McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

사용자 설명서

콘텐츠

제 1 장

소개

McAfee VirusScan Plus 는 악성 공격을 방지하는 예방적 PC 보안을 제공하므로, 고객이 소중히 여기는 것을 보호할 뿐만 아니라, 안심하고 온라인으로 파일을 탐색, 검색 및 다운로드할 수 있습니다. McAfee SiteAdvisor 의 웹 안전 등급을 사용하면 안전하지 않은 웹 사이트를 피할 수 있습니다. 이 서비스는 바이러스 백신, 스파이웨어 차단 및 방화벽 기술을 결합하여 다각적 공격을 방지하기 위한 보안 기능도 제공합니다. McAfee 의 보안 서비스는 보호 기능이 항상 최신 상태를 유지하도록 최신 소프트웨어를 지속적으로 제공합니다. 이제 사용자는 가정에서 여러 PC 에 대한 보안 기능을 쉽게 추가하고 관리할 수 있습니다. 뿐만 아니라 성능이 향상되었으므로 사용자 작업을 방해하지 않고 보호 기능이 적용됩니다.

이 장에서

제 2 장

McAfee SecurityCenter

McAfee SecurityCenter 를 사용하여 컴퓨터의 보안 상태를 모니터링하고, 컴퓨터의 바이러스, 스파이웨어, 전자 메일 및 방화벽 보호 서비스가 최신 버전인지 즉시 확인하고, 잠재적인 보안 취약성에 대해 조치를 취할 수 있습니다. McAfee SecurityCenter 는 컴퓨터 보호의 모든 영역을 조정하고 관리하는 데 필요한 탐색 도구 및 제어 기능을 제공합니다.

컴퓨터 보호 구성 및 관리를 시작하기 전에 SecurityCenter 인터페이스를 검토하고 보호 상태, 보호 범주 및 보호 서비스 간의 차이에 대해 이해해야 합니다. 그런 다음 SecurityCenter 를 업데이트하여 McAfee 에서 사용할 수 있는 최신 보호 기능을 사용하십시오.

초기 구성 작업이 완료되면 SecurityCenter 를 사용하여 컴퓨터의 보호 상태를 모니터링할 수 있습니다. SecurityCenter 가 보호 문제를 검색하면 심각도에 따라 문제를 수정하거나 무시할 수 있도록 경고 메시지를 표시합니다. 또한 이벤트 로그에서 바이러스 검색 구성 변경과 같은 SecurityCenter 이벤트를 검토할 수 있습니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

SecurityCenter 기능

SecurityCenter 에서는 다음과 같은 기능을 제공합니다.

단순화된 보호 상태

간단하게 컴퓨터의 보호 상태를 검토하고, 업데이트를 확인하고, 잠재적 보호 문제를 수정할 수 있습니다.

자동 업데이트 및 업그레이드

등록된 프로그램에 대한 업데이트를 자동으로 다운로드하고 설치할 수 있습니다. 등록된 McAfee 프로그램의 새 버전이 준비되면 등록 기간 중에는 무료 설치가 되기 때문에 항상 최신 보호 장치를 갖출 수 있습니다.

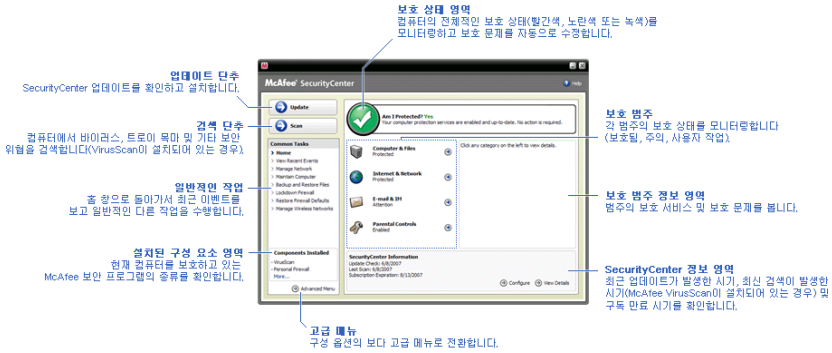
실시간 경고

보안 경고를 통해 긴급 바이러스 발생 및 보안 위협에 대해 알려 주고 이러한 위협을 제거 또는 무력화하거나 이에 대한 자세한 정보를 얻을 수 있는 옵션을 제공합니다.

제 3 장

SecurityCenter 사용

SecurityCenter 사용을 시작하기 전에 컴퓨터의 보호 상태를 관리하는 데 사용할 구성 요소 및 구성 영역을 검토합니다. 이 이미지에 사용된 용어에 대한 자세한 내용은 보호 상태 이해 (8 페이지) 및 보호 범주 이해 (9 페이지)를 참조하십시오. 그런 다음 McAfee 계정 정보를 검토하여 등록 유효 기간을 확인할 수 있습니다.



이 장에서

보호 상태 이해

SecurityCenter 홈 창의 보호 상태 영역에 컴퓨터의 보호 상태가 표시됩니다. 보호 상태는 컴퓨터가 최신 보안 위협에 대해 완전히 보호되는지 여부를 나타내고 외부 보안 공격, 기타 보안 문제 및 인터넷에 액세스하는 프로그램과 같은 요소의 영향을 받을 수 있습니다.

컴퓨터의 보호 상태는 빨간색, 노란색 또는 녹색일 수 있습니다.

보호 상태	설명
빨간색	컴퓨터가 보호되지 않습니다. SecurityCenter 홈 창의 보호 상태 영역이 빨간색이고 보호되지 않음을 나타냅니다. SecurityCenter 가 하나 이상의 심각한 보안 문제를 보고합니다. 완전히 보호하려면 각 보호 범주에서 모든 심각한 보안 문제를 수정해야 합니다(문제 범주의 상태는 [사용자 작업]으로 설정되고 빨간색으로 되어 있음). 보호 문제를 수정하는 방법에 대한 자세한 내용은 보호 문제 수정 (18 페이지)을 참조하십시오.
노란색	컴퓨터가 부분적으로 보호됩니다. SecurityCenter 홈 창의 보호 상태 영역이 노란색이고 보호되지 않음을 나타냅니다. SecurityCenter 가 하나 이상의 심각하지 않은 보안 문제를 보고합니다. 완전히 보호하려면 각 보호 범주와 관련된 심각하지 않은 보안 문제를 수정하거나 무시해야 합니다. 보호 문제를 수정하거나 무시하는 방법에 대한 자세한 내용은 보호 문제 수정 또는 무시 (17 페이지)를 참조하십시오.
녹색	컴퓨터가 완전히 보호됩니다. SecurityCenter 홈 창의 보호 상태 영역이 녹색이고 보호됨을 나타냅니다. SecurityCenter 가 심각하거나 심각하지 않은 보안 문제를 보고하지 않습니다. 각 보호 범주는 컴퓨터를 보호하고 있는 서비스를 나열합니다.

보호 범주 이해

SecurityCenter 의 보호 서비스는 컴퓨터 및 파일, 인터넷 및 네트워크, 전자 메일 및 메신저, 보호자 통제 등의 네 가지 범주로 구분됩니다. 이러한 범주는 컴퓨터를 보호하는 보안 서비스를 찾아보고 구성하도록 도와줍니다.

범주 이름을 클릭하면 보호 서비스를 구성하고 이러한 서비스에 대해 검색된 보안 문제를 볼 수 있습니다. 컴퓨터의 보호 상태가 빨간색 또는 노란색이면 하나 이상의 범주가 [사용자 작업] 또는 [주의] 메시지를 표시하여 SecurityCenter가 범주 내에서 문제를 검색했음을 나타냅니다. 보호 상태에 대한 자세한 내용은 보호 상태 이해 (8 페이지)를 참조하십시오.

보호 범주	설명
컴퓨터 및 파일	컴퓨터 및 파일 범주에서는 다음 보호 서비스를 구성할 수 있습니다. ▪ 바이러스 방지 ▪ PUP 보호 ▪ 시스템 모니터 ▪ Windows 보호
인터넷 및 네트워크	인터넷 및 네트워크 범주에서는 다음 보호 서비스를 구성할 수 있습니다. ▪ 방화벽 보호 ▪ ID 보호
전자 메일 및 메신저	전자 메일 및 메신저 범주에서는 다음 보호 서비스를 구성할 수 있습니다. ▪ 전자 메일 보호 ▪ 스팸 방지
보호자 통제	보호자 통제 범주에서는 다음 보호 서비스를 구성할 수 있습니다. ▪ 콘텐츠 차단

보호 서비스 이해

보호 서비스는 컴퓨터를 보호하기 위해 구성하는 핵심 SecurityCenter 구성 요소입니다. 보호 서비스는 McAfee 프로그램에 해당합니다. 예를 들어 VirusScan 을 설치하면 바이러스 보호, PUP 보호, 시스템 모니터 및 Windows 보호 서비스를 사용할 수 있습니다. 이러한 특정 보호 서비스에 대한 자세한 내용은 VirusScan 도움말을 참조하십시오.

기본적으로 프로그램을 설치하면 프로그램과 관련된 모든 보호 서비스가 활성화되지만 언제든지 보호 서비스를 비활성화할 수 있습니다. 예를 들어 Privacy Service 를 설치하면 콘텐츠 차단 및 ID 보호가 모두 활성화됩니다. 콘텐츠 차단 보호 서비스를 사용하지 않을 경우 이 서비스를 완전히 비활성화할 수 있습니다. 또한 설정 또는 유지 보수 작업을 수행하는 동안 일시적으로 보호 서비스를 비활성화할 수 있습니다.

McAfee 계정 관리

손쉽게 계정 정보를 액세스 및 검토하고 현재 등록 상태를 확인하여 SecurityCenter 내에서 McAfee 계정을 관리합니다.

참고: CD에서 McAfee 프로그램을 설치한 경우 McAfee 웹 사이트에서 프로그램을 등록해야 McAfee 계정을 설정하거나 업데이트할 수 있습니다. 등록한 후에만 정기적인 자동 프로그램 업데이트를 사용할 수 있습니다.

McAfee 계정 관리

SecurityCenter 에서 McAfee 계정 정보(내 계정)에 간편하게 액세스할 수 있습니다.

1 [일반적인 작업]에서 [내 계정]을 클릭합니다.

2 McAfee 계정에 로그인합니다.

등록 확인

등록 기간이 아직 만료되지 않았는지 확인합니다.

- 작업 표시줄 맨 오른쪽의 알림 영역에서 SecurityCenter 아이콘 을 마우스 오른쪽 단추로 클릭한 다음 [등록 확인]을 클릭합니다.

제 4 장

SecurityCenter 업데이트

SecurityCenter 는 4 시간마다 온라인 업데이트를 확인하고 설치하여 등록된 McAfee 프로그램이 최신 상태를 유지하도록 합니다. 설치 및 등록한 프로그램에 따라 온라인 업데이트는 최신 바이러스 정의 및 해커, 스팸, 스파이웨어 또는 개인 정보 보호 업그레이드를 포함할 수 있습니다. 기본 4 시간 이내에 업데이트를 확인하려면 언제든지 그렇게 할 수 있습니다. SecurityCenter 에서 업데이트를 확인하는 동안 다른 작업을 계속 수행할 수 있습니다.

권장되지는 않지만 SecurityCenter 가 업데이트를 확인하고 설치하는 방법을 변경할 수 있습니다. 예를 들어 업데이트를 다운로드만 하고 설치하지는 않도록 구성하거나, 업데이트를 다운로드하거나 설치하기 전에 사용자에게 알리도록 SecurityCenter 를 구성할 수 있습니다. 자동 업데이트를 비활성화할 수도 있습니다.

참고: CD에서 McAfee 프로그램을 설치한 경우 McAfee 웹 사이트에서 프로그램을 등록하지 않으면 이러한 프로그램에 대한 정기적인 자동 업데이트를 받을 수 없습니다.

이 장에서

업데이트 확인

기본적으로 SecurityCenter 는 컴퓨터가 인터넷에 연결되어 있을 때 4 시간마다 자동으로 업데이트를 확인하지만 원하는 경우 4 시간 이내에 업데이트를 확인할 수 있습니다. 자동 업데이트를 비활성화한 경우에는 사용자가 정기적으로 업데이트를 확인해야 합니다.

- [SecurityCenter 홈] 창에서 [업데이트]를 클릭합니다.

팁: 작업 표시줄의 맨 오른쪽에 있는 알림 영역에서 SecurityCenter 아이콘 을 마우스 오른쪽 단추로 클릭한 다음 [업데이트]를 클릭하여 SecurityCenter를 시작하지 않고 업데이트를 확인할 수 있습니다.

자동 업데이트 구성

기본적으로 SecurityCenter 는 컴퓨터가 인터넷에 연결되어 있을 때 4 시간마다 자동으로 업데이트를 확인하고 설치합니다. 이 기본 동작을 변경하려는 경우 업데이트를 자동으로 다운로드한 다음 업데이트를 설치할 준비가 되면 사용자에게 알리거나, 업데이트를 다운로드하기 전에 알리도록 SecurityCenter 를 구성할 수 있습니다.

참고: SecurityCenter는 경고를 사용하여 업데이트를 다운로드하거나 설치할 준비가 되면 사용자에게 알립니다. 경고로부터 업데이트를 다운로드 또는 설치하거나 업데이트를 연기할 수 있습니다. 경고에서 프로그램을 업데이트할 때 다운로드 및 설치하기 전에 등록을 확인하라는 메시지가 나타날 수 있습니다. 자세한 내용은 경고 작업 (21 페이지)을 참조하십시오.

1 [SecurityCenter 구성] 창을 엽니다.

   방식

   1. [일반적인 작업]에서 [홈]을 클릭합니다.
   2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.

2 [SecurityCenter 구성] 창의 [자동 업데이트를 사용하지 않습니다]에서 [설정]을 클릭한 다음 [고급]을 클릭합니다.

3 다음 단추 중 하나를 클릭합니다.

   - **서비스가 업데이트될 때 업데이트 자동 설치 및 통보(권장)**
   - **업데이트 설치 준비가 되면 자동으로 업데이트 다운로드 및 통보**
   - **업데이트 다운로드 전에 통보**

4 [확인]을 클릭합니다.

자동 업데이트 비활성화

자동 업데이트를 비활성화하면 사용자가 정기적으로 업데이트를 확인해야 합니다. 그렇지 않으면 최신 보안 보호를 사용하지 못하게 됩니다. 수동으로 업데이트 확인에 대한 자세한 내용은 업데이트 확인 (13 페이지)을 참조하십시오.

1 [SecurityCenter 구성] 창을 엽니다.

   방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.

2 [SecurityCenter 구성] 창의 [자동 업데이트를 사용합니다]에서 [해제]를 클릭합니다.

팁: [설정] 단추를 클릭하거나 [업데이트 옵션] 창에서 [자동 업데이트를 사용하지 않고 수동으로 업데이트 확인]을 선택 취소하여 자동 업데이트를 활성화합니다.

제 5 장

보호 문제 수정 또는 무시

SecurityCenter 는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 심각한 보호 문제는 즉각적인 조치가 필요하고 보호 상태를 손상시킵니다(색상을 빨간색으로 변경). 심각하지 않은 보호 문제는 즉각적인 조치가 필요하지는 않으며 문제 유형에 따라 보호 상태를 손상시킬 수도 있고 아닐 수도 있습니다. 보호 상태를 녹색으로 만들려면 심각한 문제는 모두 수정하고 심각하지 않은 문제는 모두 수정하거나 무시해야 합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician 을 실행할 수 있습니다. McAfee Virtual Technician 에 대한 자세한 내용은 McAfee Virtual Technician 도움말을 참조하십시오.

이 장에서

보호 문제 수정

대부분의 보안 문제는 자동으로 수정될 수 있지만 일부 문제는 사용자의 작업이 필요할 수 있습니다. 예를 들어 방화벽 보호가 비활성화되어 있는 경우에는 SecurityCenter 가 이 기능을 자동으로 활성화할 수 있지만 방화벽 보호가 설치되어 있지 않은 경우에는 사용자가 이 기능을 설치해야 합니다. 다음 표는 보호 문제를 수동으로 수정할 때 취할 수 있는 몇 가지 작업을 설명합니다.

문제	작업
지난 30 일 동안 컴퓨터 전체 검색이 수행되지 않았습니다.	컴퓨터를 수동으로 검색합니다. 자세한 내용은 VirusScan 도움말을 참조하십시오.
검색 서명 파일(DAT)이 만료되었습니다.	보호 기능을 수동으로 업데이트합니다. 자세한 내용은 VirusScan 도움말을 참조하십시오.
프로그램이 설치되어 있지 않습니다.	McAfee 웹 사이트 또는 CD 에서 프로그램을 설치합니다.
프로그램의 구성 요소가 누락되었습니다.	McAfee 웹 사이트 또는 CD 에서 프로그램을 다시 설치합니다.
프로그램이 등록되어 있지 않아서 전체 보호를 받을 수 없습니다.	McAfee 웹 사이트에서 프로그램을 등록합니다.
프로그램이 만료되었습니다.	McAfee 웹 사이트에서 계정 상태를 확인합니다.

참고: 한 가지 보호 문제가 둘 이상의 보호 범주에 영향을 주는 경우가 자주 있습니다. 이런 경우 한 범주에서 문제를 수정하면 모든 다른 보호 범주에서 문제가 없어집니다.

자동으로 보호 문제 수정

SecurityCenter는 대부분의 보호 문제를 자동으로 수정할 수 있습니다. 자동으로 보호 문제를 수정할 때 SecurityCenter가 수행한 구성 변경 사항은 이벤트 로그에 기록되지 않습니다. 이벤트에 대한 자세한 내용은 이벤트 보기 (27 페이지)를 참조하십시오.

1 [일반적인 작업]에서 [홈]을 클릭합니다.

2 [SecurityCenter 홈] 창의 보호 상태 영역에서 [수정]을 클릭합니다.

수동으로 보호 문제 수정

자동으로 보호 문제 수정을 시도한 후 하나 이상의 보호 문제가 계속되면 수동으로 문제를 수정할 수 있습니다.

1 [일반적인 작업]에서 [홈]을 클릭합니다.

2 [SecurityCenter 홈] 창에서 SecurityCenter 가 문제를 보고하는 보호 범주를 클릭합니다.

3 문제 설명 뒤에 있는 링크를 클릭합니다.

보호 문제 무시

SecurityCenter 에서 심각하지 않은 문제를 검색할 경우 수정하거나 무시할 수 있습니다. 심각하지 않은 다른 문제(예: Anti-Spam 또는 Privacy Service 가 설치되지 않은 경우)는 자동으로 무시됩니다. 무시된 문제는 컴퓨터의 보호 상태가 녹색이 아니면 SecurityCenter 홈 창의 보호 범주 정보 영역에 나타나지 않습니다. 문제를 무시하지만 나중에 컴퓨터의 보호 상태가 녹색이 아니더라도 보호 범주 정보 영역에 문제가 나타나도록 하려면 무시된 문제를 표시할 수 있습니다.

보호 문제 무시

SecurityCenter 에서 심각하지 않은 문제를 검색했고 이 문제를 수정하지 않으려면 무시할 수 있습니다. 문제를 무시하면 SecurityCenter 의 보호 범주 정보 영역에서 문제가 제거됩니다.

1 [일반적인 작업]에서 [홈]을 클릭합니다.

2 [SecurityCenter 홈] 창에서 문제가 보고되는 보호 범주를 클릭합니다.

3 보호 문제 옆에 있는 [무시] 링크를 클릭합니다.

무시된 문제 표시 또는 숨기기

문제의 심각도에 따라 무시된 보호 문제를 표시하거나 숨길 수 있습니다.

1 [경고 옵션] 창을 엽니다.

   방식

   1. [일반적인 작업]에서 [홈]을 클릭합니다.
   2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
   3. [경고]에서 [고급]을 클릭합니다.

2 [SecurityCenter 구성] 창에서 [무시된 문제점]을 클릭합니다.

3 [무시된 문제점] 창에서 다음 작업을 수행합니다.

- 문제를 무시하려면 해당 확인란을 선택합니다.
- 보호 범주 정보 영역에서 문제를 보고하려면 해당 확인란의 선택을 취소합니다.

4 [확인]을 클릭합니다.

팁: 또한 보호 범주 정보 영역의 보고된 문제 옆에 있는 [무시] 링크를 클릭해서도 문제를 무시할 수 있습니다.

제 6 장

경고 작업

경고는 특정 SecurityCenter 이벤트가 발생할 때 화면의 오른쪽 하단 모서리에 나타나는 작은 팝업 대화 상자입니다. 경고는 이벤트에 대한 자세한 정보뿐만 아니라 이벤트와 관련될 수 있는 문제를 해결하기 위한 권장 사항 및 옵션을 제공합니다. 일부 경고에는 이벤트에 대한 추가 정보 링크도 포함되어 있습니다. 이러한 링크를 통해 McAfee 의 글로벌 웹 사이트를 시작하거나 McAfee 에 문제 해결을 위한 정보를 보낼 수 있습니다.

빨간색, 노란색 및 녹색의 세 가지 경고 유형이 있습니다.

경고 유형	설명
빨간색	빨간색 경고는 사용자가 응답해야 하는 심각한 알림입니다. 빨간색 경고는 SecurityCenter 에서 자동으로 보호 문제를 수정하는 방법을 결정할 수 없을 때 발생합니다.
노란색	노란색 경고는 대개 사용자가 응답해야 하는 심각하지 않은 알림입니다.
녹색	녹색 경고는 사용자가 응답할 필요가 없는 심각하지 않은 알림입니다. 녹색 경고는 이벤트에 대한 기본 정보를 제공합니다.

경고는 보호 상태를 모니터링하고 관리하는 중요한 역할을 수행하므로 비활성화할 수 없습니다. 그러나 특정 유형의 정보 경고 표시 여부를 제어하고 일부 다른 경고 옵션(예: SecurityCenter 에서 경고와 함께 경고음을 낼지 또는 시작 시 McAfee 스플래시 화면을 표시할지 여부)을 구성할 수 있습니다.

이 장에서

정보 경고 표시 및 숨기기

정보 경고는 컴퓨터의 보안을 위협하지 않는 이벤트가 발생할 때 사용자에게 알립니다. 예를 들어 방화벽 보호를 설정한 경우 기본적으로 컴퓨터의 프로그램이 인터넷에 액세스할 수 있을 때마다 정보 경고가 나타납니다. 특정 유형의 정보 경고가 나타나지 않게 하려면 해당 경고를 숨길 수 있습니다. 정보 경고가 나타나지 않게 할 경우 모든 정보 경고를 숨길 수 있습니다. 또한 컴퓨터에서 전체 화면 모드로 게임을 할 때 모든 정보 경고를 숨길 수 있습니다. 게임을 마치고 전체 화면 모드를 종료하면 SecurityCenter 는 다시 정보 경고를 표시합니다.

실수로 정보 경고를 숨긴 경우 언제든지 다시 표시할 수 있습니다. 기본적으로 SecurityCenter 는 모든 정보 경고를 표시합니다.

정보 경고 표시 또는 숨기기

SecurityCenter 에서 일부 정보 경고를 표시하고 다른 정보 경고는 숨기거나, 모든 정보 경고를 숨기도록 구성할 수 있습니다.

1 [경고 옵션] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
3. [경고]에서 [고급]을 클릭합니다.

2 [SecurityCenter 구성] 창에서 [정보 경고]를 클릭합니다.

3 [정보 경고] 창에서 다음 작업을 수행합니다.

- 정보 경고를 표시하려면 해당 확인란의 선택을 취소합니다.
- 정보 경고를 숨기려면 해당 확인란을 선택합니다.
- 모든 정보 경고를 숨기려면 [정보 경고 표시 안 함] 확인란을 선택합니다.

4 [확인]을 클릭합니다.

팁: 또한 경고 자체에서 [이 경고 다시 표시 안 함] 확인란을 선택하여 정보 경고를 숨길 수 있습니다. 이 경우 [정보 경고] 창에서 해당 확인란의 선택을 취소하여 정보 경고를 다시 표시할 수 있습니다.

게임 실행 시 정보 경고 표시 또는 숨기기

컴퓨터에서 전체 화면 모드로 게임을 할 때 정보 경고를 숨길 수 있습니다. 게임을 마치고 전체 화면 모드를 종료하면 SecurityCenter 는 다시 정보 경고를 표시합니다.

1 [경고 옵션] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
3. [경고]에서 [고급]을 클릭합니다.

2 [경고 옵션] 창에서 [게임 모드가 검색될 때 정보 경고 표시] 확인란을 선택하거나 선택 취소합니다.

3 [확인]을 클릭합니다.

경고 옵션 구성

경고의 모양 및 빈도는 SecurityCenter 에서 구성되지만 사용자가 일부 기본 경고 옵션을 조정할 수 있습니다. 예를 들어 경고와 함께 경고음을 내거나 Windows 가 시작될 때 스플래시 화면 경고가 표시되지 않도록 할 수 있습니다. 또한 온라인 커뮤니티에서 바이러스 발생 및 기타 보안 위협에 대해 알리는 경고를 숨길 수도 있습니다.

경고와 함께 경고음 내기

경고가 발생했음을 소리로 알리려는 경우 SecurityCenter 에서 각 경고와 함께 경고음을 내도록 구성할 수 있습니다.

1 [경고 옵션] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
3. [경고]에서 [고급]을 클릭합니다.

2 [경고 옵션] 창의 [소리]에서 [경고가 발생할 때 경고음 내기] 확인란을 선택합니다.

시작 시 스플래시 화면 숨기기

기본적으로 Windows 가 시작될 때 McAfee 스플래시 화면이 잠시 나타나 SecurityCenter 가 컴퓨터를 보호하고 있음을 알립니다. 그러나 스플래시 화면이 나타나지 않게 하려면 이 화면을 숨길 수 있습니다.

1 [경고 옵션] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
3. [경고]에서 [고급]을 클릭합니다.

2 [경고 옵션] 창의 [스플래시 화면]에서 [Windows 시작 시 McAfee 스플래시 화면 표시] 확인란의 선택을 취소합니다.

팁: [Windows 시작 시 McAfee 스플래시 화면 표시] 확인란을 선택하여 스플래시 화면을 언제든지 다시 표시할 수 있습니다.

바이러스 발생 경고 숨기기

온라인 커뮤니티에서 바이러스 발생 및 기타 보안 위협에 대해 알리는 경고를 숨길 수 있습니다.

1 [경고 옵션] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. 오른쪽 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.
3. [경고]에서 [고급]을 클릭합니다.

2 [경고 옵션] 창에서 [바이러스 또는 보안 위협 발생 시 경고 표시] 확인란의 선택을 취소합니다.

팁: [바이러스 또는 보안 위협 발생 시 경고 표시] 확인란을 선택하여 바이러스 발생 경고를 언제든지 표시할 수 있습니다.

제 7 장

이벤트 보기

이벤트는 보호 범주 및 관련 보호 서비스 내에서 발생하는 작업 또는 구성 변경입니다. 각 보호 서비스는 서로 다른 유형의 이벤트를 기록합니다. 예를 들어 SecurityCenter는 보호 서비스가 활성화 또는 비활성화되는 경우 이벤트를 기록하고, 바이러스 보호는 바이러스가 검색되고 제거될 때마다 이벤트를 기록하고, 방화벽 보호는 인터넷 연결 시도가 차단될 때마다 이벤트를 기록합니다. 보호 범주에 대한 자세한 내용은 보호 범주 이해 (9 페이지)를 참조하십시오.

구성 문제를 해결하고 다른 사용자가 수행한 작업을 검토할 때 이벤트를 볼 수 있습니다. 대부분의 부모들은 이벤트 로그를 사용하여 인터넷에서 자녀들의 행동을 모니터링합니다. 최근에 발생한 30 개 이벤트만 살펴보려면 최근 이벤트를 봅니다. 발생한 모든 이벤트의 전체 목록을 살펴보려면 모든 이벤트를 봅니다. 모든 이벤트를 볼 때 SecurityCenter는 이벤트가 발생한 보호 범주에 따라 이벤트를 정렬하는 이벤트 로그를 시작합니다.

이 장에서

최신 이벤트 보기

최근에 발생한 30 개 이벤트만 살펴보려면 최근 이벤트를 봅니다.

- [일반적인 작업]에서 [최신 이벤트 보기]를 클릭합니다.

모든 이벤트 보기

발생한 모든 이벤트의 전체 목록을 살펴보려면 모든 이벤트를 봅니다.

1. [일반적인 작업]에서 [최신 이벤트 보기]를 클릭합니다.
2. [최신 이벤트] 창에서 [로그 보기]를 클릭합니다.
3. 이벤트 로그의 왼쪽 창에서 보려고 하는 이벤트 유형을 클릭합니다.

제 8 장

McAfee VirusScan

VirusScan 의 고급 검색 및 보호 서비스는 바이러스, 트로이 목마, 쿠키 추적, 스파이웨어, 애드웨어 및 기타 악성 프로그램을 포함하는 최신 보안 위협으로부터 사용자와 사용자의 컴퓨터를 보호합니다. 보호의 범위가 데스크톱에 있는 파일 및 폴더를 넘어서 전자 메일, 메신저 및 웹을 포함하여 여러 진입점으로부터의 위협 방지에 이르기까지 확장됩니다.

VirusScan 을 사용하면 컴퓨터를 즉각적이고 지속적으로 보호할 수 있으며 관리를 위해 많은 시간을 소모할 필요가 없습니다. 웹 작업을 하거나 재생, 탐색하거나 전자 메일을 확인하는 동안 프로그램은 백그라운드로 실행되며 실시간으로 잠재적 위험을 모니터링하고 검색 및 탐지합니다. 광범위한 검색을 일정에 따라 실행하고 더 세부적인 옵션 집합을 사용하여 주기적으로 컴퓨터를 확인합니다. VirusScan 은 원하는 경우 이 동작을 사용자 지정하는 유연성을 제공하지만 원하지 않으면 컴퓨터가 보호된 상태로 유지됩니다.

일반적인 컴퓨터 사용 시 바이러스, 웜 및 기타 잠재적 위협이 컴퓨터를 침투할 수 있습니다. 이 경우 VirusScan 은 위협에 대해 알리지만 일반적으로 손상되기 전에 감염된 항목을 치료하거나 격리하여 사용자 대신 위협을 처리합니다. 드물지만 때때로 추가 작업이 필요할 수 있습니다. 이러한 경우 VirusScan 은 다음에 컴퓨터를 시작할 때 다시 검색하거나, 검색된 항목을 보관하거나, 검색된 항목을 제거하는 등 사용자가 수행할 작업을 결정할 수 있게 합니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

VirusScan 기능

VirusScan 에서는 다음과 같은 기능을 제공합니다.

포괄적인 바이러스 방지

VirusScan 의 고급 검색 및 보호 서비스는 바이러스, 트로이 목마, 쿠키 추적, 스파이웨어, 애드웨어 및 기타 악성 프로그램을 포함하는 최신 보안 위협으로부터 사용자와 사용자의 컴퓨터를 보호합니다. 보호의 범위가 데스크톱에 있는 파일 및 폴더를 넘어서 전자 메일, 메신저 및 웹을 포함하여 여러 진입점으로부터의 위협 방지에 이르기까지 확장됩니다. 관리를 위해 많은 시간을 소모할 필요가 없습니다.

리소스 인식 검색 옵션

검색 속도가 느려지면 이 옵션을 비활성화하여 컴퓨터 리소스를 최소한으로 사용할 수 있지만 다른 작업보다 바이러스 방지에 높은 우선 순위가 부여됨을 염두에 두십시오. VirusScan 은 원하는 경우 실시간 및 수동 검색 옵션을 사용자 지정하는 유연성을 제공하지만 원하지 않으면 컴퓨터가 보호된 상태로 유지됩니다.

자동 복구

VirusScan 은 실시간 또는 수동 검색을 실행하는 동안 보안 위협을 검색할 경우 위협 유형에 따라 자동으로 위협을 처리하려고 합니다. 이런 방식으로 대부분의 위협을 검색하고 사용자 개입 없이 무력화할 수 있습니다. 드물지만 VirusScan 이 자체적으로 위협을 무력화하지 못할 수 있습니다. 이러한 경우 VirusScan 은 다음에 컴퓨터를 시작할 때 다시 검색하거나, 검색된 항목을 보관하거나, 검색된 항목을 제거하는 등 사용자가 수행할 작업을 결정할 수 있게 합니다.

전체 화면 모드에서 작업 일시 중지

영화를 보거나 컴퓨터 게임을 하거나 전체 컴퓨터 화면을 차지하는 활동과 같은 여가를 즐길 때 VirusScan 은 자동 업데이트 및 수동 검색을 포함하여 많은 작업을 일시 중지합니다.

실시간 바이러스 방지 시작

VirusScan은 실시간 및 수동의 두 가지 바이러스 방지 유형을 제공합니다. 실시간 바이러스 방지는 컴퓨터에서 지속적으로 바이러스 활동을 모니터링하여 사용자 또는 컴퓨터에서 파일에 액세스할 때마다 파일을 검색합니다. 수동 바이러스 방지를 사용하면 필요 시 파일을 검색할 수 있습니다. 컴퓨터가 최신 보안 위협에 지속적으로 보호되도록 하려면 실시간 바이러스 방지를 설정한 상태로 보다 포괄적인 수동 검색을 정기적으로 실행하도록 일정을 설정합니다. 기본적으로 VirusScan은 1 주일에 한 번 예약된 검색을 수행합니다. 실시간 및 수동 검색에 대한 자세한 내용은 컴퓨터 검색 (55 페이지)을 참조하십시오.

드물지만 일부 검색 옵션을 변경하거나 성능 문제 해결 등의 목적으로 일시적으로 실시간 검색을 중지하려고 할 수 있습니다. 실시간 바이러스 방지를 비활성화하면 컴퓨터가 보호되지 않고 SecurityCenter 보호 상태는 빨간색입니다. 보호 상태에 대한 자세한 내용은 SecurityCenter 도움말의 "보호 상태 이해"를 참조하십시오.

실시간 바이러스 방지 시작

실시간 바이러스 방지는 기본적으로 설정되어 있으므로 바이러스, 트로이 목마 및 기타 보안 위협에 대해 컴퓨터를 보호합니다. 실시간 바이러스 방지를 해제한 경우 계속해서 보호되도록 하려면 이 기능을 다시 설정해야 합니다.

1 [컴퓨터 및 파일 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [컴퓨터 및 파일]을 클릭합니다.

2 [바이러스 방지]에서 [열기]를 클릭합니다.

실시간 바이러스 방지 중지

일시적으로 실시간 바이러스 방지를 해제한 다음 이 기능을 계속할 시기를 지정할 수 있습니다. 컴퓨터를 다시 시작할 때 15 분, 30 분, 45 분 또는 60 분 후 자동으로 보호 기능을 계속하거나 전혀 사용하지 않을 수 있습니다.

1 [컴퓨터 및 파일 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [컴퓨터 및 파일]을 클릭합니다.

2 [바이러스 방지]에서 [닫기]를 클릭합니다.

3 대화 상자에서 실시간 검색을 계속할 시기를 선택합니다.

4 [확인]을 클릭합니다.

제 9 장

추가 보호 시작

실시간 바이러스 방지 외에도 VirusScan 은 스크립트, 스파이웨어 및 잠재적으로 유해한 전자 메일 및 메신저 첨부 파일에 대한 고급 보호 기능을 제공합니다. 기본적으로 스크립트 검색, 스파이웨어, 전자 메일 및 메신저 보호 기능이 설정되어 컴퓨터를 보호합니다.

스크립트 검색 보호

스크립트 검색 보호는 잠재적으로 유해한 스크립트를 검색하고 이러한 스크립트가 컴퓨터에서 실행되지 않도록 합니다. 이 기능은 컴퓨터에서 파일을 만들거나 복사 또는 삭제하거나, Windows 레지스트리를 여는 스크립트와 같은 의심스러운 스크립트 활동을 모니터링하고 손상이 발생하기 전에 사용자에게 경고합니다.

스파이웨어 방지

스파이웨어 방지는 스파이웨어, 애드웨어 및 기타 악성 프로그램을 검색합니다. 스파이웨어는 컴퓨터에 몰래 설치되어 사용자의 동작을 모니터링하고, 개인 정보를 수집하고, 심지어 추가 소프트웨어를 설치하거나 브라우저 활동을 리디렉션하여 컴퓨터 제어를 방해할 수 있는 소프트웨어입니다.

전자 메일 보호

전자 메일 보호는 주고받는 전자 메일 및 첨부 파일에서 의심스러운 활동을 검색합니다.

메신저 보호

메신저 보호는 수신하는 메신저 첨부 파일에서 생길 수 있는 보안 위협을 검색합니다. 또한 메신저 프로그램이 개인 정보를 공유하지 못하도록 합니다.

이 장에서

스크립트 검색 보호 시작

스크립트 검색 보호를 설정하여 잠재적으로 유해한 스크립트를 검색하고 이러한 스크립트가 컴퓨터에서 실행되지 않도록 합니다. 스크립트 검색 보호는 스크립트가 컴퓨터에 파일을 만들거나 복사 또는 삭제하려고 할 때 또는 Windows 레지스트리를 변경할 때 사용자에게 경고합니다.

1 [컴퓨터 및 파일 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [컴퓨터 및 파일]을 클릭합니다.

2 [스크립트 검색 보호]에서 [열기]를 클릭합니다.

참고: 언제든지 스크립트 검색 보호를 해제할 수 있지만 이 기능을 해제하면 컴퓨터가 유해한 스크립트에 취약한 상태로 남게 됩니다.

스파이웨어 방지 시작

스파이웨어 방지를 설정하면 사용자의 확인이나 허가 없이 정보를 수집하고 전송하는 스파이웨어, 애드웨어 및 기타 악성 프로그램을 검색하고 제거합니다.

1 [컴퓨터 및 파일 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [컴퓨터 및 파일]을 클릭합니다.

2 [스크립트 검색 보호]에서 [열기]를 클릭합니다.

참고: 언제든지 스파이웨어 방지를 해제할 수 있지만 이 기능을 해제하면 컴퓨터가 악성 프로그램에 취약한 상태로 남게 됩니다.

전자 메일 보호 시작

전자 메일 보호를 설정하면 웜을 비롯하여 아웃바운드(SMTP) 및 인바운드(POP3) 전자 메일 메시지 및 첨부 파일에서 잠재적인 위협을 검색합니다.

1 [전자 메일 및 메신저 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [전자 메일 및 메신저]를 클릭합니다.

2 [전자 메일 보호]에서 [열기]를 클릭합니다.

참고: 언제든지 전자 메일 보호를 해제할 수 있지만 이 기능을 해제하면 컴퓨터가 전자 메일 위협에 취약한 상태로 남게 됩니다.

메신저 보호 시작

메신저 보호를 설정하면 인바운드 메신저 첨부 파일에 포함될 수 있는 보안 위협을 검색합니다.

1 [전자 메일 및 메신저 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [전자 메일 및 메신저]를 클릭합니다.

2 [메신저 보호]에서 [열기]를 클릭합니다.

참고: 언제든지 메신저 보호를 해제할 수 있지만 이 기능을 해제하면 컴퓨터가 유해한 메신저 첨부 파일에 취약한 상태로 남게 됩니다.

제 10 장

바이러스 방지 설정

VirusScan 은 실시간 및 수동의 두 가지 바이러스 방지 유형을 제공합니다. 실시간 바이러스 방지는 사용자나 사용자 컴퓨터가 파일에 액세스할 때마다 파일을 검색합니다. 수동 바이러스 방지를 사용하면 필요 시 파일을 검색할 수 있습니다. 각 방지 유형에 대해 다른 옵션을 설정할 수 있습니다. 예를 들어 실시간 방지는 컴퓨터를 계속해서 모니터링하므로 특정 기본 검색 옵션 집합을 선택할 수 있으며 수동으로 진행하는 필요 시 방지 기능에는 보다 포괄적인 검색 옵션 집합을 사용할 수 있습니다.

이 장에서

실시간 검색 옵션 설정

실시간 바이러스 방지를 시작할 때 VirusScan 은 기본 옵션 집합을 사용하여 파일을 검색하지만 필요에 맞게 기본 옵션을 변경할 수 있습니다.

실시간 검색 옵션을 변경하려면 검색 중 VirusScan 이 확인할 사항을 비롯하여 검색 위치 및 파일 형식도 결정해야 합니다. 예를 들어 VirusScan 이 알 수 없는 바이러스 또는 웹 사이트에서 사용자의 동작을 추적하는 데 사용할 수 있는 쿠키를 검사할지 여부 및 컴퓨터 또는 로컬 드라이브에 매핑된 네트워크 드라이브를 검색할지 여부를 결정할 수 있습니다. 또한 모든 파일을 검색하거나, 대부분의 바이러스가 발견되는 프로그램 파일과 문서만 검색하도록 검색할 파일 형식을 결정할 수도 있습니다.

실시간 검색 옵션을 변경할 때 컴퓨터가 버퍼 오버플로를 방지하도록 해야 하는지 여부도 결정해야 합니다. 버퍼는 일시적으로 컴퓨터 정보를 보관하기 위해 사용되는 메모리의 일부입니다. 버퍼에 저장된 의심스러운 프로그램 또는 프로세스의 정보 양이 버퍼 용량을 초과하면 버퍼 오버플로가 발생할 수 있습니다. 이런 상황이 발생하면 컴퓨터가 보안 공격에 더 취약하게 됩니다.

실시간 검색 옵션 설정

실시간 검색 옵션을 설정하여 실시간 검색 중 VirusScan 이 찾을 항목을 비롯한 검색 위치 및 파일 형식을 사용자 지정합니다. 알 수 없는 바이러스와 쿠키 추적을 검색하고 버퍼 오버플로 방지 기능을 제공하는 옵션이 있습니다. 또한 실시간 검색 기능을 구성하여 컴퓨터에 매핑된 네트워크 드라이브를 검사할 수 있습니다.

1 [실시간 검색] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 바이러스 방지가 설정되어 있는지 확인한 다음 [고급]을 클릭합니다.

2 실시간 검색 옵션을 지정한 다음 [확인]을 클릭합니다.

수행할 작업...	수행 방법...
알 수 없는 바이러스 및 알려진 바이러스의 새로운 변종 검색	[경험적 기능을 사용하여 알 수 없는 바이러스 검색] 확인란을 선택합니다.
쿠키 검색	[추적 중인 쿠키 검색 및 제거] 확인란을 선택합니다.
네트워크에 연결된 드라이브의 바이러스 및 기타 잠재적 위협 검색	[네트워크 드라이브 검색] 확인란을 선택합니다.
컴퓨터의 버퍼 오버플로 방지	[버퍼 오버플로 방지 사용] 확인란을 선택합니다.
검색할 파일 형식 지정	[모든 파일(권장)] 또는 [프로그램 파일 및 문서만] 중 하나를 클릭합니다.

수동 검색 옵션 설정

수동 바이러스 방지를 사용하면 필요 시 파일을 검색할 수 있습니다. 수동 검색을 시작할 때 VirusScan 은 보다 포괄적인 검색 옵션 집합을 사용하여 컴퓨터에서 바이러스 및 기타 잠재적으로 유해한 항목을 검사합니다. 수동 검색 옵션을 변경하려면 검색 중 VirusScan 이 검사할 항목을 결정해야 합니다. 예를 들어 VirusScan 에서 알 수 없는 바이러스, 스파이웨어나 애드웨어와 같은 악성 프로그램, 컴퓨터에 대한 인증되지 않은 액세스를 부여할 수 있는 Rootkit 와 같은 은폐 프로그램, 그리고 웹 사이트에서 사용자의 동작을 추적하는 데 사용할 수 있는 쿠키를 찾을지 여부를 결정할 수 있습니다. 또한 검사되는 파일 형식에 대해서도 결정해야 합니다. 예를 들어 VirusScan 이 모든 파일을 검사할지 또는 대부분의 바이러스가 발견되는 프로그램 파일과 문서만 검사할지 여부를 결정할 수 있습니다. 또한 .zip 파일과 같은 보관 파일을 검색에 포함할지 여부도 결정할 수 있습니다.

기본적으로 VirusScan 은 수동 검색을 실행할 때마다 컴퓨터의 모든 드라이브 및 폴더를 검사하지만 필요에 맞게 기본 위치를 변경할 수 있습니다. 예를 들어 중요한 시스템 파일, 데스크톱 항목 또는 Program Files 폴더의 항목만 검색할 수 있습니다. 수동 검색을 매번 시작하기 번거로우면 정기적인 검색 일정을 설정할 수 있습니다. 예약된 검색은 항상 기본 검색 옵션을 사용하여 전체 컴퓨터를 검사합니다. 기본적으로 VirusScan 은 1 주일에 한 번 예약된 검색을 수행합니다.

검색 속도가 느려졌다고 판단되면 이 옵션을 비활성화하여 컴퓨터 리소스를 최소한으로 사용할 수 있지만 다른 작업보다 바이러스 방지에 높은 우선 순위가 부여됨을 염두에 두십시오.

참고: 영화를 보거나 컴퓨터 게임을 하거나 전체 컴퓨터 화면을 차지하는 활동과 같은 여가를 즐길 때 VirusScan은 자동 업데이트 및 수동 검색을 포함하여 많은 작업을 일시 중지합니다.

수동 검색 옵션 설정

수동 검색 옵션을 설정하여 수동 검색 중 VirusScan 이 찾을 항목을 비롯한 검색 위치 및 파일 형식을 사용자 지정합니다. 알 수 없는 바이러스, 파일 보관, 스파이웨어 및 악성 프로그램, 쿠키 추적, Rootkit 및 은폐 프로그램을 검색하는 옵션이 있습니다.

1 [수동 검색] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 바이러스 방지가 설정되어 있는지 확인하고 [고급]을 클릭합니다.
5. [바이러스 방지] 창에서 [수동 검색]을 클릭합니다.

2 수동 검색 옵션을 지정한 다음 [확인]을 클릭합니다.

수행할 작업...	수행 방법...
알 수 없는 바이러스 및 알려진 바이러스의 새로운 변종 검색	[경험적 기능을 사용하여 알 수 없는 바이러스 검색] 확인란을 선택합니다.
.zip 및 기타 보관 파일 내의 바이러스 검색 및 제거	[.zip 파일 및 기타 보관 파일 검색] 확인란을 선택합니다.
스파이웨어, 애드웨어 및 기타 악성 프로그램 검색	[스파이웨어 및 악성 프로그램 검색] 확인란을 선택합니다.
쿠키 검색	[추적 중인 쿠키 검색 및 제거] 확인란을 선택합니다.
기존 Windows 시스템 파일을 변경 및 악용할 수 있는 Rootkit 및 은폐 프로그램 검색	[Rootkit 및 기타 은폐 프로그램 검색] 확인란을 선택합니다.
검색에 보다 적은 프로세서 기능을 사용하면서 웹 탐색 또는 문서 열기와 같은 다른 작업에 더 높은 우선 순위 부여	[최소한의 컴퓨터 리소스를 사용하여 검색] 확인란을 선택합니다.
검색할 파일 형식 지정	[모든 파일(권장)] 또는 [프로그램 파일 및 문서만] 중 하나를 클릭합니다.

수동 검색 위치 설정

수동 검색 위치를 설정하여 VirusScan 이 수동 검색 중 바이러스 및 기타 유해한 항목을 찾을 위치를 결정합니다. 컴퓨터의 모든 파일, 폴더 및 드라이브를 검색할 수도 있고, 특정 폴더 및 드라이브만 검색하도록 제한할 수도 있습니다.

1 [수동 검색] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 바이러스 방지가 설정되어 있는지 확인하고 [고급]을 클릭합니다.
5. [바이러스 방지] 창에서 [수동 검색]을 클릭합니다.

2 [검색할 기본 위치]를 클릭합니다.

3 수동 검색 위치를 지정한 다음 [확인]을 클릭합니다.

수행할 작업...	수행 방법...
컴퓨터의 모든 파일 및 폴더 검색	[(내) 컴퓨터] 확인란을 선택합니다.
컴퓨터의 특정 파일, 폴더 및 드라이브 검색	[(내) 컴퓨터] 확인란의 선택을 취소하고 폴더 또는 드라이브를 하나 이상 선택합니다.
중요 시스템 파일 검색	[(내) 컴퓨터] 확인란의 선택을 취소한 다음 [중요 시스템 파일] 확인란을 선택합니다.

검색 예약

특정 요일 및 시간에 컴퓨터에서 바이러스와 기타 위협을 철저히 검사하도록 검색을 예약합니다. 예약된 검색은 항상 기본 검색 옵션을 사용하여 전체 컴퓨터를 검사합니다. 기본적으로 VirusScan 은 1 주일에 한 번 예약된 검색을 수행합니다. 검색 속도가 느려졌다고 판단되면 이 옵션을 비활성화하여 컴퓨터 리소스를 최소한으로 사용할 수 있지만 다른 작업보다 바이러스 방지에 높은 우선 순위가 부여됨을 염두에 두십시오.

1 [예약된 검색] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 바이러스 방지가 설정되어 있는지 확인한 다음 [고급]을 클릭합니다.
5. [바이러스 방지] 창에서 [예약된 검색]을 클릭합니다.

2 [예약된 검색 활성화]를 선택합니다.

3 일반적으로 검색에 사용되는 프로세서 성능을 줄이려면 [최소한의 컴퓨터 리소스를 사용하여 검색]을 선택합니다.

4 요일을 하나 이상 선택합니다.

5 시작 시간을 지정합니다.

6 [확인]을 클릭합니다.

팁: [다시 설정]을 클릭하여 기본 일정을 복원할 수 있습니다.

SystemGuards 옵션 사용

SystemGuards 는 Windows 레지스트리 또는 컴퓨터의 중요 시스템 파일에 대한 잠재적인 무단 변경을 모니터링하고 기록하고 보고하고 관리합니다. 레지스트리 및 파일이 무단으로 변경되면 컴퓨터에 피해를 주고 보안이 위험에 노출되고 중요한 시스템 파일이 손상될 수 있습니다.

레지스트리 및 파일 변경은 컴퓨터에서 일반적이고 정기적으로 발생합니다. 대부분이 해가 없으므로 SystemGuards 의 기본 설정은 심각한 유해 가능성이 있는 무단 변경에 대해 안정적이고 지능적이며 실질적인 보호 기능을 제공하도록 구성되어 있습니다. 예를 들어 SystemGuards 가 이례적이고 잠재적으로 심각한 위협을 나타내는 변경을 검색하면 즉시 활동이 보고되고 기록됩니다. 보다 일반적이지만 여전히 손상 가능성이 있는 변경은 기록만 됩니다. 그러나 표준 및 낮은 위험 수준의 변경을 모니터링하는 기능은 기본적으로 비활성화되어 있습니다. 사용자가 원하는 환경으로 보호 기능을 확장하도록 SystemGuard 기술을 구성할 수 있습니다.

SystemGuard 에는 프로그램 SystemGuard, Windows SystemGuard 및 브라우저 SystemGuard 등의 세 가지 유형이 있습니다.

프로그램 SystemGuard

프로그램 SystemGuard 는 컴퓨터의 레지스트리 및 Windows 에 필수적인 기타 중요 파일에 대한 잠재적인 무단 변경을 검색합니다. 이러한 중요 레지스트리 항목 및 파일에는 ActiveX 설치, 시작 항목, Windows 셸 실행 후크 및 셸 서비스 개체 지연 로드가 포함됩니다. 프로그램 SystemGuard 기술은 이러한 항목을 모니터링하여 Windows 가 시작될 때 자동으로 시작될 수 있는 스파이웨어 및 악성 프로그램 외에도 의심스러운 ActiveX 프로그램(인터넷에서 다운로드됨)을 중지합니다.

Windows SystemGuard

Windows SystemGuard 또한 컴퓨터의 레지스트리 및 Windows 에 필수적인 기타 중요 파일에 대한 잠재적인 무단 변경을 검색합니다. 이러한 중요 레지스트리 항목 및 파일에는 상황에 맞는 메뉴 처리기, appInit DLL 및 Windows 호스트 파일이 포함됩니다. Windows SystemGuard 기술은 이러한 항목을 모니터링하여 컴퓨터에서 인터넷을 통해 인증되지 않은 정보 또는 개인 정보를 주고받지 못하도록 도와줍니다. 또한 사용자 및 사용자의 가족에게 중요한 프로그램의 표시 및 동작을 무단으로 변경할 수 있는 의심스러운 프로그램을 중지하는 데 도움을 줍니다.

브라우저 SystemGuard

프로그램 및 Windows SystemGuard 와 마찬가지로, 브라우저 SystemGuard 도 컴퓨터의 레지스트리 및 Windows 에 필수적인 기타 중요 파일에 대한 잠재적인 무단 변경을 검색합니다. 그러나 브라우저 SystemGuard 는 Internet Explorer 추가 기능, Internet Explorer URL 및 Internet Explorer 보안 영역과 같은 중요 레지스트리 항목 및 파일에 대한 변경을 모니터링합니다. 브라우저 SystemGuard 기술은 이러한 항목을 모니터링하여 의심스러운 웹 사이트로의 리디렉션, 사용자의 확인 없이 브라우저 설정 및 옵션 변경, 그리고 의심스러운 웹 사이트에 대한 원치 않는 신뢰와 같은 인증되지 않은 브라우저 활동을 방지하는 데 도움을 줍니다.

SystemGuard 보호 활성화

SystemGuard 보호를 활성화하여 컴퓨터에서 잠재적인 무단 Windows 레지스트리 및 파일 변경을 검색하고 사용자에게 경고합니다. 레지스트리 및 파일이 무단으로 변경되면 컴퓨터에 피해를 주고 보안이 위험에 노출되고 중요한 시스템 파일이 손상될 수 있습니다.

1 [컴퓨터 및 파일 구성] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [구성] 창에서 [컴퓨터 및 파일]을 클릭합니다.

2 [SystemGuard 보호]에서 [열기]를 클릭합니다.

참고: [해제]를 클릭하여 SystemGuard 보호를 비활성화할 수 있습니다.

SystemGuard 옵션 구성

SystemGuard 창을 사용하여 Windows 파일, 프로그램 및 Internet Explorer 와 관련된 레지스트리 및 파일 무단 변경에 대한 보호, 로깅 및 경고 옵션을 구성합니다. 레지스트리 및 파일이 무단으로 변경되면 컴퓨터에 피해를 주고 보안이 위험에 노출되고 중요한 시스템 파일이 손상될 수 있습니다.

1 SystemGuard 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 SystemGuard 보호가 설정되어 있는지 확인하고 [고급]을 클릭합니다.

2 목록에서 SystemGuard 유형을 선택합니다.

- **프로그램 SystemGuard**
- **Windows SystemGuard**
- **브라우저 SystemGuard**

3 [원하는 작업]에서 다음 중 하나를 수행합니다.

- 프로그램, Windows 및 브라우저 SystemGuard 와 관련된 레지스트리 및 파일 무단 변경을 검색, 로그 및 보고하려면 [경고 표시]를 클릭합니다.
- 프로그램, Windows 및 브라우저 SystemGuard 와 관련된 레지스트리 및 파일 무단 변경을 검색 및 로그하려면 [로그 변경만]을 클릭합니다.
- 프로그램, Windows 및 브라우저 SystemGuard 와 관련된 레지스트리 및 파일 무단 변경 검색을 비활성화하려면 [SystemGuard 비활성화]를 클릭합니다.

참고: SystemGuard 유형에 대한 자세한 내용은 SystemGuard 유형 정보 (47 페이지)를 참조하십시오.

SystemGuard 유형 정보

SystemGuard 는 컴퓨터의 레지스트리 및 Windows 에 필수적인 기타 중요 파일에 대한 잠재적인 무단 변경을 검색합니다. SystemGuard 에는 프로그램 SystemGuard, Windows SystemGuard 및 브라우저 SystemGuard 등의 세 가지 유형이 있습니다.

프로그램 SystemGuard

프로그램 SystemGuard 기술은 Windows 가 시작될 때 자동으로 시작될 수 있는 스파이웨어 및 악성 프로그램 외에도 의심스러운 ActiveX 프로그램(인터넷에서 다운로드됨)을 중지합니다.

SystemGuard	검색 내용...
ActiveX 설치	컴퓨터에 피해를 주고 보안이 위험에 노출되고 중요한 시스템 파일이 손상될 수 있는 ActiveX 설치에 대한 레지스트리 무단 변경
시작 항목	시작 항목에 대한 파일 변경 사항을 설치하여 컴퓨터를 시작할 때 의심스러운 프로그램이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Windows 셸 실행 후크	Windows 셸 실행 후크를 설치하여 보안 프로그램이 제대로 실행되지 않도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
셸 서비스 개체 지연 로드	셸 서비스 개체 지연 로드에 대한 레지스트리를 변경하여 컴퓨터를 시작할 때 유해한 파일이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램

Windows SystemGuard

Windows SystemGuard 기술은 컴퓨터에서 인터넷을 통해 인증되지 않은 정보 또는 개인 정보를 주고받지 못하도록 도와줍니다. 또한 사용자 및 사용자의 가족에게 중요한 프로그램의 표시 및 동작을 무단으로 변경할 수 있는 의심스러운 프로그램을 중지하는 데 도움을 줍니다.

SystemGuard	검색 내용...
상황에 맞는 메뉴 처리기	Windows 메뉴의 표시와 동작에 영향을 줄 수 있는 Windows 상황에 맞는 메뉴 처리기에 대한 레지스트리 무단 변경. 상황에 맞는 메뉴를 사용하면 파일을 마우스 오른쪽 단추로 클릭하는 것과 같이 컴퓨터에서 작업을 수행할 수 있습니다.
AppInit DLL	컴퓨터를 시작할 때 잠재적으로 유해한 파일이 실행될 수 있는 Windows appInit DLL 에 대한 레지스트리 무단 변경
Windows 호스트 파일	Windows 호스트 파일을 무단으로 변경하여 브라우저에서 의심스러운 웹 사이트로 리디렉션하고 소프트웨어 업데이트를 차단하도록 할 수 있는 스파이웨어, 애드웨어 및 악성 프로그램
Winlogon 셸	Winlogon 셸의 레지스트리를 변경하여 다른 프로그램에서 Windows 탐색기를 바꾸도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Winlogon 사용자 초기화	Winlogon 사용자 초기화의 레지스트리를 변경하여 Windows 에 로그온할 때 의심스러운 프로그램이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Windows 프로토콜	Windows 프로토콜의 레지스트리를 변경하여 컴퓨터에서 인터넷을 통해 정보를 주고받는 방법에 영향을 줄 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Windows 계층화된 서비스 공급자	Winsock LSP(계층화된 서비스 공급자)의 설치 레지스트리를 변경하여 인터넷을 통해 주고받는 정보를 차단하고 변경할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Windows 셸 열기 명령	컴퓨터에 웜 및 기타 유해한 프로그램이 실행되도록 할 수 있는 Windows 셸 열기 명령에 대한 무단 변경
공유 작업 스케줄러	공유 작업 스케줄러의 레지스트리와 파일을 변경하여 컴퓨터를 시작할 때 잠재적으로 유해한 파일이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램

SystemGuard	검색 내용...
Windows 메신저 서비스	Windows Messenger 서비스의 레지스트리를 변경하여 컴퓨터에서 프로그램을 원격으로 실행하고 원치 않는 광고가 표시되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Windows Win.ini 파일	Win.ini 파일을 변경하여 컴퓨터를 시작할 때 의심스러운 프로그램이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램

브라우저 SystemGuard

브라우저 SystemGuard 기술은 의심스러운 웹 사이트로의 리디렉션, 사용자의 확인 없이 브라우저 설정 및 옵션 변경, 그리고 의심스러운 웹 사이트에 대한 원치 않는 신뢰와 같은 인증되지 않은 브라우저 활동을 방지하는 데 도움을 줍니다.

SystemGuard	검색 내용...
브라우저 도우미 개체	브라우저 도우미 개체를 사용하여 웹 검색을 추적하고 원치 않는 광고가 표시되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer 모음	Internet Explorer 의 표시와 동작에 영향을 줄 수 있는 Internet Explorer 모음 프로그램(예: 검색 및 즐겨찾기)에 대한 레지스트리 무단 변경
Internet Explorer 추가 기능	Internet Explorer 추가 기능을 설치하여 웹 검색을 추적하고 원치 않는 광고가 표시되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer ShellBrowser	웹 브라우저의 표시와 동작에 영향을 줄 수 있는 Internet Explorer 셸 브라우저에 대한 레지스트리 무단 변경
Internet Explorer WebBrowser	브라우저의 표시와 동작에 영향을 줄 수 있는 Internet Explorer 웹 브라우저에 대한 레지스트리 무단 변경
Internet Explorer URL 검색 후크	Internet Explorer URL 검색 후크의 레지스트리를 변경하여 웹을 검색할 때 브라우저가 의심스러운 웹 사이트로 리디렉션되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer URL	Internet Explorer URL 의 레지스트리를 변경하여 브라우저 설정에 영향을 줄 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램

SystemGuard	검색 내용...
Internet Explorer 제한	Internet Explorer 제한의 레지스트리를 변경하여 브라우저 설정 및 옵션에 영향을 줄 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer 보안 영역	Internet Explorer 보안 영역의 레지스트리를 변경하여 컴퓨터를 시작할 때 잠재적으로 유해한 파일이 실행되도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer 신뢰할 수 있는 사이트	Internet Explorer 신뢰할 수 있는 사이트의 레지스트리를 변경하여 브라우저에서 의심스러운 웹 사이트를 신뢰하도록 할 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램
Internet Explorer 정책	Internet Explorer 정책의 레지스트리를 변경하여 브라우저의 표시와 동작에 영향을 줄 수 있는 스파이웨어, 애드웨어 및 기타 악성 프로그램

신뢰하는 목록 사용

VirusScan 이 파일 또는 레지스트리 변경(SystemGuard), 프로그램 또는 버퍼 오버플로를 검색할 경우 신뢰 또는 제거할지를 묻는 메시지를 표시합니다. 항목을 신뢰하고 해당 활동에 대해 이후 알림을 받지 않는 것으로 표시하면 항목은 신뢰하는 목록에 추가되고 VirusScan 은 더 이상 이 항목을 검색하거나 해당 활동에 대해 사용자에게 알리지 않습니다. 항목을 신뢰하는 목록에 추가한 후에도 원하는 경우 해당 활동을 차단할 수 있습니다. 활동을 차단하면 항목을 실행하거나 컴퓨터에 변경을 시도할 때마다 사용자에게 알려야 합니다. 또한 신뢰하는 목록에서 항목을 제거할 수도 있습니다. 항목을 제거하면 VirusScan 은 항목의 활동을 다시 검색할 수 있습니다.

신뢰하는 목록 관리

[신뢰하는 목록] 창을 사용하여 이전에 검색되고 신뢰된 항목을 신뢰하거나 차단합니다. 또한 VirusScan 이 다시 항목을 검색하도록 신뢰하는 목록에서 항목을 제거할 수 있습니다.

1 [신뢰하는 목록] 창을 엽니다.

방식

1. [일반적인 작업]에서 [홈]을 클릭합니다.
2. [SecurityCenter 홈] 창에서 [컴퓨터 및 파일]을 클릭합니다.
3. [컴퓨터 및 파일] 정보 영역에서 [구성]을 클릭합니다.
4. [컴퓨터 및 파일 구성] 창에서 바이러스 방지가 설정되어 있는지 확인하고 [고급]을 클릭합니다.
5. [바이러스 방지] 창에서 [신뢰하는 목록]을 클릭합니다.

2 다음 신뢰하는 목록 유형 중 하나를 선택합니다.

- **프로그램 SystemGuard**
- **Windows SystemGuard**
- **브라우저 SystemGuard**
- **신뢰하는 프로그램**
- **신뢰하는 버퍼 오버플로**

3 [원하는 작업]에서 다음 중 하나를 수행합니다.

- 사용자에게 알리지 않고 검색된 항목이 Windows 레지스트리 또는 컴퓨터의 중요 시스템 파일을 변경할 수 있게 하려면 [신뢰]를 클릭합니다.

- 사용자에게 알리지 않고 검색된 항목이 Windows 레지스트리 또는 컴퓨터의 중요 시스템 파일을 변경할 수 없게 하려면 [차단]을 클릭합니다.
- 신뢰하는 목록에서 검색된 항목을 제거하려면 [제거]를 클릭합니다.

4 [확인]을 클릭합니다.

참고: 신뢰하는 목록 유형에 대한 자세한 내용은 신뢰하는 목록 유형 정보 (52 페이지)를 참조하십시오.

신뢰하는 목록 유형 정보

[신뢰하는 목록] 창의 SystemGuard 는 VirusScan 이 검색했지만 사용자가 경고 또는 [검색 결과] 창에서 허용한 이전의 무단 레지스트리 및 파일 변경을 나타냅니다. [신뢰하는 목록] 창에서는 프로그램 SystemGuard, Windows SystemGuard, 브라우저 SystemGuard, 신뢰하는 프로그램 및 신뢰하는 버퍼 오버플로 등 다섯 가지 유형의 신뢰하는 목록 유형을 관리할 수 있습니다.

옵션	설명
프로그램 SystemGuard	[신뢰하는 목록] 창의 프로그램 SystemGuard 는 VirusScan 이 검색했지만 사용자가 경고 또는 [검색 결과] 창에서 허용한 이전의 무단 레지스트리 및 파일 변경을 나타냅니다. 프로그램 SystemGuard 는 ActiveX 설치, 시작 항목, Windows 셸 실행 후크 및 셸 서비스 개체 지연 로드 활동과 관련된 레지스트리 및 파일의 무단 변경을 검색합니다. 레지스트리 및 파일이 이렇게 무단으로 변경되면 컴퓨터에 피해를 주고 보안이 위험에 노출되고 중요한 시스템 파일이 손상될 수 있습니다.
Windows SystemGuard	[신뢰하는 목록] 창의 Windows SystemGuard 는 VirusScan 이 검색했지만 사용자가 경고 또는 [검색 결과] 창에서 허용한 이전의 무단 레지스트리 및 파일 변경을 나타냅니다. Windows SystemGuard 는 상황에 맞는 메뉴 처리기, appInit DLL, Windows 호스트 파일, Winlogon 셸, Winsock LSP(계층화된 서비스 공급자) 등과 관련된 레지스트리 및 파일의 무단 변경을 검색합니다. 레지스트리 및 파일이 이렇게 무단으로 변경되면 컴퓨터가 인터넷을 통해 정보를 주고받는 방식에 영향을 주고, 프로그램의 표시 및 동작을 변경하고, 컴퓨터에서 의심스러운 프로그램의 실행을 허용할 수 있습니다.

옵션	설명
브라우저 SystemGuard	[신뢰하는 목록] 창의 브라우저 SystemGuard 는 VirusScan 이 검색했지만 사용자가 경고 또는 [검색 결과] 창에서 허용한 이전의 무단 레지스트리 및 파일 변경을 나타냅니다. 브라우저 SystemGuard 는 브라우저 도우미 개체, Internet Explorer 추가 기능, Internet Explorer URL, Internet Explorer 보안 영역 등과 관련된 레지스트리 무단 변경 및 기타 원치 않는 동작을 검색합니다. 레지스트리가 이렇게 무단으로 변경되면 의심스러운 웹 사이트로 리디렉션하고, 브라우저 설정 및 옵션을 변경하고, 의심스러운 웹 사이트를 신뢰하는 것과 같은 원치 않는 브라우저 활동이 발생할 수 있습니다.
신뢰하는 프로그램	신뢰하는 프로그램은 VirusScan 이 이전에 검색했지만 경고 또는 [검색 결과] 창에서 신뢰한 악성 프로그램입니다.
신뢰하는 버퍼 오버플로	신뢰하는 버퍼 오버플로는 VirusScan 이 검색했지만 경고 또는 [검색 결과] 창에서 신뢰한 이전의 원치 않는 활동을 나타냅니다. 버퍼 오버플로는 컴퓨터에 피해를 주고 파일을 손상시킬 수 있습니다. 버퍼에 저장된 의심스러운 프로그램 또는 프로세스의 정보 양이 버퍼 용량을 초과하면 버퍼 오버플로가 발생합니다.

제 11 장

컴퓨터 검색

SecurityCenter를 처음 시작할 때 VirusScan의 실시간 바이러스 방지는 잠재적으로 유해한 바이러스, 트로이 목마 및 기타 보안 위협으로부터 컴퓨터를 보호하기 시작합니다. 실시간 바이러스 방지를 비활성화하지 않으면 VirusScan는 사용자가 설정한 실시간 검색 옵션으로 컴퓨터에서 지속적으로 바이러스 활동을 모니터링하여 사용자 또는 컴퓨터가 파일에 액세스할 때마다 파일을 검색합니다. 컴퓨터가 최신 보안 위협에 지속적으로 보호되도록 하려면 실시간 바이러스 방지를 설정한 상태로 보다 포괄적인 수동 검색을 정기적으로 실행하도록 일정을 설정합니다. 실시간 및 수동 검색 옵션 설정에 대한 자세한 내용은 바이러스 방지 설정 (37 페이지)을 참조하십시오.

VirusScan 은 수동 바이러스 방지를 위한 세부적인 검색 옵션 집합을 제공하여 주기적으로 더 광범위한 검색을 실행할 수 있게 합니다. 설정된 스케줄에 따라 특정 위치를 대상으로 지정하여 SecurityCenter 에서 수동 검색을 실행할 수 있습니다. 그러나 작업하는 동안 Windows 탐색기에서 직접 수동 검색을 실행할 수도 있습니다. SecurityCenter 에서 검색하면 검색 옵션을 바로 변경하는 이점이 있지만, Windows 탐색기에서 검색하면 컴퓨터 보안에 편리하게 접근할 수 있습니다.

수동 검색을 SecurityCenter 에서 실행하든 Windows 탐색기에서 실행하든, 검색을 마치면 검색 결과를 볼 수 있습니다. 검색 결과를 보고 VirusScan 이 바이러스, 트로이 목마, 스파이웨어, 애드웨어, 쿠키 및 기타 악성 프로그램을 검색, 치료 또는 격리했는지 여부를 확인합니다. 검색 결과는 다른 방법으로 표시될 수 있습니다. 예를 들어 감염 상태 및 유형과 같은 검색 결과 또는 세부 정보의 기본 요약을 볼 수 있고, 일반 검색 및 검색 통계를 볼 수도 있습니다.

이 장에서

컴퓨터 검색

SecurityCenter 의 [고급] 또는 [기본] 메뉴에서 수동 검색을 실행할 수 있습니다. [고급] 메뉴에서 검색을 실행할 경우 검색하기 전에 수동 검색 옵션을 확인할 수 있습니다. [기본] 메뉴에서 검색을 실행할 경우 VirusScan 은 기존 검색 옵션을 사용하여 즉시 검색을 시작합니다. 또한 Windows 탐색기에서 기존 검색 옵션을 사용하여 검색을 실행할 수도 있습니다.

- 다음 중 하나를 수행합니다.

  SecurityCenter 로 검색

수행할 작업...	수행 방법...
기존 설정을 사용하여 검색	[기본] 메뉴에서 [검색]을 클릭합니다.
변경된 설정을 사용하여 검색	[고급] 메뉴에서 [검색]을 클릭하고 검색할 위치를 선택하고 검색 옵션을 선택한 다음 [지금 검색]을 클릭합니다.

  Windows 탐색기로 검색

  1. Windows 탐색기를 엽니다.
  2. 파일, 폴더 또는 드라이브를 마우스 오른쪽 단추로 클릭한 다음 [검색]을 클릭합니다.

참고: 검색 결과가 [검색 완료됨] 경고에 나타납니다. 결과에 검색, 감지, 복구, 격리 및 제거된 항목 수가 포함됩니다. 검색 결과에 대해 자세히 알아보거나 감염된 항목과 관련된 작업을 수행하려면 [검색 세부 정보 보기]를 클릭하십시오.

검색 결과 보기

수동 검색을 마치면 결과를 보고 검색이 발견한 항목을 확인하고 컴퓨터의 현재 보호 상태를 분석합니다. 검색 결과는 VirusScan 이 바이러스, 트로이 목마, 스파이웨어, 애드웨어, 쿠키 및 기타 악성 프로그램을 검색, 복구 또는 격리했는지 여부를 알려줍니다.

- [기본] 또는 [고급] 메뉴에서 [검색]을 클릭하고 다음 작업 중 하나를 수행합니다.

수행할 작업...	수행 방법...
경고에서 검색 결과 보기	[검색 완료됨] 경고에서 검색 결과를 봅니다.
검색 결과에 대한 추가 정보 보기	[검색 완료됨] 경고에서 [검색 세부 정보 보기]를 클릭합니다.
검색 결과의 빠른 요약 보기	작업 표시줄의 알림 영역에 있는 [검색 완료됨] 아이콘을 가리킵니다.
검색 및 감지 통계 보기	작업 표시줄의 알림 영역에 있는 [검색 완료됨] 아이콘을 두 번 클릭합니다.
검색된 항목, 감염된 상태 및 유형에 대한 세부 정보 보기	작업 표시줄의 알림 영역에 있는 [검색 완료됨] 아이콘을 두 번 클릭하고 [검색 진행률: 수동 검색] 창에서 [결과 보기]를 클릭합니다.

제 12 장

검색 결과 작업

VirusScan 은 실시간 또는 수동 검색을 실행하는 동안 보안 위협을 검색할 경우 위협 유형에 따라 자동으로 위협을 처리하려고 합니다. 예를 들어 VirusScan 은 컴퓨터에서 바이러스, 트로이 목마 또는 쿠키 추적을 검색할 경우 감염된 파일을 치료하려고 합니다. 파일을 치료할 수 없는 경우 VirusScan 은 파일을 격리합니다.

일부 보안 위협의 경우 VirusScan 이 파일을 치료하거나 격리하지 못할 수 있습니다. 이러한 경우 VirusScan 은 위협을 처리하도록 요청하는 메시지를 표시합니다. 위협 유형에 따라 다른 작업을 수행할 수 있습니다. 예를 들어 파일에서 바이러스가 검색되었지만 VirusScan 이 파일을 치료하거나 격리할 수 없는 경우 이 파일에 대한 이후 액세스를 거부합니다. 쿠키 추적이 검색되었지만 VirusScan 이 파일을 치료하거나 격리할 수 없는 경우 쿠키를 제거 또는 신뢰할지 여부를 결정할 수 있습니다. 악성 프로그램이 검색되면 VirusScan 은 자동 작업을 수행하지 않고, 대신 사용자가 프로그램을 격리 또는 신뢰할 것을 결정하도록 합니다.

VirusScan 에서 항목을 격리할 때는 항목을 암호화한 다음 폴더에 격리하여 파일, 프로그램 또는 쿠키가 컴퓨터를 손상시키지 않도록 합니다. 격리된 항목을 복원하거나 제거할 수 있습니다. 대부분의 경우 시스템에 영향을 주지 않고 격리된 쿠키를 삭제할 수 있지만 VirusScan 이 사용자가 인식하고 사용하는 프로그램을 격리한 경우에는 복원하는 것이 좋습니다.

이 장에서

바이러스 및 트로이 목마 작업

VirusScan 은 실시간 검색 또는 수동 검색 중 컴퓨터의 파일에서 바이러스 또는 트로이 목마를 검색할 경우 해당 파일을 치료하려고 합니다. 파일을 치료할 수 없는 경우 VirusScan 은 파일을 격리하려고 합니다. 격리 시도 역시 실패하면 파일에 대한 액세스가 거부됩니다(실시간 검색에서만).

1 [검색 결과] 창을 엽니다.

방식

1. 작업 표시줄 맨 오른쪽에 있는 알림 영역에서 [검색 완료됨] 아이콘을 두 번 클릭합니다.
2. [검색 진행률: 수동 검색] 창에서 [결과 보기]를 클릭합니다.

2 검색 결과 목록에서 [바이러스 및 트로이 목마]를 클릭합니다.

참고: VirusScan이 격리한 파일로 작업하려면 격리된 파일 작업 (61 페이지)을 참조하십시오.

악성 프로그램 작업

VirusScan 이 실시간 또는 수동 검색 중 악성 프로그램을 검색할 경우 프로그램을 제거하거나 신뢰할 수 있습니다. 악성 프로그램을 제거하더라도 실제로 시스템에서 삭제되지는 않습니다. 대신, 프로그램을 격리하여 프로그램이 컴퓨터 또는 파일을 손상시키지 못하도록 합니다.

1 [검색 결과] 창을 엽니다.

방식

1. 작업 표시줄 맨 오른쪽에 있는 알림 영역에서 [검색 완료됨] 아이콘을 두 번 클릭합니다.
2. [검색 진행률: 수동 검색] 창에서 [결과 보기]를 클릭합니다.

2 검색 결과 목록에서 [악성 프로그램]을 클릭합니다.

3 악성 프로그램을 선택합니다.

4 [원하는 작업]에서 [제거] 또는 [신뢰]를 클릭합니다.

5 선택한 옵션을 확인합니다.

격리된 파일 작업

VirusScan 에서 감염된 파일을 격리할 때는 파일을 암호화한 다음 폴더에 격리하여 파일이 컴퓨터를 손상시키지 않도록 합니다. 그런 다음 격리된 파일을 복원하거나 제거할 수 있습니다.

1 [격리된 파일] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [복원]을 클릭합니다.
3. [파일]을 클릭합니다.

2 격리된 파일을 선택합니다.

3 다음 중 하나를 수행합니다.

- 감염된 파일을 치료하고 컴퓨터의 원래 위치로 되돌리려면 [복원]을 클릭합니다.
- 컴퓨터에서 감염된 파일을 제거하려면 [제거]를 클릭합니다.

4 [예]를 클릭하여 선택한 옵션을 확인합니다.

팁: 여러 파일을 동시에 복원하거나 제거할 수 있습니다.

격리된 프로그램 및 쿠키 작업

VirusScan 에 악성 프로그램 또는 쿠키 추적을 격리할 때는 해당 항목을 암호화한 다음 보호된 폴더로 이동하여 프로그램 또는 쿠키가 컴퓨터를 손상시키지 않도록 합니다. 그런 다음 격리된 항목을 복원하거나 제거할 수 있습니다. 대부분의 경우 시스템에 영향을 주지 않고 격리된 항목을 삭제할 수 있습니다.

1 [격리된 프로그램 및 쿠키 추적] 창을 엽니다.

방식

1. 왼쪽 창에서 [고급 메뉴]를 클릭합니다.
2. [복원]을 클릭합니다.
3. [프로그램 및 쿠키]를 클릭합니다.

2 격리된 프로그램 또는 쿠키를 선택합니다.

3 다음 중 하나를 수행합니다.

- 감염된 파일을 치료하고 컴퓨터의 원래 위치로 되돌리려면 [복원]을 클릭합니다.

- 컴퓨터에서 감염된 파일을 제거하려면 [제거]를 클릭합니다.

4 [예]를 클릭하여 작업을 확인합니다.

팁: 여러 프로그램 및 쿠키를 동시에 복원하거나 제거할 수 있습니다.

제 13 장

McAfee Personal Firewall

Personal Firewall 은 컴퓨터 및 개인 데이터를 보다 안전하게 보호합니다. Personal Firewall 은 컴퓨터와 인터넷 사이에 장벽을 설치하여 의심되는 활동에 대해 인터넷 트래픽을 자동으로 모니터링합니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

Personal Firewall 기능

Personal Firewall 에서는 다음과 같은 기능을 제공합니다.

표준 및 사용자 정의 보호 수준

Firewall 의 기본값 또는 사용자 지정 가능한 보호 설정을 사용하여 침입과 의심스러운 활동으로부터 보호합니다.

실시간 권장 사항

동적으로 권장 사항을 받아 프로그램의 인터넷 액세스를 허용할지 네트워크 트래픽을 신뢰할지 여부를 결정하는 데 도움을 줍니다.

프로그램에 대해 지능형 액세스 관리

경고 및 이벤트 로그를 통해 프로그램에 대한 인터넷 액세스를 관리하고 특정 프로그램에 대해 액세스 권한을 구성합니다.

게임 보호

전체 화면으로 게임을 즐기는 동안 침입 시도 및 의심스러운 활동과 관련된 경고가 표시되지 않도록 합니다.

컴퓨터 시작 시 보호

Windows®가 시작되면 바로 Firewall 은 침입 시도, 악성 프로그램 및 네트워크 트래픽으로부터 컴퓨터를 보호합니다.

시스템 서비스 포트 제어

일부 프로그램이 필요로 하는 열리거나 닫힌 시스템 서비스 포트를 관리합니다.

컴퓨터 연결 관리

사용자의 컴퓨터와 다른 컴퓨터 간 원격 연결을 허용하거나 차단합니다.

HackerWatch 정보 통합

HackerWatch 웹 사이트를 통해 글로벌 해킹 및 침입 패턴을 추적합니다. 이 웹 사이트에서는 사용자의 컴퓨터에서 실행되는 프로그램에 대한 현재 보안 정보와 글로벌 보안 이벤트 및 인터넷 포트 통계를 제공합니다.

방화벽 잠금

컴퓨터와 인터넷 사이의 모든 인바운드 및 아웃바운드 트래픽을 즉시 차단합니다.

방화벽 복원

Firewall 의 원래 보호 설정을 즉시 복원합니다.

고급 트로이 목마 검색

트로이 목마와 같이 잠재적으로 해로운 응용 프로그램이 인터넷에 개인 데이터를 릴레이하는 것을 검색하고 차단합니다.

이벤트 로그 기록

최신 인바운드, 아웃바운드 및 침입 이벤트를 추적합니다.

인터넷 트래픽 모니터링

악성 공격 및 트래픽의 발생지를 보여 주는 전세계 맵을 검토합니다. 또한 발생 IP 주소에 대한 자세한 연락처/소유자 정보 및 지리적 데이터를 찾을 수 있습니다. 인바운드 및 아웃바운드 트래픽을 분석하고 프로그램 대역폭과 프로그램 활동을 모니터링합니다.

침입 방지

인터넷 위협으로부터 개인 정보를 보호합니다. 휴리스틱 기능을 사용하는 McAfee 는 공격 증상이나 해킹 시도 특징을 표시하는 항목을 차단하여 3 단계 보호를 제공합니다.

고급 트래픽 분석

인바운드 및 아웃바운드 인터넷 트래픽, 프로그램 연결, 열린 연결에 대해 활동적으로 수신하는 프로그램을 감시합니다. 이를 통해 침입에 취약한 프로그램을 감시하고 조치를 취할 수 있습니다.

제 14 장

방화벽 시작

방화벽을 설치하는 즉시 침입과 원치 않는 네트워크 트래픽으로부터 컴퓨터를 보호합니다. 또한 알려지거나 알려지지 않은 프로그램의 경고를 처리하고 인바운드 및 아웃바운드 인터넷 액세스를 관리할 수 있습니다. 스마트 권장 사항 및 신뢰 보안 수준(프로그램에 아웃바운드 전용 인터넷 액세스를 허용하는 옵션 선택)이 자동으로 활성화됩니다.

인터넷 및 네트워크 구성 창에서 방화벽을 비활성화 할 수 있지만 그렇게 하면 컴퓨터가 더 이상 침입과 원치 않는 네트워크 트래픽으로부터 보호되지 않으며 인바운드 및 아웃바운드 인터넷 연결을 효과적으로 관리할 수 없습니다. 방화벽 보호를 비활성화해야만 한다면 꼭 필요한 경우에 일시적으로 수행합니다. [인터넷 및 네트워크 구성] 패널에서 방화벽을 활성화할 수도 있습니다.

Firewall 은 자동으로 Windows® 방화벽을 비활성화하고 자신을 기본 방화벽으로 설정합니다.

참고: 방화벽을 구성하려면 인터넷 및 네트워크 구성 창을 엽니다.

이 장에서

방화벽 보호 시작

Firewall 을 활성화하여 침입과 원치 않는 네트워크 트래픽으로부터 컴퓨터를 보호하고 인바운드 및 아웃바운드 인터넷 연결을 관리할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [설정]을 클릭합니다.

방화벽 보호 중지

침입과 원치 않는 네트워크 트래픽으로부터 컴퓨터를 보호하지 않으려는 경우에는 Firewall 을 비활성화할 수 있습니다. Firewall 이 비활성화되면 인바운드 또는 아웃바운드 인터넷 연결을 관리할 수 없습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [해제]를 클릭합니다.

제 15 장

경고 작업

방화벽에서는 보안 관리를 돕기 위해 경고 배열을 채택하고 있습니다. 이러한 경고는 세 가지 기본 유형으로 그룹화할 수 있습니다.

- 빨간색 경고
- 노란색 경고
- 녹색 경고

경고는 컴퓨터에서 실행되는 프로그램에 관한 정보를 얻거나 경고 처리 방법을 결정하는 데 도움이 되는 정보를 포함할 수 있습니다.

이 장에서

경고 정보

Firewall 에는 세 가지 기본 경고 유형이 있습니다. 일부 경고는 사용자 컴퓨터에서 실행되는 프로그램에 관한 정보를 사용하거나 얻도록 도와주는 정보를 포함합니다.

빨간색 경고

빨간색 경고는 Firewall 이 사용자의 컴퓨터에서 트로이 목마를 감지한 다음 차단할 때 나타나며 추가 위협을 검색하도록 권장합니다. 트로이 목마는 합법적인 프로그램처럼 보이지만 혼란이나 손상을 초래하거나 컴퓨터에 대한 무단 액세스를 가능하게 할 수 있습니다. 이 경고는 [개방]을 제외한 모든 보안 수준에서 표시됩니다.

노란색 경고

노란색 경고는 가장 일반적인 경고 유형으로 Firewall 에서 발견한 프로그램 활동 또는 네트워크 이벤트에 대해 알려줍니다. 이 경고는 프로그램 활동 또는 네트워크 이벤트에 대해 설명한 다음 사용자의 응답을 요구하는 하나 이상의 옵션을 제공합니다. 예를 들어, Firewall 이 설치되어 있는 컴퓨터가 새 네트워크에 연결되면 [새 네트워크가 검색됨] 경고가 표시됩니다. 네트워크를 신뢰 또는 신뢰하지 않음을 선택할 수 있습니다. 네트워크를 신뢰하면 방화벽은 네트워크의 다른 컴퓨터의 트래픽을 허용하여 신뢰하는 IP 주소에 추가합니다. 스마트 권장 사항이 활성화되면 프로그램을 [프로그램 사용 권한] 창에 추가합니다.

녹색 경고

대부분의 경우 녹색 경고는 이벤트에 대한 기본 정보를 제공하고 응답이 필요하지 않습니다. 녹색 경고는 기본적으로 비활성화되어 있으며, 일반적으로 [표준], [신뢰], [강력] 및 [은폐] 보안 수준이 설정된 경우 표시됩니다.

사용자 지원

많은 방화벽 경고는 다음을 포함하는 사용자 컴퓨터의 보안을 관리하도록 돕는 추가적인 정보를 포함합니다.

- **이 프로그램에 대한 자세한 내용:** McAfee 글로벌 보안 웹사이트를 시작하여 사용자 컴퓨터에서 검색되는 방화벽 프로그램에 관한 정보를 받습니다.

- **이 프로그램에 대해 McAfee에 알려 줍니다.**: 사용자 컴퓨터에서 검색된 방화벽의 알 수 없는 파일에 관한 정보를 McAfee에 보냅니다.
- **McAfee 권장 사항**: 경고 처리에 관해 조언합니다. 예를 들어, 경고는 프로그램에 대한 액세스를 허용하도록 권장할 수 있습니다.

제 16 장

정보 경고 관리

Firewall 에서는 특정 이벤트 동안(예: 전체 화면으로 게임을 실행하는 동안) 침입 시도나 의심스러운 활동이 감지될 때 정보 경고를 표시하거나 숨길 수 있습니다.

이 장에서

게임하는 동안 경고 표시

전체 화면으로 게임을 실행하는 동안 Firewall 에서 침입 시도나 의심스러운 활동을 감지한 경우 정보 경고를 표시하도록 할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [SecurityCenter 구성] 창의 [경고]에서 [고급]을 클릭합니다.
4. [경고 옵션] 창에서 [게임 모드가 검색될 때 정보 경고 표시]를 선택합니다.
5. [확인]을 클릭합니다.

정보 경고 숨기기

Firewall 에서 침입 시도나 의심스러운 활동을 감지할 때 정보 경고를 표시하지 않도록 할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [구성]을 클릭합니다.
3. [SecurityCenter 구성] 창의 [경고]에서 [고급]을 클릭합니다.
4. [SecurityCenter 구성] 창에서 [정보 경고]를 클릭합니다.
5. [정보 경고] 창에서 다음 중 하나를 수행합니다.
   - [정보 경고 표시 안 함]을 선택하여 모든 정보 경고를 숨깁니다.
   - 숨길 경고를 선택 취소합니다.
6. [확인]을 클릭합니다.

제 17 장

방화벽 보호 구성

방화벽은 사용자 보안을 관리하는 많은 방법과 보안 이벤트 및 경고에 응답할 꼭 맞는 방법을 제공합니다.

처음 Firewall 을 설치하면 컴퓨터의 보호 보안 수준이 [신뢰]로 설정되고 프로그램에 아웃바운드 전용 인터넷 액세스가 허용됩니다. 그러나 방화벽은 매우 제한적인 수준부터 관대한 수준까지 다양한 수준을 제공합니다.

방화벽은 프로그램에 대한 경고와 인터넷 액세스 권장 사항을 수신하는 기회도 제공합니다.

이 장에서

방화벽 보안 수준 관리

Firewall 의 보안 수준은 경고를 관리하고 대응하는 수준를 제어합니다. 이러한 경고는 원치 않는 네트워크 트래픽과 인바운드 및 아웃바운드 인터넷 연결이 검색될 때 나타납니다. 기본적으로 Firewall 의 보안 수준은 아웃바운드 전용 액세스에서 [신뢰]로 설정됩니다.

[신뢰] 보안 수준이 설정되고 [스마트 권장 사항]이 활성화되면 노란색 경고는 인바운드 액세스를 필요로 하는 알려지지 않은 프로그램에 대한 액세스를 허용하거나 차단하는 옵션을 제공합니다. 알려진 프로그램을 검색하면 녹색 정보 경고가 나타나며 액세스가 자동으로 허용됩니다. 액세스를 허용하면 프로그램에서 아웃바운드 연결을 만들고 원치 않는 들어오는 연결에 대해 수신 대기할 수 있습니다.

일반적으로 보다 제한적인 보안 수준(은폐 및 강력)에는 더 많은 옵션과 경고가 표시되며, 이러한 옵션과 경고를 사용자가 처리해야 합니다.

다음 표에는 Firewall 의 6 가지 보안 수준이 가장 제한적인 수준부터 차례대로 설명되어 있습니다.

수준	설명
잠금	웹 사이트, 전자 메일 및 보안 업데이트에 대한 액세스를 비롯하여 모든 인바운드 및 아웃바운드 네트워크 연결을 차단합니다. 이 보안 수준은 인터넷 연결을 삭제하는 것과 같은 결과를 가져옵니다. 이 설정을 사용하여 시스템 서비스 창에서 열리도록 설정된 포트를 차단할 수 있습니다.
은폐	인터넷에서 컴퓨터의 존재를 숨겨서 열린 포트를 제외한 모든 인바운드 인터넷 연결을 차단합니다. Firewall 은 새 프로그램에서 아웃바운드 인터넷 연결을 시도하거나 인바운드 연결 요청을 받을 경우 알려 줍니다. 차단되거나 추가된 프로그램은 [프로그램 사용 권한] 창에 표시됩니다.
강력	새 프로그램에서 아웃바운드 인터넷 연결을 시도하거나 인바운드 연결 요청을 받을 경우 알려 줍니다. 차단되거나 추가된 프로그램은 [프로그램 사용 권한] 창에 표시됩니다. 보안 수준이 [강력]으로 설정되면 프로그램은 허용하거나 차단할 수 있는 아웃바운드 전용 액세스와 같이 그 때 필요로 하는 액세스 유형만 요청합니다. 나중에 프로그램에 인바운드 및 아웃바운드 연결이 필요하면 [프로그램 사용 권한] 창에서 프로그램 전체 액세스를 허용할 수 있습니다.

수준	설명
표준	인바운드 및 아웃바운드 연결을 모니터링하며 새 프로그램에서 인터넷 액세스를 시도할 경우 알려 줍니다. 차단되거나 추가된 프로그램은 [프로그램 사용 권한] 창에 표시됩니다.
신뢰	프로그램에 인바운드 및 아웃바운드(전체) 또는 아웃바운드 전용 인터넷 액세스를 허용합니다. 기본 보안 수준은 [신뢰]이며 프로그램에 아웃바운드 전용 액세스를 허용하는 옵션이 선택됩니다. 프로그램에 전체 액세스가 허용된 경우 Firewall 은 자동으로 이 프로그램을 신뢰하고 [프로그램 사용 권한] 창의 허용된 프로그램 목록에 추가합니다. 프로그램에 아웃바운드 전용 액세스가 허용된 경우 Firewall 은 아웃바운드 인터넷 연결의 경우에만 자동으로 이 프로그램을 신뢰합니다. 인바운드 연결은 자동으로 신뢰되지 않습니다.
개방	모든 인바운드 및 아웃바운드 인터넷 연결을 허용합니다.

또한 [방화벽 보호 기본값 복원] 창에서 보안 수준을 [신뢰]로 재설정하고 아웃바운드 전용 액세스를 허용할 수 있습니다.

보안 수준을 잠금으로 설정

Firewall 의 보안 수준을 [잠금]으로 설정하여 모든 인바운드 및 아웃바운드 네트워크 연결을 차단할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [잠금]을 현재 수준으로 표시합니다.
4. [확인]을 클릭합니다.

보안 수준을 은폐로 설정

Firewall 보안 수준을 [은폐]로 설정하면 열린 포트를 제외한 모든 인바운드 네트워크 연결을 차단하여 인터넷에서 컴퓨터의 존재를 숨길 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [은폐]를 현재 수준으로 표시합니다.
4. [확인]을 클릭합니다.

참고: 은폐 모드에서 Firewall은 새 프로그램이 아웃바운드 인터넷 연결을 요청하거나 인바운드 연결 요청을 받을 때 사용자에게 알려 줍니다.

보안 수준을 강력으로 설정

Firewall 보안 수준을 [강력]으로 설정하면 새 프로그램이 아웃바운드 인터넷 연결을 시도하거나 인바운드 연결 요청을 수신할 때 경고가 표시됩니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [강력]을 현재 수준으로 표시합니다.
4. [확인]을 클릭합니다.

참고: 강력 모드에서 프로그램은 허용하거나 차단할 수 있는 아웃바운드 전용 액세스와 같이 그 때 필요로 하는 액세스 유형만 요청합니다. 나중에 프로그램에 인바운드 및 아웃바운드 연결이 필요하면 [프로그램 사용 권한] 창에서 프로그램 전체 액세스를 허용할 수 있습니다.

보안 수준을 표준으로 설정

보안 수준을 [표준]으로 설정하면 인바운드 및 아웃바운드 연결을 모니터링하고 새 프로그램에서 인터넷 액세스를 시도할 경우 경고 메시지가 표시됩니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [표준]을 현재 수준으로 표시합니다.
4. [확인]을 클릭합니다.

보안 수준을 신뢰로 설정

Firewall 의 보안 수준을 [신뢰]로 설정하면 전체 액세스 또는 아웃바운드 전용 네트워크 액세스를 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [신뢰]를 현재 수준으로 표시합니다.
4. 다음 중 하나를 수행합니다.
   - 전체 인바운드 및 아웃바운드 네트워크 액세스를 허용하려면 [전체 액세스 허용]을 선택합니다.
   - 아웃바운드 전용 네트워크 액세스를 허용하려면 [아웃바운드 전용 액세스 허용]을 선택합니다.
5. [확인]을 클릭합니다.

참고: 기본 옵션은 [아웃바운드 전용 액세스 허용]입니다.

보안 수준을 개방으로 설정

Firewall 의 보안 수준을 [개방]으로 설정하면 모든 인바운드 및 아웃바운드 네트워크 연결을 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창에서 슬라이더를 이동하여 [개방]을 현재 수준으로 표시합니다.
4. [확인]을 클릭합니다.

경고에 대해 스마트 권장 사항 구성

프로그램이 인터넷 액세스를 시도할 때 나타나는 경고에 권장 사항을 포함, 제외 또는 표시하도록 Firewall 을 구성할 수 있습니다. 스마트 권장 사항 활성화는 경고 처리 방법의 결정을 도와줍니다.

[스마트 권장 사항]을 활성화하고 보안 수준이 [신뢰]로 설정되고 아웃바운드 전용 액세스가 활성화되어 있는 경우 Firewall 은 알려진 프로그램을 자동으로 허용하거나 차단하고, 위험할 수 있는 프로그램이 발견되면 경고에 권장 사항을 표시합니다.

[스마트 권장 사항]을 비활성화하면 Firewall 은 인터넷 액세스를 허용하거나 차단하지 않으며 경고에 권장 사항을 표시하지 않습니다.

[스마트 권장 사항]을 [표시 전용]으로 설정하면 경고에서 액세스를 허용하거나 차단할지 여부를 물으며, 경고에 권장 사항이 함께 표시됩니다.

스마트 권장 사항 활성화

[스마트 권장 사항]을 활성화하면 Firewall 에서 프로그램을 자동으로 허용하거나 차단하고, 인식되지 않거나 잠재적으로 위험한 프로그램에 대해 경고를 표시합니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창의 [스마트 권장 사항]에서 [스마트 권장 사항 활성화]를 선택합니다.
4. [확인]을 클릭합니다.

스마트 권장 사항 비활성화

[스마트 권장 사항]을 비활성화하면 Firewall 에서 프로그램을 허용하거나 차단하고, 인식되지 않거나 잠재적으로 위험한 프로그램에 대해 경고를 표시합니다. 그러나 프로그램의 액세스 처리에 대한 권장 사항은 포함되지 않습니다. Firewall 에서 의심되거나 위험 가능성이 있는 새 프로그램을 검색하면 프로그램이 인터넷에 액세스하지 못하도록 자동으로 차단합니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창의 [스마트 권장 사항]에서 [스마트 권장 사항 비활성화]를 선택합니다.
4. [확인]을 클릭합니다.

스마트 권장 사항만 표시

경고에 작업 계획에 대한 권장 사항만 표시되며 인식되지 않거나 잠재적으로 위험한 프로그램을 허용할지 차단할지 여부는 사용자가 결정하도록 [스마트 권장 사항]을 표시할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창의 [스마트 권장 사항]에서 [표시 전용]을 선택합니다.
4. [확인]을 클릭합니다.

방화벽 보안 최적화

컴퓨터 보안에는 많은 방법이 있을 수 있습니다. 예를 들어, 일부 프로그램은 Windows®가 시작되기 전에 인터넷 연결을 시도할 수 있습니다. 또한 해커가 사용자의 컴퓨터를 추적하거나 ping 을 수행하여 컴퓨터가 네트워크에 연결되어 있는지 확인할 수도 있습니다. Firewall 에서는 시작 시 보호 활성화 및 ping 요청 차단을 허용하여 이 두 가지 유형의 침입에 대해 사용자를 보호합니다. 첫 번째 설정은 Windows 시작 시 프로그램이 인터넷에 액세스하지 못하도록 차단하고, 두 번째 설정은 네트워크에서 다른 사용자가 컴퓨터를 검색하지 못하도록 ping 요청을 차단합니다.

표준 설치 설정에는 서비스 거부 공격이나 악용 같은 가장 일반적인 침입 시도에 대한 자동 탐지 기능이 포함됩니다. 표준 설치 설정을 사용하면 이런 공격이나 검색으로부터 보호 받을 수 있습니다. 그러나, 침입 탐지 창에서 하나 이상의 공격이나 검색에 대한 자동 탐지를 사용하지 않도록 설정할 수 있습니다.

시작하는 동안의 컴퓨터 보호

시작 시 인터넷 액세스를 필요로 하는 새 프로그램을 차단하여 Windows 시작 시 사용자 컴퓨터를 보호할 수 있습니다. Firewall 은 인터넷 액세스를 요청한 프로그램에 대해 관련 경고를 표시하며 사용자가 이를 허용하거나 차단할 수 있습니다. 이 옵션을 사용하려면 사용자의 보안 수준이 열기 또는 잠금으로 설정되면 안됩니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [보안 수준] 창의 [보안 설정]에서 [시작 시 보호 활성화]를 선택합니다.
4. [확인]을 클릭합니다.

참고: 차단된 연결 및 침입은 시작 시 보호가 활성화된 동안에는 로깅되지 않습니다.

ping 요청 설정 구성

네트워크에서 다른 컴퓨터 사용자가 사용자의 컴퓨터를 감지하도록 허용하거나 차단할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [보안 수준] 창의 [보안 설정]에서 다음 중 하나를 수행합니다.

- ping 요청을 사용한 네트워크상의 사용자 컴퓨터 보호를 허용하려면 [ICMP ping 요청 허용]을 선택합니다.
- ping 요청을 사용한 네트워크상의 사용자 컴퓨터 보호를 해제하려면 [ICMP ping 요청 허용]의 선택을 취소합니다.

4 [확인]을 클릭합니다.

침입 검색 구성

침입 시도를 검색하여 공격 및 권한 없는 검색으로부터 컴퓨터를 보호할 수 있습니다. Firewall 의 표준 설정에는 서비스 거부 공격 또는 악용과 같은 가장 일반적인 침입 시도에 대한 자동 탐지 기능이 포함되며, 하나 이상의 공격 또는 검색에 대해 자동 탐지를 비활성화할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [방화벽] 창에서 [침입 검색]을 클릭합니다.

4 [침입 시도 검색]에서 다음 중 하나를 수행합니다.

- 공격 또는 검색 작업을 자동으로 탐지하도록 이름을 선택합니다.
- 공격 또는 검색 작업의 자동 탐지를 비활성화하도록 이름 선택을 취소합니다.

5 [확인]을 클릭합니다.

방화벽 보호 상태 설정 구성

컴퓨터에서 발생한 특정 문제를 SecurityCenter 에 보고하지 않고 무시하도록 Firewall 을 구성할 수 있습니다.

1 McAfee SecurityCenter 창의 [SecurityCenter 정보]에서 [구성]을 클릭합니다.

2 [SecurityCenter 구성] 창의 [보호 상태]에서 [고급]을 클릭합니다.

3 [무시된 문제점] 창에서 다음 옵션 중 하나 이상을 선택합니다.

- **방화벽 보호가 비활성화되었습니다.**
- **방화벽이 개방 보안 수준으로 설정됩니다.**
- **방화벽 서비스가 실행되고 있지 않습니다.**
- **컴퓨터에 방화벽 보호가 설치되어 있지 않습니다.**
- **Windows 방화벽이 비활성화되었습니다.**
- **아웃바운드 방화벽이 컴퓨터에 설치되어 있지 않습니다.**

4 [확인]을 클릭합니다.

방화벽 잠금 및 복원

잠금은 모든 인바운드 및 아웃바운드 네트워크 트래픽을 즉시 차단하여 컴퓨터의 문제를 격리하고 해결할 수 있도록 해 줍니다.

방화벽 즉시 잠금

Firewall 을 잠가서 컴퓨터와 인터넷 간의 모든 네트워크 트래픽을 즉시 차단할 수 있습니다.

1. McAfee SecurityCenter 창의 [일반적인 작업]에서 [방화벽 잠금]을 클릭합니다.
2. [방화벽 잠금] 창에서 [잠금]을 클릭합니다.
3. [예]를 클릭하여 확인합니다.

팁: 작업 표시줄 맨 오른쪽의 알림 영역에서 SecurityCenter 아이콘 을 마우스 오른쪽 단추로 클릭한 다음 [빠른 링크]를 클릭하고 [방화벽 잠금]을 클릭하여 Firewall을 잠글 수도 있습니다.

방화벽 즉시 잠금 풀기

Firewall 의 잠금을 풀어서 컴퓨터와 인터넷 간의 모든 네트워크 트래픽을 즉시 허용할 수 있습니다.

1. McAfee SecurityCenter 창의 [일반적인 작업]에서 [방화벽 잠금]을 클릭합니다.
2. [잠금이 활성화됨] 창에서 [잠금 풀기]를 클릭합니다.
3. [예]를 클릭하여 확인합니다.

방화벽 설정 복원

방화벽을 원래 보호 설정으로 빠르게 복원합니다. 이렇게 복원하면 보안 수준이 [신뢰]로 재설정되고, 아웃바운드 전용 네트워크 액세스가 허용되며, [스마트 권장 사항]이 활성화되고, [프로그램 사용 권한] 창의 기본 프로그램과 사용 권한 목록이 복원되며, 신뢰 및 금지된 IP 주소가 제거되고, 시스템 서비스, 이벤트 로그 설정 및 침입 감지가 복원됩니다.

1 McAfee SecurityCenter 창에서 [방화벽 기본값 복원]을 클릭합니다.

2 [방화벽 보호 기본값 복원] 창에서 [기본값 복원]을 클릭합니다.

3 [예]를 클릭하여 확인합니다.

팁: 작업 표시줄 맨 오른쪽의 알림 영역에서 SecurityCenter 아이콘 을 마우스 오른쪽 단추로 클릭한 다음 [빠른 링크]를 클릭하고 [방화벽 기본값 복원]을 클릭하여 Firewall의 기본 설정을 복원할 수도 있습니다.

제 18 장

프로그램 및 권한 관리

방화벽에서 인바운드 및 아웃바운드 인터넷 액세스를 필요로 하는 기존 및 새 프로그램을 관리하고 작성하는 액세스 권한을 허용합니다. Firewall 에서는 프로그램에 대한 전체 또는 아웃바운드 전용 액세스를 제어할 수 있습니다. 프로그램 액세스를 차단할 수도 있습니다.

이 장에서

프로그램에 인터넷 액세스 허용

인터넷 브라우저와 같은 일부 프로그램들은 제대로 작동하려면 인터넷 액세스가 필요합니다.

방화벽에서 프로그램 사용 권한 페이지 사용을 허용합니다.

- 프로그램에 액세스 허용
- 프로그램에 아웃바운드 전용 액세스 허용
- 프로그램에 액세스 차단

또한 프로그램이 아웃바운드 이벤트 및 최신 이벤트 로그에서 전체 및 아웃바운드 전용 인터넷 액세스를 갖도록 허용할 수도 있습니다.

프로그램에 전체 액세스 허용

컴퓨터에서 기존의 차단된 프로그램이 전체 인바운드 및 아웃바운드 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.
4. [프로그램 사용 권한]에서 프로그램에 [차단됨] 또는 [아웃바운드 전용 액세스]를 선택합니다.
5. [작업]에서 [액세스 허용]을 클릭합니다.
6. [확인]을 클릭합니다.

새 프로그램에 전체 액세스 허용

컴퓨터의 새 프로그램이 전체 인바운드 및 아웃바운드 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.
4. [프로그램 사용 권한]에서 [허용된 프로그램 추가]를 클릭합니다.
5. [프로그램 추가] 대화 상자에서 추가할 프로그램을 찾아 선택한 다음 [열기]를 클릭합니다.

참고: 기존 프로그램과 마찬가지로 프로그램을 선택한 후 [작업]에서 [아웃바운드 전용 액세스 허용] 또는 [액세스 차단]을 클릭하여 새로 추가된 프로그램의 사용 권한을 변경할 수 있습니다.

최신 이벤트 로그에서 전체 액세스 허용

최신 이벤트 로그에 표시되는 기존의 차단된 프로그램이 전체 인바운드 및 아웃바운드 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 이벤트 설명을 선택하고 [액세스 허용]을 클릭합니다.
4. [프로그램 사용 권한] 대화 상자에서 [예]를 클릭하여 확인합니다.

관련 항목

- 아웃바운드 이벤트 보기 (115 페이지)

아웃바운드 이벤트 로그에서 전체 액세스 허용

아웃바운드 이벤트 로그에 표시되는 기존의 차단된 프로그램이 전체 인바운드 및 아웃바운드 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 [로그 보기]를 클릭합니다.
4. [인터넷 및 네트워크]를 클릭한 다음 [아웃바운드 이벤트]를 클릭합니다.
5. 프로그램을 선택하고 [원하는 작업]에서 [액세스 허용]을 클릭합니다.
6. [프로그램 사용 권한] 대화 상자에서 [예]를 클릭하여 확인합니다.

프로그램에 아웃바운드 전용 액세스 허용

컴퓨터에 설치된 일부 프로그램은 아웃바운드 인터넷 액세스를 필요로 합니다. Firewall 에서는 아웃바운드 전용 인터넷 액세스를 허용하도록 프로그램 사용 권한을 구성할 수 있습니다.

프로그램에 아웃바운드 전용 액세스 허용

프로그램에 아웃바운드 전용 인터넷 액세스 권한을 부여할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.
4. [프로그램 사용 권한]에서 프로그램에 [차단됨] 또는 [전체 액세스]를 선택합니다.
5. [작업]에서 [아웃바운드 전용 액세스 허용]을 클릭합니다.
6. [확인]을 클릭합니다.

최신 이벤트 로그에서 아웃바운드 전용 액세스 허용

최신 이벤트 로그에 표시되는 기존의 차단된 프로그램이 아웃바운드 전용 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 이벤트 설명을 선택하고 [아웃바운드 전용 액세스 허용]을 클릭합니다.
4. [프로그램 사용 권한] 대화 상자에서 [예]를 클릭하여 확인합니다.

아웃바운드 이벤트 로그에서 아웃바운드 전용 액세스 허용

아웃바운드 이벤트 로그에 표시되는 기존의 차단된 프로그램이 아웃바운드 전용 인터넷 액세스 권한을 갖도록 허용할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 [로그 보기]를 클릭합니다.
4. [인터넷 및 네트워크]를 클릭한 다음 [아웃바운드 이벤트]를 클릭합니다.
5. 프로그램을 선택하고 [원하는 작업]에서 [아웃바운드 전용 액세스 허용]을 클릭합니다.
6. [프로그램 사용 권한] 대화 상자에서 [예]를 클릭하여 확인합니다.

프로그램에 인터넷 액세스 차단

Firewall 에서는 프로그램이 인터넷에 액세스하지 못하도록 차단할 수 있습니다. 프로그램 차단이 사용자 네트워크 연결 또는 제대로 작동하려면 인터넷 액세스가 필요한 다른 프로그램을 중단시키지 않는지 확인합니다.

프로그램에 액세스 차단

프로그램에 대해 인바운드 및 아웃바운드 인터넷 액세스를 차단할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.

4 [프로그램 사용 권한]에서 프로그램에 [전체 액세스] 또는 [아웃바운드 전용 액세스]를 선택합니다.

5 [작업]에서 [액세스 차단]을 클릭합니다.

6 [확인]을 클릭합니다.

새 프로그램에 액세스 차단

새 프로그램에 대해 인바운드 및 아웃바운드 인터넷 액세스를 차단할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.

4 [프로그램 사용 권한]에서 [차단된 프로그램 추가]를 클릭합니다.

5 [프로그램 추가] 대화 상자에서 추가할 프로그램을 찾아 선택한 다음 [열기]를 클릭합니다.

참고: 프로그램을 선택한 후 [작업]에서 [아웃바운드 전용 액세스 허용] 또는 [액세스 허용]을 클릭하여 새로 추가된 프로그램의 사용 권한을 변경할 수 있습니다.

최신 이벤트 로그에서 액세스 차단

최신 이벤트 로그에 표시되는 프로그램의 인바운드 및 아웃바운드 인터넷 액세스를 차단할 수 있습니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 이벤트 설명을 선택하고 [액세스 차단]을 클릭합니다.
4. [프로그램 사용 권한] 대화 상자에서 [예]를 클릭하여 확인합니다.

프로그램의 액세스 사용 권한 제거

프로그램 사용 권한을 제거하기 전에 컴퓨터의 기능 또는 네트워크 연결에 영향을 주지 않는지 확인하십시오.

프로그램 사용 권한 제거

프로그램의 인바운드 또는 아웃바운드 인터넷 액세스를 제거할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.
4. [프로그램 사용 권한]에서 프로그램을 선택합니다.
5. [작업]에서 [프로그램 사용 권한 제거]를 클릭합니다.
6. [확인]을 클릭합니다.

참고: 일부 동작은 흐리게 표시되고 비활성화되어 사용자가 프로그램을 수정하지 못하도록 설정되어 있습니다.

프로그램에 대해 알아보기

적용할 프로그램 사용 권한을 모를 경우 McAfee 의 HackerWatch 웹 사이트에서 프로그램에 관한 정보를 얻을 수 있습니다.

프로그램 정보 얻기

McAfee 의 HackerWatch 웹 사이트에서는 인바운드 및 아웃바운드 인터넷 액세스를 허용하거나 차단할지 여부를 결정하는 데 도움이 되는 프로그램 정보를 얻을 수 있습니다.

참고: 프로그램에 대한 최신 정보, 인터넷 액세스 요구 사항 및 보안 위협을 제공하는 McAfee의 HackerWatch 웹 사이트를 브라우저에서 시작하려면 인터넷에 연결되어 있어야 합니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [프로그램 사용 권한]을 클릭합니다.
4. [프로그램 사용 권한]에서 프로그램을 선택합니다.
5. [작업]에서 [자세한 내용]을 클릭합니다.

아웃바운드 이벤트 로그에서 프로그램 정보 얻기

아웃바운드 이벤트 로그에서는 McAfee HackerWatch 웹 사이트의 프로그램 정보를 얻어 인바운드 및 아웃바운드 인터넷 액세스를 허용하거나 차단할 프로그램을 결정할 수 있습니다.

참고: 프로그램에 대한 최신 정보, 인터넷 액세스 요구 사항 및 보안 위협을 제공하는 McAfee의 HackerWatch 웹 사이트를 브라우저에서 시작하려면 인터넷에 연결되어 있어야 합니다.

1. McAfee SecurityCenter 창에서 [고급 메뉴]를 클릭합니다.
2. [보고서 및 로그]를 클릭합니다.
3. [최신 이벤트]에서 이벤트를 선택하고 [로그 보기]를 클릭합니다.
4. [인터넷 및 네트워크]를 클릭한 다음 [아웃바운드 이벤트]를 클릭합니다.
5. IP 주소를 선택하고 [자세한 내용]을 클릭합니다.

제 19 장

시스템 서비스 관리

웹 서버와 파일 공유 서버 프로그램을 포함하는 특정 프로그램이 제대로 작동하려면 지정된 시스템 서비스 포트를 통해 다른 컴퓨터로부터 원하지 않는 연결을 허용해야 합니다. 시스템 서비스 포트는 시스템에서 보안이 가장 취약한 부분이므로 방화벽에서 대개 이러한 시스템 서비스 포트를 닫습니다. 하지만 원격 컴퓨터에서 연결을 허용하려면 시스템 서비스 포트가 열려있어야 합니다.

이 장에서

시스템 서비스 포트 구성

컴퓨터의 서비스에 대한 원격 네트워크 액세스를 허용하거나 차단하도록 시스템 서비스 포트를 구성할 수 있습니다.

아래 목록은 일반적인 시스템 서비스 및 관련 포트를 보여 줍니다.

- FTP(파일 전송 프로토콜) 포트 20-21
- 메일 서버(IMAP) 포트 143
- 메일 서버(POP3) 포트 110
- 메일 서버(SMTP) 포트 25
- MSFT DS(Microsoft Directory Server) 포트 445
- MSFT SQL(Microsoft SQL Server) 포트 1433
- 네트워크 시간 프로토콜 포트 123
- 원격 데스크톱/원격 지원/터미널 서버(RDP) 포트 3389
- RPC(원격 프로시저 호출) 포트 135
- 보안 웹 서버(HTTPS) 포트 443
- UPNP(범용 플러그앤플레이) 포트 5000
- 웹 서버(HTTP) 포트 80
- Windows 파일 공유(NETBIOS) 포트 137-139

컴퓨터가 동일한 네트워크에서 연결된 다른 컴퓨터와 인터넷 연결을 공유하도록 시스템 서비스 포트를 구성할 수도 있습니다. ICS(인터넷 연결 공유)라고 하는 이 연결을 사용하면 연결을 공유하는 컴퓨터가 네트워크의 다른 컴퓨터에 대해 인터넷의 게이트웨이 역할을 할 수 있습니다.

참고: 컴퓨터에 웹 또는 FTP 서버 연결을 허용하는 응용 프로그램이 있는 경우, 연결을 공유하는 컴퓨터는 연결된 시스템 서비스 포트를 열고 이러한 포트로 들어오는 연결의 전달을 허용해야 할 수 있습니다.

기존 시스템 서비스 포트에 대한 액세스 허용

기존 포트를 열어 컴퓨터의 네트워크 서비스에 대한 원격 액세스를 허용할 수 있습니다.

참고: 시스템 서비스 포트가 열려 있으면 컴퓨터가 인터넷 보안 위협에 취약해질 수 있으므로 필요한 경우에만 포트를 엽니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [시스템 서비스]를 클릭합니다.
4. [개방형 시스템 서비스 포트]에서 포트를 열 시스템 서비스를 선택합니다.
5. [확인]을 클릭합니다.

기존 시스템 서비스 포트에 대한 액세스 차단

기존 포트를 닫아서 컴퓨터의 서비스에 대한 원격 네트워크 액세스를 차단할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [시스템 서비스]를 클릭합니다.
4. [개방형 시스템 서비스 포트]에서 포트를 닫을 시스템 서비스의 선택을 취소합니다.
5. [확인]을 클릭합니다.

새 시스템 서비스 포트 구성

컴퓨터에 대한 원격 액세스를 허용하거나 차단하기 위해 열거나 닫을 수 있는 새 네트워크 서비스 포트를 구성할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [시스템 서비스]를 클릭합니다.
4. [추가]를 클릭합니다.
5. [시스템 서비스] 창의 [포트 및 시스템 서비스]에서 다음을 입력합니다.
   - 프로그램 이름
   - 인바운드 TCP/IP 포트
   - 아웃바운드 TCP/IP 포트
   - 인바운드 UDP 포트
   - 아웃바운드 UDP 포트
6. 이 포트의 활동 정보를 인터넷 연결을 공유하는 네트워크의 다른 Windows 컴퓨터로 보내려면 [이 포트의 네트워크 활동을 인터넷 연결 공유를 사용하는 네트워크 사용자에게 전달합니다.]를 선택합니다.
7. 필요에 따라 새 구성을 설명합니다.
8. [확인]을 클릭합니다.

참고: 컴퓨터에 웹 또는 FTP 서버 연결을 허용하는 응용 프로그램이 있는 경우, 연결을 공유하는 컴퓨터는 연결된 시스템 서비스 포트를 열고 이러한 포트로 들어오는 연결의 전달을 허용해야 할 수 있습니다. ICS(인터넷 연결 공유)를 사용하는 경우에는 [신뢰하는 IP 주소] 목록에 신뢰하는 컴퓨터 연결을 추가해야 합니다. 자세한 내용은 신뢰하는 컴퓨터 연결 추가를 참조하십시오.

시스템 서비스 포트 수정

기존 시스템 서비스 포트에 대한 인바운드 및 아웃바운드 네트워크 액세스 정보를 수정할 수 있습니다.

참고: 포트 정보를 잘못 입력하면 시스템 서비스가 실패합니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [시스템 서비스]를 클릭합니다.
4. 시스템 서비스를 선택하고 [편집]을 클릭합니다.
5. [시스템 서비스] 창의 [포트 및 시스템 서비스]에서 다음을 입력합니다.
   - 프로그램 이름
   - 인바운드 TCP/IP 포트
   - 아웃바운드 TCP/IP 포트
   - 인바운드 UDP 포트
   - 아웃바운드 UDP 포트
6. 이 포트의 활동 정보를 인터넷 연결을 공유하는 네트워크의 다른 Windows 컴퓨터로 보내려면 [이 포트의 네트워크 활동을 인터넷 연결 공유를 사용하는 네트워크 사용자에게 전달합니다.]를 선택합니다.
7. 필요에 따라 수정된 구성을 설명합니다.
8. [확인]을 클릭합니다.

시스템 서비스 포트 제거

컴퓨터에서 기존 시스템 서비스 포트를 제거할 수 있습니다. 제거한 후에는 원격 컴퓨터에서 사용자 컴퓨터의 네트워크 서비스에 더 이상 액세스할 수 없습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [시스템 서비스]를 클릭합니다.
4. 시스템 서비스를 선택하고 [제거]를 클릭합니다.
5. 메시지가 표시되면 [예]를 클릭하여 확인합니다.

제 20 장

컴퓨터 연결 관리

원격 컴퓨터에 연결된 인터넷 프로토콜 주소(IP)에 기반을 둔 규칙 작성을 통해 사용자 컴퓨터에 대한 특정 원격 연결을 관리하도록 방화벽을 구성할 수 있습니다. 신뢰하는 IP 주소로 연결된 컴퓨터들은 알 수 없거나 의심되거나 신뢰할 수 없는 사용자 컴퓨터와 IP 주소 연결을 신뢰할 수 있으며 사용자 컴퓨터 연결을 금지할 수 있습니다.

연결을 허용할 때 신뢰하는 컴퓨터가 안전한지 확인하십시오. 신뢰하는 컴퓨터가 웜 또는 기타 메커니즘을 통해 감염되는 경우 사용자의 컴퓨터도 감염에 취약해집니다. 사용자가 신뢰하는 컴퓨터도 방화벽이나 최신 안티바이러스 프로그램으로 보호하는 것이 좋습니다. 방화벽은 [신뢰하는 IP 주소] 목록에 있는 IP 주소의 트래픽에 대해서는 로그를 기록하거나 이벤트 경고를 생성하지 않습니다.

알 수 없거나 의심스럽거나 또는 신뢰하지 않는 IP 주소에 연결된 컴퓨터는 사용자의 컴퓨터에 연결하지 못하도록 금지할 수 있습니다.

방화벽은 원하지 않는 모든 트래픽을 차단하므로 일반적으로 IP 주소를 금지할 필요는 없습니다. 인터넷 연결에 특정 위협이 포함된 것이 확실한 경우에만 IP 주소를 금지해야 합니다. DNS 나 DHCP 서버 또는 기타 ISP 관련 서버 같은 중요한 IP 주소는 차단해서는 안 됩니다. 보안 설정에 따라 방화벽에서 금지된 컴퓨터로부터 이벤트를 탐지하면 경고가 나타날 수 있습니다.

이 장에서

신뢰하는 컴퓨터 연결

[신뢰하거나 금지된 IP] 창의 [신뢰하는 IP 주소]에서 신뢰하는 IP 주소를 추가, 편집 및 제거할 수 있습니다.

[신뢰하거나 금지된 IP] 창의 [신뢰하는 IP 주소] 목록에서 특정 컴퓨터의 모든 트래픽이 사용자의 컴퓨터에 연결하도록 허용할 수 있습니다. 방화벽은 [신뢰하는 IP 주소] 목록에 있는 IP 주소의 트래픽에 대해서는 로그를 기록하거나 이벤트 경고를 생성하지 않습니다.

방화벽은 목록에서 확인된 IP 주소를 신뢰하고 포트의 방화벽을 통한 신뢰하는 IP 로부터의 트래픽을 항상 신뢰합니다. 신뢰하는 IP 주소에 연결된 컴퓨터와 사용자 컴퓨터 사이의 활동은 방화벽에 의해 필터링되거나 분석되지 않습니다. 기본적으로 [신뢰하는 IP 주소]에는 방화벽에서 발견한 첫 번째 개인 네트워크가 표시됩니다.

연결을 허용할 때 신뢰하는 컴퓨터가 안전한지 확인하십시오. 신뢰하는 컴퓨터가 웜 또는 기타 메커니즘을 통해 감염되는 경우 사용자의 컴퓨터도 감염에 취약해집니다. 사용자가 신뢰하는 컴퓨터도 방화벽이나 최신 안티바이러스 프로그램으로 보호하는 것이 좋습니다.

신뢰하는 컴퓨터 연결 추가

신뢰하는 컴퓨터 연결 및 관련 IP 주소를 추가할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.
4. [신뢰하거나 금지된 IP] 창에서 [신뢰하는 IP 주소]를 선택하고 [추가]를 클릭합니다.
5. [신뢰하는 IP 주소 규칙 추가]에서 다음 중 하나를 수행합니다.
   - [단일 IP 주소]를 선택하고 IP 주소를 입력합니다.
   - [IP 주소 범위]를 선택한 다음 [시작 IP 주소] 및 [끝 IP 주소] 상자에 시작 및 끝 IP 주소를 입력합니다.

6 시스템 서비스에서 ICS(인터넷 연결 공유)를 사용하는 경우 192.168.0.1~192.168.0.255 의 IP 주소 범위를 추가할 수 있습니다.

7 필요에 따라 [규칙 만료 시간]을 선택하고 규칙을 시행할 일수를 입력합니다.

8 필요에 따라 규칙에 대한 설명을 입력합니다.

9 [확인]을 클릭합니다.

10 [신뢰하거나 금지된 IP] 대화 상자에서 [예]를 클릭하여 확인합니다.

참고: ICS(인터넷 연결 공유)에 대한 자세한 내용은 새 시스템 서비스 구성을 참조하십시오.

인바운드 이벤트 로그의 신뢰하는 컴퓨터 추가

인바운드 이벤트 로그에서 신뢰하는 컴퓨터 연결 및 관련 IP 주소를 추가할 수 있습니다.

1 McAfee SecurityCenter 창의 [일반적인 작업] 창에서 [고급 메뉴]를 클릭합니다.

2 [보고서 및 로그]를 클릭합니다.

3 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

4 [인터넷 및 네트워크]를 클릭한 다음 [인바운드 이벤트]를 클릭합니다.

5 소스 IP 주소를 선택하고 [원하는 작업]에서 [이 주소 신뢰]를 클릭합니다.

6 [예]를 클릭하여 확인합니다.

신뢰하는 컴퓨터 연결 편집

신뢰하는 컴퓨터 연결 및 관련 IP 주소를 편집할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.

4 [신뢰하거나 금지된 IP] 창에서 [신뢰하는 IP 주소]를 선택합니다.

5 IP 주소를 선택하고 [편집]을 클릭합니다.

6 [신뢰하는 IP 주소 편집]에서 다음 중 하나를 수행합니다.

- [단일 IP 주소]를 선택하고 IP 주소를 입력합니다.

- [IP 주소 범위]를 선택한 다음 [시작 IP 주소] 및 [끝 IP 주소] 상자에 시작 및 끝 IP 주소를 입력합니다.

7 필요에 따라 [규칙 만료 시간]을 확인하고 규칙을 시행할 일 수를 입력합니다.

8 필요에 따라 규칙에 대한 설명을 입력합니다.

9 [확인]을 클릭합니다.

참고: 방화벽이 신뢰하는 개인 네트워크에서 자동으로 추가한 기본 컴퓨터 연결은 편집할 수 없습니다.

신뢰하는 컴퓨터 연결 제거

신뢰하는 컴퓨터 연결 및 관련 IP 주소를 제거할 수 있습니다.

1 McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.

2 [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.

3 [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.

4 [신뢰하거나 금지된 IP] 창에서 [신뢰하는 IP 주소]를 선택합니다.

5 IP 주소를 선택하고 [제거]를 클릭합니다.

6 [신뢰하거나 금지된 IP] 대화 상자에서 [예]를 클릭하여 확인합니다.

컴퓨터 연결 차단

[신뢰하거나 금지된 IP] 창의 [금지된 IP 주소]에서 금지된 IP 주소를 추가, 편집 및 제거할 수 있습니다.

알 수 없거나 의심스럽거나 또는 신뢰하지 않는 IP 주소에 연결된 컴퓨터는 사용자의 컴퓨터에 연결하지 못하도록 금지할 수 있습니다.

방화벽은 원하지 않는 모든 트래픽을 차단하므로 일반적으로 IP 주소를 금지할 필요는 없습니다. 인터넷 연결에 특정 위협이 포함된 것이 확실한 경우에만 IP 주소를 금지해야 합니다. DNS 나 DHCP 서버 또는 기타 ISP 관련 서버 같은 중요한 IP 주소는 차단해서는 안 됩니다. 보안 설정에 따라 방화벽에서 금지된 컴퓨터로부터 이벤트를 탐지하면 경고가 나타날 수 있습니다.

금지된 컴퓨터 연결 추가

금지된 컴퓨터 연결 및 관련 IP 주소를 추가할 수 있습니다.

참고: DNS나 DHCP 서버 또는 기타 ISP 관련 서버 같은 중요한 IP 주소는 차단해서는 안 됩니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.
4. [신뢰하거나 금지된 IP] 창에서 [금지된 IP 주소]를 선택하고 [추가]를 클릭합니다.
5. [금지된 IP 주소 규칙 추가]에서 다음 중 하나를 수행합니다.
   - [단일 IP 주소]를 선택하고 IP 주소를 입력합니다.
   - [IP 주소 범위]를 선택한 다음 [시작 IP 주소] 및 [끝 IP 주소] 상자에 시작 및 끝 IP 주소를 입력합니다.
6. 필요에 따라 [규칙 만료 시간]을 선택하고 규칙을 시행할 일수를 입력합니다.
7. 필요에 따라 규칙에 대한 설명을 입력합니다.
8. [확인]을 클릭합니다.
9. [신뢰하거나 금지된 IP] 대화 상자에서 [예]를 클릭하여 확인합니다.

금지된 컴퓨터 연결 편집

금지된 컴퓨터 연결 및 관련 IP 주소를 편집할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.
4. [신뢰하거나 금지된 IP] 창에서 [금지된 IP 주소]를 선택하고 [편집]을 클릭합니다.
5. [금지된 IP 주소 편집]에서 다음 중 하나를 수행합니다.
   - [단일 IP 주소]를 선택하고 IP 주소를 입력합니다.
   - [IP 주소 범위]를 선택한 다음 [시작 IP 주소] 및 [끝 IP 주소] 상자에 시작 및 끝 IP 주소를 입력합니다.
6. 필요에 따라 [규칙 만료 시간]을 선택하고 규칙을 시행할 일수를 입력합니다.
7. 필요에 따라 규칙에 대한 설명을 입력합니다.
8. [확인]을 클릭합니다.

금지된 컴퓨터 연결 제거

금지된 컴퓨터 연결 및 관련 IP 주소를 제거할 수 있습니다.

1. McAfee SecurityCenter 창에서 [인터넷 및 네트워크]를 클릭하고 [구성]을 클릭합니다.
2. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
3. [방화벽] 창에서 [신뢰하거나 금지된 IP]를 클릭합니다.
4. [신뢰하거나 금지된 IP] 창에서 [금지된 IP 주소]를 선택합니다.
5. IP 주소를 선택하고 [제거]를 클릭합니다.
6. [신뢰하거나 금지된 IP] 대화 상자에서 [예]를 클릭하여 확인합니다.

인바운드 이벤트 로그의 컴퓨터 금지

인바운드 이벤트 로그에서 컴퓨터 연결 및 관련 IP 주소를 금지할 수 있습니다.

인바운드 이벤트 로그에 표시되는 IP 주소가 차단됩니다. 따라서 주소를 금지해도 컴퓨터에서 일부러 열어 놓은 포트를 사용하거나 인터넷에 대한 액세스가 허용된 프로그램이 포함되어 있지 않은 한 보호가 추가되지 않습니다.

의도적으로 열린 하나 이상의 포트가 있는 경우와 해당 주소의 열린 포트에 대한 액세스를 차단해야 하는 경우에만 IP 주소를 [금지된 IP 주소] 목록에 추가합니다.

모든 인바운드 인터넷 트래픽의 IP 주소를 나열하는 인바운드 이벤트 페이지를 사용하여 의심스럽거나 원하지 않는 인터넷 활동의 소스인 것으로 생각되는 IP 주소를 차단할 수 있습니다.

1 McAfee SecurityCenter 창의 [일반적인 작업]에서 [고급 메뉴]를 클릭합니다.
2 [보고서 및 로그]를 클릭합니다.
3 [최신 이벤트]에서 [로그 보기]를 클릭합니다.
4 [인터넷 및 네트워크]를 클릭한 다음 [인바운드 이벤트]를 클릭합니다.
5 소스 IP 주소를 선택하고 [원하는 작업]에서 [이 주소 차단]을 클릭합니다.
6 [금지된 IP 주소 규칙 추가] 대화 상자에서 [예]를 클릭하여 확인합니다.

침입 검색 이벤트 로그의 컴퓨터 금지

침입 검색 이벤트 로그에서 컴퓨터 연결 및 관련 IP 주소를 금지할 수 있습니다.

1 McAfee SecurityCenter 창의 [일반적인 작업]에서 [고급 메뉴]를 클릭합니다.
2 [보고서 및 로그]를 클릭합니다.
3 [최신 이벤트]에서 [로그 보기]를 클릭합니다.
4 [인터넷 및 네트워크]를 클릭한 다음 [침입 검색 이벤트]를 클릭합니다.
5 소스 IP 주소를 선택하고 [원하는 작업]에서 [이 주소 차단]을 클릭합니다.
6 [금지된 IP 주소 규칙 추가] 대화 상자에서 [예]를 클릭하여 확인합니다.

제 21 장

로깅, 모니터링 및 분석

방화벽은 광범위하고 읽기 쉬운 인터넷 이벤트 및 트래픽의 로깅, 모니터링 및 분석을 제공합니다. 인터넷 트래픽과 이벤트를 이해하면 인터넷 연결을 관리하는 데 도움이 됩니다.

이 장에서

이벤트 로그 기록

방화벽을 통해 이벤트 로그 기록을 활성화하거나 비활성화하고, 활성화한 경우 로깅할 이벤트 유형을 지정할 수 있습니다. 이벤트 로그 기록을 통해 최신 인바운드, 아웃바운드 이벤트와 침입 이벤트를 볼 수 있습니다.

이벤트 로그 설정 구성

로깅할 방화벽 이벤트의 유형을 지정하고 구성할 수 있습니다. 기본적으로 이벤트 로그 기록은 모든 이벤트와 활동에 대해 활성화됩니다.

1. [인터넷 및 네트워크 구성] 창의 [방화벽 보호가 활성화됨]에서 [고급]을 클릭합니다.
2. [방화벽] 창에서 [이벤트 로그 설정]을 클릭합니다.
3. [이벤트 로그 기록 활성화]가 선택되어 있지 않은 경우 선택합니다.
4. [이벤트 로그 기록 활성화]에서 로깅할 이벤트 유형을 선택하고, 로깅하지 않을 이벤트 유형의 선택을 취소합니다. 이벤트 유형에는 다음이 포함됩니다.
   - 차단된 프로그램
   - ICMP Ping
   - 금지된 IP 주소의 트래픽
   - 시스템 서비스 포트의 이벤트
   - 알 수 없는 포트의 이벤트
   - 침입 검색(IDS) 이벤트
5. 특정 포트에 대해 로깅하지 않도록 하려면 [다음 포트의 이벤트를 기록하지 않습니다.]를 선택한 다음 단일 포트 번호를 쉼표로 구분하여 입력하거나 대시를 사용하여 포트 범위를 입력합니다(예: `137-139, 445, 400-5000`).
6. [확인]을 클릭합니다.

최신 이벤트 보기

로깅이 활성화되면 최신 이벤트를 볼 수 있습니다. [최신 이벤트] 창에는 이벤트의 날짜 및 설명이 표시됩니다. 또한 인터넷에 액세스하지 못하도록 명시적으로 차단된 프로그램의 활동이 표시됩니다.

- [고급 메뉴]의 [일반적인 작업] 창에서 [보고서 및 로그] 또는 [최근 이벤트 보기]를 클릭합니다. 또는 [기본 메뉴]의 [일반적인 작업] 창에서 [최신 이벤트 보기]를 클릭합니다.

인바운드 이벤트 보기

로깅이 활성화되면 인바운드 이벤트를 볼 수 있습니다. 인바운드 이벤트에는 날짜와 시간, 소스 IP 주소, 호스트 이름 및 정보와 이벤트 유형이 포함됩니다.

1 [고급 메뉴]가 활성화되었는지 확인합니다. [일반적인 작업] 창에서 [보고서 및 로그]를 클릭합니다.

2 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

3 [인터넷 및 네트워크]를 클릭한 다음 [인바운드 이벤트]를 클릭합니다.

참고: 인바운드 이벤트 로그의 IP 주소를 신뢰하거나 금지하고 추적할 수 있습니다.

아웃바운드 이벤트 보기

로깅이 활성화되면 아웃바운드 이벤트를 볼 수 있습니다. 아웃바운드 이벤트는 아웃바운드 액세스를 시도하는 프로그램 이름, 이벤트 날짜와 시간 및 사용자 컴퓨터의 프로그램 위치를 포함합니다.

1 [일반적인 작업] 창에서 [보고서 및 로그]를 클릭합니다.

2 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

3 [인터넷 및 네트워크]를 클릭한 다음 [아웃바운드 이벤트]를 클릭합니다.

참고: 아웃바운드 이벤트 로그의 프로그램에 대한 전체 및 아웃바운드 전용 액세스를 허용할 수 있습니다. 프로그램에 대한 추가 정보를 찾을 수도 있습니다.

침입 검색 이벤트 보기

로깅이 활성화되면 인바운드 침입 이벤트를 볼 수 있습니다. 침입 검색 이벤트에는 날짜 및 시간, 소스 IP, 이벤트의 호스트 이름 및 이벤트 유형이 표시됩니다.

1 [일반적인 작업] 창에서 [보고서 및 로그]를 클릭합니다.

2 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

3 [인터넷 및 네트워크]를 클릭한 다음 [침입 검색 이벤트]를 클릭합니다.

참고: 침입 검색 이벤트 로그의 IP 주소를 금지하고 추적할 수 있습니다.

통계 작업

방화벽은 McAfee 의 HackerWatch 보안 웹 사이트에 전체 인터넷 로그 및 포트 활동에 관한 통계를 제공하는데 영향을 줍니다.

전체 보안 이벤트 통계 보기

HackerWatch 는 SecurityCenter 에서 볼 수 있는 전세계 인터넷 보안 이벤트를 추적합니다. 추적된 사건 정보 목록은 지난 24 시간, 일주일 및 한달 동안 HackerWatch 에 보고됩니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [HackerWatch]를 클릭합니다.

3 [이벤트 추적]에서 보안 이벤트 통계를 확인합니다.

전체 인터넷 포트 활동 보기

HackerWatch 는 SecurityCenter 에서 볼 수 있는 전세계 인터넷 보안 이벤트를 추적합니다. 표시된 정보는 지난 일주일 동안 HackerWatch 에 보고된 최상위 이벤트 포트를 포함합니다. 일반적으로 HTTP, TCP 및 UDP 포트 정보가 표시됩니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [HackerWatch]를 클릭합니다.

3 [최근 포트 활동]에서 최상위 이벤트 포트 이벤트를 확인합니다.

인터넷 트래픽 추적

방화벽은 인터넷 트래픽을 추적하는 많은 옵션을 제공합니다. 이러한 옵션은 네트워크 컴퓨터를 지리적으로 추적하고 도메인 및 네트워크 정보를 얻어 인바운드 이벤트 및 침입 검색 이벤트 로그로부터 컴퓨터를 추적합니다.

네트워크 컴퓨터 지리적 추적

이름이나 IP 주소를 사용하여 연결하거나 사용자 컴퓨터에 연결을 시도하는 컴퓨터의 지리적 위치를 찾기 위해 비주얼 추적기를 사용할 수 있습니다. 비주얼 추적기를 사용하여 네트워크와 등록 정보에 액세스할 수 있습니다. 실행 중인 비주얼 추적기는 소스 컴퓨터와 사용자 컴퓨터 간에 사용되었을 가능성이 가장 큰 데이터 세계 지도를 보여 줍니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [비주얼 추적기]를 클릭합니다.

3 컴퓨터의 IP 주소를 입력하고 [추적]을 클릭합니다.

4 [비주얼 추적기]에서 [지도 보기]를 선택합니다.

참고: 루프, 개인 또는 잘못된 IP 주소 이벤트는 추적할 수 없습니다.

컴퓨터 등록 정보 얻기

Visual Trace 를 사용하여 SecurityCenter 에서 컴퓨터 등록 정보를 얻을 수 있습니다. 정보는 도메인 이름, 등록자 이름 및 주소와 관리자 연락처를 포함합니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [비주얼 추적기]를 클릭합니다.

3 컴퓨터의 IP 주소를 입력하고 [추적]을 클릭합니다.

4 [비주얼 추적기]에서 [등록자 보기]를 선택합니다.

컴퓨터 네트워크 정보 얻기

Visual Trace 를 사용하여 SecurityCenter 에서 컴퓨터 네트워크 정보를 얻을 수 있습니다. 네트워크 정보는 도메인이 있는 네트워크에 대한 자세한 정보를 포함합니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [비주얼 추적기]를 클릭합니다.

3 컴퓨터의 IP 주소를 입력하고 [추적]을 클릭합니다.

4 [비주얼 추적기]에서 [네트워크 보기]를 선택합니다.

인바운드 이벤트 로그의 컴퓨터 추적

[인바운드 이벤트] 창에서 인바운드 이벤트 로그에 나타나는 IP 주소를 추적할 수 있습니다.

1 [고급 메뉴]가 활성화되었는지 확인합니다. [일반적인 작업] 창에서 [보고서 및 로그]를 클릭합니다.

2 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

3 [인터넷 및 네트워크]를 클릭한 다음 [인바운드 이벤트]를 클릭합니다.

4 [인바운드 이벤트] 창에서 소스 IP 주소를 선택하고 [이 주소 추적]을 클릭합니다.

5 [비주얼 추적기] 창에서 다음 중 하나를 클릭합니다.

- [지도 보기]: 선택된 IP 주소를 사용하는 컴퓨터의 지리적 위치를 찾습니다.
- [등록자 보기]: 선택된 IP 주소를 사용하는 도메인 정보를 찾습니다.
- [네트워크 보기]: 선택된 IP 주소를 사용하는 네트워크 정보를 찾습니다.

6 [완료]를 클릭합니다.

침입 검색 이벤트 로그의 컴퓨터 추적

[침입 검색 이벤트] 창에서 침입 검색 이벤트 로그에 나타나는 IP 주소를 추적할 수 있습니다.

1 [일반적인 작업] 창에서 [보고서 및 로그]를 클릭합니다.

2 [최신 이벤트]에서 [로그 보기]를 클릭합니다.

3 [인터넷 및 네트워크]를 클릭한 다음 [침입 검색 이벤트]를 클릭합니다. [침입 검색 이벤트] 창에서 소스 IP 주소를 선택하고 [이 주소 추적]을 클릭합니다.

4 [비주얼 추적기] 창에서 다음 중 하나를 클릭합니다.

- [지도 보기]: 선택된 IP 주소를 사용하는 컴퓨터의 지리적 위치를 찾습니다.
- [등록자 보기]: 선택된 IP 주소를 사용하는 도메인 정보를 찾습니다.
- [네트워크 보기]: 선택된 IP 주소를 사용하는 네트워크 정보를 찾습니다.

5 [완료]를 클릭합니다.

모니터링하는 IP 주소 추적

소스 컴퓨터와 사용자 컴퓨터 간에 사용되었을 가능성이 가장 큰 데이터를 보여주는 지리적인 보기를 얻을 수 있도록 모니터링하는 IP 주소를 추적할 수 있습니다. 또한 IP 주소에 관한 등록 및 네트워크 정보를 얻을 수 있습니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [트래픽 모니터]를 클릭합니다.

3 [트래픽 모니터]에서 [활성 프로그램]을 클릭합니다.

4 프로그램과 프로그램 이름 아래에 나타나는 IP 주소를 선택합니다.

5 [프로그램 활동]에서 [이 IP 추적]을 클릭합니다.

6 [비주얼 추적기]에서 소스 컴퓨터와 사용자 컴퓨터 간에 사용되었을 가능성이 가장 큰 데이터를 보여주는 지도를 볼 수 있습니다. 또한 IP 주소에 관한 등록 및 네트워크 정보를 얻을 수 있습니다.

참고: 최신 통계를 보려면 [비주얼 추적기]에서 [새로 고침]을 클릭합니다.

인터넷 트래픽 모니터링

방화벽은 다음을 비롯하여 인터넷 트래픽을 모니터링할 수 있는 여러 가지 방법을 제공합니다.

- **트래픽 분석 그래프**: 최근 인바운드 및 아웃바운드 인터넷 트래픽을 표시합니다.
- **트래픽 사용률 그래프**: 지난 24 시간 동안 대부분 활성 프로그램이 사용한 대역폭의 비율을 표시합니다.
- **활성 프로그램**: 사용자 컴퓨터와 프로그램 액세스하는 IP 주소에 연결된 현재 가장 많이 사용하는 프로그램을 표시합니다.

트래픽 분석 그래프 정보

트래픽 분석 그래프는 인바운드 및 아웃바운드 인터넷 트래픽을 숫자와 그래픽으로 표현한 것입니다. 또한 [트래픽 모니터]는 컴퓨터에서 현재 대부분의 네트워크 연결을 사용하고 있는 응용 프로그램과 해당 응용 프로그램이 액세스하는 IP 주소를 표시합니다.

[트래픽 분석] 창에서 최근 인바운드 및 아웃바운드 인터넷 트래픽, 현재, 평균 및 최대 전송률을 볼 수 있습니다. 방화벽을 시작한 후의 트래픽 양을 포함한 트래픽 볼륨과 현재 및 이전 달의 전체 트래픽을 볼 수 있습니다.

[트래픽 분석] 창은 사용자 컴퓨터의 실시간 인터넷 활동, 사용자 컴퓨터에서의 최근 인바운드 및 아웃바운드 인터넷 트래픽 볼륨과 비율을 포함한 연결 속도 및 인터넷을 통해 전송된 총 바이트를 표시합니다.

녹색 실선은 들어오는 트래픽의 현재 전송 속도를 나타냅니다. 녹색 점선은 들어오는 트래픽의 평균 전송 속도를 나타냅니다. 현재 전송 속도와 평균 전송 속도가 같을 경우에는 그래프에 점선이 나타나지 않습니다. 이 경우 실선이 평균 및 현재 전송 속도를 모두 나타냅니다.

빨간 실선은 나가는 트래픽의 현재 전송 속도를 나타냅니다. 빨간 점선은 나가는 트래픽의 평균 전송 속도를 나타냅니다. 현재 전송 속도와 평균 전송 속도가 같을 경우에는 그래프에 점선이 나타나지 않습니다. 이 경우 실선이 평균 및 현재 전송 속도를 모두 나타냅니다.

인바운드 및 아웃바운드 트래픽 분석

트래픽 분석 그래프는 인바운드 및 아웃바운드 인터넷 트래픽을 숫자와 그래픽으로 표현한 것입니다. 또한 [트래픽 모니터]는 컴퓨터에서 현재 대부분의 네트워크 연결을 사용하고 있는 응용 프로그램과 해당 응용 프로그램이 액세스하는 IP 주소를 표시합니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [트래픽 모니터]를 클릭합니다.

3 [트래픽 모니터]에서 [트래픽 분석]을 클릭합니다.

팁: 최신 통계를 보려면 [트래픽 분석]에서 [새로 고침]을 클릭합니다.

프로그램 대역폭 모니터링

지난 24 시간 동안 컴퓨터에서 가장 활동적인 프로그램이 사용한 대역폭의 대략적인 비율을 표시하는 원형 차트를 볼 수 있습니다. 원형 차트는 프로그램에서 사용한 대역폭의 상대적인 양을 시각적으로 보여 줍니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [트래픽 모니터]를 클릭합니다.

3 [트래픽 모니터]에서 [트래픽 사용률]을 클릭합니다.

팁: 최신 통계를 보려면 [트래픽 사용률]에서 [새로 고침]을 클릭합니다.

프로그램 활동 모니터링

원격 컴퓨터 연결 및 포트를 표시하는 인바운드 및 아웃바운드 프로그램 활동을 볼 수 있습니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [트래픽 모니터]를 클릭합니다.

3 [트래픽 모니터]에서 [활성 프로그램]을 클릭합니다.

4 다음 정보를 볼 수 있습니다.

- 프로그램 활동 그래프: 활동 그래프를 표시할 프로그램을 선택합니다.
- 수신 대기 연결: 프로그램 이름 하위 항목의 수신 대기 항목을 선택합니다.

- 컴퓨터 연결: 프로그램 이름, 시스템 프로세스 또는 서비스 하위 항목의 IP 주소를 선택합니다.

참고: 최신 통계를 보려면 [활성 프로그램]에서 [새로 고침]을 클릭합니다.

제 22 장

인터넷 보안에 대해 알아보기

방화벽은 McAfee 보안 웹 사이트 HackerWatch 에 프로그램 및 전체 인터넷 활동에 관한 최신 정보를 제공하는데 영향을 줍니다. HackerWatch 는 방화벽에 관한 HTML 자습서를 제공합니다.

이 장에서

HackerWatch 자습서 시작

방화벽에 대한 자세한 내용을 보려면 SecurityCenter 의 HackerWatch 자습서에 액세스할 수 있습니다.

1 [고급 메뉴]가 활성화되었는지 확인하고 [도구]를 클릭합니다.

2 [도구] 창에서 [HackerWatch]를 클릭합니다.

3 [HackerWatch 리소스]에서 [자습서 보기]를 클릭합니다.

제 23 장

McAfee QuickClean

QuickClean 은 컴퓨터에 방해물을 만들 수 있는 파일을 삭제하여 컴퓨터의 성능을 향상시킵니다. QuickClean 은 휴지통을 비우고 임시 파일, 바로 가기, 손실된 파일 조각, 레지스트리 파일, 캐시된 파일, 쿠키, 브라우저 기록 파일, 보낸 전자 메일, 삭제한 전자 메일, 최근에 사용한 파일, Active-X 파일 및 시스템 복원 시점 파일을 삭제합니다. 또한 McAfee Shredder 구성 요소를 사용하여 이름, 주소 등의 중요한 개인 정보를 포함할 수 있는 항목을 안전하고 영구적으로 삭제하여 사용자의 개인 정보를 보호합니다. 파일 영구 제거에 대한 자세한 내용은 McAfee Shredder 를 참조하십시오.

디스크 조각 모음은 컴퓨터의 파일과 폴더가 컴퓨터의 하드 드라이브에 저장될 때 흩어지지(조각나지) 않도록 정렬합니다. 하드 드라이브에서 정기적으로 조각 모음을 수행하면 조각난 파일과 폴더가 통합되므로 이후의 검색 속도가 빨라집니다.

컴퓨터를 수동으로 유지 관리하지 않으려면 원하는 빈도에 독립된 작업으로 자동 실행되도록 QuickClean 과 디스크 조각 모음을 예약할 수 있습니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

QuickClean 기능

QuickClean 은 불필요한 파일을 안전하고 효율적으로 삭제하는 다양한 정리를 제공합니다. 이러한 파일을 삭제하면 컴퓨터 하드 드라이브의 여유 공간이 늘어나고 성능이 향상됩니다.

컴퓨터 정리

QuickClean 은 컴퓨터에 방해물을 만들 수 있는 파일을 삭제합니다. 또한 휴지통을 비우고 임시 파일, 바로 가기, 손실된 파일 조각, 레지스트리 파일, 캐시된 파일, 쿠키, 브라우저 기록 파일, 보낸 전자 메일, 삭제한 전자 메일, 최근에 사용한 파일, Active-X 파일 및 시스템 복원 시점 파일을 삭제합니다. QuickClean 은 다른 필수적인 정보에 영향을 주지 않고 이러한 항목을 삭제합니다.

QuickClean 의 정리 중 하나를 사용하여 컴퓨터에서 불필요한 파일을 삭제할 수 있습니다. 다음 표에서는 QuickClean 정리에 대해 설명합니다.

이름	기능
휴지통 정리	휴지통의 파일을 삭제합니다.
임시 파일 정리	임시 폴더에 저장된 파일을 삭제합니다.
바로 가기 정리	끊어진 바로 가기와 연결된 프로그램이 없는 바로 가기를 삭제합니다.
손실된 파일 조각 정리	사용자 컴퓨터에서 손실된 파일 조각을 삭제합니다.
레지스트리 정리	사용자 컴퓨터에 더 이상 존재하지 않는 프로그램의 Windows® 레지스트리 정보를 삭제합니다. 레지스트리는 Windows 의 구성 정보가 저장되는 데이터베이스입니다. 레지스트리에는 각 컴퓨터 사용자의 프로필과 시스템 하드웨어, 설치된 프로그램 및 속성 설정에 대한 정보가 들어 있습니다. Windows 에서는 작업 중에 이 정보를 지속적으로 참조합니다.
캐시 정리	웹 페이지를 찾아볼 때 쌓인 캐시된 파일을 삭제합니다. 이러한 파일은 대개 캐시 폴더에 임시 파일로 저장됩니다. 캐시 폴더는 컴퓨터의 임시 저장소 영역입니다. 웹 검색 속도와 효율성을 높이기 위해 사용자가 다음에 웹 페이지를 보려고 할 때 원격 서버가 아니라 캐시에서 해당 웹 페이지를 검색할 수 있습니다.

이름	기능
쿠키 정리	쿠키를 삭제합니다. 이러한 파일은 대개 임시 파일로 저장됩니다. 쿠키는 사용자 이름, 현재 날짜 및 시간 등의 정보가 포함된 작은 파일로, 웹을 검색하는 사용자의 컴퓨터에 저장됩니다. 쿠키는 주로 웹 사이트에서 이전에 사이트에 등록했거나 사이트를 방문한 사용자를 식별하는 데 사용되지만 해커가 정보를 빼내는 데 사용할 수도 있습니다.
브라우저 기록 정리	웹 브라우저 기록을 삭제합니다.
Outlook Express 및 Outlook 전자 메일 정리(보낸 편지함 및 지운 편지함)	Outlook®과 Outlook Express 에서 보낸 전자 메일과 삭제한 전자 메일을 삭제합니다.
최근에 사용한 항목 정리	다음 프로그램 중 하나로 만들어진 최근에 사용한 파일을 삭제합니다. ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office(Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX 정리	ActiveX 컨트롤을 삭제합니다. ActiveX 는 프로그램이나 웹 페이지에 혼합되어 일반적인 부분처럼 나타나는 기능을 추가하는 데 사용되는 소프트웨어 구성 요소입니다. 대부분의 ActiveX 컨트롤은 무해하지만 일부는 컴퓨터에서 정보를 캡처할 수 있습니다.
시스템 복원 시점 정리	컴퓨터에서 가장 최근의 시스템 복원 시점을 제외하고 이전 시스템 복원 시점을 삭제합니다. 시스템 복원 시점은 문제가 발생하는 경우 이전 상태로 돌아갈 수 있도록 컴퓨터의 변경 내용을 표시하기 위해 Windows 에서 만들어집니다.

컴퓨터 정리

QuickClean 의 정리 중 하나를 사용하여 컴퓨터에서 불필요한 파일을 삭제할 수 있습니다. 작업이 완료되면 [QuickClean 요약] 아래에서 정리 후 확보된 디스크 공간의 크기, 삭제된 파일 수 및 QuickClean 작업이 마지막으로 컴퓨터에서 실행된 날짜와 시간을 볼 수 있습니다.

1 McAfee SecurityCenter 창의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.

2 [McAfee QuickClean]에서 [시작]을 클릭합니다.

3 다음 중 하나를 수행합니다.

- [다음]을 클릭하여 목록의 기본 정리를 적용합니다.
- 적절한 정리를 선택하거나 선택 취소한 후 [다음]을 클릭합니다. 최근에 사용한 항목 정리를 선택하는 경우 [등록 정보]를 클릭하여 목록에 있는 프로그램을 사용하여 최근에 만들어진 파일을 선택하거나 선택 취소한 다음 [확인]을 클릭할 수 있습니다.
- [기본값 복원]을 클릭하여 기본 정리를 복원하고 [다음]을 클릭합니다.

4 분석이 수행된 후 [다음]을 클릭합니다.

5 [다음]을 클릭하여 파일 삭제를 확인합니다.

6 다음 중 하나를 수행합니다.

- [다음]을 클릭하여 기본값, 즉 [아니오, 표준 Windows 삭제를 사용하여 파일을 삭제합니다.]를 적용합니다.
- [예, Shredder 를 사용하여 파일을 안전하게 지웁니다.]를 클릭하고 통과 항목 수를 최대 10 까지 지정한 후 [다음]을 클릭합니다. 지울 정보량이 많은 경우 파일 영구 제거에 시간이 오래 걸릴 수 있습니다.

7 정리 중에 파일이나 항목이 잠겨 있으면 컴퓨터를 다시 시작하라는 메시지가 나타날 수 있습니다. [확인]을 클릭하여 메시지를 닫습니다.

8 [마침]을 클릭합니다.

참고: Shredder에서 삭제한 파일은 복구할 수 없습니다. 파일 영구 제거에 대한 자세한 내용은 McAfee Shredder를 참조하십시오.

컴퓨터 조각 모음

디스크 조각 모음은 컴퓨터의 파일과 폴더가 컴퓨터의 하드 드라이브에 저장될 때 흩어지지(조각나지) 않도록 정렬합니다. 하드 드라이브에서 정기적으로 조각 모음을 수행하면 조각난 파일과 폴더가 통합되므로 이후의 검색 속도가 빨라집니다.

컴퓨터 조각 모음

컴퓨터에서 조각 모음을 수행하여 파일과 폴더의 액세스 및 검색을 개선할 수 있습니다.

1. McAfee SecurityCenter 창의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [디스크 조각 모음]에서 [분석]을 클릭합니다.
3. 화면에 나타나는 지침을 따릅니다.

참고: 디스크 조각 모음에 대한 자세한 내용은 Windows 도움말을 참조하십시오.

작업 예약

작업 스케줄러는 QuickClean 이나 디스크 조각 모음이 컴퓨터에서 실행되는 빈도를 자동화합니다. 예를 들어, 일요일 오후 9 시마다 휴지통을 비우도록 QuickClean 작업을 예약하거나 매월 말일에 컴퓨터의 하드 드라이브에서 조각 모음을 수행하도록 디스크 조각 모음 작업을 예약할 수 있습니다. 언제든지 작업을 만들거나 수정하거나 삭제할 수 있습니다. 예약된 작업이 실행되려면 사용자가 컴퓨터에 로그인되어 있어야 합니다. 특정한 이유로 작업이 실행되지 않는 경우 사용자가 다시 로그인한 후 5 분 후로 다시 예약됩니다.

QuickClean 작업 예약

하나 이상의 정리를 사용하여 컴퓨터를 자동으로 정리하도록 QuickClean 작업을 예약할 수 있습니다. 작업이 완료되면 [QuickClean 요약] 아래에서 작업이 다시 실행되도록 예약된 날짜와 시간을 볼 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [McAfee QuickClean]을 클릭합니다.

3 [작업 이름] 상자에 작업의 이름을 입력한 다음 [만들기]를 클릭합니다.

4 다음 중 하나를 수행합니다.

- [다음]을 클릭하여 목록의 정리를 적용합니다.
- 적절한 정리를 선택하거나 선택 취소한 후 [다음]을 클릭합니다. 최근에 사용한 항목 정리를 선택하는 경우 [등록 정보]를 클릭하여 목록의 프로그램으로 최근에 만들어진 파일을 선택하거나 선택 취소한 다음 [확인]을 클릭할 수 있습니다.
- [기본값 복원]을 클릭하여 기본 정리를 복원하고 [다음]을 클릭합니다.

5 다음 중 하나를 수행합니다.

- [예약]을 클릭하여 기본값, 즉 [아니오, 표준 Windows 삭제를 사용하여 파일을 삭제합니다.]를 적용합니다.

- [예, Shredder 를 사용하여 파일을 안전하게 지웁니다.]를 클릭하고 통과 항목 수를 최대 10 까지 지정한 후 [예약]을 클릭합니다.

6 [예약] 대화 상자에서 작업을 실행할 빈도를 선택한 다음 [확인]을 클릭합니다.

7 최근에 사용한 항목 정리 등록 정보를 변경한 경우 컴퓨터를 다시 시작하라는 메시지가 나타날 수 있습니다. [확인]을 클릭하여 메시지를 닫습니다.

8 [마침]을 클릭합니다.

참고: Shredder에서 삭제한 파일은 복구할 수 없습니다. 파일 영구 제거에 대한 자세한 내용은 McAfee Shredder를 참조하십시오.

QuickClean 작업 수정

예약된 QuickClean 작업을 수정하여 QuickClean 에서 사용하는 정리를 변경하거나 컴퓨터에서 자동으로 실행되는 빈도를 변경할 수 있습니다. 작업이 완료되면 [QuickClean 요약] 아래에서 작업이 다시 실행되도록 예약된 날짜와 시간을 볼 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [McAfee QuickClean]을 클릭합니다.

3 [기존 작업을 선택합니다.] 목록에서 작업을 선택한 다음 [수정]을 클릭합니다.

4 다음 중 하나를 수행합니다.

- [다음]을 클릭하여 작업에 선택한 정리를 적용합니다.
- 적절한 정리를 선택하거나 선택 취소한 후 [다음]을 클릭합니다. 최근에 사용한 항목 정리를 선택하는 경우 [등록 정보]를 클릭하여 목록의 프로그램으로 최근에 만들어진 파일을 선택하거나 선택 취소한 다음 [확인]을 클릭할 수 있습니다.
- [기본값 복원]을 클릭하여 기본 정리를 복원하고 [다음]을 클릭합니다.

5 다음 중 하나를 수행합니다.

- [예약]을 클릭하여 기본값, 즉 [아니오, 표준 Windows 삭제를 사용하여 파일을 삭제합니다.]를 적용합니다.
- [예, Shredder 를 사용하여 파일을 안전하게 지웁니다.]를 클릭하고 통과 항목 수를 최대 10 까지 지정한 후 [예약]을 클릭합니다.

6 [예약] 대화 상자에서 작업을 실행할 빈도를 선택한 다음 [확인]을 클릭합니다.

7 최근에 사용한 항목 정리 등록 정보를 변경한 경우 컴퓨터를 다시 시작하라는 메시지가 나타날 수 있습니다. [확인]을 클릭하여 메시지를 닫습니다.

8 [마침]을 클릭합니다.

참고: Shredder에서 삭제한 파일은 복구할 수 없습니다. 파일 영구 제거에 대한 자세한 내용은 McAfee Shredder를 참조하십시오.

QuickClean 작업 삭제

예약된 QuickClean 작업을 더 이상 자동으로 실행하지 않으려면 삭제할 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [McAfee QuickClean]을 클릭합니다.

3 [기존 작업을 선택합니다.] 목록에서 작업을 선택합니다.

4 [삭제]를 클릭한 다음 [예]를 클릭하여 삭제를 확인합니다.

5 [마침]을 클릭합니다.

디스크 조각 모음 작업 예약

디스크 조각 모음 작업을 예약하여 컴퓨터의 하드 드라이브에서 자동으로 조각 모음이 수행되는 빈도를 예약할 수 있습니다. 작업이 완료되면 [디스크 조각 모음] 아래에서 작업이 다시 실행되도록 예약된 날짜와 시간을 볼 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [디스크 조각 모음]을 클릭합니다.

3 [작업 이름] 상자에 작업의 이름을 입력한 다음 [만들기]를 클릭합니다.

4 다음 중 하나를 수행합니다.

- [예약]을 클릭하여 기본값, 즉 [사용 가능한 공간이 부족해도 조각 모음 수행] 옵션을 적용합니다.
- [사용 가능한 공간이 부족해도 조각 모음 수행] 옵션을 선택 취소한 다음 [예약]을 클릭합니다.

5 [예약] 대화 상자에서 작업을 실행할 빈도를 선택한 다음 [확인]을 클릭합니다.

6 [마침]을 클릭합니다.

디스크 조각 모음 작업 수정

예약된 디스크 조각 모음 작업을 수정하여 컴퓨터에서 자동으로 실행되는 빈도를 변경할 수 있습니다. 작업이 완료되면 [디스크 조각 모음] 아래에서 작업이 다시 실행되도록 예약된 날짜와 시간을 볼 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [디스크 조각 모음]을 클릭합니다.

3 [기존 작업을 선택합니다.] 목록에서 작업을 선택한 다음 [수정]을 클릭합니다.

4 다음 중 하나를 수행합니다.

- [예약]을 클릭하여 기본값, 즉 [사용 가능한 공간이 부족해도 조각 모음 수행] 옵션을 적용합니다.
- [사용 가능한 공간이 부족해도 조각 모음 수행] 옵션을 선택 취소한 다음 [예약]을 클릭합니다.

5 [예약] 대화 상자에서 작업을 실행할 빈도를 선택한 다음 [확인]을 클릭합니다.

6 [마침]을 클릭합니다.

디스크 조각 모음 작업 삭제

예약된 디스크 조각 모음 작업을 더 이상 자동으로 실행하지 않으려면 삭제할 수 있습니다.

1 [작업 스케줄러] 창을 엽니다.

방식

1. McAfee SecurityCenter 의 [일반적인 작업]에서 [컴퓨터 유지 관리]를 클릭합니다.
2. [작업 스케줄러]에서 [시작]을 클릭합니다.

2 [예약할 작업을 선택합니다.] 목록에서 [디스크 조각 모음]을 클릭합니다.

3 [기존 작업을 선택합니다.] 목록에서 작업을 선택합니다.

4 [삭제]를 클릭한 다음 [예]를 클릭하여 삭제를 확인합니다.

5 [마침]을 클릭합니다.

제 24 장

McAfee Shredder

McAfee Shredder 는 컴퓨터의 하드 드라이브에서 항목을 영구적으로 삭제(또는 영구 제거)합니다. 파일과 폴더를 수동으로 삭제하거나, 휴지통을 비우거나, 임시 인터넷 파일 폴더를 삭제하는 경우에도 컴퓨터 포렌식 도구를 사용하여 이 정보를 복구할 수 있습니다. 또한 일부 프로그램은 열린 파일의 숨겨진 임시 복사본을 만들기 때문에 삭제된 파일을 복구할 수도 있습니다. Shredder 는 원하지 않는 이러한 파일을 안전하고 영구적으로 삭제하여 사용자의 개인 정보를 보호합니다. 영구 제거된 파일은 복원할 수 없습니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

Shredder 기능

Shredder 는 컴퓨터의 하드 드라이브에서 항목을 삭제하여 해당 항목과 관련된 정보를 복구할 수 없도록 합니다. Shredder 는 파일 및 폴더, 휴지통 및 임시 인터넷 파일 폴더의 항목, 재기록 가능 CD, 외부 하드 드라이브 및 플로피 디스크와 같은 컴퓨터 디스크의 전체 내용을 안전하고 영구적으로 삭제하여 사용자의 개인 정보를 보호합니다.

파일, 폴더 및 디스크 영구 제거

Shredder 는 특수 도구를 사용하는 경우에도 임시 인터넷 파일 폴더와 휴지통에 있는 삭제된 파일과 폴더에 포함된 정보를 복구할 수 없도록 합니다. Shredder 를 사용하면 영구 제거할 항목의 수를 10 개까지 지정할 수 있습니다. 영구 제거 통과 항목 수가 많을수록 보안 파일 삭제 수준이 높습니다.

파일 및 폴더 영구 제거

휴지통과 임시 인터넷 파일 폴더에 있는 항목을 비롯하여 컴퓨터의 하드 드라이브에서 파일과 폴더를 영구 제거할 수 있습니다.

1 [Shredder]를 엽니다.

방식

1. McAfee SecurityCenter 창의 [일반적인 작업]에서 [고급 메뉴]를 클릭합니다.
2. 왼쪽 창에서 [도구]를 클릭합니다.
3. [Shredder]를 클릭합니다.

2 [파일 및 폴더 영구 제거] 창의 [원하는 작업]에서 [파일 및 폴더 삭제]를 클릭합니다.

3 [분쇄 수준]에서 다음 분쇄 수준 중 하나를 클릭합니다.

- [빠름]: 선택한 항목을 한 번에 영구 제거합니다.
- [포괄]: 선택한 항목을 일곱 번 만에 영구 제거합니다.
- [사용자 정의]: 선택한 항목을 최대 열 번 만에 영구 제거합니다.

4 [다음]을 클릭합니다.

5 다음 중 하나를 수행합니다.

- [분쇄할 파일 선택] 목록에서 [휴지통 내용] 또는 [임시 인터넷 파일]을 클릭합니다.
- [찾아보기]를 클릭하여 영구 제거할 파일을 탐색한 다음 해당 파일을 선택하고 [열기]를 클릭합니다.

6 [다음]을 클릭합니다.

7 [시작]을 클릭합니다.

8 Shredder 가 작업을 완료하면 [완료]를 클릭합니다.

참고: Shredder가 이 작업을 완료할 때까지 파일을 사용하지 마십시오.

전체 디스크 영구 제거

디스크의 전체 내용을 한 번에 영구 제거할 수 있습니다. 외부 하드 드라이브, 기록 가능 CD 및 플로피 디스크와 같은 제거할 수 있는 드라이브만 영구 제거할 수 있습니다.

1 [Shredder]를 엽니다.

   방식

   1. McAfee SecurityCenter 창의 [일반적인 작업]에서 [고급 메뉴]를 클릭합니다.
   2. 왼쪽 창에서 [도구]를 클릭합니다.
   3. [Shredder]를 클릭합니다.

2 [파일 및 폴더 영구 제거] 창의 [원하는 작업]에서 [전체 디스크 삭제]를 클릭합니다.

3 [분쇄 수준]에서 다음 분쇄 수준 중 하나를 클릭합니다.

- [빠름]: 선택한 드라이브를 한 번에 영구 제거합니다.
- [포괄]: 선택한 드라이브를 일곱 번 만에 영구 제거합니다.
- [사용자 정의]: 선택한 드라이브를 최대 열 번 만에 영구 제거합니다.

4 [다음]을 클릭합니다.

5 [디스크 선택] 목록에서 영구 제거할 드라이브를 클릭합니다.

6 [다음]을 클릭한 후 [예]를 클릭하여 확인합니다.

7 [시작]을 클릭합니다.

8 Shredder 가 작업을 완료하면 [완료]를 클릭합니다.

참고: Shredder가 이 작업을 완료할 때까지 파일을 사용하지 마십시오.

제 25 장

McAfee Network Manager

Network Manager 에서는 홈 네트워크를 구성하는 구성 요소와 컴퓨터의 그래픽 보기를 제공합니다. Network Manager 를 사용하여 네트워크에 있는 관리된 컴퓨터의 보안 상태를 원격으로 모니터링하고 해당 컴퓨터의 보고된 보안 취약성을 원격으로 수정할 수 있습니다.

Network Manager 를 사용하기 전에 일부 기능을 익힐 수 있습니다. 이러한 기능을 구성하고 사용하는 방법에 대한 자세한 내용은 Network Manager 도움말에 제공되어 있습니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

Network Manager 기능

Network Manager 는 다음과 같은 기능을 제공합니다.

그래픽 네트워크 맵

Network Manager 의 네트워크 맵에서는 홈 네트워크를 구성하는 컴퓨터 및 구성 요소의 보호 상태에 대한 그래픽 개요를 제공합니다. 컴퓨터를 추가하는 등 네트워크를 변경하면 네트워크 맵에서 이러한 변경 사항을 인식합니다. 네트워크 맵을 새로 고치고, 네트워크 이름을 변경하고, 네트워크 맵 구성 요소를 표시하거나 숨겨서 보기를 사용자 지정할 수 있습니다. 또한 네트워크 맵에 있는 구성 요소에 대한 자세한 정보도 볼 수 있습니다.

원격 관리

Network Manager 네트워크 맵을 사용하여 홈 네트워크를 구성하는 컴퓨터의 보호 상태를 관리할 수 있습니다. 관리된 네트워크에 가입하도록 컴퓨터를 초대하고, 관리된 컴퓨터의 보호 상태를 모니터링하고, 네트워크의 원격 컴퓨터에서 알려진 보안 취약성을 해결할 수 있습니다.

Network Manager 아이콘 이해

다음 표에서는 Network Manager 네트워크 맵에서 일반적으로 사용되는 아이콘을 설명합니다.

아이콘	설명
	관리된 온라인 컴퓨터를 나타냅니다.
	관리된 오프라인 컴퓨터를 나타냅니다.
	SecurityCenter 가 설치된 관리되지 않은 컴퓨터를 나타냅니다.
	관리되지 않은 오프라인 컴퓨터를 나타냅니다.
	SecurityCenter 가 설치되지 않은 온라인 컴퓨터 또는 알 수 없는 네트워크 장치를 나타냅니다.
	SecurityCenter 가 설치되지 않은 오프라인 컴퓨터 또는 알 수 없는 오프라인 네트워크 장치를 나타냅니다.
	해당 항목이 보호되고 연결되어 있다는 것을 의미합니다.
	해당 항목에 주의가 필요하다는 것을 의미합니다.
	해당 항목에 즉각적인 주의가 필요하다는 것을 의미합니다.
	무선 홈 라우터를 나타냅니다.
	표준 홈 라우터를 나타냅니다.
	인터넷에 연결된 상태를 나타냅니다.
	인터넷에 연결되지 않은 상태를 나타냅니다.

제 26 장

관리된 네트워크 설치

관리된 네트워크를 설치하려면 네트워크 맵 항목을 작업하고 구성원(컴퓨터)을 네트워크에 추가합니다. 컴퓨터는 네트워크의 신뢰 있는 구성원이 된 후에 원격으로 관리되거나 네트워크에서 다른 컴퓨터를 원격으로 관리할 수 있는 권한을 받을 수 있습니다. 기존 네트워크 구성원(컴퓨터)이 새 컴퓨터에게 관리 권한을 줄 때 네트워크 구성원 자격이 부여됩니다.

네트워크를 변경한 이후에도(예: 컴퓨터 추가) 네트워크 맵에 표시된 모든 구성 요소와 관련된 세부 정보를 볼 수 있습니다.

이 장에서

네트워크 맵 작업

Network Manager 는 컴퓨터가 네트워크에 연결될 때 구성원(관리된 구성원 또는 관리되지 않은 구성원)의 유무, 라우터 속성, 인터넷 연결 상태 등을 확인합니다. 구성원이 확인되지 않은 경우 현재 연결된 컴퓨터를 네트워크의 첫 번째 컴퓨터로 가정하고 자동으로 관리 권한을 제공하며 관리된 구성원으로 인식합니다. 기본적으로 네트워크 이름에는 네트워크에 연결되고 SecurityCenter 가 설치된 첫 번째 컴퓨터의 작업 그룹이나 도메인 이름이 포함되지만 네트워크 이름을 언제든지 변경할 수 있습니다.

네트워크를 변경하는 경우(예: 컴퓨터를 추가하는 경우) 네트워크 맵을 사용자 지정할 수 있습니다. 예를 들어 네트워크 맵을 새로 고치고, 이름을 변경하고, 네트워크 맵 구성 요소를 표시하거나 숨겨서 보기를 사용자 지정할 수 있습니다. 또한 네트워크 맵에 표시된 구성 요소와 관련된 자세한 정보도 볼 수 있습니다.

네트워크 맵 액세스

네트워크 맵에는 홈 네트워크를 구성하는 구성 요소와 컴퓨터가 그래픽으로 제공됩니다.

- [기본] 또는 [고급] 메뉴에서 [네트워크 관리]를 클릭합니다.

참고: 네트워크 맵에 처음 액세스할 때 네트워크의 다른 컴퓨터를 신뢰하는지 묻는 메시지가 나타납니다.

네트워크 맵 새로 고침

다른 컴퓨터가 관리된 네트워크에 가입한 후를 포함하여 언제든지 네트워크 맵을 새로 고칠 수 있습니다.

1 [기본] 또는 [고급] 메뉴에서 [네트워크 관리]를 클릭합니다.

2 [원하는 작업]에서 [네트워크 맵 새로 고침]을 클릭합니다.

참고: 네트워크 맵에서 선택한 항목이 없는 경우에만 [네트워크 맵 새로 고침] 링크를 사용할 수 있습니다. 항목 선택을 취소하려면 선택한 항목을 클릭하거나 네트워크 맵의 공백 영역을 클릭합니다.

네트워크 이름 변경

기본적으로 네트워크 이름에는 네트워크에 연결되고 SecurityCenter 가 설치된 첫 번째 컴퓨터의 작업 그룹이나 도메인 이름이 포함됩니다. 다른 이름을 사용하려면 변경할 수 있습니다.

1 [기본] 또는 [고급] 메뉴에서 [네트워크 관리]를 클릭합니다.

2 [원하는 작업]에서 [네트워크 이름 변경]을 클릭합니다..

3 [네트워크 이름] 상자에 네트워크의 이름을 입력합니다.

4 [확인]을 클릭합니다.

참고: 네트워크 맵에서 선택한 항목이 없는 경우에만 [네트워크 이름 변경] 링크를 사용할 수 있습니다. 항목 선택을 취소하려면 선택한 항목을 클릭하거나 네트워크 맵의 공백 영역을 클릭합니다.

네트워크 맵에 항목 표시 또는 숨기기

기본적으로 홈 네트워크의 모든 컴퓨터와 구성 요소는 네트워크 맵에 나타납니다. 항목을 숨겼더라도 해당 항목을 언제든지 표시할 수 있습니다. 관리되지 않은 항목만 숨길 수 있고 관리된 컴퓨터는 숨길 수 없습니다.

수행할 작업...	[기본] 메뉴나 [고급] 메뉴에서 [네트워크 관리]를 클릭하고 다음 작업을 수행합니다.
네트워크 맵에서 항목 숨기기	네트워크 맵에서 항목을 클릭하고 [원하는 작업] 하위 항목에서 [이 항목 숨기기]를 클릭합니다. [확인] 대화 상자에서 [예]를 클릭합니다.
네트워크 맵에서 숨겨진 항목 표시	[원하는 작업]에서 [숨겨진 항목 표시]를 클릭합니다.

항목에 대한 세부 정보 보기

네트워크 맵에서 구성 요소를 선택하면 네트워크의 구성 요소에 대한 자세한 정보를 볼 수 있습니다. 구성 요소 이름, 보호 상태 등 구성 요소를 관리하는 데 필요한 정보를 알 수 있습니다.

1 네트워크 맵에서 항목 아이콘을 클릭합니다.

2 [세부 정보]에서 항목에 대한 정보를 봅니다.

관리된 네트워크 가입

컴퓨터는 네트워크의 신뢰 있는 구성원이 된 후에 원격으로 관리되거나 네트워크에서 다른 컴퓨터를 원격으로 관리할 수 있는 권한을 받을 수 있습니다. 기존 네트워크 구성원(컴퓨터)이 새 컴퓨터에게 관리 권한을 줄 때 네트워크 구성원 자격이 부여됩니다. 신뢰하는 컴퓨터만 네트워크에 가입하게 하려면 권한을 부여하는 컴퓨터와 가입하는 컴퓨터에 있는 사용자가 서로를 인증해야 합니다.

컴퓨터가 네트워크에 가입할 때 네트워크의 다른 컴퓨터에 해당 McAfee 보호 상태를 노출하라는 메시지가 나타납니다. 컴퓨터가 보호 상태를 노출하는 데 동의하면 관리된 네트워크 구성원이 됩니다. 컴퓨터가 보호 상태를 노출하는 것을 거부하면 관리되지 않은 네트워크 구성원이 됩니다. 관리되지 않은 네트워크 구성원은 일반적으로 다른 네트워크 기능(예: 파일 전송이나 프린터 공유)에 액세스하려는 게스트 컴퓨터입니다.

참고: 다른 McAfee 네트워킹 프로그램(예: EasyNetwork)이 설치되어 있으면 가입 후 해당 프로그램에서도 관리된 컴퓨터로 인식됩니다. Network Manager에서 컴퓨터에 지정된 권한 수준은 모든 McAfee 네트워킹 프로그램에 적용됩니다. 다른 McAfee 네트워킹 프로그램에서의 게스트, 전체 또는 관리 권한의 의미에 대한 자세한 내용은 해당 프로그램에 제공된 설명서를 참조하십시오.

관리된 네트워크 가입

관리된 네트워크에 가입하도록 초대를 받으면 수락하거나 거절할 수 있습니다. 네트워크의 컴퓨터에서 서로 보안 설정을 모니터링할지 여부(예: 컴퓨터의 바이러스 방지 서비스가 최신 상태인지 여부)를 결정할 수도 있습니다.

1 [관리된 네트워크] 대화 상자에서 [이 네트워크의 모든 컴퓨터에서 보안 설정 모니터링을 허용합니다] 확인란을 선택했는지 확인합니다.

2 [가입]을 클릭합니다.
초대를 수락하면 카드 두 장이 표시됩니다.

3 관리된 네트워크에 가입하도록 초대한 컴퓨터에 표시된 카드와 같은 것인지 확인합니다.

4 [확인]을 클릭합니다.

참고: 관리된 네트워크에 가입하도록 초대한 컴퓨터에서 현재 [보안 확인] 대화 상자에 표시되어 있는 것과 동일한 카드를 표시하고 있지 않은 경우에는 관리된 네트워크에서 보안 위반이 있음을 나타냅니다. 네트워크에 가입하면 컴퓨터가 위험에 노출될 수 있으므로 [관리된 네트워크] 대화 상자에서 [취소]를 클릭합니다.

컴퓨터를 관리된 네트워크에 가입하도록 초대

컴퓨터가 관리된 네트워크에 추가되거나 네트워크에 관리되지 않은 다른 컴퓨터가 존재할 경우 그 컴퓨터가 관리된 네트워크에 가입하도록 초대할 수 있습니다. 네트워크에서 관리 권한을 받은 컴퓨터만이 다른 컴퓨터를 가입하도록 초대할 수 있습니다. 초대장을 보낼 경우 가입하는 컴퓨터에 할당하고 싶은 권한 수준도 지정하십시오.

1 네트워크 맵에서 관리되지 않은 컴퓨터의 아이콘을 클릭합니다.

2 [원하는 작업]에서 [이 컴퓨터 모니터링]을 클릭합니다.

3 [컴퓨터를 관리된 네트워크에 가입하도록 초대합니다] 대화 상자에서 다음 중 하나를 수행합니다.

- 컴퓨터가 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 게스트 액세스 허용]을 클릭합니다(홈에서 임시 사용자를 위해 이 옵션을 사용할 수 있음).
- 컴퓨터가 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 전체 액세스 허용]을 클릭합니다.

- 컴퓨터가 관리 권한을 가지고 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 관리자 액세스 허용]을 클릭합니다. 이 경우 관리된 네트워크에 가입하려는 다른 컴퓨터에도 액세스가 허용됩니다.

4 [확인]을 클릭합니다.
관리된 네트워크에 가입하라는 초대장이 컴퓨터로 전송됩니다. 컴퓨터가 초대를 수락하면 카드 두 장이 표시됩니다.

5 관리된 네트워크에 가입하도록 초대한 컴퓨터에 표시된 카드와 같은 것인지 확인합니다.

6 [액세스 허용]을 클릭합니다.

참고: 관리된 네트워크에 가입하도록 초대한 컴퓨터에서 현재 [보안 확인] 대화 상자에 표시되어 있는 것과 동일한 카드를 표시하고 있지 않은 경우에는 관리된 네트워크에서 보안 위반이 있음을 나타냅니다. 컴퓨터에서 네트워크에 가입하도록 허용하면 다른 컴퓨터가 위험에 노출될 수 있으므로 [보안 확인] 대화 상자에서 [액세스 거부]를 클릭합니다.

네트워크의 다른 컴퓨터에 대한 신뢰 중지

실수로 네트워크의 다른 컴퓨터를 신뢰한 경우 신뢰를 중지할 수 있습니다.

- [원하는 작업]에서 [네트워크의 컴퓨터에 대한 신뢰 중지]를 클릭합니다.

참고: 사용자에게 관리 권한이 있고 네트워크에 다른 관리된 컴퓨터가 있는 경우 [이 네트워크의 컴퓨터에 대한 신뢰를 중지합니다] 링크를 사용할 수 없습니다.

제 27 장

네트워크 원격 관리

관리된 네트워크를 설치하면 네트워크를 구성하는 컴퓨터와 구성 요소들을 원격으로 관리할 수 있습니다. 컴퓨터의 상태, 권한 수준 및 구성 요소를 모니터링할 수 있고 대부분의 보안 취약성을 원격으로 수정할 수 있습니다.

이 장에서

상태 및 권한 모니터링

관리된 네트워크에는 관리된 구성원과 관리되지 않은 구성원이 있습니다. 관리된 구성원은 네트워크의 다른 컴퓨터에서 해당 McAfee 보호 상태를 모니터링할 수 있도록 허용합니다. 관리되지 않은 구성원은 이 작업을 수행할 수 없습니다. 관리되지 않은 구성원은 일반적으로 다른 네트워크 기능(예: 파일 전송이나 프린터 공유)에 액세스하려는 게스트 컴퓨터입니다. 관리되지 않은 컴퓨터는 네트워크의 다른 관리된 컴퓨터로부터 언제든지 관리된 컴퓨터가 되도록 초대받을 수 있습니다. 마찬가지로 관리된 컴퓨터는 언제든지 관리되지 않은 컴퓨터가 될 수 있습니다.

관리된 컴퓨터는 관리, 전체 또는 게스트 권한을 가집니다. 관리된 컴퓨터는 관리 권한을 통해 네트워크의 모든 관리된 컴퓨터의 보호 상태를 관리하고 다른 컴퓨터에게 네트워크 구성원 자격을 부여합니다. 전체 및 게스트 권한을 가진 컴퓨터는 네트워크에만 액세스할 수 있습니다. 컴퓨터의 권한 수준은 언제든지 수정할 수 있습니다.

관리된 네트워크에는 라우터와 같은 장치도 있을 수 있으므로 Network Manager 를 사용하여 이러한 장치들도 관리할 수 있습니다. 네트워크 맵에서 장치의 표시 등록 정보를 구성하고 수정할 수도 있습니다.

컴퓨터 보호 상태 모니터링

컴퓨터가 구성원이 아니거나 관리되지 않은 구성원이어서 네트워크에서 컴퓨터의 보호 상태가 모니터링되지 않을 경우 모니터링을 요청할 수 있습니다.

1. 네트워크 맵에서 관리되지 않은 컴퓨터의 아이콘을 클릭합니다.
2. [원하는 작업]에서 [이 컴퓨터 모니터링]을 클릭합니다.

컴퓨터 보호 상태 모니터링 중지

네트워크에서 관리된 컴퓨터의 보호 상태 모니터링을 중지할 수 있습니다. 하지만 이 경우 컴퓨터가 관리되지 않게 되어 컴퓨터의 보호 상태를 원격으로 모니터링할 수 없습니다.

1. 네트워크 맵에서 관리된 컴퓨터의 아이콘을 클릭합니다.
2. [원하는 작업]에서 [이 컴퓨터 모니터링 중지]를 클릭합니다.
3. [확인] 대화 상자에서 [예]를 클릭합니다.

관리된 컴퓨터의 권한 수정

관리된 컴퓨터의 권한을 언제든지 변경할 수 있습니다. 이를 통해 네트워크에서 어떤 컴퓨터가 다른 컴퓨터의 보호 상태를 모니터링할지 여부를 수정할 수 있습니다.

1 네트워크 맵에서 관리된 컴퓨터의 아이콘을 클릭합니다.

2 [원하는 작업]에서 [이 컴퓨터에 대한 사용 권한 수정]을 클릭합니다.

3 [권한 수정] 대화 상자에서 확인란을 선택하거나 취소해서 관리된 네트워크의 컴퓨터가 보호 상태를 모니터링할 수 있을지 여부를 결정합니다.

4 [확인]을 클릭합니다.

장치 관리

Network Manager 에서 관리 웹 페이지에 액세스하여 장치를 관리할 수 있습니다.

1 네트워크 맵에서 장치 아이콘을 클릭합니다.

2 [원하는 작업]에서 [이 장치 관리]를 클릭합니다.
웹 브라우저가 열리고 장치 관리 웹 페이지가 표시됩니다.

3 웹 브라우저에 로그인 정보를 제공하고 장치 보안 설정을 구성합니다.

참고: 장치가 무선 라우터나 액세스 포인트를 보호하는 무선 네트워크 보안일 경우 무선 네트워크 보안을 사용해서 장치 보안 설정을 구성합니다.

장치 표시 등록 정보 수정

장치 표시 등록 정보를 수정할 경우 네트워크 맵에서 장치 표시 이름을 변경하고 장치가 무선 라우터인지 여부를 지정할 수 있습니다.

1 네트워크 맵에서 장치 아이콘을 클릭합니다.

2 [원하는 작업]에서 [장치 표시 등록 정보 수정]을 클릭합니다.

3 [이름] 상자에 이름을 입력하여 장치의 표시 이름을 지정합니다.

4 장치 유형을 지정하려면 무선 라우터가 아닌 경우 [표준 라우터], 무선 라우터인 경우 [무선 라우터]를 클릭합니다.

5 [확인]을 클릭합니다.

보안 취약성 수정

관리 권한을 가진 관리된 컴퓨터는 원격으로 네트워크의 다른 관리된 컴퓨터의 McAfee 보호 상태를 모니터링하고 보고된 보안 취약성을 수정할 수 있습니다. 예를 들어 관리된 컴퓨터의 McAfee 보호 상태가 VirusScan 이 비활성화되어 있다고 나타낼 경우 관리 권한을 가진 다른 관리된 컴퓨터가 원격으로 VirusScan 을 활성화할 수 있습니다.

원격으로 보안 취약성을 수정할 때 Network Manager 는 보고된 대부분의 문제들을 복구합니다. 하지만 로컬 컴퓨터의 수동 개입을 필요로 하는 보안 취약성도 있습니다. 이 경우 Network Manager 는 원격으로 복구할 수 있는 문제를 수정한 후 보안이 취약한 컴퓨터의 SecurityCenter 로 로그인해서 제공된 권장 사항을 따라 남은 문제를 수정합니다. 원격 컴퓨터나 네트워크의 컴퓨터에 SecurityCenter 의 최신 버전을 설치하는 것이 권장되는 경우도 있습니다.

보안 취약성 수정

Network Manager 를 사용하여 관리된 원격 컴퓨터의 대부분의 보안 취약성을 수정할 수 있습니다. 예를 들어 VirusScan 이 원격 컴퓨터에서 비활성화된 경우 활성화할 수 있습니다.

1 네트워크 맵에서 항목 아이콘을 클릭합니다.

2 [세부 정보]에서 항목의 보호 상태를 확인합니다.

3 [원하는 작업]에서 [보안 취약성 수정]을 클릭합니다.

4 보안 문제가 수정되면 [확인]을 클릭합니다.

참고: Network Manager가 자동으로 대부분의 보안 취약성을 수정하지만 취약한 컴퓨터에서 SecurityCenter를 열어 제공되는 권고 사항에 따라 복구해야 하는 경우도 있습니다.

원격 컴퓨터에 McAfee 보안 소프트웨어 설치

네트워크에 있는 하나 이상의 컴퓨터에서 최신 버전의 SecurityCenter 를 실행하지 않는 경우 보호 상태를 원격으로 모니터링할 수 없습니다. 이러한 컴퓨터를 원격으로 모니터링하려면 각 컴퓨터에 SecurityCenter 의 최신 버전을 설치해야 합니다.

1. 보안 소프트웨어를 설치할 컴퓨터에서 SecurityCenter 를 엽니다.
2. [일반적인 작업]에서 [내 계정]을 클릭합니다.
3. 보안 소프트웨어를 처음 설치하여 등록할 때 사용한 전자 메일 주소와 암호를 사용하여 로그인합니다.
4. 해당 제품을 선택하고 [다운로드/설치] 아이콘을 클릭한 다음 화면에 표시되는 지침을 따릅니다.

제 28 장

McAfee EasyNetwork

EasyNetwork 를 사용하여 홈 네트워크에 있는 컴퓨터 간에 안전하게 파일을 공유하고 간단하게 파일을 전송하며 프린터를 공유할 수 있습니다. 하지만 네트워크의 컴퓨터에서 이러한 기능에 액세스하려면 EasyNetwork 를 설치해야 합니다.

EasyNetwork 를 사용하기 전에 일부 기능을 익힐 수 있습니다. 이러한 기능을 구성하고 사용하는 방법에 대한 자세한 내용은 EasyNetwork 도움말에 제공되어 있습니다.

참고: SecurityCenter는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician을 실행할 수 있습니다.

이 장에서

EasyNetwork 기능

EasyNetwork 에서는 다음과 같은 기능을 제공합니다.

파일 공유

EasyNetwork 를 사용하면 네트워크의 다른 컴퓨터와 파일을 쉽게 공유할 수 있습니다. 파일을 공유할 때는 다른 컴퓨터에서 해당 파일에 읽기 전용으로 액세스할 수 있도록 권한을 부여해야 합니다. 관리된 네트워크(구성원)에 대해 전체 또는 관리 액세스 권한을 가진 컴퓨터에서만 파일을 공유하거나 다른 구성원이 공유하는 파일에 액세스할 수 있습니다.

파일 전송

관리된 네트워크(구성원)에 대해 전체 또는 관리 액세스 권한을 가진 컴퓨터에 파일을 전송할 수 있습니다. 받은 파일은 EasyNetwork 의 받은 편지함에 보관됩니다. 받은 편지함은 네트워크의 다른 컴퓨터에서 보낸 모든 파일이 저장되는 임시 저장 위치입니다.

자동화된 프린터 공유

관리된 네트워크에 가입하면 프린터의 현재 이름을 공유 프린터 이름으로 사용하여 사용자 컴퓨터에 연결된 로컬 프린터를 다른 구성원과 공유할 수 있습니다. 또한 네트워크의 다른 컴퓨터에서 공유하는 프린터를 검색하여 사용자가 해당 프린터를 구성하고 사용할 수 있도록 허용합니다.

제 29 장

EasyNetwork 설치

EasyNetwork 를 사용하려면 먼저 EasyNetwork 를 열고 관리된 네트워크에 가입해야 합니다. 관리된 네트워크에 가입한 후에는 네트워크의 다른 컴퓨터와 파일을 공유하고 검색하며 파일을 전송할 수 있습니다. 또한 프린터를 공유할 수도 있습니다. 원하는 경우 언제든지 네트워크에서 탈퇴할 수 있습니다.

이 장에서

EasyNetwork 열기

기본적으로 설치 후에 EasyNetwork 를 시작할지 묻는 메시지가 표시되지만 나중에 EasyNetwork 를 열 수도 있습니다.

- [시작] 메뉴에서 [프로그램], [McAfee]를 차례로 가리킨 다음 [McAfee EasyNetwork]를 클릭합니다.

팁: 설치하는 동안 바탕 화면 및 빠른 실행 아이콘을 만든 경우 바탕 화면 또는 작업 표시줄 맨 오른쪽에 있는 알림 영역에서 McAfee EasyNetwork 아이콘을 두 번 클릭하여 EasyNetwork를 열 수도 있습니다.

관리된 네트워크 가입

현재 연결된 네트워크에 SecurityCenter 를 사용하는 컴퓨터가 없는 경우 사용자가 네트워크의 구성원이 되고 네트워크를 신뢰하는지 여부를 확인하는 메시지가 표시됩니다. 네트워크에 처음 가입할 때는 사용자 컴퓨터 이름이 네트워크 이름에 포함됩니다. 그러나 언제든지 네트워크 이름을 바꿀 수 있습니다.

컴퓨터가 네트워크에 연결되면 네트워크에 있는 다른 컴퓨터에 가입 요청이 전송됩니다. 이러한 요청은 네트워크에서 관리 권한을 가진 모든 컴퓨터에서 허용할 수 있습니다. 권한 부여자는 네트워크에 가입되어 있는 컴퓨터의 권한 수준도 결정할 수 있습니다. 예를 들어 게스트 권한에는 파일 전송만 허용되고, 전체/관리 권한에는 파일 전송 및 파일 공유가 허용됩니다. EasyNetwork 에서 관리 액세스 권한을 가진 컴퓨터는 다른 컴퓨터에 액세스하여 권한을 관리(컴퓨터를 승격 또는 강등)할 수 있지만 전체 액세스 권한을 가진 컴퓨터는 이러한 관리 작업을 수행할 수 없습니다.

참고: 다른 McAfee 네트워킹 프로그램(예: Network Manager)이 설치되어 있으면 가입 후 해당 프로그램에서도 관리된 컴퓨터로 인식됩니다. EasyNetwork에서 컴퓨터에 지정된 권한 수준은 모든 McAfee 네트워킹 프로그램에 적용됩니다. 다른 McAfee 네트워킹 프로그램에서의 게스트, 전체 또는 관리 권한의 의미에 대한 자세한 내용은 해당 프로그램에 제공된 설명서를 참조하십시오.

네트워크 가입

EasyNetwork 를 설치한 후 처음으로 신뢰할 수 있는 네트워크에 연결하는 경우 관리된 네트워크에 가입할지 여부를 묻는 메시지가 표시됩니다. 컴퓨터가 가입에 동의하면 네트워크에서 관리 액세스 권한을 가진 다른 모든 컴퓨터에 요청이 전송됩니다. 컴퓨터에서 프린터나 파일을 공유하거나 네트워크에서 파일을 보내고 복사하려면 먼저 이러한 요청이 허용되어야 합니다. 네트워크의 첫 번째 컴퓨터가 관리 권한을 자동으로 부여받습니다.

1 [공유 파일] 창에서 [이 네트워크에 가입합니다]를 클릭합니다.
네트워크의 관리 컴퓨터에서 요청을 허용하면 이 컴퓨터와 네트워크의 다른 컴퓨터에서 각 컴퓨터의 보안 설정을 관리하도록 허용할지 여부를 묻는 메시지가 표시됩니다.

2 이 컴퓨터와 네트워크의 다른 컴퓨터에서 각 컴퓨터의 보안 설정을 관리하도록 허용하려면 [확인]을 클릭하고, 그렇지 않으면 [취소]를 클릭합니다.

3 권한을 부여하는 컴퓨터에서 [보안 확인] 대화 상자에 표시되어 있는 카드를 표시하는지 확인한 다음 [확인]을 클릭합니다.

참고: 관리된 네트워크에 가입하도록 초대한 컴퓨터에서 현재 [보안 확인] 대화 상자에 표시되어 있는 것과 동일한 카드를 표시하고 있지 않은 경우에는 관리된 네트워크에서 보안 위반이 있음을 나타냅니다. 네트워크에 가입하면 컴퓨터가 위험에 노출될 수 있으므로 [보안 확인] 대화 상자에서 [취소]를 클릭합니다.

네트워크에 액세스 허용

관리된 네트워크에 가입을 요청하면 네트워크에서 관리 권한을 가진 다른 컴퓨터에 메시지가 전송됩니다. 응답하는 첫 번째 컴퓨터가 권한 부여자가 됩니다. 권한 부여자는 컴퓨터에 부여할 액세스 권한의 유형(게스트, 전체 또는 관리)을 결정하는 역할을 합니다.

1 보호 상태에서 적절한 액세스 수준을 클릭합니다.

2 [컴퓨터를 관리된 네트워크에 가입하도록 초대합니다] 대화 상자에서 다음 중 하나를 수행합니다.

- 컴퓨터가 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 게스트 액세스 허용]을 클릭합니다(홈에서 임시 사용자를 위해 이 옵션을 사용할 수 있음).

- 컴퓨터가 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 전체 액세스 허용]을 클릭합니다.
- 컴퓨터가 관리 권한을 가지고 네트워크에 액세스할 수 있게 하려면 [관리된 네트워크 프로그램에 대한 관리자 액세스 허용]을 클릭합니다. 이 경우 관리된 네트워크에 가입하려는 다른 컴퓨터에도 액세스가 허용됩니다.

3 [확인]을 클릭합니다.

4 컴퓨터에서 [보안 확인] 대화 상자에 표시되어 있는 카드를 표시하는지 확인한 다음 [액세스 허용]을 클릭합니다.

참고: 컴퓨터에서 현재 [보안 확인] 대화 상자에 표시되어 있는 것과 동일한 카드를 표시하지 않는 경우에는 관리된 네트워크에서 보안 위반이 있음을 나타냅니다. 이 컴퓨터에서 네트워크에 액세스하도록 허용하면 사용자 컴퓨터가 위험에 노출될 수 있으므로 [보안 확인] 대화 상자에서 [액세스 거부]를 클릭합니다.

네트워크 이름 변경

기본적으로 해당 네트워크에 가입한 첫 번째 컴퓨터의 이름이 네트워크 이름이 되지만 언제든지 네트워크 이름을 변경할 수 있습니다. 네트워크 이름을 변경하면 EasyNetwork 에 표시되는 네트워크 설명도 변경해야 합니다.

1 [옵션] 메뉴에서 [구성]을 클릭합니다.

2 [구성] 대화 상자의 [네트워크 이름] 상자에 네트워크 이름을 입력합니다.

3 [확인]을 클릭합니다.

관리된 네트워크 탈퇴

관리된 네트워크에 가입한 다음 더 이상 구성원의 자격을 유지하지 않으려는 경우 네트워크에서 탈퇴할 수 있습니다. 관리된 네트워크에서 탈퇴한 후에 언제든지 다시 가입할 수 있지만 권한을 다시 부여받아야 합니다. 가입에 대한 자세한 내용은 관리된 네트워크 가입 (162 페이지)을 참조하십시오.

관리된 네트워크 탈퇴

이전에 가입한 관리된 네트워크에서 탈퇴할 수 있습니다.

1 [도구] 메뉴에서 [네트워크 탈퇴]를 클릭합니다.

2 네트워크 탈퇴 대화 상자에서 탈퇴하려는 네트워크 이름을 선택합니다.

3 [네트워크 탈퇴]를 클릭합니다.

제 30 장

파일 공유 및 전송

EasyNetwork 를 사용하면 네트워크의 다른 컴퓨터와 파일을 쉽게 공유하고 보낼 수 있습니다. 파일을 공유할 때는 다른 컴퓨터에서 해당 파일에 읽기 전용으로 액세스할 수 있도록 권한을 부여해야 합니다. 관리된 네트워크의 구성원인 컴퓨터, 즉 전체 또는 관리 액세스 권한을 가진 컴퓨터에서만 다른 구성원 컴퓨터에서 공유하는 파일을 공유하거나 액세스할 수 있습니다.

참고: 대량의 파일을 공유하는 경우 컴퓨터 리소스에 영향을 줄 수도 있습니다.

이 장에서

파일 공유

관리된 네트워크의 구성원인 컴퓨터, 즉 전체 또는 관리 액세스 권한을 가진 컴퓨터에서만 다른 구성원 컴퓨터에서 공유하는 파일을 공유하거나 액세스할 수 있습니다. 폴더를 공유하는 경우 해당 폴더와 그 하위 폴더에 포함된 모든 파일이 공유됩니다. 그러나 나중에 폴더에 추가된 파일은 자동으로 공유되지 않습니다. 공유 파일이나 폴더를 삭제하면 [공유 파일] 창에서도 제거됩니다. 파일 공유는 언제든지 중지할 수 있습니다.

공유 파일에 액세스하려면 EasyNetwork 에서 파일을 직접 열거나 사용자 컴퓨터로 파일을 복사한 다음 컴퓨터에서 열 수 있습니다. 공유 파일 목록이 크고 파일 위치를 찾기 힘든 경우 파일을 검색할 수 있습니다.

참고: EasyNetwork 파일 공유는 보안 연결을 통해서 수행되어야 하기 때문에 EasyNetwork를 사용하여 공유하는 파일은 Windows 탐색기를 사용하여 다른 컴퓨터에서 액세스할 수 없습니다.

파일 공유

파일을 공유하면 관리된 네트워크에 대한 전체 또는 관리 액세스 권한을 가진 모든 구성원에서 해당 파일을 사용할 수 있습니다.

1. Windows 탐색기에서 공유할 파일을 찾습니다.
2. Windows 탐색기에서 찾은 파일을 EasyNetwork 의 [공유 파일] 창으로 끌어 옵니다.

팁: [도구] 메뉴의 [파일 공유]를 클릭하여 파일을 공유할 수도 있습니다. [공유] 대화 상자에서 공유할 파일이 저장되어 있는 폴더를 찾아서 파일을 선택한 후 [공유]를 클릭합니다.

파일 공유 중지

관리된 네트워크에서 파일을 공유하는 경우 언제든지 공유를 중지할 수 있습니다. 파일 공유를 중지하면 관리된 네트워크의 다른 구성원이 해당 파일에 액세스할 수 없습니다.

1. [도구] 메뉴에서 [파일 공유 중지]를 클릭합니다.
2. [공유 파일 중지] 대화 상자에서 더 이상 공유하지 않으려는 파일을 선택합니다.
3. [확인]을 클릭합니다.

공유 파일 복사

공유되지 않더라도 파일을 계속 가지고 있도록 공유 파일을 복사합니다. 관리된 네트워크에 있는 임의의 컴퓨터에서 공유 파일을 복사할 수 있습니다.

- EasyNetwork 의 공유 파일 창에서 Windows 탐색기의 원하는 위치 또는 Windows 바탕 화면으로 파일을 끌어 옵니다.

팁: EasyNetwork에서 파일을 선택한 다음 [도구] 메뉴의 [복사 위치]를 클릭하여 공유 파일을 복사할 수도 있습니다. 폴더에 복사 대화 상자에서 파일을 복사할 폴더를 찾아서 선택한 다음 [저장]을 클릭합니다.

공유 파일 검색

사용자 또는 다른 네트워크 구성원이 공유하는 파일을 검색할 수 있습니다. 검색 조건을 입력하면 EasyNetwork 에서 [공유 파일] 창에 해당 결과를 표시합니다.

1 [공유 파일] 창에서 [검색]을 클릭합니다.

2 [포함] 목록에서 적절한 옵션 (169 페이지)을 클릭합니다.

3 [파일 또는 경로 이름] 목록에 있는 파일 이름이나 경로의 전부 또는 일부를 입력합니다.

4 [형식] 목록에서 적절한 파일 형식 (169 페이지)을 클릭합니다.

5 [시작] 및 [끝] 목록에서 파일이 생성된 날짜 범위를 나타내는 날짜를 클릭합니다.

검색 조건

다음 표에서는 공유 파일을 검색할 때 지정할 수 있는 검색 조건을 설명합니다.

파일 또는 경로 이름

내용	설명
모든 단어 포함	순서에 관계 없이 [파일 또는 경로 이름] 목록에서 지정하는 모든 단어를 포함하는 파일 또는 경로 이름을 검색합니다.
단어 포함	[파일 또는 경로 이름] 목록에서 지정하는 단어 중 임의의 단어를 포함하는 파일 또는 경로 이름을 검색합니다.
정확한 문자열 포함	[파일 또는 경로 이름] 목록에서 지정하는 정확한 구를 포함하는 파일 또는 경로 이름을 검색합니다.

파일 형식

형식	설명
모두	모든 공유 파일 형식을 검색합니다.
문서	모든 공유 문서를 검색합니다.
이미지	모든 공유 이미지 파일을 검색합니다.
비디오	모든 공유 비디오 파일을 검색합니다.
오디오	모든 공유 오디오 파일을 검색합니다.
압축	모든 압축 파일을 검색합니다(예: .zip 파일).

다른 컴퓨터에 파일 보내기

관리된 네트워크의 구성원인 다른 컴퓨터에 파일을 보낼 수 있습니다. 파일을 보내기 전에 EasyNetwork 에서 해당 파일을 받을 컴퓨터에 사용 가능한 디스크 공간이 충분한지 확인합니다.

받은 파일은 EasyNetwork 의 받은 편지함에 보관됩니다. 받은 편지함은 네트워크의 다른 컴퓨터에서 보낸 파일이 저장되는 임시 저장 위치입니다. 파일을 받을 때 EasyNetwork 가 열려 있으면 해당 파일이 받은 편지함에 즉시 나타나고, 그렇지 않으면 작업 표시줄 맨 오른쪽의 알림 영역에 메시지가 표시됩니다. 알림 메시지를 받지 않으려는 경우 이 기능을 끌 수 있습니다(예: 알림 메시지가 작업을 방해하는 경우). 받은 편지함에 이름이 같은 파일이 이미 있으면 새 파일의 이름이 접미 번호가 포함된 이름으로 변경됩니다. 파일은 사용자가 수락할 때까지, 즉 사용자 컴퓨터에 해당 파일을 복사할 때까지 받은 편지함에 남아 있습니다.

다른 컴퓨터에 파일 보내기

파일을 공유하지 않고 관리된 네트워크의 다른 컴퓨터에 파일을 보낼 수 있습니다. 받는 컴퓨터의 사용자가 파일을 보려면 해당 파일을 로컬 위치에 저장해야 합니다. 자세한 내용은 다른 컴퓨터에서 파일 허용 (172 페이지)을 참조하십시오.

1 Windows 탐색기에서 보낼 파일을 찾습니다.

2 Windows 탐색기에서 찾은 파일을 EasyNetwork 의 활성 컴퓨터 아이콘으로 끌어 옵니다.

팁: 컴퓨터에 여러 파일을 보내려면 Ctrl 키를 누르고 파일을 선택합니다. 또한 [도구] 메뉴에서 [보내기]를 클릭해서도 파일을 보낼 수 있습니다. 파일을 선택한 후 [보내기]를 클릭합니다.

다른 컴퓨터에서 파일 허용

관리된 네트워크의 다른 컴퓨터에서 파일을 보낸 경우에는 해당 파일을 사용자 컴퓨터에 저장하여 이를 수락해야 합니다. 파일을 받을 때 EasyNetwork 가 실행 중이 아닌 경우 작업 표시줄 맨 오른쪽의 알림 영역에 알림 메시지가 표시됩니다. 이 경우 알림 메시지를 클릭하면 EasyNetwork 를 열고 파일에 액세스할 수 있습니다.

- [받음]을 클릭한 다음 EasyNetwork 받은 편지함에서 Windows 탐색기 폴더로 파일을 끌어 옵니다.

팁: EasyNetwork 받은 편지함에서 파일을 선택하고 [도구] 메뉴의 [수락]을 클릭하면 다른 컴퓨터에서 보낸 파일을 받을 수 있습니다. [폴더에 허용] 대화 상자에서 받으려는 파일을 저장할 폴더를 찾아서 선택한 다음 [저장]을 클릭합니다.

파일이 전송된 경우 알림 받음

관리된 네트워크의 다른 컴퓨터에서 파일을 전송한 경우 알림 메시지를 받을 수 있습니다. EasyNetwork 가 실행 중이 아닌 경우 작업 표시줄 맨 오른쪽의 알림 영역에 알림 메시지가 표시됩니다.

1. [옵션] 메뉴에서 [구성]을 클릭합니다.
2. [구성] 대화 상자에서 [다른 컴퓨터가 나에게 파일을 보내면 알립니다] 확인란을 선택합니다.
3. [확인]을 클릭합니다.

제 31 장

프린터 공유

관리된 네트워크에 가입하면 EasyNetwork 에서 사용자 컴퓨터에 연결된 로컬 프린터를 공유하며, 프린터의 현재 이름을 공유 프린터 이름으로 사용합니다. 또한 EasyNetwork 가 네트워크의 다른 컴퓨터에서 공유하는 프린터를 검색하여 사용자가 해당 프린터를 구성하고 사용할 수 있도록 합니다.

네트워크 인쇄 서버(예: 무선 USB 인쇄 서버)를 통해 인쇄하도록 프린터 드라이버를 구성한 경우 EasyNetwork 에서는 해당 프린터를 로컬 프린터로 간주하여 네트워크에서 공유합니다. 프린터 공유는 언제든지 중지할 수 있습니다.

이 장에서

공유 프린터 작업

EasyNetwork 에서는 네트워크의 컴퓨터에서 공유하는 프린터를 검색합니다. EasyNetwork 에서 사용자 컴퓨터에 연결되어 있지 않은 원격 프린터를 검색한 경우 EasyNetwork 를 처음 열면 [공유 파일] 창에 [사용 가능한 네트워크 프린터] 링크가 나타납니다. 그런 다음 사용 가능한 프린터를 설치하거나 사용자 컴퓨터에 이미 연결되어 있는 프린터를 제거할 수 있습니다. 또한 최신 정보를 볼 수 있도록 프린터 목록을 새로 고칠 수도 있습니다.

관리된 네트워크에 가입하지 않았지만 연결되어 있는 경우 Windows 프린터 제어판에서 공유 프린터에 액세스할 수 있습니다.

프린터 공유 중지

프린터 공유를 중지하면 구성원이 프린터를 사용할 수 없습니다.

1 [도구] 메뉴에서 [프린터]를 클릭합니다.

2 [네트워크 프린터 관리] 대화 상자에서 더 이상 공유하지 않을 프린터 이름을 클릭합니다.

3 [공유하지 않음]을 클릭합니다.

사용 가능한 네트워크 프린터 설치

관리된 네트워크의 구성원인 경우 공유되는 프린터에 액세스할 수 있지만 프린터가 사용하는 프린터 드라이버를 설치해야 합니다. 프린터 소유자가 프린터 공유를 중지하면 프린터를 사용할 수 없습니다.

1 [도구] 메뉴에서 [프린터]를 클릭합니다.

2 [사용 가능한 네트워크 프린터] 대화 상자에서 프린터 이름을 클릭합니다.

3 [설치]를 클릭합니다.

참조

용어집에는 McAfee 제품에서 볼 수 있는 자주 사용되는 보안 용어가 정의되어 있습니다.

용어집

8

802.11

무선 네트워크에서 데이터를 전송하기 위한 일련의 IEEE 표준입니다. 802.11 은 일반적으로 Wi-Fi 라고 합니다.

802.11a

5GHz 대역에서 최대 54Mbps 로 데이터를 전송하는 802.11 의 확장입니다. 802.11b 보다 전송 속도는 빠르지만 사정 거리가 훨씬 짧습니다.

802.11b

2.4GHz 대역에서 최대 11Mbps 로 데이터를 전송하는 802.11 의 확장입니다. 802.11a 보다 전송 속도는 느리지만 사정 거리가 더 깁니다.

802.1x

유선 및 무선 네트워크에서의 인증에 대한 IEEE 표준입니다. 802.1x 는 일반적으로 802.11 무선 네트워킹과 함께 사용됩니다.

감시 위치

Data Backup 이 모니터링하는 컴퓨터의 폴더입니다.

감시 파일 형식

감시 위치 내에서 Data Backup 이 백업하거나 보관하는 파일의 형식으로 .doc, .xls 등이 있습니다.

게시

백업 파일을 인터넷에 공용화합니다. Data Backup 라이브러리를 검색하여 게시된 파일에 액세스할 수 있습니다.

격리

격리시키는 동작입니다. 예를 들어, VirusScan 에서는 의심스러운 파일을 감지하여 컴퓨터나 파일을 손상시키지 못하도록 격리시킵니다.

공유

전자 메일 수신자가 선택된 백업 파일을 제한된 시간 동안 액세스할 수 있도록 허용합니다. 파일을 공유할 경우 백업된 파일의 복사본을 지정한 전자 메일 수신자에게 보냅니다. 수신자는 Data Backup 으로부터 파일이 공유되었다는 전자 메일 메시지를 받습니다. 전자 메일에도 공유된 파일의 링크가 있습니다.

공유 암호

통신을 시작하기 전에 두 통신 주체 간에 공유하는 문자열 또는 키(일반적으로 암호)입니다. 공유 암호는 RADIUS 메시지의 중요한 부분을 보호하는 데 사용됩니다.

관리된 네트워크

관리된 구성원과 관리되지 않은 구성원의 두 가지 구성원 유형이 있는 홈 네트워크입니다. 관리된 구성원은 네트워크의 다른 컴퓨터에서 해당 보호 상태를 모니터링할 수 있도록 허용합니다. 관리되지 않은 구성원은 이 작업을 수행할 수 없습니다.

네트워크

액세스 포인트 및 연결된 사용자의 모음으로 ESS 와 같습니다.

네트워크 드라이브

네트워크상에서 여러 사용자가 공유하는 서버에 연결된 디스크 또는 테이프 드라이브로, 경우에 따라 원격 드라이브라고도 합니다.

네트워크 맵

홈 네트워크를 구성하는 컴퓨터와 구성 요소에 대한 그래픽 표현입니다.

노드

네트워크에 연결된 단일 컴퓨터입니다.

다이얼러

인터넷에 연결하는 데 사용되는 소프트웨어입니다. 악의적으로 사용되는 경우 다이얼러는 사용자에게 추가 비용에 대해 알리지 않고 기본 ISP(인터넷 서비스 공급자)가 아닌 다른 곳으로 인터넷 연결을 리디렉션할 수 있습니다.

단순 감시 위치

Data Backup 이 변경하려고 모니터링하는 사용자 컴퓨터의 폴더입니다. 단순 감시 위치를 설정할 경우 Data Backup 이 해당 폴더 내의 감시 파일 형식을 백업하지만 하위 폴더는 백업하지 않습니다.

대역폭

일정한 시간에 전송할 수 있는 데이터의 양입니다.

도메인

로컬 하위 네트워크 또는 인터넷에서 사이트에 대한 설명자입니다.

LAN(Local Area Network)에서 도메인은 단일 보안 데이터베이스로 제어되는 클라이언트와 서버 컴퓨터로 구성된 하위 네트워크입니다. 이러한 구성에서 도메인은 성능을 향상시킬 수 있습니다. 인터넷에서 도메인은 모든 웹 주소의 일부입니다. 예를 들어, www.abc.com 에서는 abc 가 도메인입니다.

동기화

백업된 파일과 로컬 컴퓨터에 저장된 파일이 일치하지 않는 문제를 해결합니다. 온라인 백업 리포지토리의 파일이 다른 컴퓨터의 파일보다 최신 버전일 경우 파일을 동기화합니다.

라우터

네트워크 사이에 데이터 패킷을 전송하는 네트워크 장치입니다. 내부 라우팅 테이블에 기반하는 라우터는 들어오는 각 패킷을 읽은 다음 소스와 대상 주소의 조합 및 현재 트래픽 상태(예: 부하, 회선 비용, 불량 회선)에 따라 패킷을 전송하는 방법을 결정합니다. 라우터를 AP(액세스 포인트)라고도 합니다.

라이브러리

백업하고 게시한 파일의 온라인 저장소 영역입니다. Data Backup 라이브러리는 인터넷에 액세스한 사람이면 누구나 액세스할 수 있는 웹 사이트입니다.

런치패드

U3 USB 프로그램을 시작하고 관리하는 시작점 역할을 하는 U3 인터페이스 구성 요소입니다.

레지스트리

Windows 에서 구성 정보를 저장하는 데이터베이스입니다. 레지스트리에는 각 컴퓨터 사용자의 프로필과 시스템 하드웨어, 설치된 프로그램 및 속성 설정에 대한 정보가 들어 있습니다. Windows 에서는 작업 중에 이 정보를 지속적으로 참조합니다.

로밍

서비스 중단이나 연결 손실 없이 AP(액세스 포인트) 적용 범위 간에 이동할 수 있는 기능입니다.

무선 어댑터

컴퓨터 또는 PDA 에 무선 기능을 추가하는 장치로, USB 포트, PC 카드(카드 버스) 슬롯, 메모리 카드 슬롯을 사용하여 연결되거나 PCI 버스에 내부적으로 연결됩니다.

바로 가기

컴퓨터에 있는 다른 파일의 위치가 들어 있는 파일입니다.

바이러스

파일이나 데이터를 변경할 수 있는 자기 복제 프로그램입니다. 신뢰할 수 있는 사람이 보낸 것처럼 표시되거나 유용한 내용이 포함된 것처럼 표시되는 경우가 많습니다.

방화벽

개인 네트워크에 대한 무단 액세스를 방지하도록 설계된 시스템(하드웨어, 소프트웨어 또는 둘 다)입니다. 방화벽은 주로 인터넷 사용자가 인터넷, 특히 인트라넷에 연결된 개인 네트워크에 액세스하지 못하도록 방지하는 데 사용됩니다. 인트라넷으로 들어오고 나가는 모든 메시지는 방화벽을 통과하며, 방화벽은 각 메시지를 검사하여 지정된 보안 기준에 맞지 않는 메시지를 차단합니다.

백업

보안 온라인 서버에서 중요한 파일의 복사본을 만드는 작업입니다.

버퍼 오버플로

의심스러운 프로그램이나 프로세스가 컴퓨터의 버퍼(임시 저장소 영역)에 한도보다 더 많은 데이터를 저장하려 할 때 발생하는 상황입니다. 버퍼 오버플로는 인접한 버퍼에 있는 유효한 데이터를 손상시키거나 덮어씁니다.

보관

CD, DVD, USB 드라이브, 외장 하드 드라이브 또는 네트워크 드라이브에 중요한 파일의 복사본을 만드는 작업입니다.

보호자 통제

아이들이 웹을 검색하는 동안 보거나 할 수 있는 작업을 통제하는 설정입니다. 보호자 통제를 설정하려면 이미지 필터링을 활성화하거나 비활성화하고, 콘텐츠 등급 그룹을 선택하고, 웹 검색 시간 제한을 설정할 수 있습니다.

복원

온라인 백업 리포지토리 또는 보관에서 파일의 복사본을 검색합니다.

브라우저

인터넷의 웹 페이지를 보는 데 사용하는 프로그램입니다. 많이 사용되는 웹 브라우저에는 Microsoft Internet Explorer 및 Mozilla Firefox 가 있습니다.

브루트 포스 공격

지능적인 전략 대신 반복적인 무작위 대입을 통해(브루트 포스) 암호와 같은 암호화된 데이터를 해독하는 방법입니다. 브루트 포스는 시간이 많이 걸리지만 가장 확실한 공격 방법으로 간주됩니다. 브루트 포스 공격을 브루트 포스 침입이라고도 합니다.

블랙 리스트

피싱 차단에서 사기성 사이트로 간주되는 웹 사이트 목록입니다.

빠른 보관

마지막 전체 보관 또는 빠른 보관 이후에 변경된 파일만 보관합니다. 참고: 전체 보관

사전 공격

일반 단어를 사용하여 암호를 알아내려고 하는 일종의 브루트 포스 공격입니다.

서버

다른 컴퓨터나 프로그램의 연결을 수락하고 적절한 응답을 반환하는 컴퓨터 또는 프로그램입니다. 예를 들어, 전자 메일 프로그램은 전자 메일 메시지를 보내고 받을 때마나 전자 메일 서버에 연결합니다.

서비스 거부

네트워크의 트래픽 속도를 저하시키거나 중단시키는 공격 유형입니다. 네트워크에 너무 많은 추가 요청이 몰려들어 일반 트래픽의 속도가 저하되거나 완전히 중단되는 경우 DoS(서비스 거부) 공격이 발생한 것입니다. 이 공격은 일반적으로 정보를 빼내거나 기타 보안 취약성을 야기하지는 않습니다.

스마트 드라이브

참고: USB 드라이브

스크립트

사용자의 개입 없이 자동으로 실행할 수 있는 명령 목록입니다. 스크립트는 프로그램과 달리 일반 텍스트 형식으로 저장되며 실행될 때마다 컴파일됩니다. 매크로와 배치 파일을 스크립트라고도 합니다.

시스템 복원 지점

컴퓨터 메모리 또는 데이터베이스 내용을 포함하는 스냅숏(이미지)입니다. Windows 는 주기적으로 또는 프로그램이나 드라이버가 설치되는 경우처럼 중요한 시스템 이벤트가 발생할 때 복원 지점을 만듭니다. 또한 언제든지 사용자 자신의 복원 지점을 만들고 이름을 지정할 수 있습니다.

신뢰하는 목록

신뢰하기 때문에 검색되지 않는 항목을 포함합니다. 악성 프로그램 또는 레지스트리 변경과 같이 실수로 특정 항목을 신뢰한 경우이거나 해당 항목을 검색하려면 이 목록에서 해당 항목을 제거해야 합니다.

실시간 검색

사용자나 컴퓨터가 파일이나 폴더에 액세스할 때 이러한 파일과 폴더에 바이러스나 다른 활동이 없는지 검사합니다.

암호

컴퓨터, 프로그램 또는 웹 사이트에 액세스하는 데 사용하는 코드로, 일반적으로 문자와 숫자로 구성됩니다.

암호 볼트

개인 암호를 위한 보안 저장소 영역입니다. 암호 볼트를 사용하면 다른 사용자(관리자 포함)가 액세스할 수 없는 비밀 장소에 암호를 저장할 수 있습니다.

암호 텍스트

암호화된 텍스트입니다. 암호 텍스트는 해독된 일반 텍스트로 변환해야 읽을 수 있습니다.

암호화

데이터를 텍스트에서 코드로 전환하여 암호 해독법을 모르는 사람은 읽을 수 없도록 정보를 숨기는 프로세스입니다. 암호화된 데이터를 암호 텍스트라고도 합니다.

압축

파일의 전송 또는 저장에 필요한 공간을 최소화하는 형식으로 압축하는 프로세스입니다.

액세스 포인트

이더넷 허브나 스위치에 연결되어 무선 사용자의 물리적 서비스 범위를 확장하는 네트워크 장치를 말하며, 일반적으로 무선 라우터라고 합니다. 무선 사용자가 모바일 장치로 로밍하는 경우 AP(액세스 포인트) 간에 전송이 전달되어 연결 상태를 유지합니다.

온라인 백업 리포지토리

파일을 백업한 후 저장하는 온라인 서버의 위치입니다.

완전 감시 위치

Data Backup 이 변경하려고 모니터링하는 사용자 컴퓨터의 폴더입니다. 완전 감시 위치를 설정하면 Data Backup 에서 해당 폴더 및 하위 폴더에 있는 감시 파일 형식을 백업합니다.

외장 하드 드라이브

컴퓨터 외부에 있는 하드 드라이브입니다.

워드라이버

Wi-Fi 컴퓨터와 몇 가지 특수한 하드웨어 또는 소프트웨어를 갖추고 Wi-Fi(802.11) 네트워크를 찾아 도시를 주행하는 사용자입니다.

웜

활성 메모리에 상주하며 전자 메일을 통해 자체 복사본을 전송할 수 있는 자기 복제 바이러스입니다. 웜은 시스템 자원을 복제하고 소모하므로 성능이 느려지고 작업이 중단됩니다.

웹 메일

인터넷을 통해 온라인으로 주고받는 메시지입니다. 참고: 전자 메일

웹 버그

사용자의 HTML 페이지에 삽입되고 무단 소스가 사용자 컴퓨터의 쿠키를 설정하도록 하는 작은 그래픽 파일입니다. 이러한 쿠키는 무단 소스에 정보를 전송할 수 있습니다. 웹 버그는 웹 비콘, 픽셀 태그, 투명한 GIF 또는 보이지 않는 GIF 라고도 합니다.

위험한 액세스 포인트

권한 없는 액세스 포인트입니다. 위험한 액세스 포인트는 보안 회사 네트워크에 설치되어 권한 없는 사용자에게 네트워크 액세스를 허용할 수 있습니다. 또한 공격자가 man-in-the-middle 공격을 수행하도록 할 수도 있습니다.

이미지 필터링

부적절할 수 있는 웹 이미지가 표시되지 않도록 차단하는 보호자 통제 옵션입니다.

이벤트

사용자, 장치 또는 응답을 실행하는 컴퓨터 자체에서 시작한 작업입니다. McAfee 는 이벤트를 이벤트 로그에 기록합니다.

인증

주로 고유한 이름 및 암호를 기반으로 개인을 식별하는 프로세스입니다.

인터넷

인터넷은 데이터 위치 및 전송에 TCP/IP 프로토콜을 사용하는 수많은 내부 연결 네트워크로 구성됩니다. 인터넷은 미국 국방부의 후원으로 ARPANET 이라는 대학 컴퓨터의 연결(1960 년대 후반 및 1970 년대 초반)로부터 발전했습니다. 오늘날의 인터넷은 약 100,000 개의 독립 네트워크로 구성된 전역 네트워크입니다.

인트라넷

일반적으로 조직 내에서 권한 있는 사용자만 액세스할 수 있는 개인 컴퓨터 네트워크입니다.

일반 텍스트

암호화되지 않은 텍스트입니다. 참고: 암호화

임시 파일

운영 체제 또는 일부 다른 프로그램에서 세션 중에 사용한 후 삭제하기 위해 메모리나 디스크에 만드는 파일입니다.

전자 메일

(Electronic Mail) 컴퓨터 네트워크를 통해 전자적으로 보내고 받는 메시지입니다. 참고: 웹 메일

전자 메일 클라이언트

컴퓨터에서 전자 메일을 보내고 받기 위해 실행하는 프로그램(예: Microsoft Outlook)입니다.

전체 보관

사용자가 설정한 파일 형식 및 위치에 기반하여 완성된 데이터 집합을 보관합니다. 참고: 빠른 보관

캐시

컴퓨터의 임시 저장소 영역입니다. 예를 들어, 웹 검색 속도와 효율성을 높이기 위해 사용자가 다음에 웹 페이지를 보려고 할 때 원격 서버가 아니라 캐시에서 해당 웹 페이지를 검색할 수 있습니다.

콘텐츠 등급 그룹

보호자 통제에서 사용자가 속한 연령 그룹입니다. 콘텐츠는 사용자가 속한 콘텐츠 등급 그룹에 따라 사용 가능하거나 차단됩니다. 콘텐츠 등급 그룹은 미취학 아동, 아동, 16 세 이하 청소년, 19 세 이하 청소년 및 성인으로 분류됩니다.

쿠키

사용자 이름, 현재 날짜 및 시간 등의 정보가 포함된 작은 파일로, 웹을 검색하는 사용자의 컴퓨터에 저장됩니다. 쿠키는 주로 웹 사이트에서 이전에 사이트에 등록했거나 사이트를 방문한 사용자를 식별하는 데 사용되지만 해커가 정보를 빼내는 데 사용할 수도 있습니다.

클라이언트

개인 컴퓨터 또는 워크스테이션에서 실행되는 응용 프로그램으로, 서버를 기반으로 작업을 수행합니다. 예를 들어, 전자 메일 클라이언트는 전자 메일을 보내고 받을 수 있는 응용 프로그램입니다.

키

두 장치 간에 통신을 인증하는 데 사용되는 일련의 문자 및 숫자입니다. 두 장치 모두 이러한 키가 있어야 합니다. 참고: WEP, WPA, WPA2, WPA-PSK 및 WPA2- PSK

키워드

같은 키워드가 할당된 다른 파일과의 관계 또는 연결을 설정하도록 백업된 파일에 할당할 수 있는 단어입니다. 파일에 키워드를 할당하면 인터넷에 게시한 파일을 보다 쉽게 찾을 수 있습니다.

통합 게이트웨이

AP(액세스 포인트), 라우터 및 방화벽 기능이 통합된 장치입니다. 일부 장치에는 향상된 보안 기능 및 브리징 기능도 포함될 수 있습니다.

트로이 목마

정상적인 프로그램처럼 보이지만 중요한 파일을 손상시키고 성능을 저하시키며 사용자 컴퓨터에 무단 액세스를 허용하는 프로그램입니다.

파일 조각

디스크에 흩어져 있는 파일의 작은 부분입니다. 파일 조각화는 파일을 추가하거나 삭제할 때 발생하며 컴퓨터의 성능을 저하시킬 수 있습니다.

팝업

컴퓨터 화면에서 다른 창의 맨 위에 나타나는 작은 창입니다. 보통 팝업 창은 웹 브라우저에서 광고를 표시하는 데 사용됩니다.

포트

컴퓨터로 정보가 들어오고 나가는 위치입니다. 예를 들어, 기존 아날로그 모뎀은 직렬 포트에 연결됩니다.

표준 전자 메일 계정

참고: POP3

프로토콜

두 장치 간에 데이터를 전송하기 위한 형식(하드웨어 또는 소프트웨어)입니다. 다른 컴퓨터와 통신하려면 사용자 컴퓨터나 장치에서 올바른 프로토콜을 지원해야 합니다.

프록시

외부 사이트에 단일 네트워크 주소만 제공하여 네트워크와 인터넷 사이의 장벽 역할을 하는 컴퓨터 또는 컴퓨터에서 실행되는 소프트웨어입니다. 프록시는 모든 내부 컴퓨터를 나타내어 인터넷에 대한 액세스를 계속 제공하면서 네트워크 ID 를 보호합니다. 참고: 프록시 서버

프록시 서버

LAN(Local Area Network)에서 들어오고 나가는 인터넷 트래픽을 관리하는 방화벽 구성 요소입니다. 프록시 서버는 자주 사용되는 웹 페이지 같이 자주 요청되는 데이터를 제공하여 성능을 향상시킬 수 있고 소유 파일에 대한 무단 액세스 요청 같이 소유자가 적절하다고 생각하지 않는 요청을 필터링하고 삭제할 수 있습니다.

플러그인

대형 프로그램과 함께 작동하며 추가 기능을 제공하는 작은 소프트웨어 프로그램입니다. 예를 들어, 플러그인을 통해 웹 브라우저는 HTML 문서에 포함된 일반적으로 인식할 수 없는 형식의 파일(예: 애니메이션, 비디오 및 오디오 파일)에 액세스하고 이를 실행할 수 있습니다.

피싱

사기를 목적으로 개인 모르게 신용 카드와 주민 등록 번호, 사용자 ID 및 암호와 같은 중요한 정보를 가져오도록 설계된 인터넷 스캠입니다.

필요 시 검색

필요 시 즉, 작업을 시작할 때 시작되는 검색입니다. 실시간 검색과 달리 필요 시 검색은 자동으로 시작되지 않습니다.

핫스폿

Wi-Fi(802.11) AP(액세스 포인트)에 의해 서비스가 가능한 지리적 경계입니다. 핫스폿 신호가 있고 즉, 핫스폿 지역임을 알리고 인증이 필요하지 않은 경우 사용자는 핫스폿 지역에서 무선 랩톱을 사용하여 인터넷에 연결할 수 있습니다. 핫스폿은 주로 공항처럼 사람이 많이 모이는 지역에 위치합니다.

허용 목록

사기성 사이트가 아닌 것으로 간주되어 사용자의 액세스가 허용된 웹 사이트 목록입니다.

홈 네트워크

가정에서 파일 및 인터넷 액세스를 공유할 수 있도록 둘 이상의 컴퓨터가 연결되어 있는 네트워크입니다. 참고: LAN

휴지통

Windows 에서 삭제된 파일과 폴더의 시뮬레이션된 휴지통입니다.

A

ActiveX 컨트롤

프로그램이나 웹 페이지의 정상적인 일부로 나타나는 기능을 추가하기 위해 프로그램이나 웹 페이지에서 사용하는 소프트웨어 구성 요소입니다. 대부분의 ActiveX 컨트롤은 무해하지만 일부는 컴퓨터에서 정보를 캡처할 수 있습니다.

D

DAT

(데이터 서명 파일) 컴퓨터나 USB 드라이브에서 바이러스, 트로이 목마, 스파이웨어, 애드웨어 및 기타 악성 프로그램을 검색할 때 사용되는 정의가 들어 있는 파일입니다.

DNS

(Domain Name System) 호스트 이름이나 도메인 이름을 IP 주소로 변환하는 시스템입니다. 웹에서 DNS 는 웹 사이트를 검색할 수 있도록 알아보기 쉬운 웹 주소(예: www.myhostname.com)를 IP 주소(예: 111.2.3.44)로 변환하는 데 사용됩니다. DNS 가 없으면 웹 브라우저에 IP 주소를 직접 입력해야 합니다.

DNS 서버

(Domain Name System 서버) 호스트 또는 도메인 이름과 연결된 IP 주소를 반환하는 컴퓨터입니다. 참고: DNS

E

ESS

(Extended Service Set) 단일 하위 네트워크를 형성하는 둘 이상의 네트워크의 집합입니다.

I

IP 위조

IP 패킷에서 IP 주소를 위조합니다. 세션 가로채기를 포함한 많은 유형의 공격에서 사용되는 방식입니다. 또한 스팸 전자 메일 헤더를 속여 제대로 추적할 수 없도록 하는 데도 사용됩니다.

IP 주소

TCP/IP 네트워크에서 컴퓨터 또는 장치를 식별하는 식별자입니다. TCP/IP 프로토콜을 사용하는 네트워크는 대상 컴퓨터의 IP 주소를 기반으로 메시지를 라우팅합니다. IP 주소 형식은 네 자리마다 마침표(.)로 구분된 32 비트 숫자입니다. 각 숫자는 0 에서 255 사이일 수 있습니다(예: 192.168.1.100).

L

LAN

(Local Area Network) 비교적 작은 영역(예: 건물 하나)에 걸쳐 있는 컴퓨터 네트워크입니다. LAN 에 있는 컴퓨터는 서로 통신하고 프린터 및 파일과 같은 리소스를 공유할 수 있습니다.

M

MAC 주소

(Media Access Control 주소) 네트워크에 액세스하는 실제 장치에 지정된 고유한 일련 번호입니다.

MAC(메시지 인증 코드)

컴퓨터 간에 전송되는 메시지를 암호화하는 데 사용되는 보안 코드입니다. 컴퓨터에서 암호 해독된 코드를 유효하다고 인식하는 경우 메시지를 허용합니다.

man-in-the-middle 공격

통신하고 있는 두 사용자가 통신 연결이 노출되었음을 모르는 상태로 두 사용자 간의 메시지를 가로채 수정하는 방법입니다.

MAPI

(Messaging Application Programming Interface) 여러 메시징 및 작업 그룹 응용 프로그램(예: 전자 메일, 음성 메일 및 팩스)에서 Exchange 클라이언트와 같은 단일 클라이언트를 통해 작업할 수 있도록 허용하는 Microsoft 인터페이스 규격입니다.

MSN

(Microsoft Network) 검색 엔진, 전자 메일, 메신저 및 포털을 비롯하여 Microsoft Corporation 에서 제공하는 웹 기반 서비스 그룹입니다.

N

NIC

(Network Interface Card) 랩톱이나 기타 장치에 장착되어 해당 장치를 LAN 에 연결하는 카드입니다.

P

PCI 무선 어댑터 카드

(Peripheral Component Interconnect) 컴퓨터 내부의 PCI 확장 슬롯에 연결하는 무선 어댑터 카드입니다.

POP3

(Post Office Protocol 3) 전자 메일 클라이언트 프로그램과 전자 메일 서버 간의 인터페이스입니다. 대부분의 일반 사용자는 표준 전자 메일 계정이라고도 하는 POP3 전자 메일 계정을 사용합니다.

PPPoE

(Point-to-Point Protocol Over Ethernet) 전송할 때 이더넷에서 PPP(Point-to-Point Protocol) 전화 접속 프로토콜을 사용하는 방법입니다.

PUP(악성 프로그램)

사용자의 허가 없이 개인 정보를 수집하고 전송하는 프로그램(예: 스파이웨어 및 애드웨어)입니다.

R

RADIUS

(Remote Access Dial-In User Service) 일반적으로 원격 액세스 환경에서 사용자 인증을 허용하는 프로토콜입니다. RADIUS 프로토콜은 원래 전화 접속 원격 액세스 서버에서 사용하도록 정의되었지만 지금은 WLAN 사용자 공유 암호의 802.1x 인증을 포함하여 다양한 인증 환경에서 사용됩니다.

Rootkit

사용자에게 컴퓨터나 컴퓨터 네트워크에 대한 관리자 수준 액세스 권한을 부여하는 도구(프로그램) 모음입니다. Rootkit 에는 스파이웨어 및 컴퓨터 데이터와 개인 정보에 대한 추가 보안 또는 개인 정보 보호 위험을 초래할 수 있는 악성 프로그램이 포함됩니다.

S

SMTP

(Simple Mail Transfer Protocol) 네트워크에서 컴퓨터 간에 메시지를 보내기 위한 TCP/IP 프로토콜입니다. 이 프로토콜은 인터넷상에서 전자 메일을 라우팅하는 데 사용됩니다.

SSID

(Service Set Identifier) Wi-Fi(802.11) 네트워크를 식별하는 토큰(보안 키)입니다. SSID 는 네트워크 관리자가 설정하며 네트워크에 가입하려는 사용자가 제공해야 합니다.

SSL

(Secure Sockets Layer) 인터넷에서 개인 문서 전송용으로 Netscape 에서 개발한 프로토콜입니다. SSL 은 공개 키를 사용하여 SSL 연결을 통해 전송되는 데이터를 암호화하는 방식으로 작동합니다. SSL 연결이 필요한 URL 은 http: 대신 https:로 시작합니다.

SystemGuard

컴퓨터에 대한 무단 변경을 검색하고 변경이 발생하면 알림을 보내는 McAfee 경고입니다.

T

TKIP

(Temporal Key Integrity Protocol) WEP 보안의 취약점, 특히 암호화 키의 재사용과 관련된 문제를 해결하는 프로토콜입니다. TKIP 는 10,000 패킷마다 임시 키를 변경하는 동적 배포 방법을 통해 네트워크 보안을 강화합니다. TKIP(보안) 프로세스는 클라이언트와 액세스 포인트(AP) 사이의 128 비트 임시 키 공유에서부터 시작됩니다. 즉, TKIP 는 임시 키를 클라이언트의 MAC 주소와 통합한 다음 비교적 큰 128 비트 초기화 벡터를 추가하여 데이터를 암호화하는 키를 생성합니다. 이 프로시저를 통해 각 스테이션에서는 다른 키 스트림을 사용하여 데이터를 암호화할 수 있습니다. TKIP 는 RC4 를 사용하여 암호화를 수행합니다.

U

U3

(You: Simplified, Smarter, Mobile) USB 드라이브에서 직접 Windows 2000 또는 Windows XP 프로그램을 실행하는 플랫폼입니다. U3 이니셔티브는 2004 년 M-Systems 와 SanDisk 에 의해 만들어졌으며 컴퓨터에 데이터 또는 설정을 설치하거나 저장하지 않고도 Windows 컴퓨터에서 U3 프로그램을 실행할 수 있도록 합니다.

URL

(Uniform Resource Locator) 인터넷 주소의 표준 형식입니다.

USB

(Universal Serial Bus) 컴퓨터에 키보드, 조이스틱, 프린터와 같은 주변 장치를 연결할 수 있게 하는 표준화된 직렬 컴퓨터 인터페이스입니다.

USB 드라이브

컴퓨터의 USB 포트에 연결되는 작은 메모리 드라이브입니다. USB 드라이브는 작은 디스크 드라이브처럼 작동하여 한 컴퓨터에서 다른 컴퓨터로의 파일 전송을 용이하게 합니다.

USB 무선 어댑터 카드

컴퓨터의 USB 슬롯에 연결되는 무선 어댑터 카드입니다.

V

VPN

(Virtual Private Network) 공용 네트워크 관리의 이점을 활용하기 위해 공용 네트워크 내에 구성된 개인 네트워크입니다. VPN 은 기업에서 지리적으로 넓은 영역을 포함하는 WAN(광역 네트워크)을 만드는 데 사용되어 지사에 대한 사이트 간 연결을 제공하거나 이동 중인 사용자가 회사 LAN 에 전화 접속할 수 있도록 합니다.

W

WEP

(Wired Equivalent Privacy) Wi-Fi(802.11) 표준의 일부로 정의된 암호화 및 인증 프로토콜입니다. 초기 버전은 RC4 암호를 기반으로 하며 많은 취약점이 있습니다. WEP 는 무선상의 데이터를 암호화하는 방식으로 보안을 제공하여 끝점 간에 전송되는 데이터를 보호합니다. 그러나 WEP 는 기대만큼 안전하지 않을 것으로 확인되었습니다.

Wi-Fi

(Wireless Fidelity) Wi-Fi Alliance 에서 모든 유형의 802.11 네트워크를 나타낼 때 사용하는 용어입니다.

Wi-Fi Alliance

선도적인 무선 하드웨어 및 소프트웨어 공급자로 구성된 조직입니다. Wi-Fi Alliance 는 모든 802.11 기반 제품의 상호 운용성을 인증하고, Wi-Fi 라는 용어를 802.11 기반 무선 LAN 제품 시장에서 글로벌 브랜드 이름으로 사용하도록 홍보하는 업무를 수행합니다. 이 조직은 업계의 성장을 활성화하는 공급업체들의 컨소시엄, 테스트 연구소 및 정보 센터의 역할을 합니다.

Wi-Fi Certified

Wi-Fi Alliance 의 테스트를 거쳐 승인됩니다. Wi-Fi Certified 제품은 서로 다른 제조업체에서 만들어진 경우에도 상호 운용 가능한 것으로 간주됩니다. Wi-Fi Certified 제품의 사용자는 모든 브랜드의 액세스 포인트(AP)를 인증된 다른 브랜드의 클라이언트 하드웨어와 함께 사용할 수 있습니다.

WLAN

(Wireless Local Area Network) 무선 연결을 사용하는 LAN 입니다. WLAN 에서는 유선보다는 고주파 무선을 사용하여 컴퓨터 간에 통신할 수 있도록 합니다.

WPA

(Wi-Fi Protected Access) 현재와 미래의 무선 LAN 시스템에 대한 데이터 보호 및 액세스 제어 수준을 크게 강화하는 사양 표준입니다. 기존 하드웨어에서 소프트웨어 업그레이드로 실행되도록 설계된 WPA 는 IEEE 802.11i 표준에서 파생된 것으로 이 표준과 호환됩니다. WPA 를 올바르게 설치할 경우 무선 LAN 사용자는 데이터를 보호된 상태로 유지하고 권한 있는 네트워크 사용자만 네트워크에 액세스할 수 있도록 보안을 강화할 수 있습니다.

WPA-PSK

강력한 엔터프라이즈급 보안이 필요하지 않으며, 인증 서버에 대한 액세스 권한이 없는 개인 사용자용으로 특별히 설계된 WPA 모드입니다. 이 모드에서는 개인 사용자가 시작 암호를 수동으로 입력하여 미리 공유한 키 모드에서 Wi-Fi 보호 액세스를 활성화하고, 각 무선 컴퓨터 및 액세스 포인트에서 정기적으로 패스 구문을 변경해야 합니다. 참고: WPA2-PSK 및 TKIP

WPA2

WPA 보안 표준의 업데이트로, 802.11i IEEE 표준을 기반으로 합니다.

WPA2-PSK

WPA-PSK 와 유사한 특수 WPA 모드로, WPA2 표준을 기반으로 합니다. 이전 장치에서는 일반적으로 한 번에 하나의 암호화 모드만 지원하여 모든 클라이언트에서 동일한 암호화 모드를 사용해야 했지만 WPA2-PSK 장치에서는 여러 암호화 모드(예: AES, TKIP)를 동시에 지원합니다.

McAfee 정보

캘리포니아주 산타클라라에 본사를 두고 있는 McAfee, Inc.는 침입 방지 및 보안 위험 관리 분야의 세계적인 선도 업체로서 전세계에 시스템 및 네트워크를 안전하게 보호하는 입증된 예방 솔루션과 서비스를 제공합니다. McAfee 는 최고의 보안 전문 기술을 바탕으로 기술 혁신을 통해 개인 사용자, 기업, 공공 기관, 서비스 공급자가 공격을 차단하고, 시스템 중단을 방지하고, 보안 상태를 지속적으로 추적하여 보안을 향상시킬 수 있도록 도와줍니다.

Copyright

사용권

모든 사용자에 대한 고지 사항: 사용자가 구입한 사용권에 대한 올바른 법적 계약서를 주의 깊게 읽으십시오. 정식 소프트웨어의 사용에 대한 일반 사항과 조건이 명시되어 있습니다. 구입한 사용권의 종류를 잘 모르겠으면, 영업부에 문의하시거나 기타 관련 사용권 허가서 또는 소프트웨어 포장에 포함되어 있는 구입 주문서 또는 구입의 일부로서 별도로 받은 사용권 허가서(책자, 제품 CD 에 있는 파일, 소프트웨어 패키지를 다운로드한 웹 사이트에 있는 파일)를 참조하십시오. 계약서에 언급된 내용에 동의하지 않을 경우에는 소프트웨어를 설치하지 마십시오. 가능한 경우 제품을 MCAFEE, INC.나 구매처로 반환하여 전액 환불을 받을 수 있습니다.

제 32 장

고객 및 기술 지원

SecurityCenter 는 보호 문제의 심각성 여부에 관계 없이 보호 문제가 검색되는 즉시 보고합니다. 심각한 보호 문제는 즉각적인 조치가 필요하고 보호 상태를 손상시킵니다(색상을 빨간색으로 변경). 심각하지 않은 보호 문제는 즉각적인 조치가 필요하지는 않으며 문제 유형에 따라 보호 상태를 손상시킬 수도 있고 아닐 수도 있습니다. 보호 상태를 녹색으로 만들려면 심각한 문제는 모두 수정하고 심각하지 않은 문제는 모두 수정하거나 무시해야 합니다. 보호 문제 진단 시 도움이 필요하면 McAfee Virtual Technician 을 실행할 수 있습니다. McAfee Virtual Technician 에 대한 자세한 내용은 McAfee Virtual Technician 도움말을 참조하십시오.

McAfee가 아닌 다른 파트너 또는 공급자가 제공하는 보안 소프트웨어를 구입한 경우 웹 브라우저를 열고 www.mcafeehelp.com으로 이동하십시오. 그런 다음 [파트너 링크]에서 McAfee Virtual Technician에 액세스할 파트너 또는 공급자를 선택하십시오.

참고: McAfee Virtual Technician을 설치 및 실행하려면 Windows 관리자로 컴퓨터에 로그인해야 합니다. 그렇게 하지 않으면 MVT가 문제를 해결하지 못할 수 있습니다. Windows 관리자로 로그인에 대한 자세한 내용은 Windows 도움말을 참조하십시오. Windows Vista™에서는 MVT 실행 시 메시지가 표시됩니다. 메시지가 표시되면 [승인]을 클릭합니다. Virtual Technician은 Mozilla® Firefox에서는 작동하지 않습니다.

이 장에서

McAfee Virtual Technician 사용

Virtual Technician은 개인 기술 지원 담당자처럼 SecurityCenter 프로그램에 대한 정보를 수집하여 사용자 컴퓨터의 보호 문제를 해결할 수 있습니다. Virtual Technician을 실행하면 SecurityCenter 프로그램이 올바르게 작동하는지 확인합니다. 문제가 발견되면 Virtual Technician은 문제를 수정하거나 문제에 대한 자세한 정보를 제공합니다. 작업을 마치면 분석 결과가 표시되고 필요한 경우 McAfee로부터 추가 기술 지원을 받을 수 있게 합니다.

Virtual Technician 은 컴퓨터 및 파일의 보안 및 무결성을 유지하기 위해 개인 신상 정보를 수집하지 않습니다.

참고: Virtual Technician에 대한 자세한 내용은 Virtual Technician에서 도움말 아이콘을 클릭하십시오.

Virtual Technician 시작

Virtual Technician 은 SecurityCenter 프로그램에 대한 정보를 수집하여 사용자의 보호 문제를 해결할 수 있습니다. 개인 정보 보호를 위해 이 정보에 개인 신상 정보는 포함되지 않습니다.

1. [일반적인 작업]에서 [McAfee Virtual Technician]을 클릭합니다.
2. 화면에 나타나는 지침에 따라 Virtual Technician 을 다운로드하고 실행합니다.

지원 및 다운로드

사용자 설명서를 포함하여 해당 국가의 McAfee 지원 및 다운로드 사이트에 대해서는 다음 표를 참조하십시오.

지원 및 다운로드

국가	McAfee 지원	McAfee 다운로드
오스트레일리아	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
브라질	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
캐나다(영어)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
캐나다(프랑스어)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
중국어(chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
중국어(tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
체코	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
덴마크	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
핀란드	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
프랑스	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
독일	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
영국	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
이탈리아	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
일본	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
대한민국	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
멕시코	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp

노르웨이	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
폴란드	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
포르투갈	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
스페인	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
스웨덴	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
터키	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
미국	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection 사용자 설명서

국가	McAfee 사용자 설명서
오스트레일리아	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
브라질	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
캐나다(영어)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
캐나다(프랑스어)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
중국어(chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
중국어(tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
체코	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
덴마크	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
핀란드	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
프랑스	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
독일	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
영국	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf

네덜란드	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
이탈리아	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
일본	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
대한민국	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
멕시코	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
노르웨이	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
폴란드	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
포르투갈	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
스페인	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
스웨덴	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
터키	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
미국	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security 사용자 설명서

국가	McAfee 사용자 설명서
오스트레일리아	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
브라질	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
캐나다(영어)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
캐나다(프랑스어)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
중국어(chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
중국어(tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf

체코	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
덴마크	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
핀란드	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
프랑스	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
독일	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
영국	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
네덜란드	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
이탈리아	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
일본	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
대한민국	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
멕시코	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
노르웨이	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
폴란드	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
포르투갈	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
스페인	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
스웨덴	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
터키	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
미국	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus 사용자 설명서

국가	McAfee 사용자 설명서
오스트레일리아	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf

브라질	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
캐나다(영어)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
캐나다(프랑스어)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
중국어(chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
중국어(tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
체코	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
덴마크	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
핀란드	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
프랑스	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
독일	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
영국	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
네덜란드	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
이탈리아	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
일본	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
대한민국	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
멕시코	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
노르웨이	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
폴란드	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
포르투갈	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
스페인	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
스웨덴	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf

터키	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
미국	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan 사용자 설명서

국가	McAfee 사용자 설명서
오스트레일리아	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
브라질	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
캐나다(영어)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
캐나다(프랑스어)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
중국어(chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
중국어(tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
체코	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
덴마크	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
핀란드	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
프랑스	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
독일	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
영국	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
네덜란드	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
이탈리아	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
일본	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
대한민국	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
멕시코	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf

노르웨이	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
폴란드	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
포르투갈	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
스페인	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
스웨덴	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
터키	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
미국	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

해당 국가의 McAfee Threat Center 및 바이러스 정보 사이트에 대해서는 다음 표를 참조하십시오.

국가	Security HQ	바이러스 정보
오스트레일리아	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
브라질	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
캐나다(영어)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
캐나다(프랑스어)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
중국어(chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
중국어(tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
체코	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
덴마크	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
핀란드	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
프랑스	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo

독일	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
영국	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
네덜란드	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
이탈리아	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
일본	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
대한민국	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
멕시코	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
노르웨이	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
폴란드	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
포르투갈	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
스페인	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
스웨덴	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
터키	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
미국	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

해당 국가의 HackerWatch 사이트에 대해서는 다음 표를 참조하십시오.

국가	HackerWatch
오스트레일리아	www.hackerwatch.org
브라질	www.hackerwatch.org/?lang=pt-br
캐나다(영어)	www.hackerwatch.org
캐나다(프랑스어)	www.hackerwatch.org/?lang=fr-ca
중국어(chn)	www.hackerwatch.org/?lang=zh-cn
중국어(tw)	www.hackerwatch.org/?lang=zh-tw

체코	www.hackerwatch.org/?lang=cs
덴마크	www.hackerwatch.org/?lang=da
핀란드	www.hackerwatch.org/?lang=fi
프랑스	www.hackerwatch.org/?lang=fr
독일	www.hackerwatch.org/?lang=de
영국	www.hackerwatch.org
네덜란드	www.hackerwatch.org/?lang=nl
이탈리아	www.hackerwatch.org/?lang=it
일본	www.hackerwatch.org/?lang=jp
대한민국	www.hackerwatch.org/?lang=ko
멕시코	www.hackerwatch.org/?lang=es-mx
노르웨이	www.hackerwatch.org/?lang=no
폴란드	www.hackerwatch.org/?lang=pl
포르투갈	www.hackerwatch.org/?lang=pt-pt
스페인	www.hackerwatch.org/?lang=es
스웨덴	www.hackerwatch.org/?lang=sv
터키	www.hackerwatch.org/?lang=tr
미국	www.hackerwatch.org

색인

ㅁ

ㅂ

ㅃ

ㅅ

ㅇ

P

Q

R

S

T

U

V

W