System Center

Endpoint Protection(Mac용)

설치 설명서 및 사용자 설명서

Microsoft

목차

System Center Endpoint Protection

Unix 기반 운영 체제의 사용률이 높아지면서 맬웨어 작성자들이 Mac 사용자를 겨냥하여 점점 더 많은 위협을 개발하고 있습니다. System Center Endpoint Protection에서는 이와 같이 새롭게 등장하는 위협에 대한 강력하고도 효율적인 보호 기능을 제공합니다. 또한 System Center Endpoint Protection에는 Windows 위협 차단 기능도 포함되어 있으므로 Windows 사용자와 Mac 사용자 간의 상호 작용도 보호합니다. Windows 맬웨어가 Mac에서도 직접적인 위협을 유발하는 것은 아니지만, Mac 컴퓨터를 감염시킨 맬웨어를 비활성화하면 해당 맬웨어가 로컬 네트워크나 인터넷을 통해 Windows 기반 컴퓨터로 확산되지 않도록 할 수 있습니다.

시스템 요구 사항

System Center Endpoint Protection 성능을 최적화하려면 시스템이 다음 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다.

System Center Endpoint Protection:

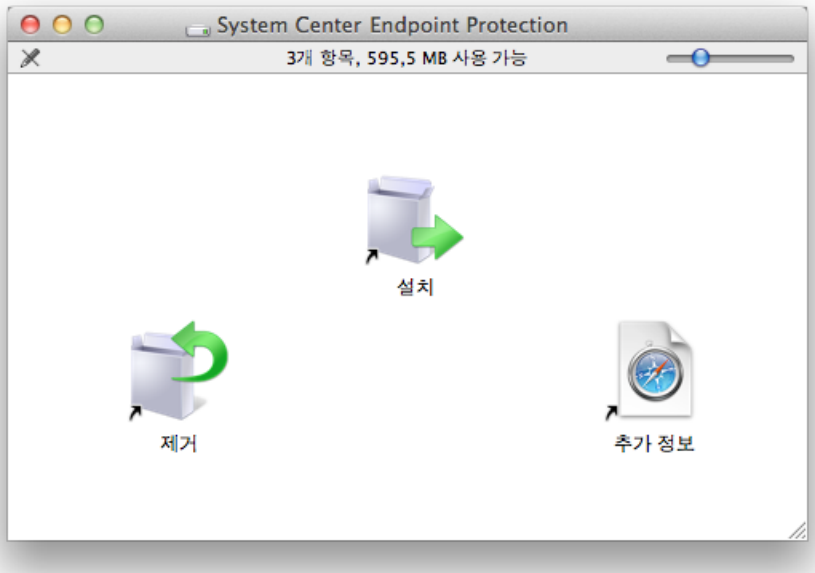
	시스템 요구 사항
프로세서 아키텍처	32비트, 64비트 Intel
운영 체제	Mac OS X 10.6 이상
메모리	512MB
남은 디스크 용량	100MB

설치

설치 프로세스를 시작하기 전에 컴퓨터에서 열려 있는 모든 프로그램을 닫으십시오. System Center Endpoint Protection에 포함된 구성 요소는 컴퓨터에 이미 설치되어 있을 수 있는 다른 안티바이러스 프로그램과 충돌할 수 있습니다. 문제 발생을 방지하려면 다른 안티바이러스 프로그램은 제거하는 것이 좋습니다. System Center Endpoint Protection은 설치 CD 또는 웹 사이트에서 다운로드한 파일을 사용하여 설치할 수 있습니다.

설치 마법사를 시작하려면 다음 중 하나를 수행하십시오.

- 설치 CD/DVD로 설치하는 경우 컴퓨터에 CD/DVD를 넣고 바탕 화면이나 Finder 창에서 연 다음 **설치** 아이콘을 두 번 클릭합니다.
- 다운로드한 파일로 설치하는 경우에는 다운로드한 파일을 열고 **설치** 아이콘을 두 번 클릭합니다.



설치 관리자를 실행하면 설치 마법사가 기본적인 설정 과정을 안내합니다. 소프트웨어 사용권 계약에 동의하고 개인 정보 보호 정책을 읽은 후 다음 설치 유형 중에서 선택합니다.

- 표준 4
- 사용자 지정 5

표준 설치

표준 설치 모드에는 대부분의 사용자에게 적합한 구성 옵션이 포함됩니다. 이러한 설정은 최고의 보안 기능과 우수한 시스템 성능을 제공합니다. 표준 설치가 기본 옵션이며, 특정 설정에 대한 특별한 요구 사항이 없는 경우 이 옵션을 사용하는 것이 좋습니다.

표준 설치 모드를 선택한 경우 **사용자가 원치 않는 응용 프로그램 검색**을 구성합니다. 잠재적으로 원치 않는 응용 프로그램이 반드시 악성 응용 프로그램인 것은 아니지만 운영 체제의 동작에 부정적인 영향을 줄 수 있습니다. 이러한 응용 프로그램은 다른 프로그램과 함께 제공되어 설치 프로세스 중에는 알아차리기 어려울 수 있습니다. 이러한 응용 프로그램이 일반적으로 설치 중에 알림을 표시하기는 하지만 사용자의 동의 없이 쉽게 설치될 수 있습니다.

System Center Endpoint Protection을 설치했으면 컴퓨터에서 악성 코드 검사를 수행해야 합니다. 기본 프로그램 창에서 **컴퓨터 검사**를 클릭한 다음 **스마트 검사**를 클릭합니다. 수동 컴퓨터 검사에 대한 자세한 내용은 수동 컴퓨터 검사 11 섹션을 참조하십시오.

사용자 지정 설치

사용자 지정 설치 모드는 설치 프로세스 중에 고급 설정을 수정하려는 숙련된 사용자를 위한 것입니다.

사용자 지정 설치 모드를 선택하면 **프록시 서버** 설정을 구성하라는 메시지가 표시됩니다. 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 선택하여 해당 파라미터를 정의할 수 있습니다. **주소** 필드에 프록시 서버의 IP 주소 또는 URL을 입력합니다. 포트 필드에 프록시 서버가 연결을 허용하는 포트(기본적으로 3128)를 지정합니다. 프록시 서버에 인증이 필요한 경우 올바른 **사용자 이름** 및 **비밀번호**를 입력하여 프록시 서버에 대한 접근을 부여합니다. 프록시 서버를 사용하지 않으려는 경우에는 **프록시 서버 사용 안 함** 옵션을 선택합니다. 프록시 서버 사용 여부를 모르는 경우에는 **시스템 설정 사용(권장)**을 선택하여 현재 시스템 설정을 사용하면 됩니다.

다음 단계에서는 프로그램 구성을 편집할 수 있는 **권한 있는 사용자 정의**를 수행할 수 있습니다. 왼쪽의 사용자 목록에서 사용자를 선택하고 **추가**를 클릭하여 **권한 있는 사용자** 목록에 추가합니다. 모든 시스템 사용자를 표시하려면 **모든 사용자 표시** 옵션을 선택합니다.

설치 프로세스의 다음 단계는 **사용자가 원치 않는 응용 프로그램 검색**을 구성하는 단계입니다. 잠재적으로 원치 않는 응용 프로그램이 반드시 악성 응용 프로그램인 것은 아니지만 운영 체제의 동작에 부정적인 영향을 줄 수 있습니다. 이러한 응용 프로그램은 다른 프로그램과 함께 제공되어 설치 프로세스 중에는 알아차리기 어려울 수 있습니다. 이러한 응용 프로그램이 일반적으로 설치 중에 알림을 표시하기는 하지만 사용자의 동의 없이 쉽게 설치될 수 있습니다.

System Center Endpoint Protection을 설치했으면 컴퓨터에서 악성 코드 검사를 수행해야 합니다. 기본 프로그램 창에서 **컴퓨터 검사**를 클릭한 다음 **스마트 검사**를 클릭합니다. 수동 검사에 대한 자세한 내용은 수동 검사 11 섹션을 참조하십시오.

제거

컴퓨터에서 System Center Endpoint Protection을 제거하려면 다음 중 하나를 수행합니다.

- 컴퓨터에 System Center Endpoint Protection 설치 CD/DVD를 넣고 바탕 화면이나 Finder 창에서 연 다음 **제거** 아이콘을 두 번 클릭합니다.
- System Center Endpoint Protection 설치 파일(.dmg)을 열고 **제거** 아이콘을 두 번 클릭합니다.
- Finder를 시작하고 하드 드라이브에서 **응용 프로그램** 폴더를 연 다음 Ctrl 키를 누르고 System Center Endpoint Protection 아이콘을 클릭한 다음 **패키지 내용 표시** 옵션을 선택합니다. 그런 다음 Contents > Helper 폴더를 열고 Uninstaller 아이콘을 두 번 클릭합니다.

초보자용 설명서

이 장에서는 System Center Endpoint Protection의 초기 개요 및 해당 기본 설정에 대해 설명합니다.

사용자 인터페이스

System Center Endpoint Protection의 기본 프로그램 창은 두 개의 기본 섹션으로 구분됩니다. 오른쪽의 기본 창은 왼쪽의 기본 메뉴에서 선택한 옵션에 해당하는 정보를 표시합니다.

다음은 기본 메뉴 내의 옵션에 대한 설명입니다.

- **보호 상태** - System Center Endpoint Protection의 보호 상태에 대한 정보를 제공합니다. **고급 모드**를 활성화하면 **통계** 하위 메뉴가 표시됩니다.
- **컴퓨터 검사** - 이 옵션을 사용하면 수동 검사를 구성 및 시작할 수 있습니다.
- **업데이트** - 바이러스 시그니처 DB 업데이트에 대한 정보를 표시합니다.
- **설정** - 컴퓨터의 보안 수준을 조정하려면 이 옵션을 선택합니다. **고급 모드**를 활성화하면 **안티바이러스, 안티스파이웨어** 하위 메뉴가 표시됩니다.
- **도구** - **로그 파일**, **검역소** 및 **스케줄러**에 접근할 수 있습니다. 이 옵션은 **고급 모드**에서만 표시됩니다.
- **도움말** - 프로그램 정보를 제공하며 도움말 파일에 접근할 수 있습니다.

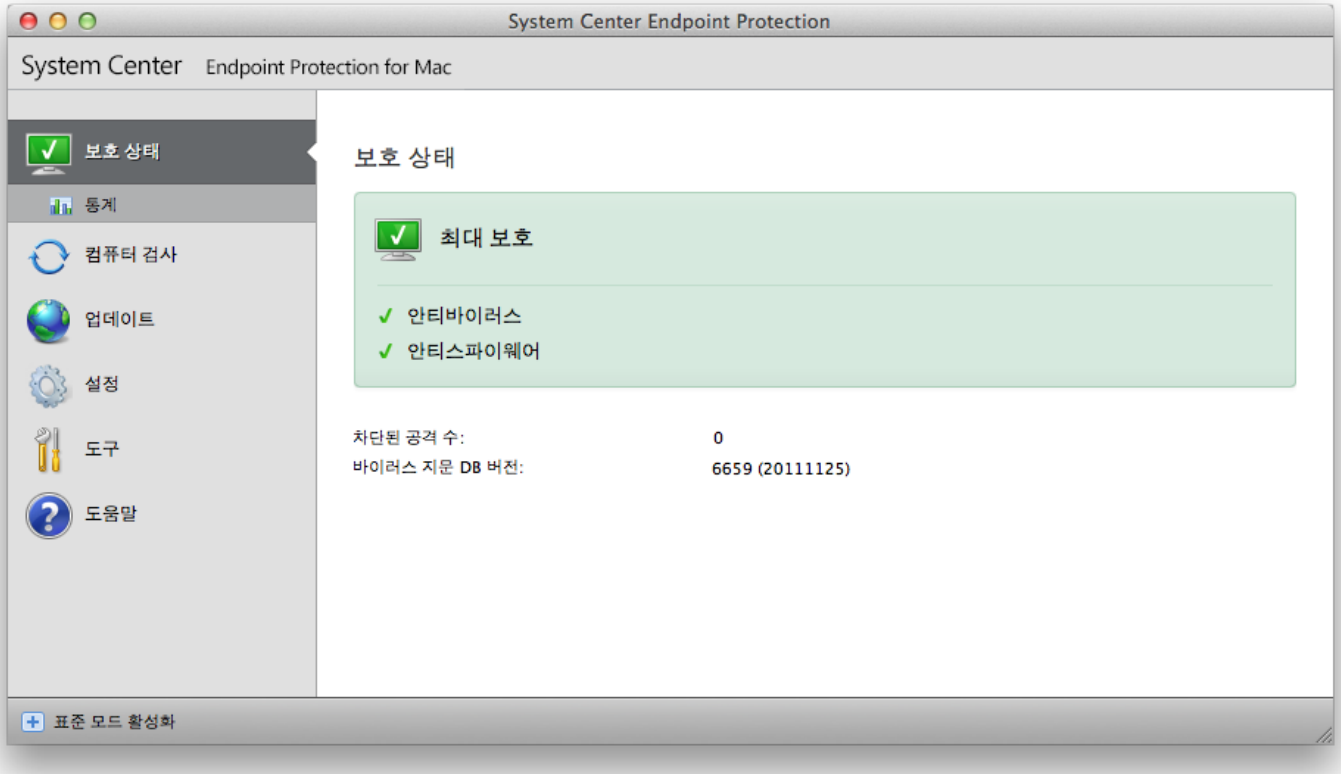
System Center Endpoint Protection 사용자 인터페이스를 통해 표준 모드와 고급 모드 간에 전환할 수 있습니다. 표준 모드에서는 일반 작업에 필요한 기능에 접근할 수 있으며. 고급 옵션은 표시되지 않습니다. 모드 간을 전환하려면 기본 프로그램 창 왼쪽 아래에 있는 **고급 모드 활성화/표준 모드 활성화** 옆의 더하기 아이콘(+)을 클릭하거나 cmd+M을 누릅니다.

고급 모드로 전환하면 기본 메뉴에 **도구** 옵션이 추가로 표시됩니다. **도구** 옵션을 통해 **로그 파일**, **검역소** 및 **스케줄러** 하위 메뉴에 접근할 수 있습니다.

참고: 이 설명서의 모든 나머지 지침은 **고급 모드**에 적용되는 것입니다.

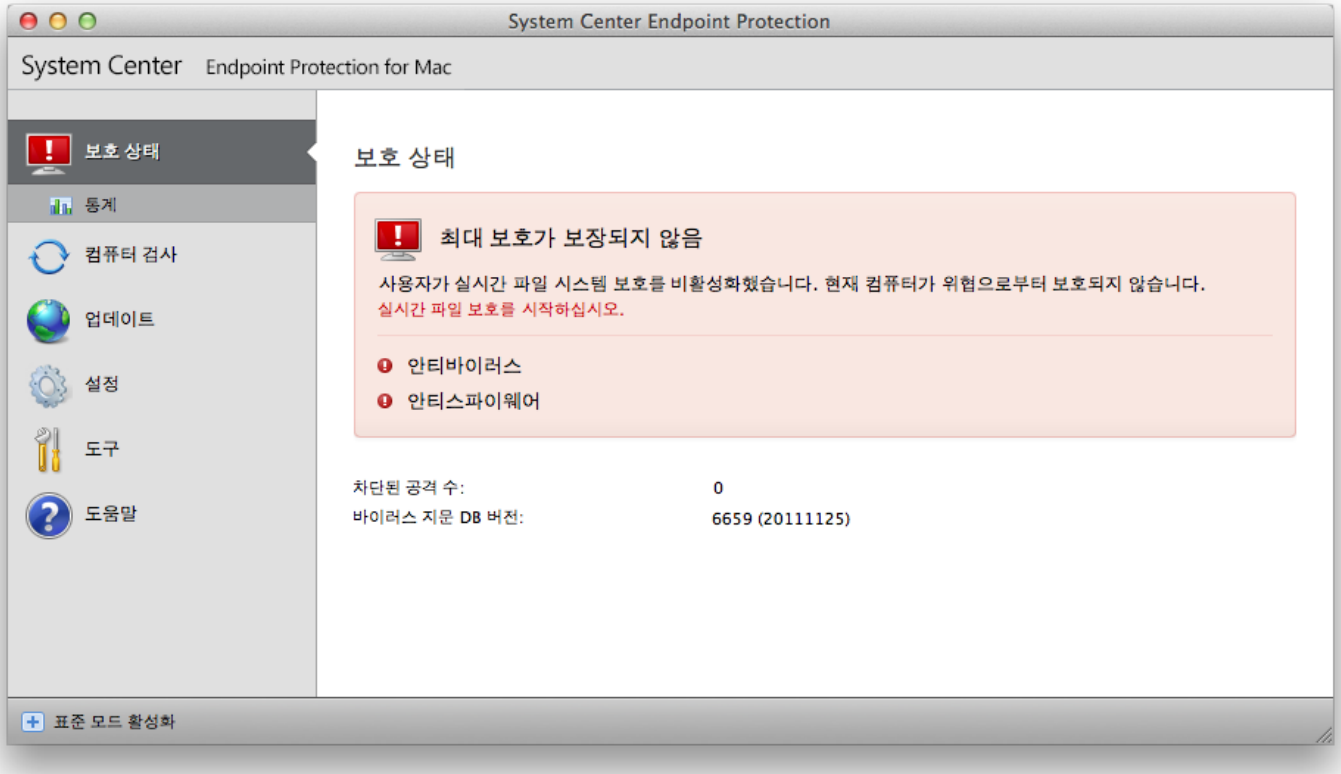
시스템 작동 확인

보호 상태를 확인하려면 기본 메뉴에서 맨 위 옵션을 클릭합니다. 그러면 System Center Endpoint Protection 작동에 대한 상태 요약과 **통계** 하위 메뉴가 기본 창에 표시됩니다. 해당 하위 메뉴를 선택하면 시스템에서 수행된 컴퓨터 검사에 대한 상세 정보 및 통계를 확인할 수 있습니다. 통계 창은 고급 모드에서만 사용할 수 있습니다.



프로그램이 제대로 작동하지 않는 경우 수행할 작업

활성화된 모듈이 제대로 작동하는 경우 녹색 확인 아이콘이 지정됩니다. 제대로 작동하지 않는 경우 빨간색 느낌표나 주황색 알림 아이콘이 표시되고 모듈에 대한 추가 정보가 창의 위쪽 부분에 표시됩니다. 모듈 해결에 대한 권장 해결 방법도 표시됩니다. 개별 모듈의 상태를 변경하려면 기본 메뉴에서 **설정**을 클릭하고 원하는 모듈을 클릭합니다.



System Center Endpoint Protection 사용

안티바이러스, 안티스파이웨어 보호

안티바이러스 보호는 잠재적 위협을 유발하는 파일을 수정하여 악의적인 시스템 공격으로부터 보호합니다. 악성 코드를 통한 위협이 검출되면 안티바이러스 모듈은 먼저 해당 코드를 차단한 후에 치료 또는 삭제하거나 검역소로 보내는 방법으로 위협을 제거할 수 있습니다.

실시간 파일 시스템 보호

실시간 파일 시스템 보호 기능은 시스템 내의 모든 안티바이러스 관련 이벤트를 제어합니다. 컴퓨터에서 파일을 열거나 생성하거나 실행할 때마다 악성 코드가 있는지 검사합니다. 시스템 시작 시 실시간 파일 시스템 보호도 시작됩니다.

실시간 보호 설정

실시간 파일 시스템 보호는 모든 미디어 유형을 검사하며 다양한 이벤트를 기준으로 검사를 트리거합니다. 새로 생성한 파일과 기존 파일에 대해 실시간 파일 시스템 보호는 다르게 작동할 수 있습니다. 새로 생성한 파일의 경우에는 더 자세한 제어 수준을 적용할 수 있습니다.

기본적으로 시스템 시작 시 실시간 보호가 시작되며 중단 없이 검사를 수행합니다. 다른 실시간 검사기와 충돌하는 등의 특수한 경우에는 화면 위쪽의 메뉴 모음에 있는 System Center Endpoint Protection 아이콘을 클릭한 다음 **실시간 파일 시스템 보호 비활성화** 옵션을 선택하여 실시간 보호를 종료할 수 있습니다. 기본 프로그램 창에서 **설정** > **안티바이러스, 안티스파이웨어** > **비활성화**를 눌러서도 실시간 보호를 종료할 수도 있습니다.

실시간 보호의 고급 설정을 수정하려면 **설정** > **응용 프로그램 기본 설정 입력...** > **보호** > **실시간 보호**로 이동하여 **고급 옵션**(고급 검사 옵션 9 섹션에 설명되어 있음) 옆에 있는 **설정...** 버튼을 클릭합니다.

검사(이벤트로 트리거되는 검사)

기본적으로 **파일 열기**, **파일 생성** 또는 **파일 실행** 시에는 모든 파일을 검사합니다. 컴퓨터에 대한 최대 수준의 실시간 보호를 제공하는 기본 설정을 유지하는 것이 좋습니다.

고급 검사 옵션

이 창에서는 **고급 인공지능**을 활성화/비활성화하여 검사 엔진에서 검사할 오브젝트 유형을 정의할 수 있으며, 압축파일 및 파일 캐시의 설정을 수정할 수 있습니다.

압축파일의 압축 수준 값을 크게 지정하면 시스템 성능이 저하될 수 있으므로, 특정 문제를 해결하는 데 필요한 경우가 아니면 **기본 압축파일 설정** 섹션의 기본값을 변경하지 않는 것이 좋습니다.

개별 엔진 파라미터 섹션에서 **고급 인공지능** 확인란을 클릭하여 실행, 생성 및 수정된 파일에 대한 고급 인공지능 검사를 개별적으로 전환할 수 있습니다.

실시간 보호 사용 시 시스템 공간을 최소화하기 위해, 최적화 캐시의 크기를 정의할 수 있습니다. 이 동작은 **감염되지 않은 파일 캐시 활성화** 옵션 사용 시 활성화됩니다. 이 옵션이 비활성화된 경우 파일에 접근할 때마다 해당 파일이 검사됩니다. 캐시된 파일은 정의된 캐시 크기가 될 때까지 반복하여 검사하지 않습니다(파일이 수정된 경우는 제외). 각 바이러스 시그니처 DB 업데이트 직후 파일이 다시 검사됩니다.

이 기능을 활성화/비활성화하려면 **감염되지 않은 파일 캐시 활성화**를 클릭합니다. 캐시할 파일 크기를 설정하려면 **캐시 크기** 옆의 입력 필드에 원하는 값을 입력하면 됩니다.

엔진 설정 창에서 추가 검사 파라미터를 설정할 수 있습니다. 검사할 **오브젝트**의 유형, 사용할 **옵션** 및 **치료** 수준, 그리고 실시간 파일 시스템 보호의 **확장명** 및 파일 크기 **제한**을 정의할 수 있습니다. 고급 설정 창의 **엔진** 옆에 있는 **설정...** 버튼을 클릭하여 엔진 설정 창을 표시할 수 있습니다. 엔진 파라미터에 대한 자세한 내용은 엔진 파라미터 설정 14을 참조하십시오.

검사에서 제외

이 섹션에서는 특정 파일 및 폴더를 검사에서 제외할 수 있습니다.

- **경로** - 제외된 파일 및 폴더의 경로입니다.
- **위협** - 제외된 파일 옆에 위협 이름이 있으면 해당 파일은 완전히 제외된 것이 아니라 지정된 위협에 대해서만 제외된 것입니다. 따라서 해당 파일이 나중에 다른 맬웨어로 감염되면 안티바이러스 모듈에서 해당 파일을 검출합니다.
- **추가...** - 오브젝트를 검출에서 제외합니다. 오브젝트의 경로를 입력하거나(* 및 ? 와일드카드를 사용할 수 있음) 트리 구조에서 파일 또는 폴더를 선택합니다.
- **편집...** - 선택한 항목을 편집할 수 있습니다.
- **삭제** - 선택한 항목을 삭제합니다.
- **기본값** - 모든 제외 항목을 취소합니다.

실시간 보호 구성을 수정해야 하는 경우

실시간 보호는 보안 시스템을 유지 관리하는 데 있어 가장 중요한 구성 요소입니다. 실시간 보호 파라미터를 수정할 때는 주의해야 합니다. 다른 안티바이러스 프로그램의 실시간 검사기나 특정 응용 프로그램과. 충돌하는 등의 특수한 상황에서만 실시간 보호 파라미터를 수정하는 것이 좋습니다.

System Center Endpoint Protection을 설치하고 나면 사용자에게 최대 시스템 보호 수준을 제공하기 위해 모든 설정이 최적화됩니다. 기본 설정을 복원하려면 **실시간 보호** 창(**설정** > **응용 프로그램 기본 설정 입력...** > **보호** > **실시간 보호**) 왼쪽 아래에 있는 **기본값** 버튼을 클릭합니다.

실시간 보호 검사

실시간 보호가 작동 중이며 바이러스를 검출하고 있는지 확인하려면 eicar.com 테스트 파일을 사용합니다. 이 테스트 파일은 모든 안티바이러스 프로그램에서 검출되는 무해한 특수 파일로, EICAR 협회(European Institute for Computer Antivirus Research)에서 안티바이러스 프로그램의 기능을 테스트하기 위해 생성한 것입니다.

원격으로 실시간 보호 상태를 확인하려면 **터미널**을 사용하여 클라이언트 컴퓨터에 연결하고 다음 명령을 수행합니다.
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

실시간 검사기의 상태는 `RTPStatus=Enabled` 또는 `RTPStatus=Disabled`(으)로 표시됩니다.

터미널 배쉬(Terminal bash)의 출력에는 다음 상태도 포함됩니다.

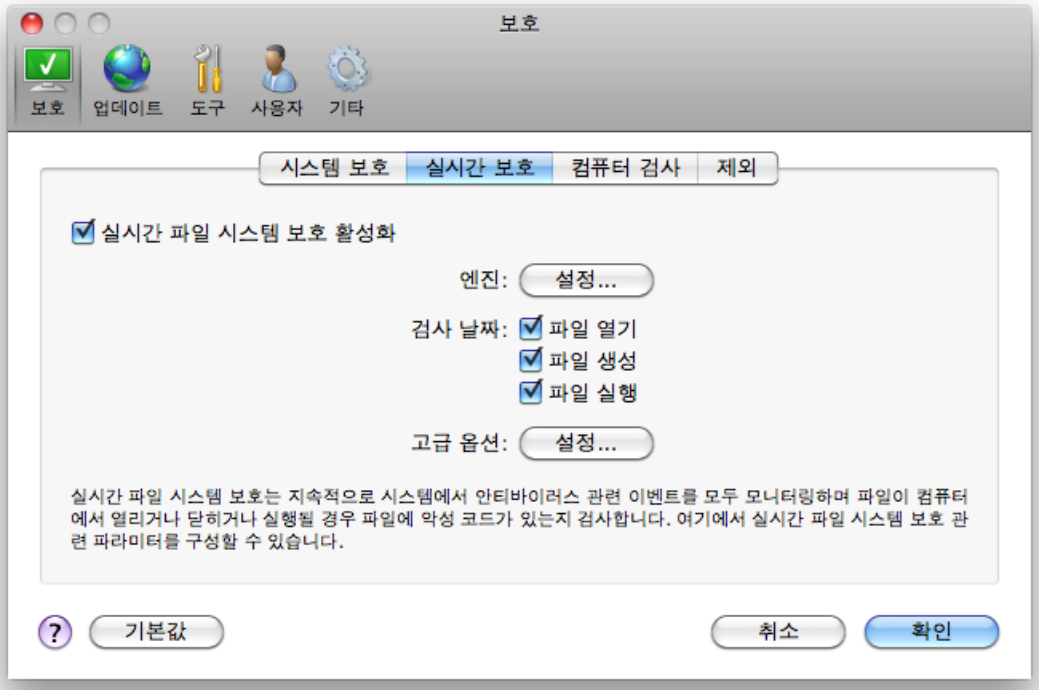
- 클라이언트 컴퓨터에 설치된 System Center Endpoint Protection 버전
- 바이러스 시그니처 DB의 날짜 및 버전
- 업데이트 서버의 경로

참고: 터미널은 고급 사용자만 사용하는 것이 좋습니다.

실시간 보호가 작동하지 않는 경우 수행할 작업

이 장에서는 실시간 보호를 사용할 때 발생할 수 있는 문제 상황과 이러한 문제를 해결하는 방법에 대해 설명합니다.

실시간 보호가 비활성화됨
사용자가 실수로 실시간 보호를 비활성화한 경우에는 다시 활성화해야 합니다. 실시간 보호를 다시 활성화하려면 **설정** > **안티바이러스, 안티스파이웨어**로 이동하여 기본 프로그램 창 오른쪽의 **실시간 파일 시스템 보호 활성화** 링크를 클릭합니다. **보호** > **실시간 보호** 아래의 고급 설정 창에서 **실시간 파일 시스템 보호 활성화** 옵션을 선택하여 실시간 파일 시스템 보호를 활성화할 수도 있습니다.



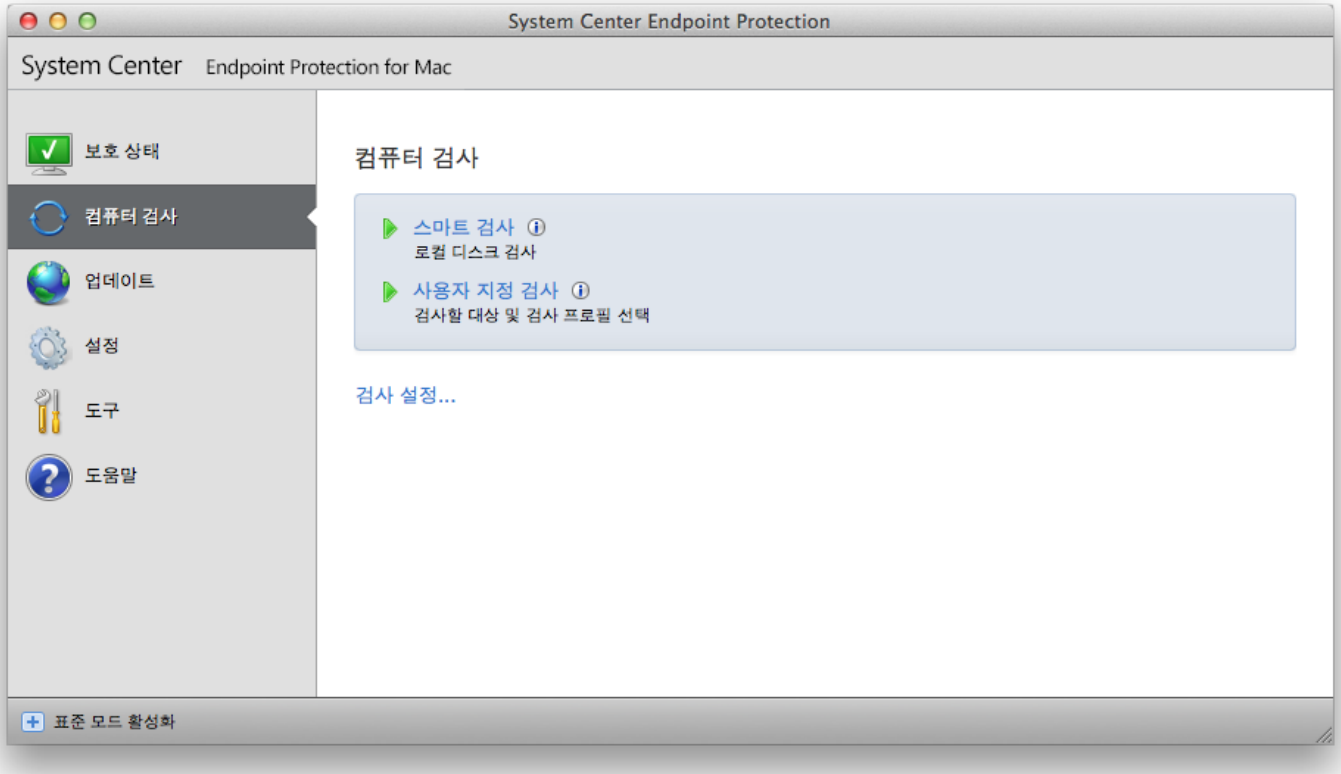
실시간 보호가 침입을 검출 및 치료하지 않음
컴퓨터에 다른 안티바이러스 프로그램이 설치되어 있지는 않은지 확인합니다. 두 실시간 보호 프로그램을 동시에 활성화하면 서로 충돌할 수 있습니다. 따라서 시스템의 다른 안티바이러스 프로그램을 제거하는 것이 좋습니다.

실시간 보호가 시작되지 않음
시스템 시작 시 실시간 보호가 시작되지 않으면 다른 프로그램과 충돌하기 때문일 수 있습니다. 이러한 경우 고객 지원 전문가에게 문의하십시오.

수동 검사

컴퓨터가 오작동을 일으키는 등 감염된 것으로 의심되는 경우에는 **컴퓨터 검사** > **스마트 검사**를 실행하여 컴퓨터에 침입이 있는지 검사합니다. 보호 수준을 최대화하려면 감염이 의심될 때만이 아니라 일상적인 보안 조치의 일환으로 정기적으로 컴퓨터 검사를 실행해야 합니다. 정기적인 검사를 수행하면 침입 항목이 디스크에 저장되었을 때 실시간 검사기가 검출하지 못한 침입을 검출할 수 있습니다. 감염 시 실시간 검사기가 비활성화되어 있었거나 바이러스 시그니처 DB가 최신 상태가 아니었던 경우 등이 이에 해당합니다.

수동 검사는 적어도 한달에 한 번 이상 수행하는 것이 좋습니다. **도구** > **스케줄러**에서 검사를 예약된 작업으로 구성할 수 있습니다.



데스크탑 또는 Finder 창에서 선택한 파일 및 폴더를 System Center Endpoint Protection 기본 화면, Dock 아이콘, 메뉴 모음 아이콘(화면 맨 위) 또는 응용 프로그램 아이콘(*/응용 프로그램* 폴더에 있음)으로 끌어 놓을 수도 있습니다.

검사 유형

두 가지 유형의 수동 검사를 사용할 수 있습니다. **스마트 검사**는 검사 파라미터를 더 구성할 필요 없이 시스템을 빠르게 검사합니다. **사용자 지정 검사**에서는 미리 정의된 검사 프로필 및 특정 검사 대상을 선택할 수 있습니다.

스마트 검사

스마트 검사를 사용하면 컴퓨터 검사를 빠르게 시작하며, 사용자의 간섭없이 감염된 파일을 치료할 수 있습니다. 이 방법의 가장 큰 장점은 검사를 상세하게 구성하지 않아도 되므로 작업이 간편하다는 것입니다. 스마트 검사에서는 모든 폴더의 모든 파일을 검사하고 검출된 침입 항목을 자동으로 치료하거나 삭제합니다. 치료 수준은 기본값으로 자동 설정됩니다. 치료 유형에 대한 자세한 내용은 치료 15의 섹션을 참조하십시오.

사용자 지정 검사

검사 대상 및 검사 방법과 같은 검사 파라미터를 지정하려는 경우에는 **사용자 지정 검사**를 사용하는 것이 가장 적합합니다. 사용자 지정 검사를 실행하는 경우의 장점은 파라미터를 상세히 구성할 수 있다는 점입니다. 여러 구성을 사용자 정의 검사 프로필에 저장할 수 있는데 이는 동일한 파라미터로 검사를 반복적으로 수행하는 경우에 유용할 수 있습니다.

검사 대상을 선택하려면 **컴퓨터 검사** > **사용자 지정 검사**를 선택하고 트리 구조에서 특정 **검사 대상**을 선택합니다. 포함할 폴더 또는 파일 경로를 입력하여 검사 대상을 보다 정확하게 지정할 수도 있습니다. 추가 치료 동작 없이 시스템을 검사만 하려는 경우에는 **치료하지 않고 검사** 옵션을 선택합니다. 또한 **설정...** > **치료**를 클릭하면 세 가지 치료 수준 중에서 선택할 수 있습니다.

이전에 안티바이러스 프로그램을 사용해 본 적이 있는 고급 사용자의 경우 사용자 지정 검사를 사용하여 컴퓨터 검사를 수행하는 것이 좋습니다.

검사 대상

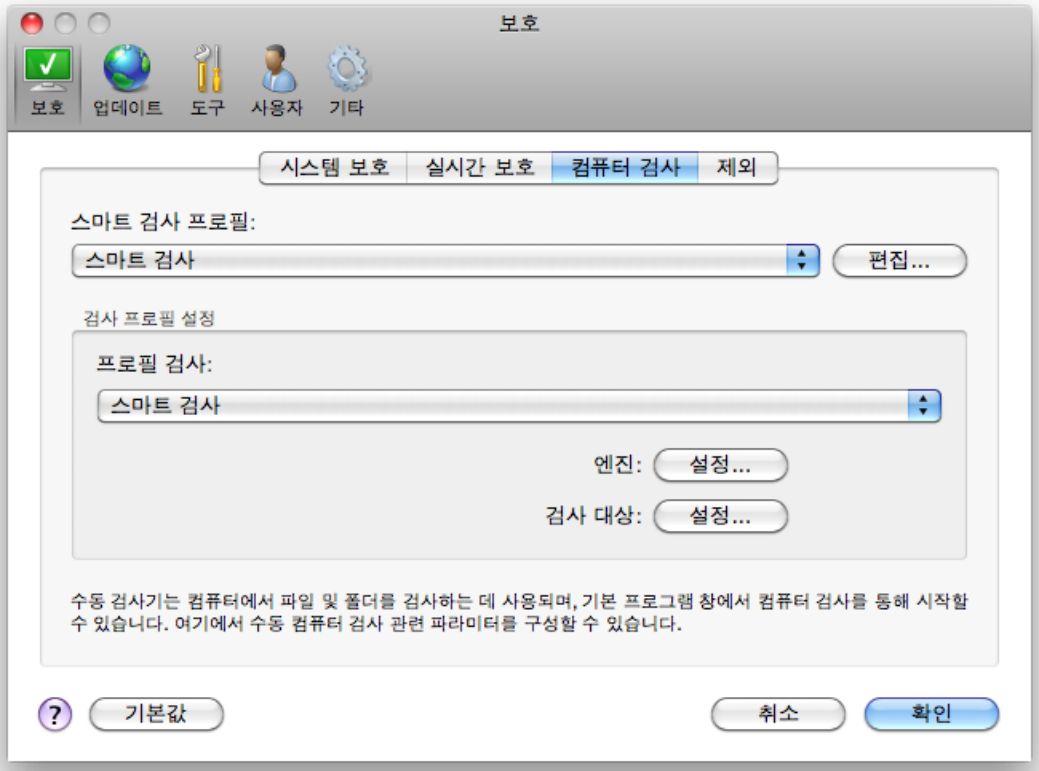
검사 대상 트리 구조에서는 바이러스를 검사할 파일 및 폴더를 선택할 수 있습니다. 프로필 설정에 따라 폴더를 선택할 수도 있습니다.

검사에 포함할 폴더 또는 파일 경로를 입력하여 검사 대상을 보다 정확하게 정의할 수 있습니다. 컴퓨터에서 사용 가능한 모든 폴더가 나열된 트리 구조에서 대상을 선택합니다.

검사 프로필

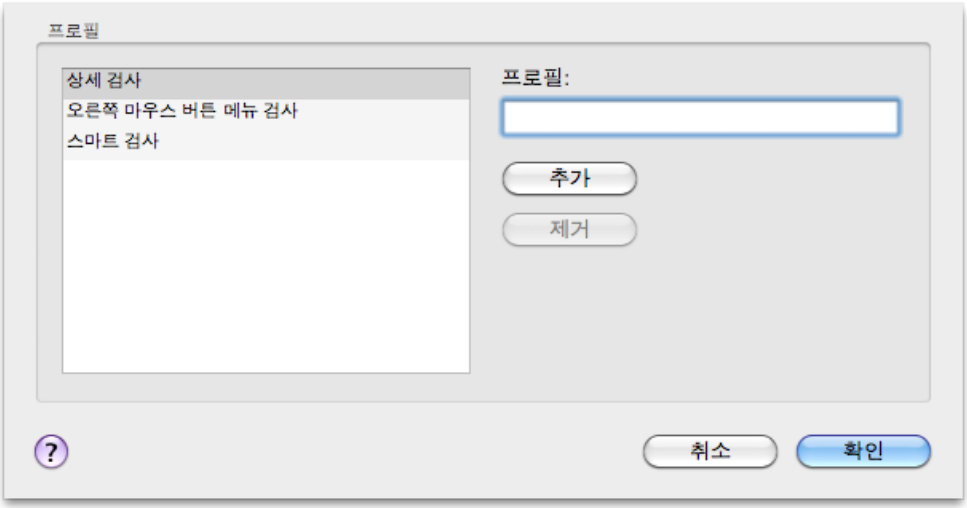
향후 검사를 위해 기본 검사 설정을 저장할 수 있습니다. 정기적으로 사용되는 각 검사에 대해 서로 다른 프로필(다양한 검사 대상, 검사 방법 및 기타 파라미터 포함)을 생성하는 것이 좋습니다.

새 프로필을 생성하려면 **설정** > **응용 프로그램 기본 설정 입력...** > **보호** > **컴퓨터 검사**로 이동한 다음 현재 프로필 목록 옆의 **편집...**을 클릭합니다.



필요에 맞게 검사 프로필을 생성하려면 엔진 파라미터 설정 14 섹션에서 검사 설정의 각 파라미터 설명을 참조하십시오.

예: 부분적으로는 스마트 검사 구성이 적합하지만 런타임 패커나 사용자에게 안전하지 않을 수 있는 응용 프로그램은 검사하지 않고 엄격한 치료를 적용하려는 고유의 검사 프로필을 생성하려 한다고 가정합니다. 이 경우 **수동 검사기 프로필 목록** 창에 프로필 이름을 입력하고 **추가** 버튼을 클릭한 후에 **확인**을 클릭하여 입력한 이름을 확인합니다. 그런 다음 **엔진** 및 **검사 대상**을 설정하여 파라미터를 요구 사항에 맞게 조정합니다.



엔진 파라미터 설정

System Center Endpoint Protection에서는 선제적 검사 기술을 사용합니다. 즉, 새로운 위협이 확산되기 이전에도 보호를 제공한다는 의미입니다. 또한 함께 작동하면 시스템 보안을 크게 향상시킬 수 있는 코드 분석, 코드 에뮬레이션, 일반 시그니처, 바이러스 시그니처 등 다양한 방법을 조합해 사용합니다. 검사 엔진은 여러 데이터 스트림을 동시에 제어하여 효율성과 검출 비율을 최대화할 수 있습니다. 이 기술은 루트킷도 방지할 수 있습니다.

엔진 기술 설정 옵션을 사용하여 다음과 같은 여러 가지 검사 파라미터를 지정할 수 있습니다.
- 검사할 파일 형식 및 확장명
- 다양한 검출 방법의 조합
- 치료 수준 등

설정 창을 표시하려면 **설정** > **안티바이러스, 안티스파이웨어** > **고급 안티바이러스, 안티스파이웨어 보호 설정**을 클릭하고 **시스템 보호**, **실시간 보호** 및 **컴퓨터 검사** 와일드카드에 있는 **설정...** 버튼을 클릭합니다. 각 보안 시나리오에 따라 서로 다른 구성이 필요할 수 있습니다. 이를 염두에 두고 다음 보호 모듈에 대해 엔진 파라미터를 개별적으로 구성할 수 있습니다.
- **시스템 보호** > 자동 시작 파일 검사
- **실시간 보호** > 실시간 파일 시스템 보호
- **컴퓨터 검사** > 수동 검사

엔진 파라미터는 각 모듈에 맞게 최적화되어 있으므로 이를 수정하면 시스템 작동에 큰 영향을 줄 수 있습니다. 예를 들어 항상 런타임 패커를 검사하도록 설정을 변경하거나 실시간 파일 시스템 보호 모듈에서 고급 인공지능을 활성화하면 시스템이 느려질 수 있습니다. 따라서 컴퓨터 검사를 제외한 모든 모듈에 대해서는 기본 엔진 파라미터를 변경하지 않는 것이 좋습니다.

오브젝트

오브젝트 섹션에서는 침입에 대해 검사할 컴퓨터 파일을 정의할 수 있습니다.

- **파일** - 프로그램, 그림, 오디오, 비디오 파일, 데이터베이스 파일 등 모든 일반 파일 형식을 검사합니다.
- **기호화된 링크** - 운영 체제에서 다른 파일 또는 디렉터리로의 경로로 해석하며 이를 따르는 텍스트 문자열이 포함된 특수 파일 형식을 검사합니다(수동 검사기에만 해당됨).
- **이메일 파일** - 이메일 메시지가 포함된 특수 파일을 검사합니다(실시간 보호에서는 사용할 수 없음).
- **사서함** - 시스템의 사용자 사서함을 검사합니다(실시간 보호에서는 사용할 수 없음). 이 옵션을 잘못 사용하면 이메일 클라이언트와의 충돌이 발생할 수 있습니다.
- **압축파일** - 압축파일(.rar, .zip, .arj, .tar, etc.)로 압축된 파일을 검사합니다(실시간 보호에서는 사용할 수 없음).
- **자체 압축 해제 파일** - 자체 압축 해제 파일에 포함된 파일을 검사합니다(실시간 보호에서는 사용할 수 없음).
- **런타임 패커** - 런타임 패커는 표준 압축파일 형식과는 달리 표준 정적 패커(UPX, yoda, ASPack, FGS 등)뿐 아니라 메모리에서도 압축을 해제합니다.

옵션

옵션 섹션에서는 시스템에서 침입을 검사할 때 사용하는 방법을 선택할 수 있습니다. 사용할 수 있는 옵션은 다음과 같습니다.

- **인공지능** - 인공지능은 프로그램의 악의적 활동을 분석하는 알고리즘을 사용합니다. 인공지능 검출의 가장 큰 장점은 이전에는 존재하지 않았거나 알려진 바이러스 목록(바이러스 시그니처 DB)에 포함되지 않은 새로운 악성 소프트웨어를 검출할 수 있다는 점입니다.
- **고급 인공지능** - 고급 인공지능은 컴퓨터 웜 및 트로잔 목마 검출용으로 최적화되어 있으며 높은 수준의 프로그래밍 언어로 작성된 고유 인공지능 알고리즘으로 구성됩니다. 고급 인공지능을 사용하는 경우 프로그램의 검출 기능이 크게 향상됩니다.
- **사용자가 원치 않는 응용 프로그램** - 반드시 악성 프로그램은 아니지만 컴퓨터의 성능을 저하시킬 수 있는 응용 프로그램입니다. 이러한 응용 프로그램의 경우 보통 설치 동의가 필요합니다. 이러한 응용 프로그램이 컴퓨터에 설치되어 있는 경우 시스템이 응용 프로그램 설치 전의 상태와 다르게 동작합니다. 가장 뚜렷한 변화로는 원치 않는 팝업 창, 숨겨진 프로세스 활성화 및 실행, 시스템 리소스 사용량 증가, 검색 결과 변경, 응용 프로그램과 원격 서버의 통신 등이 있습니다.
- **사용자에게 안전하지 않은 응용 프로그램** - 이러한 응용 프로그램은 사용자가 모르는 상태에서 설치되는 경우 공격자가 악용할 수 있는 적법한 상용 소프트웨어입니다. 이 분류에는 원격 접근 도구 등의 프로그램이 포함되므로 이 옵션은 기본적으로 비활성화됩니다.

치료

치료 설정에 따라 검사기가 감염된 파일을 치료하는 방식이 결정됩니다. 치료 수준에는 다음과 같은 세 가지가 있습니다.

- **치료 안 함** - 감염된 파일을 자동으로 치료하지 않습니다. 프로그램에 표시되는 경고 창을 통해 사용자가 동작을 선택할 수 있습니다.
- **표준 치료** - 감염된 파일을 프로그램이 자동 치료하거나 삭제합니다. 적절한 동작을 자동으로 선택할 수 없는 경우, 프로그램에서는 후속 동작 선택 항목을 표시합니다. 미리 정의된 동작을 완료할 수 없는 경우에도 후속 동작 선택 항목이 표시됩니다.
- **엄격한 치료** - 프로그램이 압축파일을 포함하여 감염된 파일을 모두 치료 또는 삭제합니다. 단, 시스템 파일의 경우는 예외입니다. 감염된 파일을 치료할 수 없는 경우 경고 창에 수행할 수 있는 동작이 표시됩니다.

경고: 기본값인 표준 치료 모드에서는 포함된 파일이 모두 감염된 경우에만 전체 압축파일을 삭제합니다. 적법한 파일이 함께 포함되어 있는 압축파일은 삭제되지 않습니다. 엄격한 치료 모드에서는 감염된 압축파일이 검출되면 감염되지 않은 파일이 포함되어 있더라도 전체 압축파일이 삭제됩니다.

확장명

확장명은 파일 이름에서 마침표 뒤에 있는 부분으로, 파일의 형식과 내용을 정의합니다. 엔진 파라미터 설정의 이 섹션에서는 검사에서 제외할 파일 형식을 정의할 수 있습니다.

기본적으로 확장명에 관계없이 모든 파일을 검사합니다. 검사에서 제외되는 파일 목록에 원하는 확장명을 추가할 수 있습니다. **추가** 및 **제거** 버튼을 사용하면 원하는 확장명의 검사를 활성화하거나 금지할 수 있습니다.

특정 파일 형식을 검사하면 프로그램이 제대로 실행되지 않는 경우 해당 파일 확장명을 검사에서 제외해야 할 수 있습니다. 예를 들어 .log, .cfg 및 .tmp 확장명은 제외하는 것이 좋습니다.

제한

제한 섹션에서는 최대 오브젝트 크기와 검사할 다중 압축파일 수준을 지정할 수 있습니다.

- **최대 크기:** 검사할 오브젝트의 최대 크기를 정의합니다. 안티바이러스 모듈에서는 지정한 크기보다 작은 오브젝트만 검사합니다. 일반적으로는 기본값을 수정할 필요가 없으므로 변경하지 않는 것이 좋습니다. 큰 오브젝트를 검사에서 제외해야 하는 특별한 이유가 있는 고급 사용자만 이 옵션을 변경할 수 있습니다.
- **최대 검사 시간:** 오브젝트 검사에 할당되는 최대 시간을 정의합니다. 여기에 사용자 정의 값을 입력한 경우 해당 시간이 지나면 검사 완료 여부에 관계없이 안티바이러스 모듈이 오브젝트 검사를 중지합니다.
- **최대 다중 압축 수준:** 최대 압축파일 검사 수준을 지정합니다. 일반적인 상황에서는 기본값을 수정할 필요가 없으므로 기본값인 10을 변경하지 않는 것이 좋습니다. 다중 압축파일 수로 인해 검사가 중간에 종료된 경우 압축파일은 검사되지 않은 상태로 유지됩니다.
- **최대 파일 크기:** 이 옵션을 사용하면 검사할 압축파일에 포함된 파일의 최대 파일 크기(압축 해제 시)를 지정할 수 있습니다. 이 제한으로 인해 검사가 중간에 종료된 경우 압축파일은 검사되지 않은 상태로 유지됩니다.

기타

스마트 최적화를 활성화하면 가장 효율적인 검사 수준과 최고 검사 속도를 유지하기 위한 최적의 설정이 사용됩니다. 다양한 보호 모듈이 여러 검사 방법을 활용하고 해당 방법을 특정 파일 형식에 적용하는 방식으로 지능적 검사를 수행합니다. 스마트 최적화는 제품 내에 엄밀하게 정의되어 있지는 않습니다. 개발 팀에서는 새로운 변경 사항을 지속적으로 구현하고 있으며, 이러한 변경 사항은 정기적인 업데이트를 통해 System Center Endpoint Protection에 통합됩니다. 스마트 최적화를 비활성화하면 검사를 수행할 때 특정 모듈의 엔진 코어에서 사용자가 정의한 설정만 적용됩니다.

ADS(대체 데이터 스트림) 검사(수동 검사기에만 해당됨)
파일 시스템에서 사용되는 ADS(대체 데이터 스트림)(리소스/데이터 분기)는 일반 검사 기술을 사용할 때는 표시되지 않는 파일 및 폴더 연결입니다. 대체 데이터 스트림으로 가장하여 검출을 피하려고 하는 침입이 많이 있습니다.

침입이 검출됨

웹 페이지, 공유 폴더, 이메일 또는 이동식 컴퓨터 장치(USB, 외부 디스크, CD, DVD, 디스켓 등)와 같은 시스템의 여러 진입점에서 침입이 발생할 수 있습니다.

컴퓨터가 맬웨어에 감염된 증상(예: 속도가 느려짐, 작동이 자주 중단됨 등)을 보이면 다음 단계를 수행하는 것이 좋습니다.

1. System Center Endpoint Protection을 열고 **컴퓨터 검사**를 클릭합니다.
2. **스마트 검사**(자세한 내용은 스마트 검사 12 섹션 참조)를 클릭합니다.
3. 검사를 마치면 검사한 파일, 감염된 파일 및 치료된 파일 수가 표시된 로그를 검토합니다.

디스크의 특정 부분만 검사하려면 **사용자 지정 검사**를 클릭하고 바이러스를 검사할 대상을 선택합니다.

System Center Endpoint Protection에서 침입을 처리하는 방법의 일반적인 예로, 기본 치료 수준을 사용하는 실시간 파일 시스템 모니터에서 침입이 검출되었다고 가정합니다. 이 경우 파일 시스템 모니터는 파일을 치료 또는 삭제하려고 합니다. 실시간 보호 모듈에 대해 수행 가능한 동작이 미리 정의되어 있지 않으면 경고 창에 옵션을 선택하라는 메시지가 표시됩니다. 일반적으로 **치료**, **삭제** 및 **무시** 옵션을 사용할 수 있습니다. 감염된 파일을 그대로 유지하는 **무시**는 선택하지 않는 것이 좋습니다. 단, 파일이 무해하며 잘못 검출된 것이 확실하다면 무시를 선택해도 됩니다.

치료 및 삭제 - 파일에 악성 코드를 첨부하는 바이러스에 의해 파일이 공격을 받았다면 치료를 적용합니다. 이 경우라면 먼저 감염된 파일을 치료해 원래 상태로 복원합니다. 악성 코드만 포함된 파일은 삭제됩니다.

압축파일의 파일 삭제 - 기본 치료 모드에서는 압축파일에 감염된 파일이 포함되어 있으며, 감염되지 않은 파일은 없는 경우에만 전체 압축파일을 삭제합니다. 즉, 무해하며 감염되지 않는 파일이 압축파일에 포함되어 있다면 압축파일은 삭제되지 않는다는 의미입니다. 그러나 **엄격한 치료** 모드에서는 감염된 파일이 하나라도 포함되어 있으면 압축파일 내의 다른 파일의 상태는 관계없이 압축파일을 삭제하므로, 이를 수행하는 경우에는 주의해야 합니다.

프로그램 업데이트

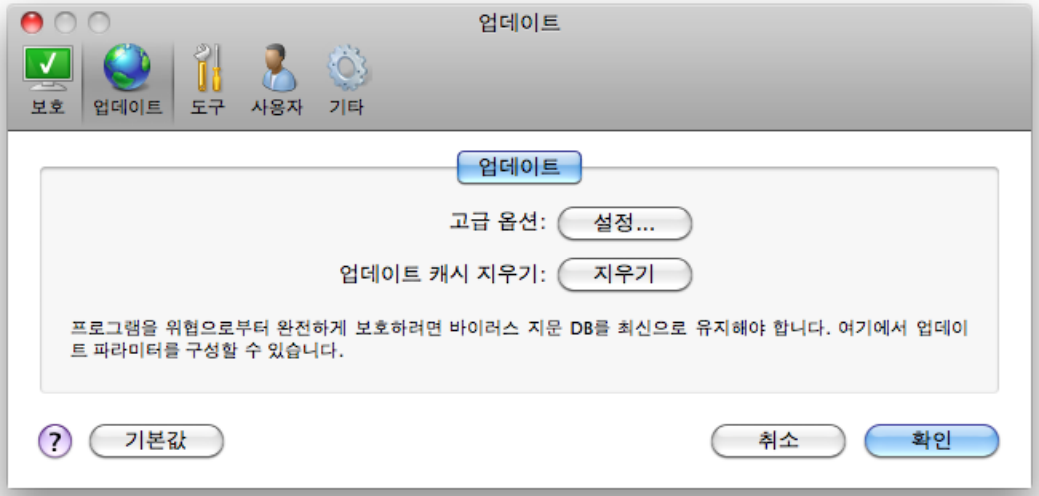
보안을 최고 수준으로 유지하려면 System Center Endpoint Protection을 정기적으로 업데이트해야 합니다. 업데이트 모듈을 사용하면 최신 바이러스 시그니처 DB를 다운로드하여 프로그램을 항상 최신 상태로 유지할 수 있습니다.

기본 메뉴에서 **업데이트**를 클릭하면 마지막으로 성공한 업데이트 날짜 및 시간, 업데이트가 필요한지 여부 등 현재 업데이트 상태를 확인할 수 있습니다. 업데이트 프로세스를 수동으로 시작하려면 **바이러스 시그니처 DB 업데이트**를 클릭합니다.

일반적인 환경에서 업데이트가 제대로 다운로드되면 *업데이트할 필요가 없습니다. 설치된 바이러스 시그니처 DB가 최신 버전입니다.*라는 메시지가 업데이트 창에 나타납니다.

업데이트 창에는 바이러스 시그니처 DB 버전에 대한 정보도 포함되어 있습니다. 이 숫자 표시기는 웹 사이트에 대한 활성 링크로서 지정된 업데이트 중에 추가된 모든 시그니처가 나열되어 있습니다.

업데이트 설정



테스트 모드 사용을 활성화하고 해당 업데이트를 다운로드하려면 **고급 옵션** 옆의 **설정...** 버튼을 클릭하고 **테스트 모드 활성화** 확인란을 선택합니다. 각 업데이트가 성공한 후에 표시되는 시스템 트레이 알림을 비활성화하려면 **성공한 업데이트에 대한 알림 표시 안 함** 확인란을 선택합니다.

임시로 저장된 업데이트 데이터를 모두 삭제하려면 **업데이트 캐시 지우기** 옆의 **지우기** 버튼을 클릭합니다. 이 옵션은 업데이트 중에 문제가 발생하는 경우 사용하십시오.

업데이트 작업을 생성하는 방법

기본 메뉴에서 **업데이트**를 클릭한 후 표시되는 기본 창에서 **바이러스 시그니처 DB 업데이트**를 클릭하여 수동으로 업데이트를 트리거할 수 있습니다.

또한 예약된 작업으로 업데이트를 실행할 수도 있습니다. 예약된 작업을 구성하려면 **도구** > **스케줄러**를 클릭합니다. 기본적으로 System Center Endpoint Protection에는 다음 작업이 활성화되어 있습니다.

- **정기적 자동 업데이트**
- **사용자 로그온 후 자동 업데이트**

필요에 맞게 각 업데이트 작업을 수정할 수 있습니다. 기본 업데이트 작업 외에 사용자 정의 구성을 사용하여 새 업데이트 작업을 생성할 수 있습니다. 업데이트 작업 생성 및 구성에 대한 자세한 내용은 스케줄러 18 섹션을 참조하십시오.

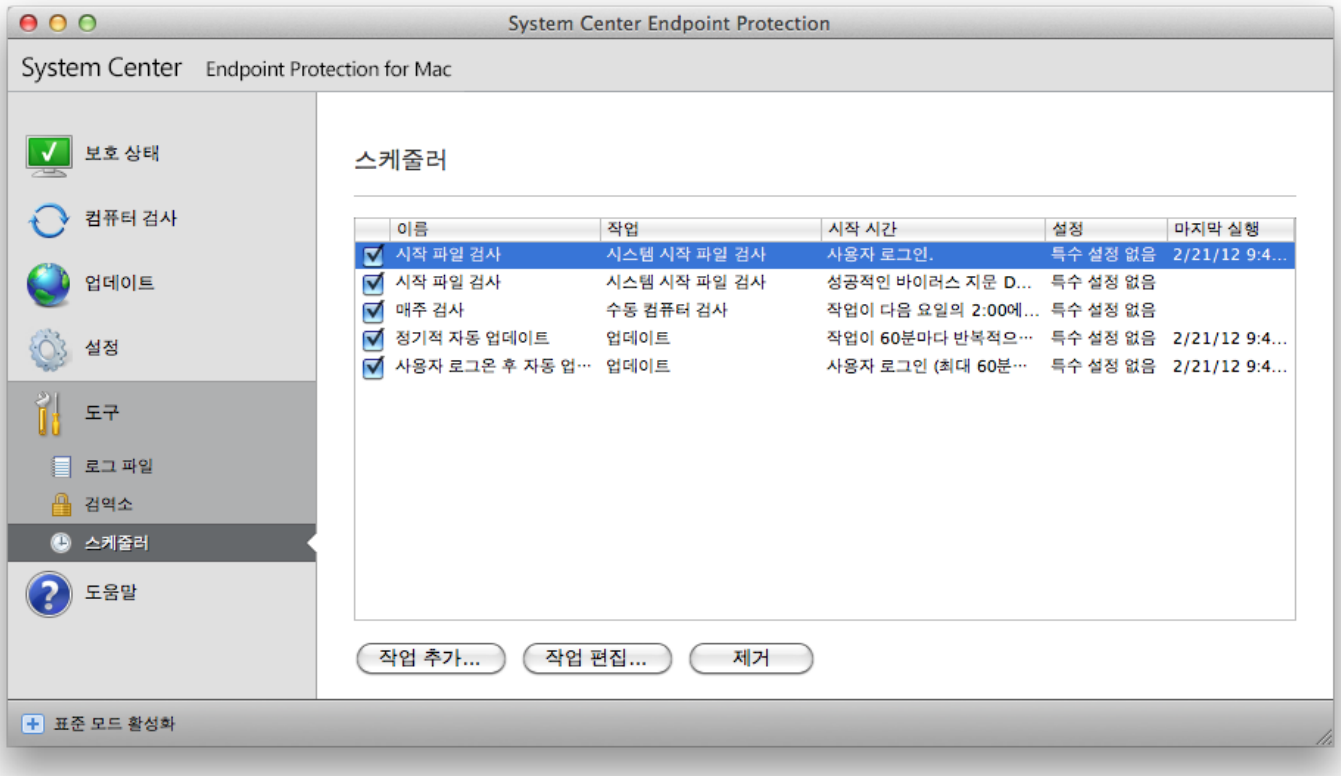
새 빌드로 업그레이드

보호 기능을 최대화하려면 최신 System Center Endpoint Protection 빌드를 사용해야 합니다. 새 버전을 확인하려면 왼쪽의 기본 메뉴에서 **업데이트**를 클릭합니다. 새 빌드를 사용할 수 있는 경우 창 아래쪽에 *새 버전의 제품이 출시되었습니다!*가 표시됩니다. **자세히...**를 클릭하면 새 빌드의 버전 번호와 변경 로그가 포함된 새 창이 표시됩니다.

최신 빌드를 다운로드하려면 **다운로드**를 클릭합니다. 창을 닫고 업그레이드를 나중에 다운로드하려면 **닫기**를 클릭합니다.

스케줄러

System Center Endpoint Protection의 고급 모드가 활성화되어 있으면 **스케줄러**를 사용할 수 있습니다. 스케줄러는 System Center Endpoint Protection 기본 메뉴의 **도구**에 있습니다. **스케줄러**에는 모든 예약된 작업 및 구성 속성(예: 미리 정의된 날짜, 시간 및 사용된 검사 프로필) 목록이 포함되어 있습니다.



기본적으로 스케줄러에는 다음과 같은 예약된 작업이 표시됩니다.

- 정기적 자동 업데이트
- 사용자 로그온 후 자동 업데이트
- 사용자 로그온 후 시작 파일 검사
- 바이러스 시그니처 DB 업데이트 후 시작 파일 검사
- 로그 유지 관리(스케줄러 설정에서 **시스템 작업 표시** 옵션을 활성화하고 나면 표시됨)
- 매주 검사

예약된 기존 작업(기본 작업 및 사용자 정의 작업 모두 포함)의 구성을 편집하려면 Ctrl 키를 누르고 수정할 작업을 클릭한 후에 **편집...**을 선택하거나 작업을 선택하고 **작업 편집...** 버튼을 클릭합니다.

작업을 예약하는 목적

스케줄러는 미리 정의된 구성 및 속성을 사용하여 예약된 작업을 관리하고 시작합니다. 구성 및 속성에는 작업 실행 중 사용하도록 지정한 프로필을 비롯하여 날짜 및 시간과 같은 정보가 포함됩니다.

새 작업 생성

스케줄러에서 새 작업을 생성하려면 **작업 추가...** 버튼을 클릭하거나 Ctrl 키를 누르고 빈 필드를 클릭한 후에 오른쪽 마우스 버튼 메뉴에서 **추가...**를 선택합니다. 예약된 작업 유형에는 다음과 같이 다섯 가지가 있습니다.

- **응용 프로그램 실행**
- **업데이트**
- **로그 유지 관리**
- **수동 검사**
- **시스템 시작 파일 검사**

업데이트는 가장 자주 사용되는 예약된 작업 중 하나이므로 아래에서는 새 업데이트 작업을 추가하는 방법에 대해 설명합니다.

예약된 작업 드롭다운 메뉴에서 **업데이트**를 선택합니다. **작업 이름** 필드에 작업의 이름을 입력합니다. **작업 실행** 드롭다운 메뉴에서는 작업 빈도를 선택합니다. 사용할 수 있는 옵션은 다음과 같습니다. **사용자 정의**, **한 번**, **반복적으로**, **매일**, **매주** 및 **이벤트가 트리거됨** 선택한 빈도에 따라 서로 다른 업데이트 파라미터가 포함된 메시지가 표시됩니다.

사용자 정의를 선택한 경우 cron 형식으로 날짜/시간을 지정하라는 메시지가 표시됩니다(자세한 내용은 사용자 정의 작업 생성 19 섹션 참조).

그런 다음 예약된 시간에 작업을 수행하거나 완료할 수 없는 경우 수행할 동작을 정의합니다. 다음과 같은 세 가지 옵션을 사용할 수 있습니다.

- **다음 예약 시간까지 대기**
- **최대한 빨리 작업 실행**
- **마지막으로 실행한 이후 시간이 지정된 간격을 초과한 경우 즉시 작업 실행**(**최소 작업 간격** 옵션을 사용하여 간격 정의 가능)

다음 단계에서는 현재 예약된 작업에 대한 정보가 포함된 요약 창이 표시됩니다. **마침** 버튼을 클릭합니다.

새로 예약된 작업이 현재 예약된 작업 목록에 추가됩니다.

기본적으로 시스템에는 제품 기능의 정상 작동을 위한 필수 예약 작업이 포함되어 있습니다. 이러한 작업은 변경해서는 안 되며, 기본적으로 숨겨집니다. 이 옵션을 변경하여 필수 예약 작업을 표시하려면 **설정** > **응용 프로그램 기본 설정 입력...** > **도구** > **스케줄러**로 이동한 다음 **시스템 작업 표시** 옵션을 선택합니다.

사용자 정의 작업 생성

사용자 정의 작업의 날짜와 시간은 연도 연장 cron 형식(공백으로 구분된 6개의 필드를 구성하는 문자열)으로 입력해야 합니다.
분(0-59) 시(0-23) 일(1-31) 월(1-12) 연도(1970-2099) 주(0-7) (일요일 = 0 또는 7)

예:
```
30 6 22 3 2012 4
```

cron 표현식에 지원되는 특수 문자는 다음과 같습니다.
- 별표(*) - 표현식이 필드의 모든 값과 일치합니다(예를 들어 세 번째 필드(일)에 별표가 표시된 경우 1-31까지 모든 일을 의미함)
- 하이픈(-) - 범위를 정의합니다(예: `3-9`
- 쉼표(,) - 목록의 항목을 구분합니다(예: `1,3,7,8`
- 슬래시(/) - 범위 증분을 정의합니다(예를 들어 세 번째 필드(일)에 `3-28/5` 가 표시된 경우 해당 월의 세 번째 일에 실행되고 그 이후 5일마다 실행됨을 의미함).

일 이름(월요일-일요일)과 월 이름(1월-12월)은 지원되지 않습니다.

참고: 일과 주를 모두 정의한 경우에는 두 필드가 일치할 때만 명령이 실행됩니다.

검역소

검역소의 기본 작업은 감염된 파일을 안전하게 저장하는 것입니다. 치료할 수 없는 파일, 안전하지 않거나 삭제하는 것이 좋은 파일 또는 System Center Endpoint Protection에서 잘못 검출된 파일은 검역소로 보내야 합니다.

모든 파일을 검역소로 보내도록 선택할 수 있습니다. 동작이 의심스럽지만 안티바이러스 검사기에서 검색되지 않는 파일은 검역소로 보내는 것이 좋습니다.

검역소 폴더에 저장된 파일은 표로 볼 수 있습니다. 이 표에는 검역소로 보낸 날짜 및 시간, 감염된 파일의 원래 위치 경로, 파일 크기(바이트), 이유(예: 사용자가 추가함)와 위협 수(예: 여러 침입이 포함된 압축파일의 경우)가 표시됩니다. 검역소로 보낸 파일이 들어 있는 검역소 폴더(/Library/Application Support/Microsoft/scep/cache/quarantine)는 System Center Endpoint Protection 제거 후에도 시스템에 유지됩니다. 검역소로 보낸 파일은 안전하게 암호화된 형식으로 저장되며 System Center Endpoint Protection 설치 후 다시 복원할 수 있습니다.

파일을 검역소로 보내기

System Center Endpoint Protection에서는 삭제된 파일을 자동으로 검역소로 보냅니다(경고 창에서 이 옵션을 취소하지 않은 경우). 원하는 경우 **검역소...** 버튼을 클릭하여 감염 의심 파일을 수동으로 검역소로 보낼 수 있습니다. 오른쪽 마우스 버튼 메뉴를 사용할 수도 있습니다. 이렇게 하려면 Ctrl 키를 누르고 빈 필드를 클릭한 후에 **검역소...**를 선택하고 검역소로 보낼 파일을 선택한 다음 **열기** 버튼을 클릭합니다.

검역소에서 복원

검역소에 있는 파일을 원래 위치로 복원할 수도 있습니다. 이렇게 하려면 **복원** 버튼을 사용합니다. 오른쪽 마우스 버튼 메뉴를 통해 복원할 수도 있습니다. 이렇게 하려면 Ctrl 키를 누르고 **검역소** 창에서 지정된 파일을 클릭한 후에 **복원**을 클릭합니다. 오른쪽 마우스 버튼 메뉴에는 파일이 삭제된 위치 이외의 위치로 파일을 복원할 수 있는 **복원 대상...** 옵션도 있습니다.

로그 파일

로그 파일은 발생한 모든 중요 프로그램 이벤트에 대한 정보를 포함하고 있고 검출된 위협에 대한 개요를 제공합니다. 로깅은 시스템을 분석하고, 위협을 검출하고, 문제를 해결하는 데 사용하는 기본 도구입니다. 로깅은 사용자 상호 작용 없이 백그라운드에서 수행됩니다. 정보는 현재 로그 상세 수준 설정에 따라 기록됩니다. System Center Endpoint Protection 환경에서 직접 텍스트 메시지 및 로그뿐만 아니라 압축파일 로그를 볼 수 있습니다.

System Center Endpoint Protection 기본 메뉴에서 **도구** > **로그 파일**을 클릭하여 로그 파일에 접근할 수 있습니다. 창 맨 위에 있는 **로그** 드롭다운 메뉴를 사용하여 원하는 로그 유형을 선택합니다. 다음과 같은 로그를 사용할 수 있습니다.

1. **검출된 위협** - 침입 검출과 관련된 이벤트에 대한 모든 정보를 확인하려면 이 옵션을 사용합니다.
2. **이벤트** - 이 옵션은 시스템 관리자 및 사용자가 문제를 해결하는 데 사용하도록 고안되었습니다. System Center Endpoint Protection에서 수행한 중요한 모든 동작이 이벤트 로그에 기록됩니다.
3. **컴퓨터 검사** - 모든 완료된 검사의 결과가 이 창에 표시됩니다. 각 수동 검사의 상세 정보를 보려면 항목을 두 번 클릭합니다.

각 섹션에 표시된 정보는 항목을 선택하고 **복사** 버튼을 클릭하여 클립보드로 직접 복사할 수 있습니다.

로그 유지 관리

기본 프로그램 창에서 System Center Endpoint Protection의 로깅 구성에 접근할 수 있습니다. **설정** > **응용 프로그램 기본 설정 입력...** > **도구** > **로그 파일**을 클릭합니다. 다음과 같은 옵션을 지정하여 로그 파일에 사용할 수 있습니다.

- **오래된 로그 기록 자동 삭제** - 지정한 기간(일)보다 오래된 로그 항목이 자동으로 삭제됩니다.
- **로그 파일 자동 최적화** - 사용되지 않는 레코드 수가 지정한 비율을 초과하면 로그 파일 자동 조각 모음을 활성화합니다.

그래픽 사용자 인터페이스에 표시된 모든 관련 정보, 위협 및 이벤트 메시지는 일반 텍스트 또는 CSV(쉼표로 구분된 값) 형식과 같이 사람이 읽을 수 있는 텍스트 형식으로 저장할 수 있습니다. 이러한 파일을 타사 도구를 사용하여 처리할 수 있게 하려면 **텍스트 파일에 로깅 활성화** 옆의 확인란을 선택합니다.

로그 파일을 저장할 대상 폴더를 정의하려면 **고급 설정** 옆의 **설정...**을 클릭합니다.

텍스트 로그 파일: 편집 아래에서 선택한 옵션에 따라 다음 정보가 포함된 로그를 저장할 수 있습니다.

- 시작 검사기, 실시간 보호 또는 컴퓨터 검사에서 검출한 위협은 threatslog.txt로 이름이 지정된 파일에 저장됩니다.
- *잘못된 사용자 이름 및 비밀번호*, *바이러스 시그니처 DB를 업데이트할 수 없습니다.* 등의 이벤트는 eventslog.txt 파일에 작성됩니다.
- 모든 완료된 검사의 결과는 scanlog.숫자.txt 형식으로 저장됩니다.

기본 컴퓨터 검사 로그 기록 필터를 구성하려면 이 옵션 바로 옆의 **편집...** 버튼을 클릭하고 로그 유형을 필요한 대로 선택하거나 선택 취소합니다. 이러한 로그 유형에 대한 자세한 설명은 이 장 21에서 확인할 수 있습니다.

로그 필터링

로그는 중요한 시스템 이벤트에 대한 정보를 저장합니다. 로그 필터링 기능을 사용하여 특정 유형의 이벤트에 대한 레코드를 표시할 수 있습니다.

가장 자주 사용되는 로그 유형은 다음과 같습니다.

- **주요 경고** - 안티바이러스 보호가 시작되지 않는 등의 심각한 시스템 오류
- **오류** - "*파일을 다운로드하는 중 오류 발생*"과 같은 오류 메시지 및 심각한 오류
- **경고** - 경고 메시지
- **정보 레코드** - 업데이트 성공, 경고 등의 정보 메시지
- **진단 레코드** - 위에 설명된 모든 레코드 및 프로그램 미세 조정에 필요한 정보.

사용자 인터페이스

System Center Endpoint Protection의 사용자 인터페이스 구성 옵션을 통해 필요에 따라 작업 환경을 조정할 수 있습니다. **설정** > **응용 프로그램 기본 설정 입력...** > **사용자** > **인터페이스**에서 이러한 구성 옵션에 접근할 수 있습니다.

이 섹션에서 고급 모드 옵션을 사용하여 고급 모드로 전환할 수 있습니다. 고급 모드에는 System Center Endpoint Protection에 대한 상세 설정 및 추가 컨트롤이 표시됩니다.

시작 화면 기능을 활성화하려면 **시작할 때 시작 화면 표시** 옵션을 선택합니다.

표준 메뉴 사용 섹션에서는 **표준 모드/고급 모드** 옵션을 선택하여 개별 표시 모드의 기본 프로그램 창에서 표준 메뉴를 사용하도록 할 수 있습니다.

툴팁을 활성화하려면 **툴팁 표시** 옵션을 선택합니다. **숨겨진 파일 표시** 옵션을 사용하면 **컴퓨터 검사**의 **검사 대상** 설정에서 숨겨진 파일을 확인 및 선택할 수 있습니다.

경고 및 알림

경고 및 알림 섹션에서는 System Center Endpoint Protection에서 경고 및 시스템 알림을 처리하는 방법을 구성할 수 있습니다.

경고 표시 옵션을 비활성화하면 모든 경고 창이 취소되므로 특수한 상황에만 이 옵션을 비활성화해야 합니다. 대부분의 사용자의 경우 이 옵션을 기본 설정(활성화)으로 두는 것이 좋습니다.

바탕 화면에 알림 표시 옵션을 선택하면 경고 창이 활성화됩니다. 이 창은 사용자가 상호 작용을 수행하지 않아도 바탕 화면(기본적으로 화면 오른쪽 위)에 표시됩니다. **다음 시간 후 자동으로 알림 닫기** X **초** 값을 조정하여 알림을 표시할 기간을 정의할 수 있습니다.

경고 및 알림 고급 설정

사용자 상호 작용이 필요한 알림만 표시(I)
이 옵션을 사용하면 사용자 상호 작용이 필요한 메시지 표시를 전환할 수 있습니다.

전체 화면 모드로 응용 프로그램을 실행할 때 사용자 상호 작용이 필요한 알림만 표시(F)
이 옵션은 전체 화면에 표시해야 하는 프레젠테이션 또는 기타 작업을 수행할 때 유용합니다.

권한

조직의 보안 정책에 있어 System Center Endpoint Protection 설정은 매우 중요할 수 있습니다. 무단 수정은 시스템의 안정성과 보호 상태를 위험하게 할 수 있습니다. 따라서 프로그램 구성 편집 권한을 부여할 사용자를 선택할 수 있습니다.

권한 있는 사용자를 지정하려면 **설정** > **응용 프로그램 기본 설정 입력...** > **사용자** > **권한**으로 이동합니다.

시스템을 최대한 보호하려면 프로그램을 올바르게 구성해야 합니다. 구성을 무단으로 수정하면 중요한 데이터가 손실될 수 있습니다. 권한 있는 사용자 목록을 설정하려면 왼쪽의 **사용자** 목록에서 사용자를 선택하고 **추가** 버튼을 클릭하면 됩니다. 사용자를 제거하려면 오른쪽의 **권한 있는 사용자** 목록에서 사용자 이름을 선택하고 **제거**를 클릭합니다.

참고: 권한 있는 사용자 목록을 비워 두면 시스템의 모든 사용자에게 프로그램 설정 편집 권한이 부여됩니다.

오른쪽 마우스 버튼 메뉴

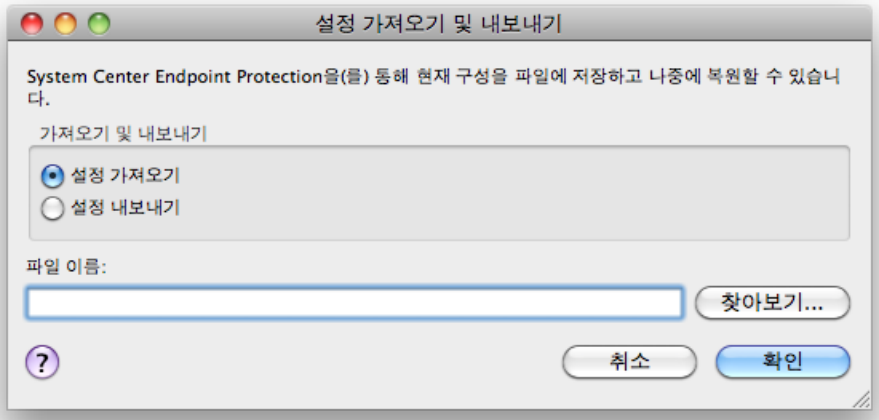
설정 > **응용 프로그램 기본 설정 입력...** > **사용자** > **오른쪽 마우스 버튼 메뉴** 섹션에서 **오른쪽 마우스 버튼 메뉴로 통합** 확인란을 활성화하여 오른쪽 마우스 버튼 메뉴 통합을 활성화할 수 있습니다.

고급 사용자

설정 가져오기 및 내보내기

System Center Endpoint Protection의 구성은 고급 모드의 **설정**에서 가져오거나 내보낼 수 있습니다.

가져오기 및 내보내기 모두 압축파일을 사용하여 구성을 저장합니다. 가져오기 및 내보내기는 나중에 사용할 수 있도록 현재 System Center Endpoint Protection 구성을 백업해야 하는 경우 유용합니다. 또한 구성 파일을 가져와서 원하는 설정을 쉽게 전송할 수 있으므로, 내보내기 설정 옵션은 여러 시스템에서 System Center Endpoint Protection의 기본 설정 구성을 사용하려는 사용자에게 편리한 옵션입니다.



설정 가져오기

구성을 가져오는 것은 매우 쉽습니다. 주 메뉴에서 **설정** > **설정 가져오기 및 내보내기...**를 클릭한 다음 **설정 가져오기** 옵션을 선택합니다. 구성 파일의 이름을 입력하거나 **찾아보기...** 버튼을 클릭하여 가져올 구성 파일을 찾습니다.

설정 내보내기

구성을 내보내는 단계는 매우 유사합니다. 주 메뉴에서 **설정** > **설정 가져오기 및 내보내기...**를 클릭합니다. **설정 내보내기** 옵션을 선택하고 구성 파일의 이름을 입력합니다. 브라우저를 사용하여 구성 파일을 저장할 컴퓨터 위치를 선택합니다.

프록시 서버 설정

프록시 서버 설정은 **기타** > **프록시 서버**에서 구성할 수 있습니다. 이 수준에서 프록시 서버를 지정하면 모든 System Center Endpoint Protection 기능에 대한 전체 프록시 서버 설정이 정의됩니다. 여기의 파라미터는 인터넷 연결이 필요한 모든 모듈에서 사용됩니다.

이 수준에 대한 프록시 서버 설정을 지정하려면 **프록시 서버 사용** 확인란을 선택한 다음 **프록시 서버** 필드에 프록시 서버 URL이나 IP 주소를 입력합니다. 포트 필드에 프록시 서버가 연결을 허용하는 포트(기본적으로 3128)를 지정합니다. 프록시 서버와의 통신에 인증이 필요한 경우 **프록시 서버에 인증 필요** 확인란을 선택한 다음 각 필드에 올바른 **사용자 이름** 및 **비밀번호**를 입력합니다.

이동식 미디어 차단

CD나 USB 키 등의 이동식 미디어에 악성 코드가 포함되어 컴퓨터가 위험해질 수 있습니다. 이동식 미디어를 차단하려면 **이동식 미디어 차단 활성화** 옆의 확인란을 선택합니다. 특정 미디어 유형에 대한 접근을 허용하려면 허용을 원하는 미디어 유형 옆의 확인란을 선택 취소합니다.

이러한 설정을 CD, DVD, FireWire 또는 USB 이외의 미디어 유형에 적용하려면 **기타** 옆의 확인란을 선택합니다. 이 설정은 특히 컴퓨터에 연결된 모든 주변기기에 Thunderbolt 인터페이스를 통해 적용됩니다.

용어집

침입 유형

침입은 사용자 컴퓨터에 침입하여 손상시키려는 악의적인 소프트웨어의 한 종류입니다.

바이러스

컴퓨터 바이러스는 컴퓨터에 있는 기존 파일을 손상시키는 침입입니다. 컴퓨터 간에 확산되는 방식이 생물학적 바이러스와 유사해서 바이러스라고 명명되었습니다.

컴퓨터 바이러스는 주로 실행 파일, 스크립트 및 문서를 공격합니다. 바이러스는 복제하기 위해 자신의 "몸체"를 대상 파일의 끝에 첨부합니다. 간단히 말하자면 컴퓨터 바이러스는 감염된 파일이 실행되면 원래 응용 프로그램보다 먼저 자신을 활성화하여 미리 정의된 작업을 수행합니다. 그런 후에만 원래 응용 프로그램이 실행될 수 있습니다. 사용자가 실수로 또는 의도적으로 악성 프로그램을 실행하거나 열지 않으면 바이러스는 컴퓨터를 감염시킬 수 없습니다.

컴퓨터 바이러스는 목적 및 심각도에 따라 등급을 지정할 수 있습니다. 일부 바이러스는 하드 드라이브에서 파일을 의도적으로 삭제할 수 있으므로 매우 위험합니다. 반면에 어떤 바이러스는 손상을 일으키지는 않고 사용자를 귀찮게 하거나 바이러스 작성자의 기술을 보여주기만 합니다.

트로잔 목마 또는 스파이웨어와 비교했을 때 바이러스는 악성 소프트웨어 작성자에게 상업적 이득을 가져다 주지 않으므로 점차적으로 줄어드는 추세입니다. 또한 "바이러스"라는 용어는 종종 모든 유형의 침입을 나타내는 데 잘못 사용되고 있습니다. 이러한 사용은 점차적으로 없어지고 보다 정확한 새로운 용어인 "맬웨어"(악성 소프트웨어)로 대체되고 있습니다.

컴퓨터가 바이러스에 감염되면 감염된 파일을 원래 상태로 복원해야 합니다. 즉, 안티바이러스 프로그램을 사용하여 해당 파일을 치료해야 합니다.

바이러스의 예로는 OneHalf, Tenga, Yankee Doodle 등이 있습니다.

웜

컴퓨터 웜은 호스트 컴퓨터를 공격하고 네트워크를 통해 유포되는 악성 코드가 포함된 프로그램입니다. 바이러스와 웜의 기본적인 차이점은 웜의 경우 스스로 복제하여 이동한다는 데 있습니다. 웜은 호스트 파일(또는 부트 영역)과 관계가 없습니다. 웜은 연락처 목록의 이메일 주소를 통해 확산되거나 네트워크 응용 프로그램의 보안 취약점을 악용합니다.

따라서 웜은 컴퓨터 바이러스보다 더 쉽게 확산됩니다. 인터넷이 널리 보급됨에 따라 웜은 유포 시점부터 몇 시간, 심지어는 단 몇 분 내에 전 세계에 퍼질 수 있습니다. 웜은 독립적으로 빠르게 복제가 가능하므로 다른 유형의 맬웨어보다 훨씬 더 위험합니다.

시스템에서 활성화된 웜은 파일을 삭제하거나, 시스템 성능을 저하시키거나, 심지어 프로그램을 비활성화하기도 하는 등 다양한 문제를 야기할 수 있습니다. 컴퓨터 웜은 그 특성상 다른 유형의 침입에 대한 "전송 수단"의 역할을 합니다.

컴퓨터가 웜에 감염되면 악성 코드가 포함되어 있을 수 있으므로 감염된 파일을 삭제하는 것이 좋습니다.

잘 알려진 웜의 예로는 Lovsan/Blaster, Stration/Warezov, Bagle, Netsky 등이 있습니다.

트로잔 목마

지금까지 컴퓨터 트로잔 목마는 유용한 프로그램으로 가장해 사용자를 속여서 프로그램을 실행하도록 하는 침입 범주의 하나로 정의되어 왔습니다. 그러나 트로잔 목마는 더 이상 유용한 프로그램으로 가장할 필요가 없습니다. 트로잔 목마의 유일한 목적은 가능한 한 쉽게 침입하여 악의적인 목적을 달성하는 데 있습니다. "트로잔 목마"는 특정 범주의 침입에 국한되지 않고 모든 침입을 나타내는 매우 일반적인 용어가 되었습니다.

트로잔 목마는 매우 광범위한 범주이므로 대개 다음과 같은 여러 가지 하위 범주로 구분됩니다.

- 다운로더 - 인터넷에서 다른 침입을 다운로드할 수 있는 기능을 갖춘 악성 프로그램입니다.
- 드롭퍼 - 손상된 컴퓨터에 다른 유형의 맬웨어를 설치하도록 고안된 트로잔 목마의 한 유형입니다.

- 백도어 - 원격 공격자와 통신하여 원격 공격자가 시스템에 대한 접근 권한을 얻어 해당 시스템을 제어할 수 있도록 하는 응용 프로그램입니다.
- 키로거 - 키스트로크 로거의 줄임말. 사용자가 입력한 각 키 입력을 기록하여 원격 공격자에게 해당 정보를 보내는 프로그램입니다.
- 다이얼러 - 할증 요금 전화 번호로 연결하도록 고안된 프로그램입니다. 사용자는 새로운 연결이 생성된 것을 거의 알아차릴 수 없습니다. 다이얼러는 일반적으로 사용되지 않는 전화 접속 모뎀을 사용하는 사용자에게만 해를 입힐 수 있습니다.
- 일반적으로 트로잔 목마는 실행 파일 형식입니다. 컴퓨터에 트로잔 목마로 검출된 파일이 있으면 악성 코드가 포함되었을 가능성이 높으므로 해당 파일을 삭제하는 것이 좋습니다.

잘 알려진 트로잔 목마의 예로는 NetBus, Trojandownloader.Small.ZL, Slapper 등이 있습니다.

애드웨어

애드웨어(Adware)는 광고 지원 소프트웨어(advertising-supported software)의 약어입니다. 광고 자료를 표시하는 프로그램이 이러한 범주에 포함됩니다. 일반적으로 애드웨어 응용 프로그램은 자동으로 인터넷 브라우저에 광고가 포함된 새 팝업 창을 열거나 브라우저의 홈페이지를 변경합니다. 애드웨어는 주로 프리웨어 프로그램과 함께 제공되어 프리웨어 프로그램 생성자가 응용 프로그램(일반적으로 유용함)의 개발 비용을 회수할 수 있도록 합니다.

애드웨어 자체는 위험하지 않습니다. 단지 광고 때문에 사용자가 성가실 뿐입니다. 실제로 애드웨어의 위험성은 스파이웨어처럼 추적 기능을 수행할 수도 있다는 데 있습니다.

프리웨어 제품을 사용하려는 경우에는 특히 프로그램 설치에 주의하십시오. 설치 프로그램은 사용자에게 추가 애드웨어 프로그램을 설치한다는 것을 알릴 가능성이 높습니다. 대개 사용자는 애드웨어 설치를 취소하거나 애드웨어를 제외한 채 프로그램을 설치할 수 있습니다.

일부 프로그램의 경우 애드웨어 없이는 설치되지 않거나 기능에 제한이 있습니다. 즉, 대부분의 경우 애드웨어는 사용자가 동의하기 때문에 시스템에 "합법적인" 방법으로 접근할 수 있습니다. 이 경우 나중에 문제가 발생하는 것보다 안전하게 예방하는 것이 더 낫습니다. 컴퓨터에 애드웨어로 검출된 파일이 있으면 악성 코드가 포함되었을 가능성이 높으므로 해당 파일을 삭제하는 것이 좋습니다.

스파이웨어

이 범주에서는 사용자의 동의를 받지 않거나 사용자가 인지하지 못한 상태에서 개인 정보를 전송하는 모든 응용 프로그램에 대해 다룹니다. 스파이웨어는 추적 기능을 사용하여 방문한 웹 사이트 목록, 사용자 연락처 목록의 이메일 주소 또는 기록된 키 입력 목록과 같은 다양한 통계 데이터를 전송합니다.

스파이웨어 작성자는 이러한 기법을 통해 사용자의 요구와 관심에 대해 한층 자세히 파악하여 보다 세분화된 표적 광고를 수행할 수 있다고 주장합니다. 문제는 유용한 응용 프로그램과 악성 응용 프로그램이 명확하게 구분되지 않으며 검색된 정보가 악용되지 않는다는 것을 누구도 확신할 수 없다는 것입니다. 스파이웨어 응용 프로그램으로 획득한 데이터에는 보안 코드, PIN, 은행 계좌 번호 등이 있을 수 있습니다. 스파이웨어는 대개 작성자가 무료 버전 프로그램과 함께 제공하여 수익을 창출하거나 해당 소프트웨어를 구입하도록 유인하는 것이 목적입니다. 사용자는 종종 프로그램 설치 중 스파이웨어의 존재를 알게 되고 스파이웨어가 포함되지 않은 유료 버전으로 업그레이드하도록 유인됩니다.

스파이웨어와 함께 제공되는 잘 알려진 프리웨어 제품으로 P2P(피어 투 피어) 네트워크의 클라이언트 응용 프로그램이 있습니다. Spyfalcon 또는 Spy Sheriff(및 여러 응용 프로그램)는 특정 스파이웨어 하위 범주에 속합니다. 이러한 응용 프로그램은 안티스파이웨어 프로그램처럼 보이지만 실제로는 그 자체가 스파이웨어 프로그램입니다.

컴퓨터에 스파이웨어로 검출된 파일이 있으면 악성 코드가 포함되었을 가능성이 높으므로 해당 파일을 삭제하는 것이 좋습니다.

사용자에게 안전하지 않은 응용 프로그램

네트워크로 연결된 컴퓨터 관리 작업을 간소화하는 여러 가지 적법한 프로그램이 있습니다. 그러나 나쁜 의도를 가진 사용자가 이러한 프로그램을 악의적인 용도로 잘못 사용할 수 있습니다. System Center Endpoint Protection은 이러한 위협을 검출할 수 있는 옵션을 제공합니다.

"잠재적으로 안전하지 않은 응용 프로그램"은 적법한 상용 소프트웨어에 사용되는 분류입니다. 이러한 분류에는 원격 접근 도구, 비밀번호 크랙 응용 프로그램, 키로거(사용자의 각 키 입력을 기록하는 프로그램) 등의 프로그램이 포함됩니다.

자신이 직접 설치하지 않은, 잠재적으로 안전하지 않은 응용 프로그램이 컴퓨터에 있으며 실행 중인 경우 네트워크 관리자에게 문의하거나 해당 응용 프로그램을 제거하십시오.

사용자가 원치 않는 응용 프로그램

잠재적으로 원치 않는 응용 프로그램은 반드시 악성 프로그램은 아니지만 올바르지 않은 방식으로 컴퓨터의 성능에 영향을 줄 수 있습니다. 이러한 응용 프로그램의 경우 보통 설치 동의가 필요합니다. 이러한 응용 프로그램이 컴퓨터에 설치되어 있는 경우 시스템이 응용 프로그램 설치 전과 다르게 동작합니다. 가장 뚜렷한 변화는 다음과 같습니다.

- 이전에는 표시된 적이 없었던 새 창이 열립니다.
- 숨겨진 프로세스가 활성화 및 실행됩니다.
- 시스템 리소스가 더 많이 사용됩니다.
- 검색 결과가 달라집니다.
- 응용 프로그램이 원격 서버와 통신합니다.