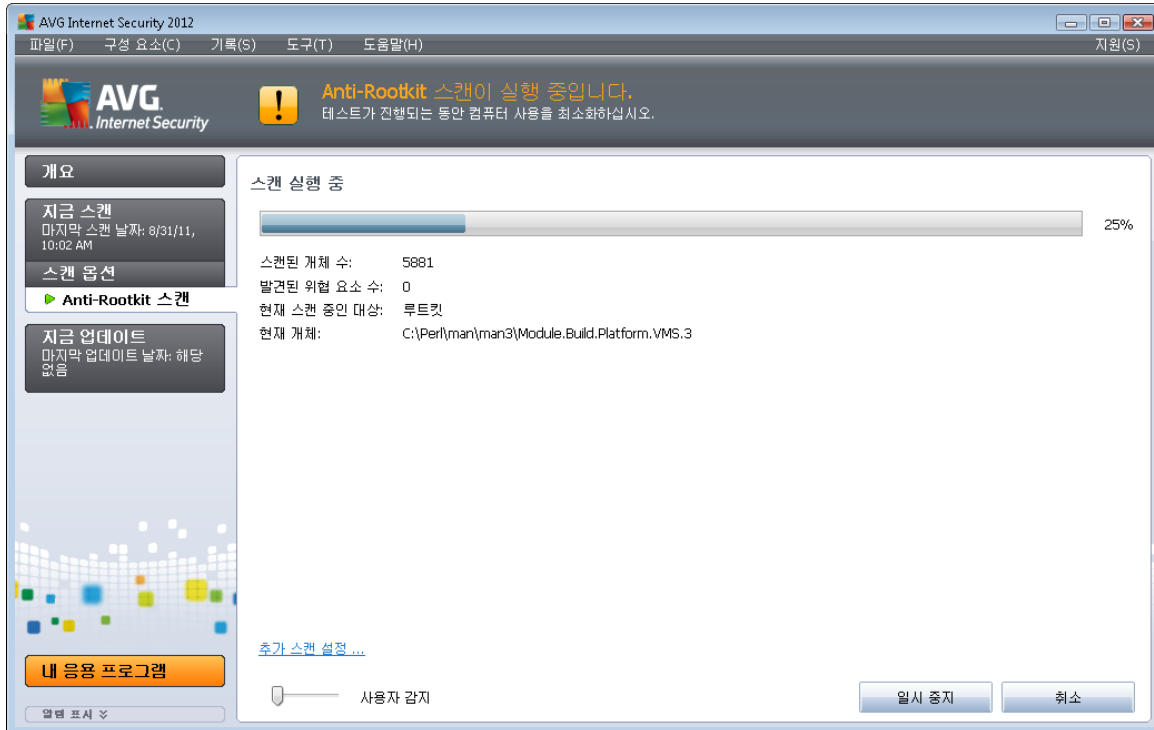
경고: 이 스캔 설정은 [AVG 스캔/스캔 일정/스캔 방법](#) 장에 설명된, 새로 정의한 스캔의 매개 변수와 같습니다. **특정 파일 또는 폴더 스캔**의 기본 구성을 변경하기로 한 경우 새 설정을 기본 구성으로 저장하여 이후에 특정 파일 또는 폴더를 스캔하는 데 사용할 수 있습니다. 또한 이 구성을 새로 예약된 모든 스캔의 템플릿으로 사용할 수도 있습니다. **모든 사용자 지정 스캔은 특정 파일 또는 폴더 스캔의 현재 구성을 기준으로 실행됩니다.**

11.2.3. 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

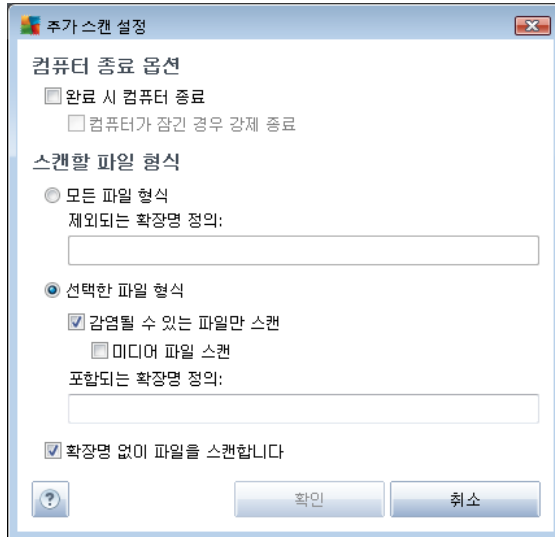
Anti-Rootkit 스캔은 스캔 아이콘을 클릭하여 [스캔 인터페이스](#)에서 직접 시작할 수 있습니다. 이 유형의 스캔에 대해 더 이상 특정 설정을 구성할 필요가 없으면 **스캔 실행 중** 대화 상자(**스크린샷 참조**)에서 즉시 스캔이 시작됩니다. 필요한 경우 스캔을 일시적으로 중단(**일시 중지**)하거나 취소(**중지**)할 수 있습니다.



스캔 구성 편집

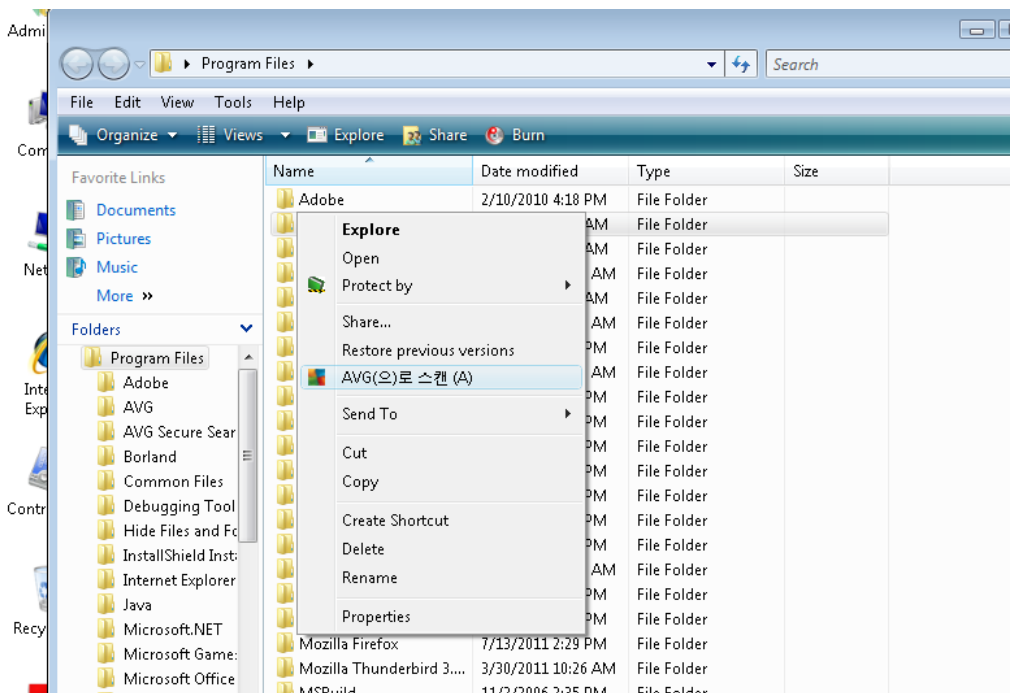
Anti-Rootkit 스캔은 기본적으로 항상 시작되도록 설정되어 있으며 [AVG 고급 설정 / Anti-Rootkit](#) 대화 상자에서만 스캔 매개 변수를 편집할 수 있습니다. 스캔 인터페이스에서는 다음 구성이 제공됩니다. 단, 스캔을 실행하는 동안에만 이러한 구성을 사용할 수 있습니다.

- **자동 스캔** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 **사용자 감지** 수준으로 설정되어 있습니다. 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 실행합니다 (**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**).



11.3. Windows 탐색기에서 스캔

전체 컴퓨터 또는 선택한 영역에 대해 미리 정의된 스캔을 시작하는 옵션 외에도 **AVG Internet Security 2012** 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.



- **AVG 로 스캔** 옵션을 선택하여 파일이 다음으로 스캔되도록 합니다. **AVG Internet Security 2012**

11.4. 명령줄 스캔

AVG Internet Security 2012에는 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 /?**)를 사용하여 각각의 명령을 입력합니다. 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 명령줄 스캔을 시작할 수도 있습니다. 스캔 자체가 명령줄에서 시작되며 **명령줄 작성기** 대화 상자를 통해서만 사용이 간편한 그래픽 인터페이스에서 대부분의 스캔 매개 변수를 지정할 수 있습니다.

이 대화 상자는 Windows 안전 모드에서만 액세스할 수 있으므로 이 대화 상자에 대한 자



세한 설명은 대화 상자에서 직접 열 수 있는 도움말 파일을 참조하십시오.

11.4.1. 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 /파일 이름/
- **/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 /파일 이름/에 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



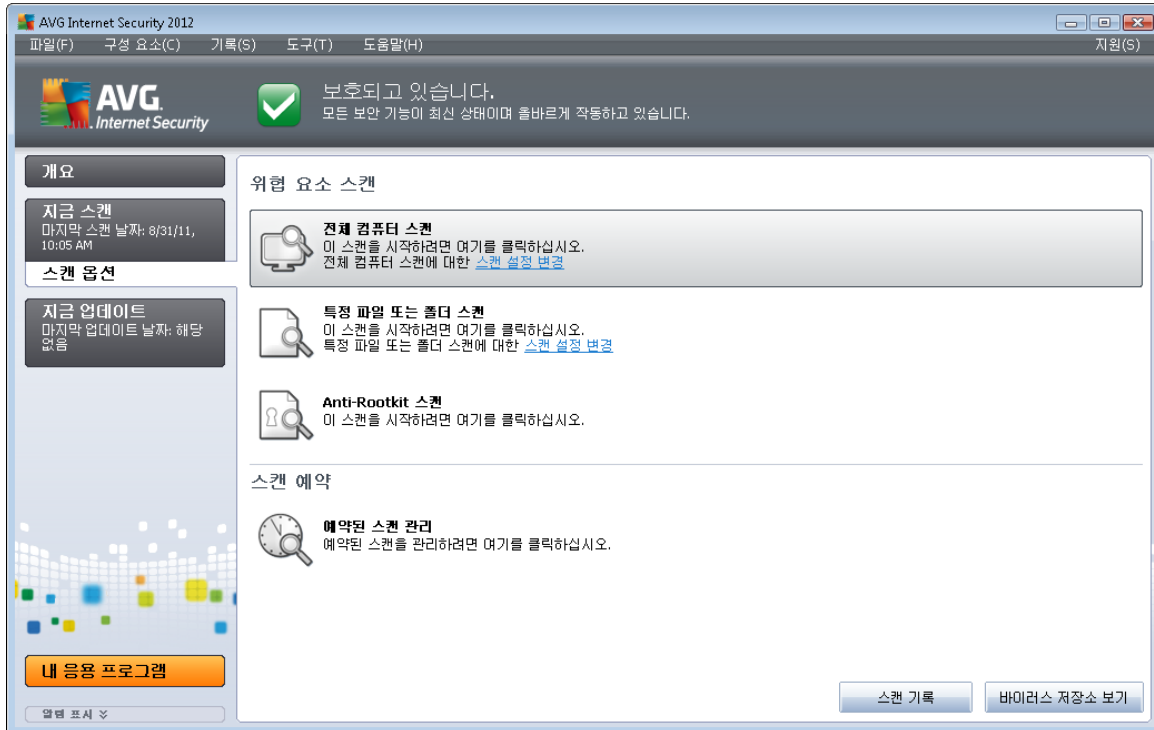
- **/COO** 쿠키 스캔
- **/?** 이 항목에 대한 도움말 표시
- **/HELP** 이 항목에 대한 도움말 표시
- **/PRIORITY** 스캔 우선 순위를 /낮음, 자동, 높음/으로 설정([고급 설정/스캔 참조](#))
- **/SHUTDOWN** 스캔 완료 시 컴퓨터 종료
- **/FORCESHUTDOWN** 스캔 완료 후 컴퓨터 자동 종료
- **/ADS** 대체 데이터 스트림 스캔(*NTFS 전용*)
- **/ARCBOMBSW** 재압축된 파일 보고

11.5. 스캔 일정

AVG Internet Security 2012 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.

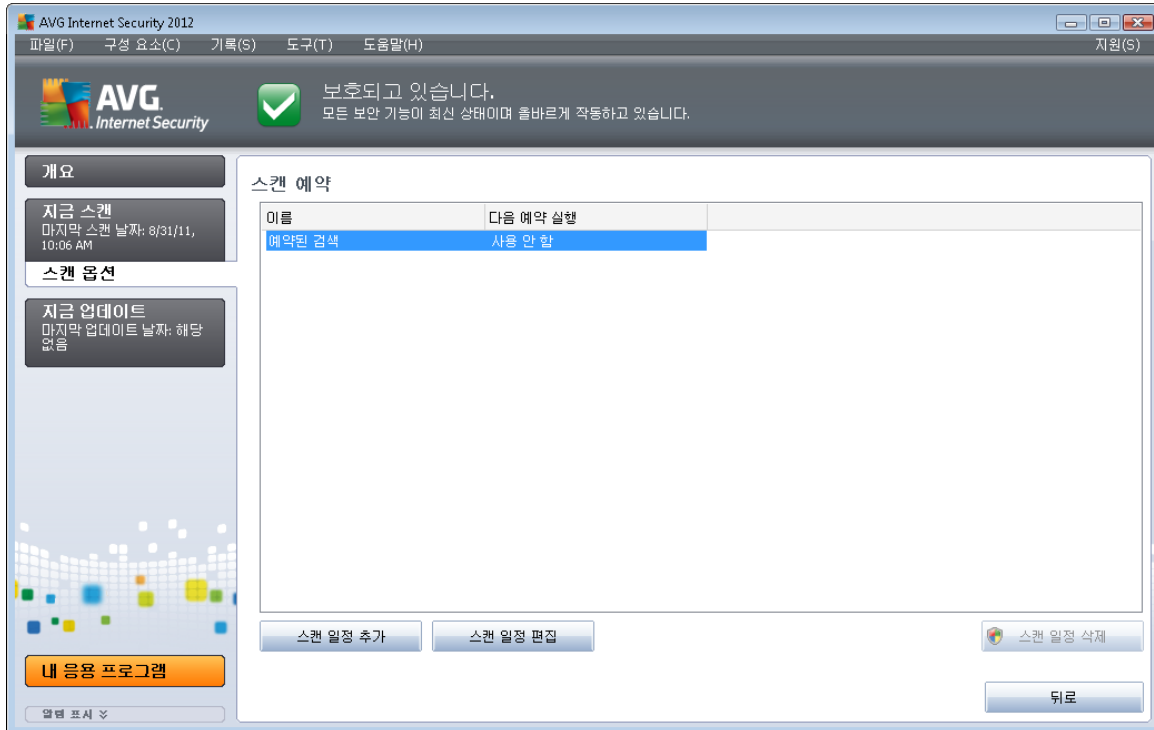
최소한 매주 한 번은 [전체 컴퓨터 스캔](#)을 실행해야 합니다. 하지만 가능하다면 스캔 일정 기본 구성의 설정에 따라 매일 전체 컴퓨터의 스캔을 시작하십시오. 컴퓨터가 "항상 켜져 있는 경우"에는 업무 시간이 아닌 시간에 스캔이 발생하도록 예약할 수 있습니다. 컴퓨터를 가끔씩 끄는 경우에는 [스캔 작업 기회를 놓쳤을 때 컴퓨터 시작 시](#) 스캔이 발생하도록 예약하십시오.

새 스캔 일정을 만들려면 [AVG 스캔 인터페이스](#)에서 하단에 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.

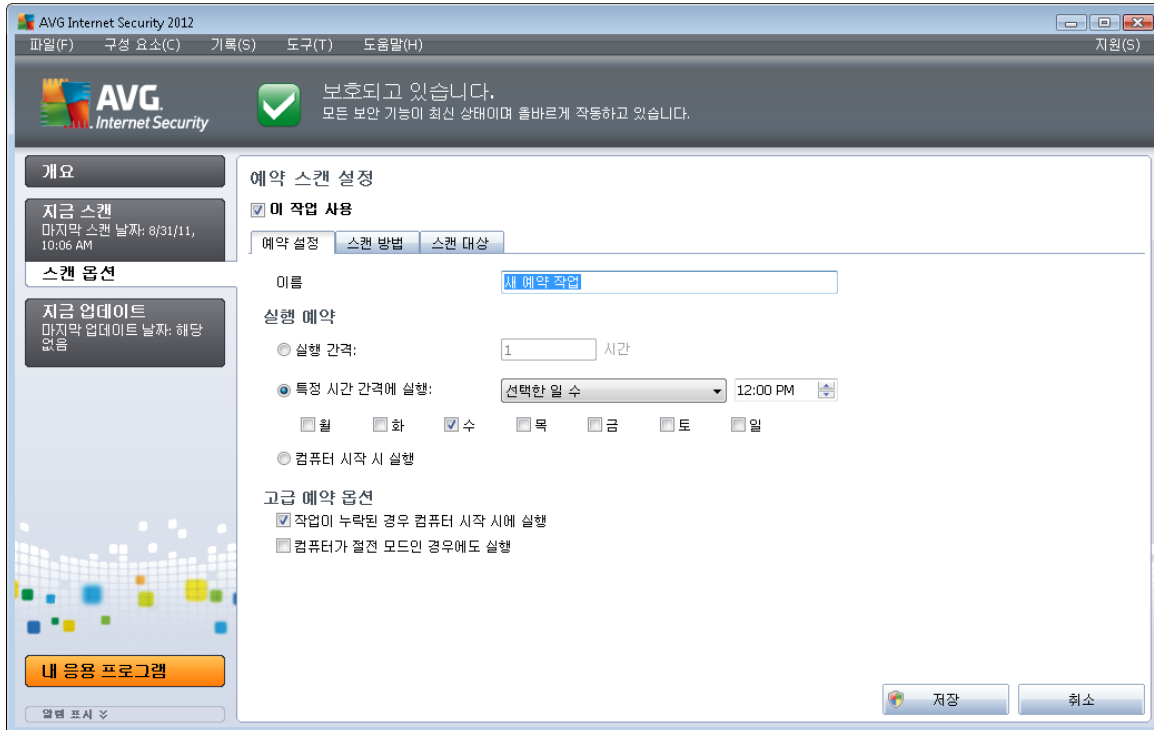


다음 제어 단추를 사용하여 스캔을 편집/추가할 수 있습니다.

- **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.](#)

11.5.1. 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 스캔의 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** 탭에는 사용 가능한 제어 단추가 두 개 있으며, 이들 단추는 현재 사용하는 탭과 상관없이 다음과 같은 기능을 동일하게 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.

11.5.2. 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 설정됨): 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 설정됨): **Anti-Spyware** 엔진을 활성화하고 스파이웨어뿐 아니라 바이러스도 스캔하려는 경우 선택합니다. 스파이웨어는 의심되는 맬웨어 범주로, 일반적으로 보안 위험을 나타내지만

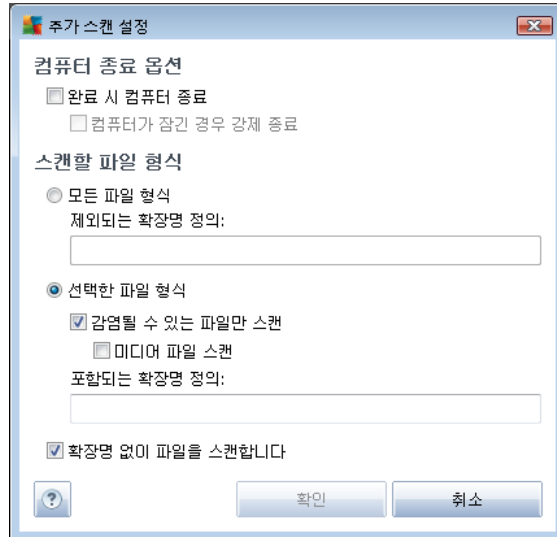


이들 프로그램의 일부는 의도적으로 설치될 수 있습니다. 이 기능은 컴퓨터 보안을 향상시키므로 계속 활성화하는 것이 좋습니다.

- **향상된 일련의 원치 않는 프로그램 보고**(기본적으로 해제되어 있음): 스파이웨어의 확장 패키지를 검색하려면 선택합니다. 스파이웨어 프로그램은 제조업체에서 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 해제되어 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 특정 정보를 인증, 추적 및 유지 관리하는 데 사용됩니다.
- **압축 파일 내용물 스캔**(기본적으로 해제되어 있음): 이 매개 변수는 스캔에서 ZIP, RAR 등의 압축 파일 형식으로 압축된 파일을 포함하여 모든 파일을 검사하도록 정의합니다.
- **지능형 방식 사용**(기본적으로 설정됨): 지능형 분석(가상 컴퓨터 환경에서 스캔된 개체의 동적 에뮬레이션 지침)은 스캔하는 중에 바이러스 검색에 사용되는 방법 중 하나입니다.
- **시스템 환경 스캔**(기본적으로 설정됨): 스캔 시 컴퓨터의 시스템 영역도 검사합니다.
- **전체 스캔 사용**(기본적으로 해제되어 있음) - 컴퓨터가 감염된 것으로 의심되는 경우와 같은 특정 상황에서 컴퓨터에서 감염 가능성이 거의 없는 영역까지 모두 스캔하는 전체 스캔 알고리즘을 활성화하려면 이 옵션을 선택할 수 있습니다. 이 방법은 시간이 많이 소요됩니다.
- **루트킷 스캔**(기본적으로 해제되어 있음): 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.



o **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.

o **스캔할 파일 형식** - 스캔할 항목을 더 자세히 정의할 수 있습니다.

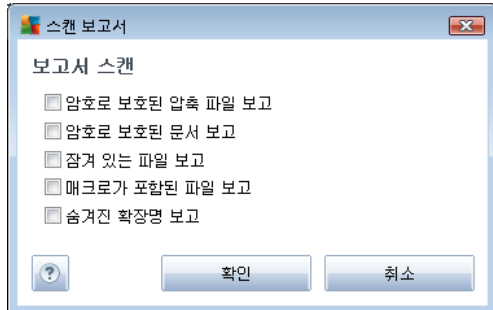
➤ **모든 파일 형식**은 스캔하지 않아야 할 파일의 확장명을 심표로 구분된 목록으로 제공하여 스캔에서 제외할 항목을 정의하는 기능이 있습니다.

➤ **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 그대로 유지하는 것이 좋습니다. 확장명이 없는 파일은 다소 의심스럽기 때문에 항상 스캔해야 합니다.

• **스캔 완료 속도 조정** - 슬라이더를 사용하여 스캔 프로세스 우선 순위를 변경할 수 있습니다. 기본적으로 이 옵션 값은 자동 리소스 사용량의 **사용자 감지** 수준으로 설정되어 있습니다. 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 실행합니다(예: 컴퓨터 일시적으로 무인 모드로 작동하는 경우).

• **추가 스캔 보고서 설정** - 이 링크를 클릭하면 보고할 검색 결과 유형을 선택할 수 있는 새로운 **스캔 보고서** 대화 상자가 열립니다.



제어 단추

예약 스캔 설정 대화 상자의 세 가지 탭인 [예약 설정](#), [스캔 방법](#) 및 [스캔 대상](#)에는 사용 가능한 제어 단추가 두 개 있으며, 이들 단추는 현재 사용 중인 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.

11.5.3. 스캔 대상





스캔 대상 탭에서 [전체 컴퓨터 스캔](#)을 예약할지 아니면 [특정 파일 또는 폴더 스캔](#)을 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.

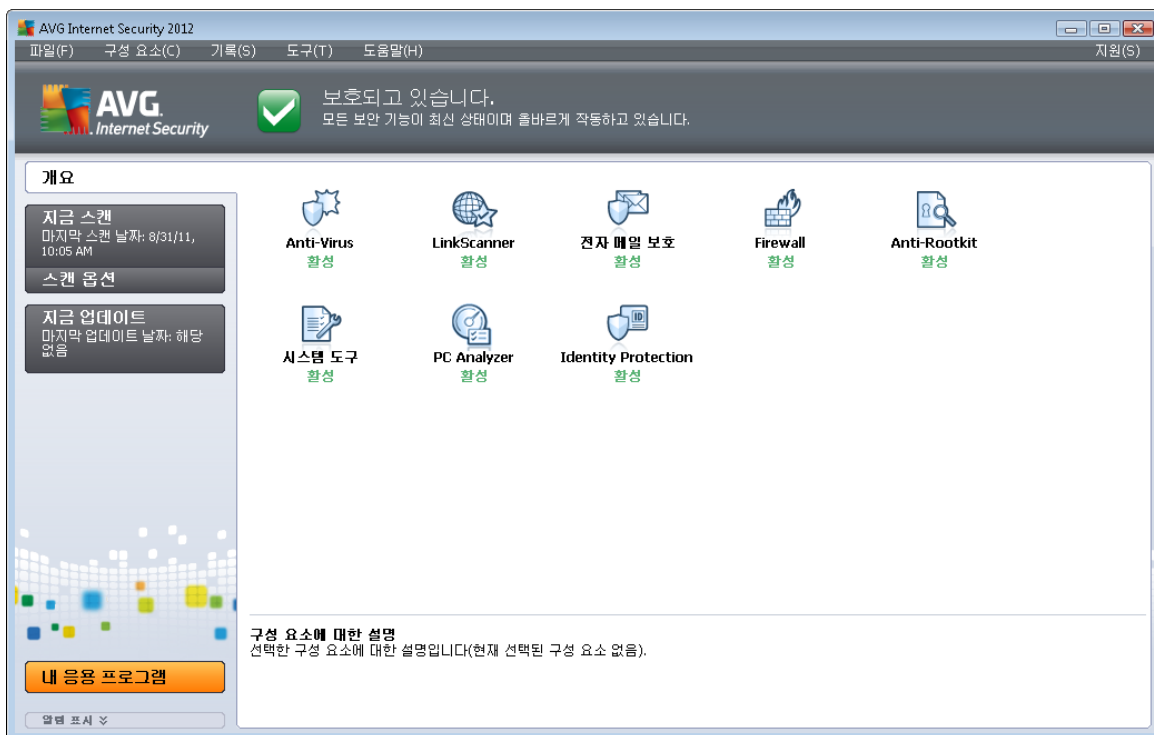
- **로컬 하드 드라이브** - 컴퓨터의 모든 하드 드라이브
- **프로그램 파일**
 - o C:\Program Files\
 - o 64비트 버전 C:\Program Files (x86)
- **내 문서 폴더**
 - o Win XP의 경우: C:\Documents and Settings\Default User\My Documents\
 - o Windows Vista/7의 경우: C:\Users\user\Documents\
- **공유 문서**
 - o Win XP의 경우: C:\Documents and Settings\All Users\Documents\
 - o Windows Vista/7의 경우: C:\Users\Public\Documents\
- **Windows 폴더** - C:\Windows\
- **기타**
 - o 시스템 드라이브 - 운영 체제가 설치된 하드 드라이브(일반적으로 C:)
 - o 시스템 폴더 - C:\Windows\System32\
 - o 임시 파일 폴더 - C:\Documents and Settings\User\Local\ (Windows XP) 또는 C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
 - o 임시 인터넷 파일 - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP) 또는 C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

제어 단추

예약 스캔 설정 대화 상자에 있는 [예약 설정](#), [스캔 방법](#) 및 스캔 대상의 세 가지 탭에는 사용 가능한 제어 단추가 두 개 있습니다.

- **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.

11.6. 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. 완전한 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 감염의 수
- **스파이웨어** - 검색/제거된 스파이웨어의 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.](#)

11.7. 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.

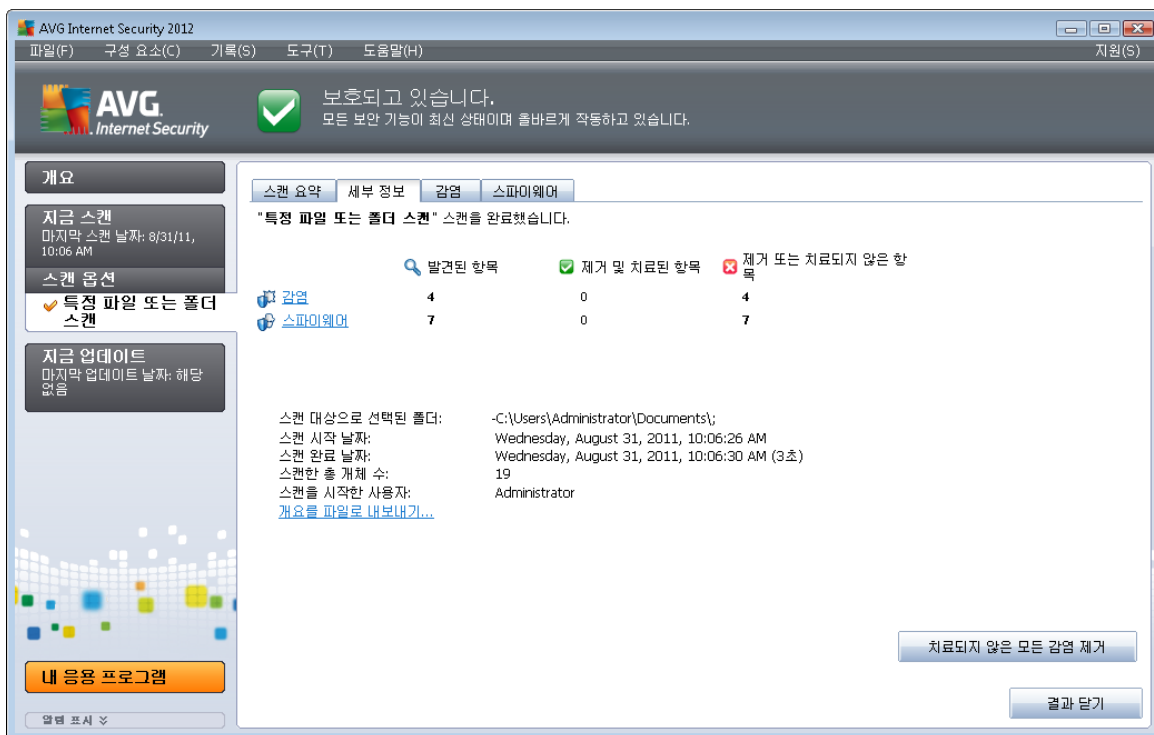
- [결과 개요](#) - 이 탭은 항상 표시되며 스캔 진행 상황을 안내하는 통계 데이터를 제



공합니다.

- [감염](#) - 이 탭은 스캔 중에 바이러스 감염이 발견된 경우에만 표시됩니다.
- [스파이웨어](#) - 이 탭은 스캔 중에 스파이웨어가 발견된 경우에만 표시됩니다.
- [경고](#) - 이 탭은 스캔 중에 쿠키가 검색되는 등의 경우에 표시됩니다.
- [루트킷](#) - 이 탭은 스캔 중에 루트킷이 발견된 경우에만 표시됩니다.
- [정보](#) - 이 탭은 일부 잠재적인 위험 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.

11.7.1. 결과 개요 탭



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

- 검색된 바이러스 감염/스파이웨어
- 제거된 바이러스 감염/스파이웨어
- 제거하거나 치료할 수 없는 바이러스 감염/스파이웨어의 수

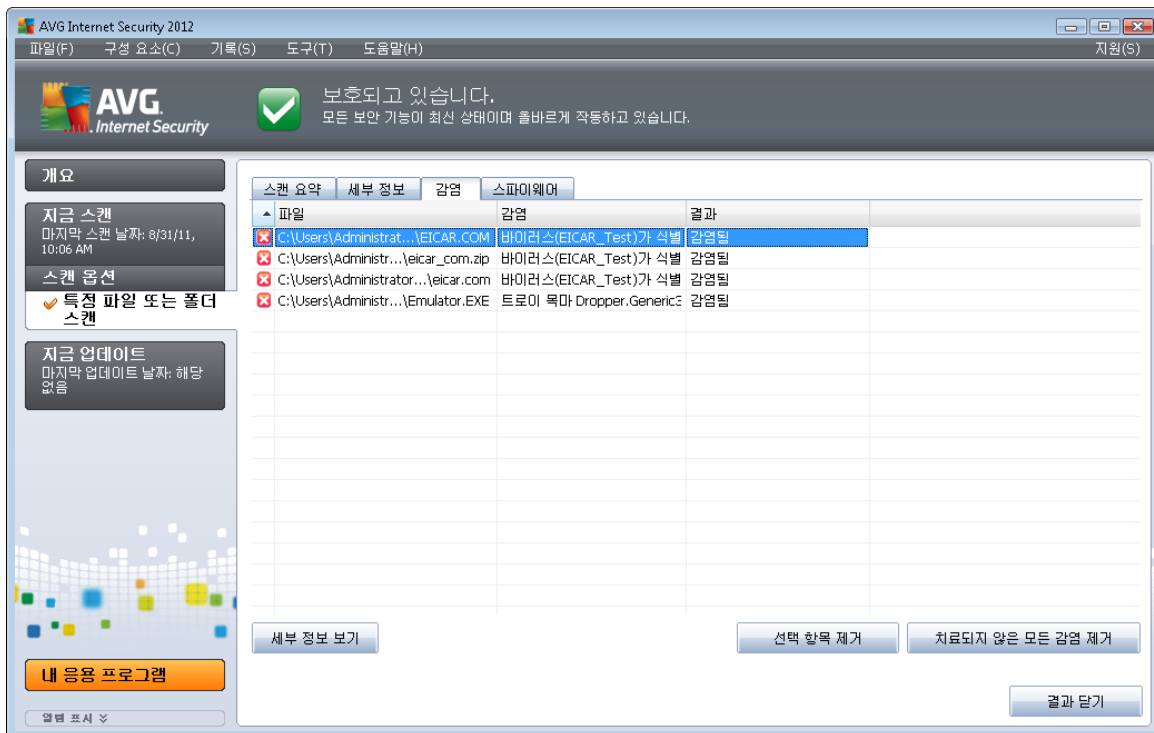
또한 스캔이 시작된 날짜 및 정확한 시간, 스캔된 개체의 총 개수, 스캔 기간 및 스캔 중에 발생한 오류 수에 대한 정보도 찾을 수 있습니다.



제어 단추

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

11.7.2. 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.

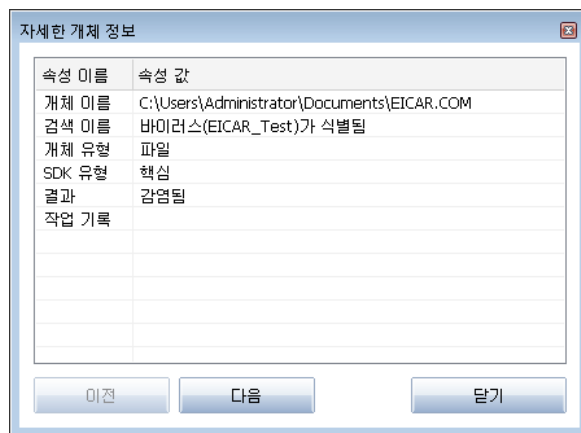
- **파일** - 감염된 개체의 원래 위치에 대한 전체 경로입니다.
- **감염** - 발견된 바이러스의 이름입니다. 특정 바이러스에 대한 자세한 내용은 [온라인 바이러스 백과사전](#)을 참조하십시오.
- **결과** - 스캔 중에 발견된 감염된 개체의 현재 상태를 다음과 같이 정의합니다.
 - **감염됨** - 감염된 개체가 발견되어 원래 위치에 남아 있습니다(예: 특정 스캔 설정에서 [자동 치료 옵션을 해제](#)한 경우).
 - **치료됨** - 감염된 개체가 자동으로 치료되어 원래 위치에 남아 있습니다.
 - **바이러스 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.

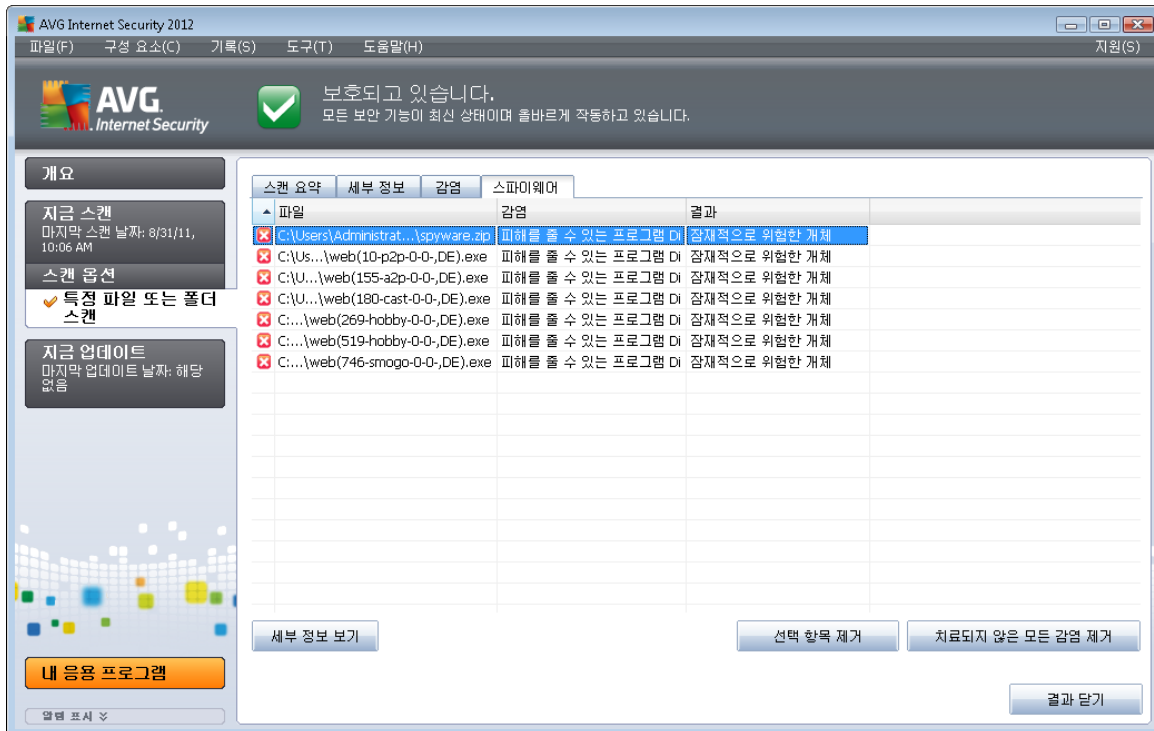
- **세부 정보 보기** - 이 단추를 클릭하면 **자세한 개체 정보**라는 이름의 새 대화 상자 창이 열립니다.



이 대화 상자에서 검색된 감염 개체에 대한 자세한 정보(예: 감염된 개체 이름과 위치, 개체 유형, SDK 유형, 검색 결과 및 검색된 개체와 관련된 작업 기록)를 확인할 수 있습니다. **이전/다음** 단추를 사용하여 특정 검색 결과에 대한 정보를 볼 수 있습니다. 이 대화 상자를 닫으려면 **닫기** 단추를 사용합니다.

- **선택 항목 제거** - 선택한 검색 결과를 [바이러스 저장소](#)로 이동하려면 이 단추를 사용합니다.
- **치료되지 않은 모든 감염 제거** - 이 단추를 사용하여 치료할 수 없거나 [바이러스 저장소](#)로 이동된 모든 검색 결과를 삭제합니다.
- **결과 닫기** - 자세한 정보 개요를 종료하고 [스캔 결과 개요](#) 대화 상자로 돌아갑니다.

11.7.3. 스파이웨어 탭



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

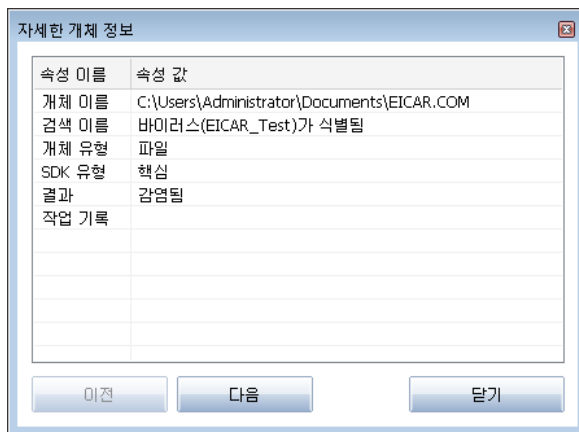
- **파일** - 감염된 개체의 원래 위치에 대한 전체 경로입니다.
- **감염** - 발견된 스파이웨어의 이름입니다. 특정 바이러스에 대한 자세한 내용은 온라인 [바이러스 백과 사전](#)을 참조하십시오.
- **결과** - 스캔 중에 발견된 개체의 현재 상태를 정의합니다.
 - **감염됨** - 감염된 개체가 발견되어 원래 위치에 남아 있습니다(예: 특정 스캔 설정에서 [자동 치료 옵션을 해제](#)한 경우).
 - **치료됨** - 감염된 개체가 자동으로 치료되어 원래 위치에 남아 있습니다.
 - **바이러스 저장소로 이동됨** - 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 상자에서 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 개체 정보**라는 이름의 새 대화 상자 창이 열립니다.



이 대화 상자에서 검색된 감염 개체에 대한 자세한 정보(예: 감염된 개체 이름과 위치, 개체 유형, SDK 유형, 검색 결과 및 검색된 개체와 관련된 작업 기록)를 확인할 수 있습니다. **이전/다음** 단추를 사용하여 특정 검색 결과에 대한 정보를 볼 수 있습니다. 이 대화 상자를 닫으려면 **닫기** 단추를 사용합니다.

- **선택 항목 제거** - 선택한 검색 결과를 [바이러스 저장소](#)로 이동하려면 이 단추를 사용합니다.
- **치료되지 않은 모든 감염 제거** - 이 단추를 사용하여 치료할 수 없거나 [바이러스 저장소](#)로 이동된 모든 검색 결과를 삭제합니다.
- **결과 닫기** - 자세한 정보 개요를 종료하고 [스캔 결과 개요](#) 대화 상자로 돌아갑니다.

11.7.4. 경고 탭

경고 탭에는 스캔 중에 발견된 "의심스러운" 개체(일반적으로 파일)에 대한 정보가 표시됩니다. Resident Shield에 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 위협 요소가 되지 않습니다. 일반적으로 이러한 파일에 대한 정보는 컴퓨터에서 애드웨어나 스파이웨어가 발견된 경우에 유용합니다. 테스트 결과에 **AVG**



Internet Security 2012 프로그램에서 검색한 경고만 있는 경우에는 별도의 작업이 필요하지 않습니다.

다음은 그러한 개체의 가장 일반적인 사례에 대한 간략한 설명입니다.

- **숨겨진 파일** - 숨겨진 파일은 기본적으로 Windows에 표시되지 않으며, 일부 바이러스나 위협 요소는 자신이 검색되지 않도록 하기 위해 파일이 저장될 때 이러한 특성을 이용합니다. AVG Internet Security 2012에서 악의적인 파일로 의심되는 숨겨진 파일을 보고하는 경우 이를 [바이러스 저장소](#)로 이동시킬 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.

11.7.5. 루트킷 탭

루트킷 탭에는 [Anti-Rootkit 스캔](#)을 실행한 경우 스캔 중에 감지된 루트킷 관련 정보가 표시됩니다.

루트킷이란 시스템 소유자 및 합법적인 관리자의 승인 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. 대부분 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.

11.7.6. 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 Internet Security 2012 스캔에서는 감염 여부가 의심스러운 파일을 검색할 수 있습니다. 이러한 파일은 [경고](#) 또는 정보로 보고됩니다.

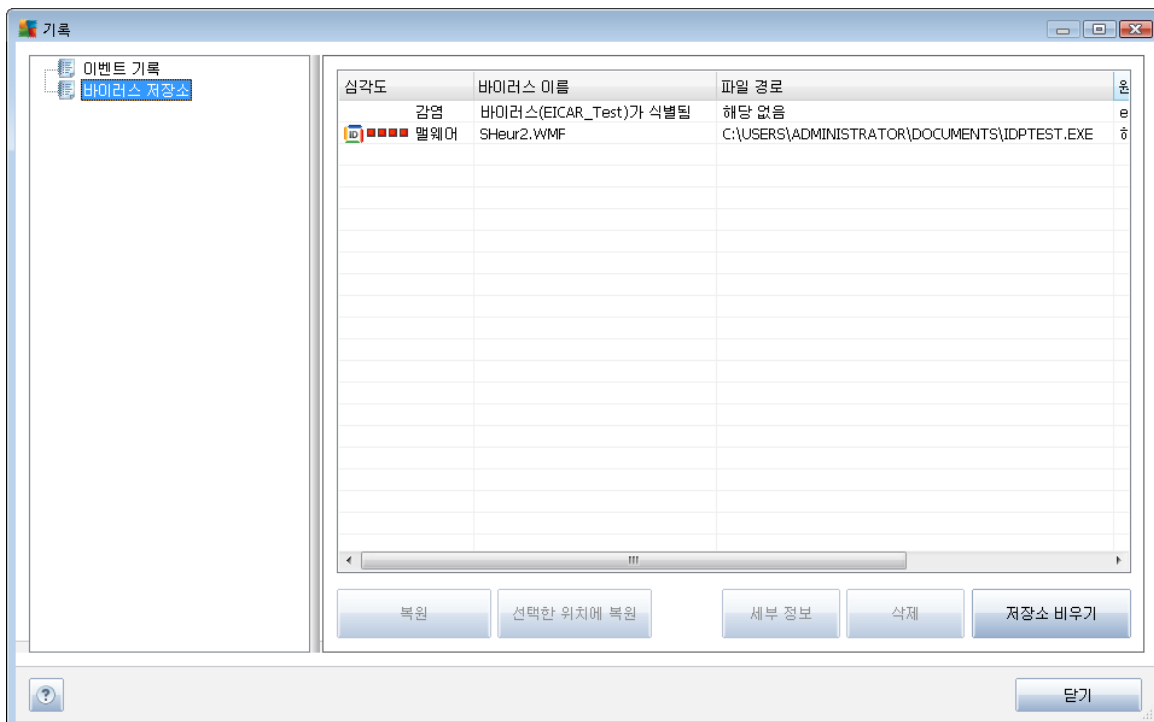
다음 이유 중 하나로 인해 심각도 **정보**가 보고될 수 있습니다.

- **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 Internet Security 2012(또는 일반적인 다른 맬웨어 백신 프로그램)으로 스캔할 수 없습니다.

다.

- **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. Windows 에서 두 번째 확장명은 기본적으로 보이지 않지만 **AVG Internet Security 2012**는 그와 같은 파일을 실수로 열지 않도록 보고합니다.
- **잘못된 파일 경로** - 중요한 시스템 파일이 기본 경로가 아닌 다른 경로에서 실행되는 경우(예: *winlogon.exe*가 Windows 폴더가 아닌 폴더에서 실행되는 경우) **AVG Internet Security 2012**는 이러한 불일치를 보고합니다. 바이러스가 시스템에서 자신의 존재를 숨기기 위해 표준 시스템 프로세스의 이름을 사용하는 경우가 있습니다.
- **잠긴 파일** - 보고된 파일이 잠겨 있어 **AVG Internet Security 2012**에서 스캔할 수 없습니다. 이것은 대개 해당 파일이 시스템에서 지속적으로 사용되고 있다는 의미입니다(예: 스왑 파일).

11.8. 바이러스 저장소



바이러스 저장소는 AVG 테스트 중에 발견된 의심스럽거나 감염된 개체를 관리할 수 있는 안전한 환경입니다. 일단 스캔 중에 감염된 개체가 발견되고 AVG 가 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.

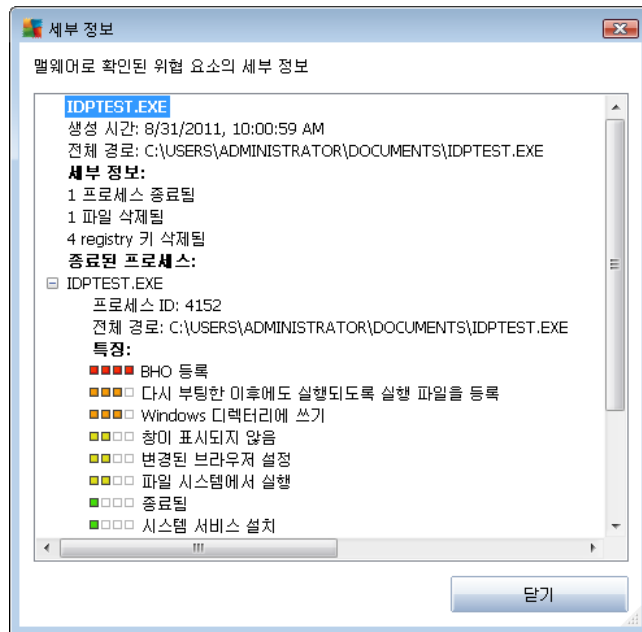
바이러스 저장소 인터페이스는 별도의 창으로 열리며 검역소로 이동된 감염된 개체에 대한 정보의 개요를 제공합니다.

- **심각도** - [Identity Protection](#) 구성 요소를 **AVG Internet Security 2012** 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 시간입니다.

제어 단추

바이러스 저장소 인터페이스에서 다음 제어 단추에 액세스할 수 있습니다.

- **복원** - 감염된 파일을 디스크의 원래 위치로 되돌려 보냅니다.
- **선택한 위치에 복원** - 감염된 파일을 선택한 폴더로 이동합니다.
- **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 저장소**에서 파일을 제거하면 해당 파일이 휴지통으로 이동되지 않고 디스크에서 영구적으로 제거됩니다.



12. AVG 업데이트

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 흔히 발생합니다. 이러한 이유로 소프트웨어 공급업체는 새로 발견된 보안 취약점을 해결하기 위해 업데이트 및 보안 패치를 지속적으로 발표합니다.

새로 출현하는 모든 컴퓨터 위협 요소와 이들의 전파 속도를 고려해 볼 때 **AVG Internet Security 2012** 를 정기적으로 업데이트하는 것은 절대적으로 중요합니다. 가장 좋은 해결책은 자동 업데이트가 구성된 프로그램 기본 설정을 그대로 유지하는 것입니다. **AVG Internet Security 2012** 의 바이러스 데이터베이스가 최신 상태가 아니면 프로그램이 최신 위협 요소를 감지할 수 없다는 점을 명심해야 합니다.

따라서 AVG 를 정기적으로 업데이트하는 것이 중요합니다. 필수적인 바이러스 정의는 가능하면 매일 업데이트해야 합니다. 긴급도가 낮은 프로그램 업데이트는 매주 진행할 수 있습니다.

12.1. 업데이트 시작

최상의 보안 수준을 제공하기 위해 **AVG Internet Security 2012** 프로그램은 기본적으로 4 시간마다 새로운 업데이트를 검색하도록 예약되어 있습니다. AVG 업데이트는 정해진 일정에 따르는 것이 아니라 새로운 위협의 양과 심각도에 따라 릴리스되기 때문에 항상 AVG 바이러스 데이터베이스를 최신 상태로 유지하는 것이 좋습니다.

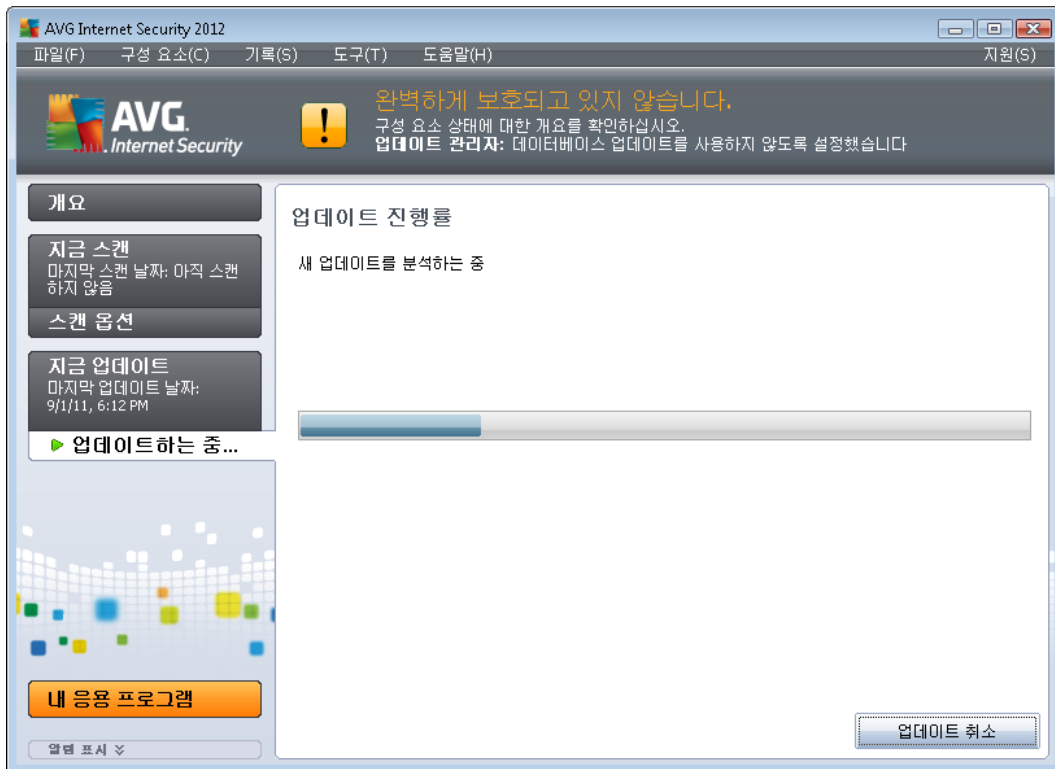
업데이트 시작 횟수를 줄이려는 경우에는 업데이트 시작 매개 변수를 설정할 수 있습니다. 하지만 적어도 하루에 한 번은 업데이트를 실행하는 것이 좋습니다. 구성은 [고급 설정/예약](#) 섹션의 다음 대화 상자에서 편집할 수 있습니다.

- [정의 업데이트 일정](#)
- [프로그램 업데이트 일정](#)
- [Anti-Spam 업데이트 일정](#)

새로운 업데이트 파일을 즉시 확인하려면 기본 사용자 인터페이스에 있는 [지금 업데이트](#) 빠른 링크를 사용합니다. 이 링크는 모든 [사용자 인터페이스](#) 대화 상자에서 언제든지 사용할 수 있습니다.

12.2. 업데이트 진행률

일단 업데이트를 시작하면 먼저 사용할 수 있는 새 업데이트 파일이 있는지 여부를 확인합니다. 파일이 있는 경우 **AVG Internet Security 2012**에서는 다운로드를 시작하고 업데이트 프로세스를 실행합니다. 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: 각 AVG 프로그램 업데이트가 시작되기 전에 시스템 복원 지점이 만들어집니다. 업데이트 프로세스가 실패하여 운영 체제가 중단되는 경우 언제든지 운영 체제를 이 지점에서 원래 구성으로 복원할 수 있습니다. 이 옵션은 Windows 메뉴의 시작 / 모든 프로그램 / 보조 프로그램 / 시스템 도구 / 시스템 복원을 통해 액세스할 수 있습니다. 숙련된 사용자만 사용하는 것이 좋습니다.

12.3. 업데이트 수준

AVG Internet Security 2012에서는 다음 두 가지 업데이트 수준 중에 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 정의의 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 다음 두 가지 업데이트 수준에 대한 특정 매개 변수를 정의할 수 있습니다.

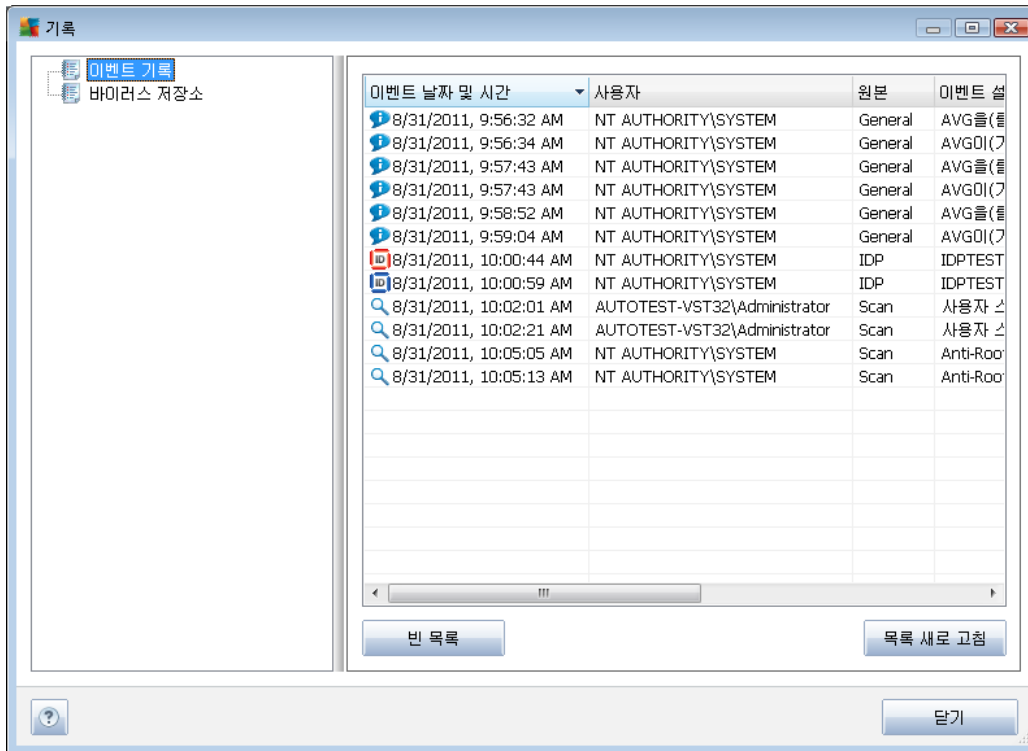
- [정의 업데이트 일정](#)
- [프로그램 업데이트 일정](#)

참고: 예약된 프로그램 업데이트와 예약된 스캔이 같은 시간에 진행될 경우 업데이트 프



로세스의 우선 순위가 더 높으므로 스캔이 중단됩니다.

13. 이벤트 기록



기록 대화 상자는 [시스템 메뉴](#)의 **기록/이벤트 기록 로그** 항목을 통해 액세스할 수 있습니다. 이 대화 상자에서는 **AVG Internet Security 2012** 작업 중 발생한 중요한 이벤트에 대한 요약 내용을 확인할 수 있습니다. 기록에서는 다음과 같은 유형의 이벤트를 기록합니다.

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

각 이벤트에 대해 다음 정보가 나열됩니다.

- **이벤트 날짜 및 시간**은 이벤트가 발생한 정확한 날짜와 시간을 나타냅니다.
- **사용자**는 이벤트가 발생했을 때 로그인되어 있던 사용자의 이름을 나타냅니다.
- **원본**은 이벤트를 트리거한 원본 구성 요소 또는 AVG 시스템의 다른 부분에 대한 정보를 나타냅니다.
- **이벤트 설명** 실제로 발생한 내용을 간략하게 요약하여 표시합니다.



제 어 단 추

- **목록 비우기** - 이 단추를 누르면 이벤트 목록의 모든 항목이 삭제됩니다.
- **목록 새로 고침** - 이 단추를 누르면 이벤트 목록의 모든 항목이 업데이트됩니다.

14. FAQ 및 기술 지원

AVG Internet Security 2012 응용 프로그램과 관련하여 판매 또는 기술 관련 문제가 발생할 경우 다음 옵션 중 하나를 선택하여 적절한 도움을 받을 수 있습니다.

- 고객 지원에 문의:** AVG 응용 프로그램 내에서 AVG의 전문적인 고객 지원 센터에 문의할 수 있습니다. **도움말/온라인 도움말 보기** 기본 메뉴 항목을 선택하면 24 시간 연중무휴 고객 지원 서비스와 통신할 수 있는 온라인 연락처 양식 페이지에 연결됩니다. 라이선스 번호가 자동으로 입력됩니다. 웹 페이지에 나오는 지시에 따라 진행하십시오.
- 지원(기본 메뉴 링크):** 기본 사용자 인터페이스 위쪽에 있는 AVG 응용 프로그램 메뉴에는 **지원** 링크가 있습니다. 이 링크를 클릭하면 도움이 필요할 때 찾아볼 수 있는 모든 종류의 정보가 포함된 대화 상자가 새로 열립니다. 이 대화 상자에는 사용자 컴퓨터에 설치되어 있는 AVG 프로그램에 대한 기본 데이터(**프로그램/데이터베이스 버전**), 라이선스 세부 정보 및 다음과 같은 빠른 지원 링크 목록이 포함되어 있습니다.



- 도움말 파일에서 문제 해결:** AVG Internet Security 2012에 포함되어 있는 도움말 파일에서 새로운 **문제 해결** 섹션을 바로 사용할 수 있습니다. 이 섹션에는 기술적인 문제에 대한 전문적인 도움이 요구되는 자주 발생하는 상황의 목록이 포함됩니다. 문제를 가장 잘 설명하는 상황을 선택한 후 클릭하면 문제 해결을 안내하는 자세한 지침을 볼 수 있습니다.
- AVG 웹 사이트 Support Center:** 또는 AVG 웹 사이트 (<http://www.avg.com/>)에서 문제에 대한 해결 방법을 직접 찾아볼 수 있습니다. **지원 센터** 섹션에서는 판매 및 기술 문제 둘 모두와 관련된 개요가 주제별로 그룹화되어 있습니다.
- 질문과 대답:** AVG 웹 사이트 (<http://www.avg.com/>)에는 질문과 대답 섹션도 별도로



준비되어 있습니다. 이 섹션은 **지원 센터/질문과 대답** 메뉴 옵션을 통해 액세스할 수 있습니다. 이 섹션에도 모든 질문이 판매, 기술 및 바이러스 범주로 분류되어 있습니다.

- **바이러스 및 위협 정보**: AVG 웹 사이트 (<http://www.avg.com/>)에서 바이러스 문제와 관련된 특별한 장입니다. 메뉴에서 **지원 센터/바이러스 및 위협 정보**를 선택하면 온라인 위협 요소와 관련된 체계적인 개요 페이지가 열립니다. 이 페이지에서는 바이러스와 스파이웨어를 제거하는 방법 및 보안을 유지하는 방법에 대한 조언도 볼 수 있습니다.
- **토론 포럼**: AVG 사용자 토론 포럼 (<http://forums.avg.com>)도 이용할 수 있습니다.