



## **Symantec<sup>™</sup> Endpoint Protection 14.3 릴리스 정보**

마지막 업데이트: **2020년 6월**

## Table of Contents

저작권 정보.....	3
<b>Symantec Endpoint Protection 14.3의 새로운 기능.....</b>	<b>4</b>
알려진 문제 및 해결 방법.....	6
<b>Symantec Endpoint Protection(SEP)에 대한 시스템 요구 사항.....</b>	<b>10</b>
<b>Symantec Endpoint Protection 14.x 최신 버전에 대한 지원되는 업그레이드 경로.....</b>	<b>17</b>
추가 정보.....	19

---

## 저작권 정보

---

Broadcom, 펄스 로고, Connecting Everything 및 Symantec은 Broadcom의 상표입니다.

용어 “Broadcom”은 Broadcom Inc. 및/또는 그 자회사를 나타냅니다. 자세한 내용은 [www.broadcom.com](http://www.broadcom.com)(영문)에서 확인하십시오.

Broadcom은 신뢰성, 기능 또는 디자인을 개선하기 위한 목적으로 추가 통지 없이 해당 문서의 모든 제품 또는 데이터를 변경할 수 있는 권한이 있습니다. Broadcom에서 제공한 정보는 정확하고 신뢰할 수 있는 정보로 간주합니다. 그러나 Broadcom은 해당 정보의 적용 또는 사용으로 인해 발생하거나 해당 문서에 설명된 제품 또는 회로의 적용 또는 사용으로 인해 발생하는 문제에 대해 어떠한 책임도 지지 않으며, 해당 특허 권한 또는 타사 권한을 이용하여 라이선스를 부여하지 않습니다.

# Symantec Endpoint Protection 14.3의 새로운 기능

이 섹션에서는 14.3 릴리스의 새로운 기능을 설명합니다.

## 보호 기능

- 타사 응용 프로그램 개발자는 동적 스크립트 기반 멀웨어와 전통적인 방식을 따르지 않는 사이버 공격으로부터 고객을 보호할 수 있습니다. 타사 응용 프로그램은 Windows AMSI 인터페이스를 호출하여 Symantec Endpoint Protection 클라이언트로 라우팅되는 사용자 제공 스크립트의 검사를 요청합니다. 클라이언트는 응답으로 스크립트 동작이 악의적인지 여부를 나타내는 판정을 보냅니다. 동작이 악의적이지 않으면 스크립트 실행이 진행됩니다. 스크립트의 동작이 악의적이면 응용 프로그램이 해당 스크립트를 실행하지 않습니다. 클라이언트에서는 탐지 결과 대화 상자에 "액세스 거부됨" 상태가 표시됩니다. 타사 스크립트의 예로는 Windows PowerShell, JavaScript 및 VBScript가 있습니다. 자동 보호를 실행해야 합니다. 이 기능은 Windows 10 이상의 시스템에서 작동합니다.

[How the Antimalware Scan Interface \(AMSI\) helps you defend against malware\(영문\)](#)

[Antimalware Scan Interface \(AMSI\)\(영문\)](#)

## Symantec Endpoint Protection Manager

- Symantec Endpoint Protection 원격 콘솔은 이제 Java 8 대신 Java 11을 지원합니다. 원격 콘솔에 액세스하려면 지원되는 웹 브라우저를 연 다음 주소 상자에 `http://SEPMServer:9090/symantec.html`을 입력하고 새 원격 콘솔 패키지를 다운로드하십시오. 표시되는 지침을 따르십시오. 이전 버전의 Symantec Endpoint Protection Manager 원격 콘솔은 더 이상 지원되지 않습니다.

[Symantec Endpoint Protection 로그인](#)

- 사이트의 Symantec Endpoint Protection Manager 중 하나를 마스터 로그 서버로 구성하여 syslog 서버로 로그를 전달할 수 있습니다. 마스터 로그 서버가 오프라인 상태가 되면 두 번째 관리 서버가 해당 역할을 이어받아 syslog 서버로 로그를 전달합니다. 마스터 로그 서버가 다시 온라인 상태가 되면 이 서버가 로그 전달을 재개합니다.

[외부 로그를 위한 장애 조치 서버 구성](#)

- 통합 정책에는 WSS 트래픽 리디렉션을 위해 LPS 사용자 정의 PAC 파일 실행이라는 새로운 옵션이 포함되었습니다. 이 옵션을 사용하면 클라이언트의 LPS 서버에서 호스팅하는 기본 PAC 파일을 사용자 정의 PAC 파일로 대체할 수 있습니다. 사용자 정의 PAC 파일은 타사 응용 프로그램이 루프백 어댑터에서 수신 대기하는 로컬 프록시 서버와 연동되지 않는 호환성 문제를 해결합니다.

[WSS 트래픽 리디렉션 구성](#)

- Microsoft SQL Server 2019 데이터베이스가 지원됩니다.
- 이제 바이러스 차단 검사 프로세스는 기본 비보안 서비스와는 별도의 서비스를 사용합니다. 이 새로운 검사 프로세스는 메모리 사용을 보다 효율화하고, 지속적 보호를 보장하며, 기본 서비스의 문제에 대한 종속성을 줄입니다.
- 데이터베이스 스키마에 향후 릴리스를 위한 기능의 일부로 새 열이 포함되었습니다. (AGENT\_SECURITY\_LOG\_1, AGENT\_SECURITY\_LOG\_2, SEM\_AGENT 테이블)
- Rest API의 /sepm/api/v1/computer API 응답 JSON에 시스템 상태 리포트를 호출하고 다운로드하기 위한 quarantineStatus, quarantineCode, wssStatus, pskVersion 필드가 포함되었습니다.
- Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite 등의 타사 구성 요소가 최신 버전으로 업그레이드되었습니다.
- 클라우드 콘솔에 Symantec Endpoint Protection Manager 도메인을 등록하려면 먼저 Symantec Endpoint Security 콘솔을 통해 등록 토큰을 받아야 합니다. 이전에는 클라우드 페이지에서 시작을 눌러 등록 토큰을 받았습니다.

## 클라이언트 및 플랫폼 업데이트

- Windows 클라이언트는 Windows 10 20H1(Windows 10 버전 2004)을 지원합니다.
- Linux 클라이언트는 이제 Ubuntu 18.04, RHEL 8 및 CentOS 8를 지원합니다.
- AppRemover 도구가 최신 버전으로 업데이트되었습니다. AppRemover 도구는 Windows 클라이언트를 설치하기 전에 타사 응용 프로그램을 제거합니다. 제거되는 응용 프로그램에 대한 자세한 내용은 [Third-party security software removal in Endpoint Protection 14.3\(영문\)](#)를 참조하십시오.

#### 제거된 기능

- 위험 요소 확산, 단일 위험 요소 이벤트 및 새 위험 요소 탐지 통지에 위험 요소 심각도 및 위험 요소 유형 필드가 더 이상 표시되지 않습니다.

[What's new in all releases of Symantec Endpoint Protection\(영문\)](#)

## 알려진 문제 및 해결 방법

이 섹션의 항목은 이 릴리스의 Symantec Endpoint Protection에 적용됩니다.

**Table 1:** 업그레이드 문제

문제	설명 및 해결책
FIPS 모드가 실행되는 경우 SQL Server가 버전 2017에서 버전 2019로 업그레이드되지 않음 [14.3]	<p>이 경우 "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms."과 같은 오류가 표시될 수 있습니다. 이 문제는 FIPS 실행 Symantec Endpoint Protection Manager 14.3을 사용하는 경우 Microsoft SQL Server 2017에서 2019로 업그레이드하면 발생합니다. [SEP-61473]</p> <p>이 문제를 해결하려면 운영 체제 수준에서 FIPS를 실행 중지하십시오.</p> <ol style="list-style-type: none"> <li>1. C:\ProgramData\Microsoft\Windows\##\##\####\##\##에서 로컬 보안 정책 &gt; 로컬 정책 &gt; 보안 옵션을 누르고 시스템 암호화: 암호화, 해시, 서명에 <b>FIPS</b> 규격 알고리즘 사용을 실행 중지하십시오.</li> <li>2. SQL Server 버전 2017에서 버전 2019로 업그레이드하십시오.</li> <li>3. SQL Server가 성공적으로 업그레이드된 후 FIPS를 다시 실행하십시오.</li> </ol> <p><a href="#">SQL upgrade from 2017 to 2019 fails with FIPS mode enabled(영문)</a></p>
사용자 정의 이름으로 인해 14.2 이상으로 업그레이드 중 방화벽 정책이 업데이트되지 못할 수 있음	<p>일부 기본 이름을 변경한 경우 Symantec Endpoint Protection 14.2 이상으로 업그레이드할 때 방화벽 정책이 IPv6 변경 사항을 통합하지 못합니다. 기본 이름에는 기본 정책의 이름과 기본 규칙 이름이 포함됩니다. 업그레이드 중 규칙을 업데이트할 수 없는 경우 IPv6 옵션이 나타나지 않습니다. 업그레이드 후에 생성하는 모든 새 정책 또는 규칙은 영향을 받지 않습니다. 가능하면 변경된 모든 이름을 기본 이름으로 되돌리십시오. 그렇지 않으면 기본 정책에 추가한 사용자 정의 규칙이 IPv6 통신을 어떤 방식으로든 차단하지 않는지 확인하십시오. 추가하는 모든 새 정책 또는 규칙에 대해 동일하게 확인하십시오.</p>

Table 2: Symantec Endpoint Protection Manager 문제

문제	설명 및 해결책
하이브리드 관리 옵션과 프록시 서버를 사용하는 경우 Symantec Endpoint Security에서 추가 URL을 허용 목록에 추가 [14.2.2.1 이상]	<p>최근 Broadcom이 Symantec Enterprise Security를 인수하면서 14.2.2.1에서 클라이언트 간 통신용 URL이 변경되었습니다. [CDM-42467]</p> <p>다음과 같은 경우 클라이언트를 버전 빌드 14.2.5569.2100 이상으로 업그레이드해야 합니다.</p> <ul style="list-style-type: none"> <li>온-프레미스 Symantec Endpoint Protection Manager 도메인이 클라우드 콘솔에 등록되어 있을 때 Symantec Endpoint Security를 사용하여 클라이언트 및 정책을 관리합니다.</li> <li>프록시 서버를 사용합니다.</li> </ul> <p>클라우드 단독 관리 또는 하이브리드 관리 에이전트에서 URL을 허용 목록에 추가하려면 Symantec Endpoint Security에서 URL을 허용 목록에 추가해야 합니다.</p> <ol style="list-style-type: none"> <li>Symantec Endpoint Security에서 엔드포인트(<b>Endpoint</b>) &gt; 정책(<b>Policies</b>) &gt; [policy name] 허용 목록 정책([policy name] <b>Whitelist Policy</b>)으로 이동합니다.</li> <li>허용 목록 정책에서 도메인별 제외(<b>Excluded by Domain</b>) 옆의 추가(<b>Add</b>)를 선택하고 다음 URL을 한 번에 하나씩 추가한 다음 추가(<b>Add</b>)를 선택하십시오. us.spoc.securitycloud.symantec.com eu.spoc.securitycloud.symantec.com(유럽에 장치가 있는 경우 추가) 이후 버전으로 클라이언트를 계속 관리하려는 경우 spoc.norton.com은 그대로 유지하십시오.</li> <li>정책 저장(<b>Save Policy</b>)을 선택한 다음 Yes(예)를 선택하여 정책을 업데이트하고 기존 그룹에 적용하십시오.</li> </ol> <p><a href="#">URLs to whitelist for Symantec Endpoint Security(영문)</a>를 참조하십시오. <a href="#">Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1 or later by May 4, 2020(영문)</a>를 참조하십시오.</p>
Symantec Endpoint Protection Manager 원격 콘솔이 더 이상 32비트 Windows 플랫폼을 지원하지 않음 [14.3]	<p>14.3부터는 32비트 버전의 Windows를 실행하는 경우 Symantec Endpoint Protection Manager 원격 콘솔에 로그인할 수 없습니다. Oracle Java SE Runtime Environment는 더 이상 32비트 버전의 Microsoft Windows를 지원하지 않습니다. [SEP-61106]</p> <p>다음과 같은 메시지가 표시되면 Symantec Endpoint Protection Manager에 로컬로 로그인하십시오.</p> <p>"이 버전의 C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe는 현재 실행 중인 Windows 버전과 호환되지 않습니다. 컴퓨터의 시스템 정보를 확인한 다음 소프트웨어 게시자에게 문의하십시오."</p> <p><a href="#">Symantec Endpoint Protection Manager 로그인</a></p>
Symantec Endpoint Protection Manager 설치 중에 "Microsoft Visual C++ Runtime을 설치하지 못했습니다."라는 오류가 나타남 [14.3]	<p>Windows 2012 R2에 Symantec Endpoint Protection Manager를 설치하는 중에 "Microsoft 비 Visual C++ Runtime을 설치하지 못했습니다."라는 오류가 나타날 수 있습니다. [SEP-60396]</p> <p>이 문제를 해결하려면 Windows를 활성화하고 Windows 업데이트를 설치하십시오. Windows 업데이트는 Windows 2012 R2에 Symantec Endpoint Protection Manager 14.3을 설치하기 위한 필수 요건인 Visual C++ 2017 재배포 가능 패키지를 설치합니다.</p>
Windows에서 TLS 1.1 및 TLS 1.2를 WinHTTP의 기본 보안 프로토콜로 실행하기 위한 업데이트 [14.3]	<p>클라우드 콘솔에 등록된 Symantec Endpoint Protection Manager 버전 14.3으로 업그레이드하거나 이를 설치한 후에 관리 서버가 더 이상 클라우드에 로그를 성공적으로 업로드하지 못합니다. uploader.log에는 다음과 같은 오류가 표시될 수 있습니다.</p> <pre>&lt;SEVERE&gt; WinHttpRequest: 12175: A security error occurred</pre> <p>이 문제는 TLS 1.1 및 1.2에 대한 지원을 제공하는 Microsoft 업데이트가 누락되었기 때문에 발생합니다.</p> <p>문제를 해결하려면 Microsoft 업데이트 KB3140245를 설치하십시오. 자세한 내용은 다음을 참조하십시오.</p> <p><a href="#">Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows(영문)</a></p>

문제	설명 및 해결책
클라이언트가 Endpoint Threat Defense for AD에 대한 업데이트된 정책을 수신한 후에도 Symantec Endpoint Protection Manager에 계속 "배포 중"으로 나타남 [14.2 RU1 MP1 이상]	이는 예상된 동작입니다. Endpoint Threat Defense for AD 3.3 정책은 버전 14.2 RU1 MP1 이후의 클라이언트에서만 지원됩니다. Symantec Endpoint Threat Defense for Active Directory 3.3에 대한 정책을 그룹에 적용하십시오. 이 그룹에는 Symantec Endpoint Protection 14.2 RU1 이하를 실행하는 일부 클라이언트가 포함됩니다. 이러한 클라이언트는 정상적으로 정책을 수신하고 적용하지만 Symantec Endpoint Protection Manager에서는 상태가 계속 배포 중이라는 메시지로 표시됩니다.

Table 3: Windows, Mac 및 Linux 클라이언트 문제

문제	설명 및 해결책
HA-2 지원을 처음 설치하는 경우가 아니면 Symantec Endpoint Protection 14.3 Windows 클라이언트 설치가 실패할 수 있음 [14.3]	기존 운영 체제 버전(Windows 7 RTM/SP1, Windows Server 2008 R2/R2 SP1/R2 SP2)을 실행하는 경우 2019년 7월 이후에 릴리스된 Windows 업데이트를 설치하려면 장치에 SHA-2 코드 서명 지원이 설치되어 있어야 합니다. SHA-2 지원이 없으면 Windows 클라이언트 설치가 실패할 수 있습니다. 클라이언트를 처음 설치하던 이전 릴리스에서 자동으로 업그레이드하던 관계없이 설치가 실패할 수 있습니다. [SEP-61175/61403] Microsoft를 통해 SHA-2 코드 서명 지원을 적용하려면 다음을 참조하십시오. <a href="#">Windows 및 WSUS의 2019 SHA-2 코드 서명 지원 요구 사항</a> <a href="#">Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed(영문)</a>
UWF가 실행되는 Windows 10 1803에 설치된 Symantec Endpoint Protection Windows 클라이언트는 실행되지 않음 [14.3]	Symantec Endpoint Protection 클라이언트가 Windows 10 RS4 1803 32비트 운영 체제에서 실행되는 경우 UWF(통합 쓰기 필터)가 실행되어 Windows 클라이언트가 설치된 드라이브를 보호하고 있으면 클라이언트가 제대로 실행되지 않습니다. 이 Windows 운영 체제에는 Windows 클라이언트가 실행되지 않도록 하는 UWF 결함이 있습니다. 이 문제를 해결하려면 다음과 같이 하십시오. <ul style="list-style-type: none"> <li>결함이 없는 다른 운영 체제 버전으로 업그레이드하십시오.</li> <li>UWF를 실행 중지하십시오. <a href="#">Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled(영문)</a>를 참조하십시오.</li> </ul>
WSS 트래픽 리디렉션을 실행하는 Mac 클라이언트가 LiveUpdate에 사용자 정의 프록시 설정을 적용하지 않음 [14.2 RU1 MP1 이상]	외부 통신 설정을 통해 Symantec Endpoint Protection 14.2 RU1 MP1용 중앙 관리 Mac 클라이언트에서 LiveUpdate에 사용자 정의 프록시 설정을 사용하도록 구성했습니다. 하지만 Symantec Endpoint Protection Manager 정책을 통해 Mac 클라이언트에 대해 WTR(WSS 트래픽 리디렉션)을 실행하면 LiveUpdate 트래픽이 더 이상 사용자 정의 프록시 설정을 적용하지 않습니다. 대신 LiveUpdate에서 직접 연결을 시도합니다. 이 문제를 해결하려면 WSS 트래픽 리디렉션을 실행 중지한 경우에만 LiveUpdate에 사용자 정의 프록시 설정을 사용하십시오.
강화가 실행된 상태에서 Microsoft Edge가 예기치 않게 PDF 다운로드를 허용함 [14.2 RU1 MP1 이상]	Symantec Endpoint Protection 클라이언트에서 응용 프로그램 강화를 실행한 상태에서 Microsoft Edge 브라우저를 사용하는 경우 예기치 않게 PDF 파일을 다운로드할 수 있습니다. 다른 브라우저에서는 PDF 파일 다운로드 차단이 예상대로 작동합니다. 이 문제는 향후 릴리스에서 수정될 예정입니다.

Broadcom은 최근 Symantec Enterprise Protection이 Broadcom에 공식적으로 합병되었다고 발표했으며 그와 동시에 시منتек 설명서는 Broadcom의 [Symantec Security Tech Docs Portal](#)로 마이그레이션되었습니다.

Endpoint Protection 설명서를 찾으려면 **Symantec Security Software** 탭을 누른 다음 **Endpoint Security and Management > Endpoint Protection**을 누르십시오.



**Table 4:** 설명서 문제

문제	설명 및 해결책
HOWTO 문서가 만료됨	Symantec Endpoint Protection Manager 도움말 항목과 중복되었던 HOWTO 문서는 <a href="#">Endpoint Protection</a> 사이트에 다시 게시되었으며 따라서 URL이 달라졌습니다. 문서를 찾으려면 검색 필드를 사용하십시오.
PDF 파일	시만텍은 모든 PDF 파일을 DOC 문서에 게시했습니다. 이러한 페이지는 만료되었습니다. PDF 파일의 최신 릴리스 버전을 찾으려면 <a href="#">관련 문서</a> 페이지로 이동하십시오. 앞으로 Broadcom은 기존 PDF 파일과 번역된 PDF 파일을 추가할 예정입니다.

해결된 문제를 확인하려면 [New fixes and components for Symantec Endpoint Protection 14.3\(영문\)](#)를 참조하십시오.

## Symantec Endpoint Protection(SEP)에 대한 시스템 요구 사항

일반적으로 다음 제품에 대한 시스템 요구 사항은 이를 지원하는 운영 체제의 요구 사항과 동일합니다.

### NOTE

이전 버전의 Symantec Endpoint Protection Manager는 이후 버전을 사용하는 클라이언트를 올바르게 관리하지 못할 수 있습니다. 콘텐츠 업데이트 및 클라이언트 관리 시 문제가 발생할 수 있습니다. 예를 들어 Symantec Endpoint Protection Manager 14.0.1 이하는 버전 14.2 클라이언트에 해당 버전에 맞는 모니터를 올바르게 제공할 수 없습니다. 14 MP2 이전 버전의 Symantec Endpoint Protection Manager는 14.0.1 이후 버전의 클라이언트에 해당 버전에 맞는 모니터를 올바르게 제공할 수 없습니다.

다음 표에서는 Symantec Endpoint Protection에 대한 소프트웨어 및 하드웨어 요구 사항을 설명합니다.

**Table 5: Symantec Endpoint Protection Manager(SEPM) 소프트웨어 시스템 요구 사항**

구성 요소	요구 사항
운영 체제	<ul style="list-style-type: none"> <li>Windows Server 2008 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2016</li> <li>Windows Server 2019</li> </ul> <p><b>Note:</b> 데스크톱 운영 체제는 지원되지 않습니다.</p> <p><b>Note:</b> Windows Server Core 버전은 지원되지 않습니다. Windows Server Core에는 Symantec Endpoint Protection Manager가 작동하는 데 필요한 Internet Explorer가 포함되어 있지 않습니다.</p>
웹 브라우저	<p>다음과 같은 브라우저가 Symantec Endpoint Protection Manager 웹 콘솔 액세스와 Symantec Endpoint Protection Manager 도움말 보기를 지원합니다.</p> <ul style="list-style-type: none"> <li>Microsoft Edge 참고: 32비트 버전의 Windows 10은 Edge 브라우저를 사용한 웹 콘솔 액세스를 지원하지 않습니다.</li> <li>Microsoft Internet Explorer 11</li> <li>Mozilla Firefox 5.x ~ 68.x</li> <li>Google Chrome 75.x</li> </ul>

구성 요소	요구 사항
데이터베이스	<p><b>Symantec Endpoint Protection Manager</b>에는 내장 데이터베이스가 포함되어 있습니다. 대신 다음 <b>Microsoft SQL Server</b> 버전의 데이터베이스 중 하나를 사용하도록 선택할 수도 있습니다.</p> <ul style="list-style-type: none"> <li>• SQL Server 2008, SP4</li> <li>• SQL Server 2008 R2, SP3</li> <li>• SQL Server 2012, RTM - SP4</li> <li>• SQL Server 2014, RTM - SP3</li> <li>• SQL Server 2016, RTM, SP1, SP2</li> <li>• SQL Server 2017, RTM</li> <li>• SQL Server 2019, RTM(14.3부터)</li> </ul> <p><b>Note:</b> SQL Server Express Edition 데이터베이스는 지원되지 않습니다. Amazon RDS에서 호스팅되는 SQL Server 데이터베이스는 지원됩니다(14.0.1 MP2부터).</p> <p><b>Note:</b> Symantec Endpoint Protection에서 SQL Server 데이터베이스를 사용하고 환경에서 TLS 1.2만 사용하는 경우 SQL Server가 TLS 1.2를 지원하는지 확인하십시오. SQL Server에 패치를 적용해야 할 수 있습니다. 이 권장 사항은 SQL Server 2008, 2012 및 2014에 적용됩니다. TLS 1.2를 지원하는 SQL Server 패치가 없으면 Symantec Endpoint Protection 12.1에서 14로 업그레이드할 때 문제가 발생할 수 있습니다.</p> <p><b>Note:</b> <a href="#">TLS 1.2 support for Microsoft SQL Server(영문)</a></p>
기타 환경 요구 사항	순수 IPv6 네트워크에서는 IPv4 스택이 계속 설치되고 실행 중지되어야 합니다. IPv4 스택이 설치되지 않으면 Symantec Endpoint Protection Manager이(가) 작동하지 않습니다.

**Table 6: Symantec Endpoint Protection Manager 하드웨어 시스템 요구 사항**

구성 요소	요구 사항
프로세서	Intel Pentium Dual-Core 또는 동급 이상, 8-Core 이상 권장 <b>Note:</b> Intel Itanium IA-64 프로세서는 지원되지 않습니다.
실제 RAM	최소 2GB RAM, 8 GB 이상 권장 <b>Note:</b> 이미 설치된 기타 응용 프로그램의 RAM 요구 사항에 따라 Symantec Endpoint Protection Manager 서버에서 추가 RAM을 필요로 할 수 있습니다. 예를 들어 Symantec Endpoint Protection Manager 서버에 Microsoft SQL Server가 설치되어 있는 경우 서버에는 최소 8GB가 필요합니다.
디스플레이	1024 x 768 이상
시스템 드라이브에 설치 시 하드 드라이브	내장 데이터베이스 또는 로컬 <b>SQL Server</b> 데이터 베이스와 함께 <ul style="list-style-type: none"> <li>• 관리 서버 및 데이터베이스의 경우 최소 40GB(200GB 권장)</li> </ul> 원격 <b>SQL Server</b> 데이터베이스와 함께 <ul style="list-style-type: none"> <li>• 관리 서버의 경우 최소 40GB(100GB 권장)</li> <li>• 데이터베이스에 대해 원격 서버에서 추가 사용 가능 디스크 공간</li> </ul>
대체 드라이브에 설치 시 하드 드라이브	내장 데이터베이스 또는 로컬 <b>SQL Server</b> 데이터 베이스와 함께 <ul style="list-style-type: none"> <li>• 시스템 드라이브에 최소 15GB 필요(100GB 권장)</li> <li>• 설치 드라이브에 최소 25GB 필요(100GB 권장)</li> </ul> 원격 <b>SQL Server</b> 데이터베이스와 함께 <ul style="list-style-type: none"> <li>• 시스템 드라이브에 최소 15GB 필요(100GB 권장)</li> <li>• 설치 드라이브에 최소 25GB 필요(100GB 권장)</li> <li>• 데이터베이스에 대해 원격 서버에서 추가 사용 가능 디스크 공간</li> </ul>

SQL Server 데이터베이스를 사용하는 경우 사용할 수 있는 디스크 공간을 더 만들어야 할 수 있습니다. 추가 공간의 양과 위치는 SQL Server에서 사용하는 드라이브, 데이터베이스 유지 관리 요구 사항 및 다른 데이터베이스 설정에 따라 다릅니다.

**Table 7: Windows용 Symantec Endpoint Protection 클라이언트 소프트웨어 시스템 요구 사항**

구성 요소	요구 사항
운영 체제(데스크톱)	<ul style="list-style-type: none"> <li>Windows 7(32비트/64비트, RTM 및 SP1)</li> <li>Windows Embedded 7 Standard, POSReady 및 Enterprise(32비트 및 64비트)</li> <li>Windows 8(32비트, 64비트)</li> <li>Windows Embedded 8 Standard(32비트 및 64비트)</li> <li>Windows 8.1(32비트, 64비트), Windows To Go 포함</li> <li>2014년 4월 Windows 8.1 업데이트(32비트, 64비트)</li> <li>2014년 8월 Windows 8.1 업데이트(32비트, 64비트)</li> <li>Windows Embedded 8.1 Pro, Industry Pro 및 Industry Enterprise(32비트 및 64비트)</li> <li>Windows 10(버전 1507)(32비트, 64비트), Windows 10 Enterprise 2015 LTSC 포함</li> <li>Windows 10 11월 업데이트(버전 1511)(32비트, 64비트)</li> <li>Windows 10 1주년 업데이트(버전 1607)(32비트, 64비트), Windows 10 Enterprise 2016 LTSC 포함</li> <li>Windows 10 크리에이터스 업데이트(버전 1703)(32비트, 64비트)</li> <li>Windows 10 Fall Creators Update(버전 1709)(32비트, 64비트)</li> <li>Windows 10 2018년 4월 업데이트(버전 1803)(32비트, 64비트)</li> <li>Windows 10 2018년 10월 업데이트(버전 1809)(32비트, 64비트), Windows 10 Enterprise 2019 LTSC 포함</li> <li>Windows 10 2019년 5월 업데이트(버전 1903)(32비트, 64비트)</li> <li>Windows 10 2019년 11월 업데이트(버전 1909)(32비트, 64비트)(14.2 RU1 이상)</li> <li>Windows 10 20H1(Windows 10 버전 2004)(14.3부터)</li> </ul>
운영 체제(서버)	<ul style="list-style-type: none"> <li>Windows Server 2008 R2</li> <li>Windows Small Business Server 2011</li> <li>Windows Server 2012</li> <li>Windows Server 2012 R2</li> <li>2014년 4월 Windows Server 2012 R2 업데이트</li> <li>2014년 8월 Windows Server 2012 R2 업데이트</li> <li>Windows Server 2016</li> <li>Windows Server 2019</li> <li>Windows Server 버전 1803(Server Core)(14.2 이상)</li> <li>Windows Server 버전 1809(Server Core)</li> <li>Windows Server 버전 1903(Server Core)(14.2 RU1 이상)</li> <li>Windows Server 버전 1909(Server Core)(14.2 RU1 이상)</li> </ul>
브라우저 침입 차단	<p>브라우저 침입 차단에 대한 지원은 클라이언트 침입 탐지 시스템(CIDS) 엔진의 버전을 기준으로 결정됩니다.</p> <p><a href="#">Supported browsers for Browser Intrusion Prevention in Endpoint Protection(영문)</a>을 참조하십시오.</p>

**Table 8: Windows용 Symantec Endpoint Protection 클라이언트 하드웨어 시스템 요구 사항**

구성 요소	요구 사항
프로세서(실제 시스템용)	<ul style="list-style-type: none"> <li>2비트 프로세서: 4GHz Intel Pentium 4 또는 동급 이상(Intel Pentium 4 또는 동급 권장)</li> <li>64비트 프로세서: x86-64 지원 2GHz Pentium 4 또는 동급 이상</li> </ul> <p><b>Note:</b> Itanium 프로세서는 지원되지 않습니다.</p>
프로세서(가상 시스템용)	<p>최소 1GHz에서 가상 소켓 1개와 소켓당 1개의 코어(2GHz에서 가상 소켓 1개와 소켓당 2개의 코어 권장)</p> <p><b>Note:</b> 하이퍼바이저 리소스 예약을 실행해야 합니다.</p>
실제 RAM	1GB, 운영 체제에서 필요한 경우 그 이상(2GB 권장)

구성 요소	요구 사항
디스플레이	800 x 600 이상
하드 드라이브	<p>디스크 공간 요구 사항은 설치하는 클라이언트 유형, 설치할 드라이브 및 프로그램 데이터 파일이 저장될 위치에 따라 다릅니다. 프로그램 데이터 폴더는 일반적으로 시스템 드라이브 기본 위치 C:\ProgramData에 있습니다.</p> <p>선택하는 설치 드라이브 위치에 관계 없이 항상 시스템 드라이브에 사용 가능한 디스크 공간이 필요합니다.</p> <p>하드 드라이브 시스템 요구 사항</p> <ul style="list-style-type: none"> <li>• <a href="#">시스템 드라이브에 설치되었을 때 Windows용 Symantec Endpoint Protection 클라이언트에 사용할 수 있는 하드 드라이브 시스템 요구 사항</a>에서는 대체 드라이브에 Symantec Endpoint Protection가 설치되었을 때의 하드 드라이브 시스템 요구 사항을 설명합니다.</li> <li>• <a href="#">대체 드라이브에 설치되었을 때 Windows용 Symantec Endpoint Protection 클라이언트에 사용할 수 있는 하드 드라이브 시스템 요구 사항</a>에서는 대체 드라이브에 Symantec Endpoint Protection가 설치되었을 때의 하드 드라이브 시스템 요구 사항을 설명합니다.</li> </ul> <p><b>Note:</b> 공간 요구 사항은 NTFS 파일 시스템을 기준으로 합니다. 추가 공간은 콘텐츠 업데이트 및 로그에도 필요합니다.</p>

**Table 9:** 시스템 드라이브에 설치되었을 때 **Windows용 Symantec Endpoint Protection** 클라이언트에 사용할 수 있는 하드 드라이브 시스템 요구 사항

클라이언트 유형	요구 사항
Standard	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 395MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더 포함:</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 180MB</li> <li>• 대체 설치 드라이브: 350MB</li> </ul>
Embedded/VDI	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 245MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더 포함:</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 180MB</li> <li>• 대체 설치 드라이브: 200MB</li> </ul>
다크 네트워크	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 545MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더 포함:</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 180MB</li> <li>• 대체 설치 드라이브: 500MB</li> </ul>

\* 설치하는 동안 추가 135MB가 필요합니다.

**Table 10: 대체 드라이브에 설치되었을 때 Windows용 Symantec Endpoint Protection 클라이언트에 사용할 수 있는 하드 드라이브 시스템 요구 사항**

클라이언트 유형	요구 사항
Standard	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 380MB</li> <li>• 대체 설치 드라이브: 15MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 30MB</li> <li>• 프로그램 데이터 드라이브: 350MB</li> <li>• 대체 설치 드라이브: 150MB</li> </ul>
Embedded/VDI	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 230MB</li> <li>• 대체 설치 드라이브: 15MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 30MB</li> <li>• 프로그램 데이터 드라이브: 200MB</li> <li>• 대체 설치 드라이브: 150MB</li> </ul>
다크 네트워크	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 530MB</li> <li>• 대체 설치 드라이브: 15MB*</li> </ul> <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브: 30MB</li> <li>• 프로그램 데이터 드라이브: 500MB</li> <li>• 대체 설치 드라이브: 150MB</li> </ul>

\* 설치하는 동안 추가 135MB가 필요합니다.

\*\* 프로그램 데이터 폴더가 대체 설치 드라이브와 동일한 경우 총 용량에 대해 프로그램 데이터 드라이브에 15MB를 추가하십시오. 그러나 설치하는 동안 대체 설치 드라이브에는 설치 프로그램에서 사용할 수 있는 전체 150MB가 여전히 필요합니다.

**Table 11: Windows Embedded용 Symantec Endpoint Protection 클라이언트 시스템 요구 사항**

구성 요소	요구 사항
프로세서	1GHz Intel Pentium
실제 RAM	256MB <b>Note:</b> 이 수치는 Symantec Endpoint Protection 내장 클라이언트의 설치를 위한 것입니다. EDR 같은 통합 솔루션에서 추가 기능도 구현하는 경우 추가적인 물리적 RAM이 필요합니다.
하드 드라이브	<p>Symantec Endpoint Protection Embedded/VDI 클라이언트에는 다음 사용할 수 있는 하드 디스크 공간이 필요합니다.</p> <ul style="list-style-type: none"> <li>• 시스템 드라이브에 설치됨: 245MB</li> <li>• 대체 드라이브에 설치됨: 시스템에 230MB 및 대체 드라이브에 15MB</li> </ul> <p>설치하는 동안 추가 135MB가 필요합니다.</p> <p>이 그림에서는 프로그램 데이터 폴더가 시스템 드라이브에 있다고 가정합니다. 자세한 내용 또는 다른 클라이언트 유형의 요구 사항은 Windows용 Symantec Endpoint Protection 클라이언트 시스템 요구 사항을 참조하십시오.</p>

구성 요소	요구 사항
Embedded 운영 체제	<ul style="list-style-type: none"> <li>Windows Embedded Standard 7(32비트 및 64비트)</li> <li>Windows Embedded POSReady 7(32비트 및 64비트)</li> <li>Windows Embedded Enterprise 7(32비트 및 64비트)</li> <li>Windows Embedded 8 Standard(32비트 및 64비트)</li> <li>Windows Embedded 8.1 Industry Pro(32비트 및 64비트)</li> <li>Windows Embedded 8.1 Industry Enterprise(32비트 및 64비트)</li> <li>Windows Embedded 8.1 Pro(32비트 및 64비트)</li> </ul>
최소 필수 구성 요소	<ul style="list-style-type: none"> <li>필터 관리자(FitMgr.sys)</li> <li>성능 데이터 도우미(pdh.dll)</li> <li>Windows Installer 서비스</li> </ul>
템플릿	<ul style="list-style-type: none"> <li>응용 프로그램 호환성(기본값)</li> <li>디지털 서명</li> <li>산업 자동화</li> <li>IE, Media Player, RDP</li> <li>셋톱박스</li> <li>씬(Thin) 클라이언트</li> </ul> <p>최소 구성 템플릿은 지원되지 않습니다. EWF(강화된 쓰기 필터) 및 UWF(통합 쓰기 필터)는 지원되지 않습니다. 권장 쓰기 필터는 레지스트리 필터와 함께 설치되는 FBWF(파일 기반 쓰기 필터)입니다.</p>

Table 12: Mac용 Symantec Endpoint Protection 클라이언트 시스템 요구 사항

구성 요소	요구 사항
프로세서	64비트 Intel Core 2 Duo 이상
실제 RAM	2 GB RAM
하드 드라이브	설치를 위한 500MB의 하드 디스크 여유 공간
디스플레이	800 x 600
운영 체제	<ul style="list-style-type: none"> <li>macOS 10.13</li> <li>macOS 10.14</li> <li>macOS 10.15 ~ 10.15.5</li> </ul> <p>macOS 10.14.5 이상은 kext 공중 요구 사항을 지원합니다. 자세한 내용은 <a href="#">Endpoint Protection 14.2 RU1 and kext notarization for macOS 10.14.5(영문)</a>를 참조하십시오. 이전 릴리스의 지원되는 운영 체제 목록은 <a href="#">Mac compatibility with the Endpoint Protection client(영문)</a>를 참조하십시오.</p>

**Table 13: Linux용 Symantec Endpoint Protection 클라이언트 시스템 요구 사항**

구성 요소	요구 사항
하드웨어	<ul style="list-style-type: none"> <li>Intel Pentium 4(2GHz) 이상 프로세서</li> <li>1GB RAM</li> <li>7GB의 하드 디스크 여유 공간</li> </ul>
운영 체제	<ul style="list-style-type: none"> <li>Amazon Linux</li> <li>CentOS 6U3 ~ 6U9, 7 ~ 7U7, 8 - 32비트 및 64비트</li> <li>Debian 6.0.5 Squeeze, Debian 8 Jessie - 32비트 및 64비트</li> <li>Fedora 16, 17 - 32비트 및 64비트</li> <li>Oracle Linux(OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4</li> <li>Red Hat Enterprise Linux 서버(RHEL) 6U2 ~ 6U9, 7 ~ 7U8, 8 ~ 8U2</li> <li>SUSE Linux Enterprise Server(SLES) 11 SP1~11 SP4(32비트 및 64비트), 12, 12 SP1~12 SP3(64비트)</li> <li>SUSE Linux Enterprise Desktop(SLED) 11 SP1~11 SP4(32비트 및 64비트), 12 SP3(64비트)</li> <li>Ubuntu 12.04, 14.04, 16.04, 18.04(14.3부터) - 32비트 및 64비트</li> </ul> <p>이전 릴리스의 지원되는 운영 체제 커널 목록은 <a href="#">Supported Linux kernels for Symantec Endpoint Protection(영문)</a>을 참조하십시오.</p>
그래픽 데스크톱 환경	<p>다음 그래픽 데스크톱 환경을 사용하여 Linux 클라이언트용 Symantec Endpoint Protection을(를) 볼 수 있습니다.</p> <ul style="list-style-type: none"> <li>KDE</li> <li>Gnome</li> <li>Unity</li> </ul>
기타 환경 요구 사항	<ul style="list-style-type: none"> <li>Glibc glibc 2.6 이하를 실행하는 모든 운영 체제는 지원되지 않습니다.</li> <li>64비트 시스템의 i686 기반 종속 패키지 다수의 Linux 클라이언트 실행 파일은 32비트 프로그램입니다. 64비트 시스템인 경우에는 Linux 클라이언트를 설치하기 전에 i686 기반 종속 패키지를 설치해야 합니다. i686 기반 종속 패키지가 아직 설치되지 않았다면 명령줄을 이용해 설치하실 수 있습니다. 이 설치에는 superuser 권한이 필요하며 다음 명령에서 sudo로 표시됩니다. <ul style="list-style-type: none"> <li>Red Hat 기반 배포의 경우: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code></li> <li>Debian 기반 배포의 경우: <code>sudo apt-get install ia32-libs</code></li> <li>Ubuntu 기반 배포의 경우: <ul style="list-style-type: none"> <li><code>sudo dpkg --add-architecture i386</code></li> <li><code>sudo apt-get update</code></li> <li><code>sudo apt-get install gcc-multilib libx11-6:i386</code></li> </ul> </li> </ul> </li> <li>net-tools 또는 iproute2 Symantec Endpoint Protection에서는 시스템에 이미 설치되어 있는 도구에 따라 이 두 도구 중 하나를 사용합니다.</li> <li>개발자 도구 자동 보호 커널 모듈에 대한 프로세스를 자동 컴파일 및 수동 컴파일하려면 특정 개발자 도구를 설치해야 합니다. 이러한 개발자 도구에는 gcc 및 커널 소스 및 헤더 파일이 포함됩니다. 특정 Linux 버전 전에 대한 설치 항목 및 설치 방법에 대한 자세한 내용은 다음을 참조하십시오. <a href="#">Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux(영문)</a></li> </ul>

[Release notes and system requirements for all versions of Symantec Endpoint Protection\(영문\)](#)



## Symantec Endpoint Protection 14.x 최신 버전에 대한 지원되는 업그레이드 경로

### NOTE

일반적으로 최신 버전 이전의 Symantec Endpoint Protection 버전의 경우 목록에 있는 최신 버전 이전의 모든 버전이 지원됩니다. 그러나 특정 버전에 대한 릴리스 정보를 참조하여 지원 여부를 확인해야 합니다.

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection\(영문\)](#)

### Symantec Endpoint Protection Manager 및 Windows 클라이언트

다음 버전의 Symantec Endpoint Protection Manager 및 Symantec Endpoint Protection Windows 클라이언트는 현재 버전으로 직접 업그레이드할 수 있습니다.

- 11.x 및 Small Business Edition 12.0(지원되는 운영 체제에 대해 Symantec Endpoint Protection 클라이언트만 해당)
- 12.1.x, 최대 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

### 마이그레이션 경로

다음 버전의 Mac용 Symantec Endpoint Protection 클라이언트는 현재 버전으로 직접 업그레이드할 수 있습니다.

- 12.1.4 - 12.1.6 MP9  
버전 12.1.6 MP10으로 업데이트되지 않은 Mac 클라이언트.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

### NOTE

14.0.1 MP2에서는 Mac용 Symantec Endpoint Protection 클라이언트가 업데이트되지 않았습니다.

## Linux 클라이언트

다음 버전의 Linux용 Symantec Endpoint Protection 클라이언트는 현재 버전으로 직접 업그레이드할 수 있습니다.

- 12.1.x, 최고 12.1.6 MP9  
버전 12.1.6 MP10으로 업데이트되지 않은 Linux 클라이언트
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Symantec AntiVirus for Linux 1.0.14는 Symantec Endpoint Protection으로 직접 마이그레이션할 수 있는 유일한 버전입니다. 먼저 Symantec AntiVirus for Linux의 다른 모든 버전을 제거해야 합니다. 중앙 관리 클라이언트는 단독 실행 클라이언트로 마이그레이션할 수 없습니다.

### 지원되지 않는 업그레이드 경로

모든 시만텍 제품은 Symantec Endpoint Protection 제품으로 마이그레이션할 수 없습니다. Symantec Endpoint Protection 클라이언트를 설치하려면 먼저 다음 제품을 제거해야 합니다.

- 지원되지 않는 시만텍 제품(Symantec AntiVirus 및 Symantec Client Security)
- 모든 시만텍 Norton™ 제품
- Windows XP Embedded 5.1용 Symantec Endpoint Protection
- 12.1.4 이하의 Mac용 Symantec Endpoint Protection 버전

Symantec Endpoint Protection Manager 11.0.x 또는 Symantec Endpoint Protection Manager Small Business Edition 12.0.x를 Symantec Endpoint Protection Manager 14 버전으로 직접 업그레이드할 수 없습니다. 14.x로 업그레이드하기 전에 먼저 해당 버전을 제거하거나 12.1.x로의 업그레이드를 수행해야 합니다.

Symantec Endpoint Protection Manager 12.1.6 MP7을 버전 14로 업그레이드할 수 없습니다. 12.1.6 MP7의 데이터베이스 스키마 버전이 14에 사용된 버전보다 최신이기 때문입니다. 대신 12.1.6 MP7을 14 MP1 이상으로 업그레이드해야 합니다.

14 MP1(14.0.2332.0100)에서 14 MP1 새로 고침 빌드(14.0.2349.0100)로의 업그레이드는 지원되지 않습니다.

다운그레이드 경로는 지원되지 않습니다. 예를 들어 Symantec Endpoint Protection 14.2.1.1에서 12.1.6 MP10으로 마이그레이션하는 경우 먼저 Symantec Endpoint Protection 14.2.1.1를 제거해야 합니다.

빌드 번호를 알고 있지만 해당하는 릴리스 버전을 모르는 경우 다음을 참조하십시오.

- [Released versions of Symantec Endpoint Protection\(영문\)](#)
- [Endpoint Protection 릴리스 유형 및 버전](#)

## 추가 정보

Endpoint Protection 웹 사이트 정보에는 베스트 프랙티스, 문제 해결 정보, 그리고 제품 사용에 도움이 되는 기타 리소스를 얻을 수 있는 웹 사이트가 나와 있습니다.

**Table 14: Endpoint Protection 웹 사이트 정보**

정보 유형	웹 사이트 링크
평가판	계정 담당자에게 문의하십시오.
설명서 및 문서 업데이트	<ul style="list-style-type: none"> <li>최신 릴리스의 제품 설명서(영어)</li> <li>최신 릴리스의 제품 설명서(기타 언어)</li> <li>모든 버전의 Symantec Endpoint Protection 14.x 제품 설명서</li> </ul> 다른 언어:
기술 지원	<a href="#">Endpoint Protection Technical Support(영문)</a> 기술 자료 문서, 제품 릴리스 상세 내역, 업데이트 및 패치, 지원에 대한 문의 옵션이 포함됩니다.
위협 요소 정보 및 업데이트	<a href="#">Symantec Security Center(영문)</a>
교육	<a href="#">교육 서비스</a> 교육 과정, eLibrary 등에 액세스합니다.
Symantec Connect 포럼	<a href="#">Endpoint Protection(영문)</a>

