



Symantec™ Endpoint Protection 14.3 RU1 MP1 릴리스 정보

Updated: March 1, 2021

Table of Contents

Copyright statement.....	3
Symantec Endpoint Protection 14.3 RU1 MP1의 새로운 기능.....	4
Symantec Endpoint Protection의 알려진 문제 및 해결 방법.....	5
Symantec Endpoint Protection(SEP) 14.3 RU1 MP1에 대한 시스템 요구 사항.....	9
Symantec Endpoint Protection 14.x 최신 버전에 대한 지원되는 업그레이드 경로 및 지원되지 않는 업그레이드 경로.....	17
추가 정보.....	19

Copyright statement

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright ©2021 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Symantec Endpoint Protection 14.3 RU1 MP1의 새로운 기능

이 섹션에서는 이 릴리스의 새로운 기능을 설명합니다.

14.3 RU1 MP1

- AD 형식(예: username@domain.com 또는 domain(username))의 인증 정보를 사용하여 Symantec Endpoint Protection Manager에 로그인하는 기능이 추가되었습니다.
- Active Directory(UserPrincipalName 및 Windows 2000 이전 로그인 이름 - sAMAccountName)에서 두 형식으로 사용자 이름을 동기화하는 기능이 추가되었습니다. Symantec Endpoint Protection Manager는 더 이상 중복 항목을 생성하지 않고 예상대로 두 사용자 이름을 모두 처리합니다.
- 설치 기능 및 설정에서 업데이트 시 기존 클라이언트 기능 유지라는 새 옵션을 사용하면 클라이언트는 새 버전으로 업그레이드되지만 구성, 클라이언트 통신 또는 설치된 기능을 변경하지 않고 클라이언트 패키지를 생성하고 내보낼 수 있습니다.
- 멀웨어 방지 AMSI 검사는 이제 스크립트 파일을 실행하기 전에 검사할 때 파일/폴더 예외를 고려합니다.
- Active Directory에서 macOS 상세 내역을 동기화하는 기능이 추가되었습니다.
- 로그의 추가 정보:
 - 로그 항목에는 전체 클라이언트 그룹 정보가 포함됩니다.
 - Live Update 이벤트에는 리비전 정보가 포함됩니다.
- 데이터베이스 스키마에 다음과 같은 테이블 변경 사항이 포함되었습니다.
 - SEM_CLIENT 테이블에 새 열 "user_name_2"가 추가되었습니다.

Symantec Endpoint Protection의 알려진 문제 및 해결 방법

이 섹션의 항목은 이 릴리스의 Symantec Endpoint Protection에 적용됩니다.

Table 1: 업그레이드 문제

문제	설명 및 해결책
업그레이드 중 LiveUpdate가 실행되지 않아 다크 네트워크의 Symantec Endpoint Protection Manager이(가) 오래된 CIDS(클라이언트 침입 탐지 시스템) 콘텐츠를 새 클라이언트로 다운로드함 [14.3 RU1]	14.3 RU1 Symantec Endpoint Protection Manager는 인터넷 또는 LUA(LiveUpdate 관리자) 서버에 액세스할 수 없는 경우 캐시에 호환되지 않는 오래된 콘텐츠를 보관합니다. 일반적으로 이 오래된 콘텐츠가 새 클라이언트에게 전달됩니다. 관리 서버 캐시의 콘텐츠를 업데이트하려면 인증된 바이러스 정의 및 CIDS .jdb 파일을 수동으로 다운로드합니다. [SEP-69125] 새 클라이언트가 오래된 콘텐츠를 다운로드하지 않게 하려면 새 클라이언트를 설치하거나 이전 클라이언트를 업그레이드하기 전에 SEPM에 CIDS .jdb 파일을 수동으로 설치합니다. Download .jdb files to update definitions for Endpoint Protection Manager(영문)
네트워크 인터페이스 카드가 실행 중지된 경우 Symantec Endpoint Protection Manager(SEPM)에 로그인할 수 없음 [14.3 RU1]	Symantec Endpoint Protection Manager를 설치한 후 콘솔에 로그인할 수 없고 다음 오류 메시지가 나타납니다. ### ## ## #####. SEPM을 설치할 때 시스템의 네트워크 인터페이스 카드가 실행 중지되어 서버 인증서가 생성되지 못하는 경우 이 문제가 발생할 수 있습니다. [SEP-67040] 네트워크 인터페이스 카드가 실행 중지된 상태에서 SEPM이 설치되었는지 확인하려면 서버 인증서를 확인하십시오. Unexpected server error at SEPM login if it was installed on a server without an enabled NIC(영문)
SEPM을 제거하고, 기본 데이터베이스를 제거하고 SQL Server Express 인스턴스를 유지하는 옵션을 사용하는 경우: "##### ## ## ## ## ## ## ##" 오류가 나타남[14.3 RU1]	Symantec Endpoint Protection Manager를 제거하고, DB 만 제거하고 SEPM 에 설치된 SQL Server Express 인스턴스는 유지 옵션을 선택하는 경우 "##### ## ## ## ## ## ##" 오류가 나타날 수 있습니다. 이 문제는 기본 사용자 DBA에 대한 인증 정보를 추가한 후 발생하며 사용자 권한과 관련이 있을 수 있습니다. [SEP-68670] 이 문제를 해결하려면 SEPM setup.exe 파일을 실행하고 제거 중 DB 만 제거하고 SEPM 에 설치된 SQL Server Express 인스턴스는 유지 옵션을 눌러 제거를 수행합니다.
FIPS 모드가 실행되는 경우 SQL Server가 버전 2017에서 버전 2019로 업그레이드되지 않음 [14.3]	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] 이 문제를 해결하려면 운영 체제 수준에서 FIPS를 실행 중지하십시오. 1. C:\ProgramData\Microsoft\Windows\## ##\#####\## ##에서 로컬 보안 정책 > 로컬 정책 > 보안 옵션을 누르고 시스템 암호화: 암호화, 해시, 서명에 FIPS 규격 알고리즘 사용을 실행 중지하십시오. 2. SQL Server 버전 2017에서 버전 2019로 업그레이드하십시오. 3. SQL Server가 성공적으로 업그레이드된 후 FIPS를 다시 실행하십시오. SQL upgrade from 2017 to 2019 fails with FIPS mode enabled(영문)
사용자 정의 이름으로 인해 14.2 이상으로 업그레이드 중 방화벽 정책이 업데이트되지 못할 수 있음	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.

Table 2: Symantec Endpoint Protection Manager 문제

문제	설명 및 해결책
일부 EDR 이벤트가 클라이언트에 나타나지 않음 [14.3 RU1]	Symantec Endpoint Protection 클라이언트는 Windows 10 빌드 14393 이상에서 실행되어야 Symantec EDR ETW(Windows용 이벤트 추적) 이벤트를 수집할 수 있습니다. [SEP-67175]
네트워크 트래픽 리디렉션 기능에 몇 가지 제한 사항이 있음 [14.3 RU1]	<ul style="list-style-type: none"> Symantec Web Security Service는 IPv6가 아니라 IPv4를 통해 제공됩니다. [SEP-68700] 터널 리디렉션 방법: <ul style="list-style-type: none"> Windows 10 x64 버전 1703 이상(반기 서비스 채널)에서만 실행됩니다. 이 방법은 다른 Windows 운영 체제 또는 Mac 클라이언트를 지원하지 않습니다. [SEP-67927] HVCI 지원 Windows 10 64비트 장치를 지원하지 않습니다. [SEP-67648] Symantec Endpoint Protection 클라이언트로부터의 아웃바운드 트래픽은 클라이언트의 방화벽 또는 URL 평판 규칙에 의해 평가되기 전에 WSS로 리디렉션됩니다. 대신 해당 트래픽은 WSS 방화벽 및 URL 규칙에 따라 평가됩니다. 예를 들어 SEP 클라이언트 방화벽 규칙이 google.com을 차단하고 WSS 규칙은 google.com을 허용하는 경우 이 클라이언트에서는 사용자가 google.com에 액세스할 수 있습니다. 클라이언트에 대한 인바운드 로컬 트래픽은 여전히 Symantec Endpoint Protection 방화벽에서 처리됩니다. [SEP-67488] WSS 캡티브 포털은 터널 방법에 사용할 수 없으며 클라이언트는 요청 인증 정보를 무시합니다. 향후 릴리스에서는 WSS Agent의 SAML 인증이 캡티브 포털을 대체하며 Symantec Endpoint Protection 클라이언트에서 사용할 수 있습니다. 클라이언트 시스템이 터널 방법을 사용하여 WSS에 연결하고 가상 시스템을 호스팅하는 경우 각 게스트 사용자는 WSS 포털에 제공된 SSL 인증서를 설치해야 합니다. 홈 디렉터리 또는 Active Directory 인증과 같은 로컬 네트워크의 트래픽은 리디렉션되지 않습니다. Microsoft DirectAccess VPN과 호환되지 않습니다. <p>터널 방법은 현재 베타 기능으로 간주됩니다.</p>
14.2.x에서 14.3 MP1 이상으로 업그레이드한 후 에이전트 등록 항목이 중복됨 [14.3 RU1]	<p>Symantec Endpoint Protection 클라이언트를 14.2.x에서 14.3 MP1 이상으로 업그레이드하면 Symantec Endpoint Protection Manager의 클라이언트 페이지에 이러한 클라이언트에 대한 에이전트 등록 항목이 중복 생성됩니다.</p> <p>기능상의 영향은 없으며 14.3 RU1 클라이언트에 대한 새 항목으로 작업을 계속할 수 있습니다. Symantec Endpoint Protection Manager는 이전 에이전트 항목을 제거합니다.</p>
하이브리드 관리 옵션, 프록시 서버 또는 경계 방화벽을 사용하는 경우 Symantec Endpoint Security에서 URL이 허용됨 [14.3]	<p>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"> 온-프레미스 Symantec Endpoint Protection Manager 도메인이 클라우드 콘솔에 등록되어 있을 때 Symantec Endpoint Security를 사용하여 클라이언트 및 정책을 관리합니다. 프록시 서버를 사용합니다. <p>클라우드 단독 관리 또는 하이브리드 관리 에이전트 중 하나에서 URL을 허용하여 프록시 서버 및/또는 경계 방화벽에서 해당 URL을 허용하십시오.</p> <p>SEP 및 SES가 시만텍 서버에 연결할 수 있는 허용된 URL을 참조하십시오.</p> <p>참조: Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1 or later(영문)</p>
Symantec Endpoint Protection Manager 원격 콘솔이 더 이상 32비트 Windows 플랫폼을 지원하지 않음 [14.3]	<p>14.3 이상에서는 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>

문제	설명 및 해결책
Symantec Endpoint Protection Manager 설치 중에 "Microsoft Visual C++ Runtime을 설치하지 못했습니다."라는 오류가 나타남 [14.3]	Windows 2012 R2에 Symantec Endpoint Protection Manager를 설치하는 중에 "Microsoft Visual C++ Runtime을 설치하지 못했습니다."라는 오류가 나타날 수 있습니다. [SEP-60396] 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.
Windows에서 TLS 1.1 및 TLS 1.2를 WinHTTP의 기본 보안 프로토콜로 실행하기 위한 업데이트 [14.3]	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. <SEVERE> WinHttpRequest: 12175: A security error occurred 이 문제는 TLS 1.1 및 1.2에 대한 지원을 제공하는 Microsoft 업데이트가 누락되었기 때문에 발생합니다. 문제를 해결하려면 Microsoft 업데이트 KB3140245를 설치하십시오. 자세한 내용은 다음을 참조하십시오. Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows(영문)
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
설치에 새로 사용되는 업그레이드 설치 패키지는 기본 기능 세트를 설치합니다. [14.3 RU1 MP1 이하]	업데이트 시 기존 클라이언트 기능 유지 옵션이 선택된 상태에서 업그레이드 설치 패키지를 생성하고 이 패키지를 사용하여 새로 설치하면 기본 기능 세트가 클라이언트 장치에 설치됩니다. 사용자 정의 기능 세트를 설치하려면 새로 설치할 별도의 설치 패키지를 생성해야 합니다.
Symantec Agent for Linux 설치 프로그램 로그에 잘못된 메시지가 표시됨 [14.3 RU1]	일부 경우에 에이전트 설치 프로그램은 일치하지 않는 드라이버 버전 또는 재시작 필요 여부와 관련된 잘못된 메시지를 기록합니다. 이러한 메시지는 에이전트 기능에는 영향을 주지 않습니다.
SuSe Linux 장치에서 zypper 명령을 실행하면 'at' 패키지가 제거되면서 SEP Linux 클라이언트 패키지도 제거됩니다. [14.3 RU1]	SuSe Linux 장치에서 'zypper remove at' 명령을 실행하면 SEP Linux 클라이언트 패키지가 제거됩니다. 이는 'at' 패키지가 필수 종속 패키지로 추가되었고 zypper 명령은 자동으로 SEP 클라이언트 패키지 'sdcss-kmod' 및 'sdcss-sepagent'를 사용하지 않는 종속 항목이 있는 패키지로 간주해 제거하려고 시도하기 때문입니다. 해결 방법: 'at' 패키지를 제거하려면 'rpm -e --nodeps at' 명령을 실행하십시오.
macOS 10.15 이상의 업그레이드 문제 [14.3 MP1]	macOS 10.15 이상에서 클라이언트 배포 마법사의 원격 시스템에 Symantec Endpoint Protection 설치 기능이 이전 버전의 Symantec Endpoint Protection 클라이언트를 14.3 MP1 버전으로 업그레이드하지 못합니다. 해결 방법: macOS 10.15 이상에서 Symantec Endpoint Protection 클라이언트 업그레이드를 수행하려면 Symantec Endpoint Protection Manager 자동 업그레이드를 사용하십시오.
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. Windows 및 WSUS의 2019 SHA-2 코드 서명 지원 요구 사항 Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed(영문)

문제	설명 및 해결책
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"> 결함이 없는 다른 운영 체제 버전으로 업그레이드하십시오. UWF를 실행 중지하십시오. Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled(영문)를 참조하십시오.
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 시만텍 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 Endpoint Protection 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 관련 문서 페이지로 이동하십시오. 앞으로 Broadcom은 기존 PDF 파일과 번역된 PDF 파일을 추가할 예정입니다.

해결된 문제는 다음을 참조하십시오.

[New fixes and components for Symantec Endpoint Protection 14.3 RU1 MP1\(영문\)](#)

[New fixes and components for Symantec Endpoint Protection 14.3 RU1\(영문\)](#)

[New fixes and components for Symantec Endpoint Protection 14.3 MP1\(영문\)](#)

[New fixes and components for Symantec Endpoint Protection 14.3\(영문\)](#)

Symantec Endpoint Protection(SEP) 14.3 RU1 MP1에 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"> Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 <p>Note: 데스크톱 운영 체제는 지원되지 않습니다.</p> <p>Note: 14.2x 이하에서는 Windows Server Core 버전이 지원되지 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"> Microsoft Edge Chromium 기반 브라우저(14.3 이상) Microsoft Edge <p>참고: 32비트 버전의 Windows 10은 Edge 브라우저를 사용한 웹 콘솔 액세스를 지원하지 않습니다.</p> <ul style="list-style-type: none"> Microsoft Internet Explorer 11(14.2.x 이하) Mozilla Firefox 5.x ~ 83 Google Chrome 87

구성 요소	요구 사항
데이터베이스	<p>Symantec Endpoint Protection Manager에는 다음과 같은 기본 데이터베이스가 포함되어 있습니다.</p> <ul style="list-style-type: none"> • Microsoft SQL Server Express 2014(Windows Server 2008 R2용) • Microsoft SQL Server Express 2017 • Sybase 내장 데이터베이스(14.3 MPx 이하 전용) <p>대신 다음 Microsoft SQL Server 버전의 데이터베이스 중 하나를 사용하도록 선택할 수도 있습니다.</p> <ul style="list-style-type: none"> • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014 RTM - SP3 • SQL Server 2016 RTM - SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM(14.3 이상) <p>Note: Amazon RDS에서 호스팅되는 SQL Server 데이터베이스는 지원됩니다(14.0.1 MP2부터).</p> <p>Note: 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>Note: TLS 1.2 support for Microsoft SQL Server(영문)</p>
기타 환경 요구 사항	<p>순수 IPv6 네트워크에서는 IPv4 스택이 계속 설치되고 실행 중지되어야 합니다. IPv4 스택이 설치되지 않으면 Symantec Endpoint Protection Manager이(가) 작동하지 않습니다.</p>

Table 6: Symantec Endpoint Protection Manager 하드웨어 시스템 요구 사항

구성 요소	요구 사항
프로세서	<p>Intel Pentium Dual-Core 또는 동급 이상, 8-Core 이상 권장</p> <p>Note: Intel Itanium IA-64 프로세서는 지원되지 않습니다.</p>
실제 RAM	<p>최소 2GB RAM, 8 GB 이상 권장</p> <p>Note: 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.</p>
디스플레이	1024 x 768 이상
시스템 드라이브에 설치 시 하드 드라이브	<p>로컬 SQL Server 데이터베이스 사용 시:</p> <ul style="list-style-type: none"> • 관리 서버 및 데이터베이스의 경우 최소 40GB(200GB 권장) <p>원격 SQL Server 데이터베이스와 함께</p> <ul style="list-style-type: none"> • 관리 서버의 경우 최소 40GB(100GB 권장) • 데이터베이스에 대해 원격 서버에서 추가 사용 가능 디스크 공간
대체 드라이브에 설치 시 하드 드라이브	<p>로컬 SQL Server 데이터베이스 사용 시:</p> <ul style="list-style-type: none"> • 시스템 드라이브에 최소 15GB 필요(100GB 권장) • 설치 드라이브에 최소 25GB 필요(100GB 권장) <p>원격 SQL Server 데이터베이스와 함께</p> <ul style="list-style-type: none"> • 시스템 드라이브에 최소 15GB 필요(100GB 권장) • 설치 드라이브에 최소 25GB 필요(100GB 권장) • 데이터베이스에 대해 원격 서버에서 추가 사용 가능 디스크 공간
기타	실행되는 네트워크 인터페이스 카드

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"> • Windows 7(32비트/64비트, RTM 및 SP1) • Windows Embedded 7 Standard, POSReady 및 Enterprise(32비트 및 64비트) • Windows 8(32비트, 64비트) • Windows Embedded 8 Standard(32비트 및 64비트) • Windows 8.1(32비트, 64비트), Windows To Go 포함 • 2014년 4월 Windows 8.1 업데이트(32비트, 64비트) • 2014년 8월 Windows 8.1 업데이트(32비트, 64비트) • Windows Embedded 8.1 Pro, Industry Pro 및 Industry Enterprise(32비트 및 64비트) • Windows 10(버전 1507)(32비트, 64비트), Windows 10 Enterprise 2015 LTSC 포함 • Windows 10 11월 업데이트(버전 1511)(32비트, 64비트) • Windows 10 1주년 업데이트(버전 1607)(32비트, 64비트), Windows 10 Enterprise 2016 LTSC 포함 • Windows 10 크리에이터스 업데이트(버전 1703)(32비트, 64비트) • Windows 10 Fall Creators Update(버전 1709)(32비트, 64비트) • Windows 10 2018년 4월 업데이트(버전 1803)(32비트, 64비트) • Windows 10 2018년 10월 업데이트(버전 1809)(32비트, 64비트), Windows 10 Enterprise 2019 LTSC 포함 • Windows 10 2019년 5월 업데이트(버전 1903)(32비트, 64비트) • Windows 10 2019년 11월 업데이트(버전 1909)(32비트, 64비트)(14.2 RU1 이상) • Windows 10 20H1(Windows 10 버전 2004)(14.3 이상) • Windows 10 20H2(Windows 10 버전 2009)(14.3 RU1부터)
운영 체제(서버)	<ul style="list-style-type: none"> • Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • 2014년 4월 Windows Server 2012 R2 업데이트 • 2014년 8월 Windows Server 2012 R2 업데이트 • Windows Server 2016 • Windows Server 2019 • Windows Server 버전 1803(Server Core)(14.2 이상) • Windows Server 버전 1809(Server Core) • Windows Server 버전 1903(Server Core)(14.2 RU1 이상) • Windows Server 버전 1909(Server Core)(14.2 RU1 이상) • Windows Server 버전 2004 • Windows Server 버전 20H2(14.3 RU1) <p>이전 릴리스에서 지원되는 운영 체제 목록은 다음을 참조하십시오. Windows compatibility with the Endpoint Protection client(영문) Endpoint Protection support for Windows 10 updates and Windows Server 2016 / Server 2019(영문)</p>
브라우저 침입 차단	<p>브라우저 침입 차단에 대한 지원은 클라이언트 침입 탐지 시스템(CIDS) 엔진의 버전을 기준으로 결정됩니다. Supported browsers for Browser Intrusion Prevention in Endpoint Protection(영문)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"> 2비트 프로세서: 4GHz Intel Pentium 4 또는 동급 이상(Intel Pentium 4 또는 동급 권장) 64비트 프로세서: x86-64 지원 2GHz Pentium 4 또는 동급 이상 <p>Note: 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>Note: 하이퍼바이저 리소스 예약을 실행해야 합니다.</p>
실제 RAM	1GB, 운영 체제에서 필요한 경우 그 이상(2GB 권장)
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>Note: 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 클라이언트 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"> 395MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 시스템 드라이브: 180MB 대체 설치 드라이브: 350MB
Embedded/VDI	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 245MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 시스템 드라이브: 180MB 대체 설치 드라이브: 200MB
비공개 네트워크	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 545MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 시스템 드라이브: 180MB 대체 설치 드라이브: 500MB

* 설치하는 동안 추가 135MB가 필요합니다.

Table 10: 대체 드라이브에 설치되었을 때 Windows용 Symantec Endpoint Protection 클라이언트 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"> 시스템 드라이브: 380MB 대체 설치 드라이브: 15MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> 시스템 드라이브: 30MB 프로그램 데이터 드라이브: 350MB 대체 설치 드라이브: 150MB
Embedded/VDI	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 시스템 드라이브: 230MB 대체 설치 드라이브: 15MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> 시스템 드라이브: 30MB 프로그램 데이터 드라이브: 200MB 대체 설치 드라이브: 150MB
비공개 네트워크	<p>시스템 드라이브에 있는 프로그램 데이터 폴더와 함께</p> <ul style="list-style-type: none"> 시스템 드라이브: 530MB 대체 설치 드라이브: 15MB* <p>대체 드라이브에 있는 프로그램 데이터 폴더와 함께**</p> <ul style="list-style-type: none"> 시스템 드라이브: 30MB 프로그램 데이터 드라이브: 500MB 대체 설치 드라이브: 150MB

* 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 Note: 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"> 시스템 드라이브에 설치됨: 245MB 대체 드라이브에 설치됨: 시스템에 230MB 및 대체 드라이브에 15MB <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"> Windows Embedded Standard 7(32비트 및 64비트) Windows Embedded POSReady 7(32비트 및 64비트) Windows Embedded Enterprise 7(32비트 및 64비트) Windows Embedded 8 Standard(32비트 및 64비트) Windows Embedded 8.1 Industry Pro(32비트 및 64비트) Windows Embedded 8.1 Industry Enterprise(32비트 및 64비트) Windows Embedded 8.1 Pro(32비트 및 64비트)
최소 필수 구성 요소	<ul style="list-style-type: none"> 필터 관리자(FitMgr.sys) 성능 데이터 도우미(pdh.dll) Windows Installer 서비스
템플릿	<ul style="list-style-type: none"> 응용 프로그램 호환성(기본값) 디지털 서명 산업 자동화 IE, Media Player, RDP 셋톱박스 씬(Thin) 클라이언트 <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	2GB RAM
하드 드라이브	설치를 위한 1GB의 하드 디스크 여유 공간
디스플레이	800 x 600
운영 체제	<ul style="list-style-type: none"> macOS 10.15 ~ 10.15.7 Intel Core i5 프로세서 이상의 macOS 11(Big Sur) <p>이전 릴리스의 지원되는 운영 체제 목록은 Mac compatibility with the Endpoint Protection client(영문)를 참조하십시오.</p>

Table 13: Linux용 Symantec Endpoint Protection 클라이언트 시스템 요구 사항

구성 요소	요구 사항
하드웨어	<ul style="list-style-type: none"> • Intel Pentium 4(2GHz) 이상 프로세서 • 사용 가능한 500MB의 RAM(4GB RAM 권장) • /var, /opt 및 /tmp가 동일한 파일 시스템 또는 볼륨을 공유하는 경우 2GB의 디스크 공간 사용 가능 • 서로 다른 볼륨에 있는 경우 /var, /opt 및 /tmp 각각에 500MB의 디스크 공간 사용 가능
운영 체제	<p>버전 14.3 RU1부터 지원되는 운영 체제:</p> <ul style="list-style-type: none"> • Amazon Linux 2 • CentOS 6, 7, 8 • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS <p>버전 14.3 MP1 이하에서 지원되는 운영 체제:</p> <ul style="list-style-type: none"> • Amazon Linux • CentOS 6U3 ~ 6U9, 7 ~ 7U7, 8 - 32비트 및 64비트 • Debian 6.0.5 Squeeze, Debian 8 Jessie - 32비트 및 64비트 • Fedora 16, 17 - 32비트 및 64비트 • Oracle Linux(OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux 서버(RHEL) 6U2 ~ 6U9, 7 ~ 7U8, 8 ~ 8U2 • SUSE Linux Enterprise Server(SLES) 11 SP1~11 SP4(32비트 및 64비트), 12, 12 SP1~12 SP3(64비트) • SUSE Linux Enterprise Desktop(SLED) 11 SP1~11 SP4(32비트 및 64비트), 12 SP3(64비트) • Ubuntu 12.04, 14.04, 16.04, 18.04(14.3부터) - 32비트 및 64비트 <p>이전 릴리스의 지원되는 운영 체제 커널 목록은 List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x(영문)를 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"> • KDE • Gnome • Unity <p>Symantec Agent for Linux 14.3 RU1에는 그래픽 사용자 인터페이스가 없습니다.</p>

구성 요소	요구 사항
기타 환경 요구 사항(14.3 MP1 이하)	<ul style="list-style-type: none"> • Glibc glibc 2.6 이하를 실행하는 모든 운영 체제는 지원되지 않습니다. • net-tools 또는 iproute2 Symantec Endpoint Protection에서는 시스템에 이미 설치되어 있는 도구에 따라 이 두 도구 중 하나를 사용합니다. • OpenSSL 1.0.2k-fips 이상 • 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. Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux(영문) • 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 명령이 sudo를 포함하여 표시합니다. <ul style="list-style-type: none"> – Red Hat 기반 배포의 경우: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code> – Debian 기반 배포의 경우: <code>sudo apt-get install ia32-libs</code> – Ubuntu 기반 배포의 경우: <pre>sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386</pre>

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

Symantec Endpoint Protection 14.x 최신 버전에 대한 지원되는 업그레이드 경로 및 지원되지 않는 업그레이드 경로

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

지원되는 업그레이드 경로

- 내장 데이터베이스가 있는 Symantec Endpoint Protection Manager 버전 12.1.6 MP10 이상은 Microsoft SQL Server Express 데이터베이스 버전 14.3 RU1 MP1으로 원활하게 업그레이드됩니다. 12.1.6 MP9 및 이전 버전에서 14.3 RU1 MP1으로 업그레이드는 차단됩니다.
- Symantec Endpoint Protection Manager 14.x는 Windows Server 2003(데스크톱 운영 체제 및 32비트 운영 체제)과 일부 버전의 SQL Server와 같이 지원이 중단된 경우를 제외하고는 12.1.x를 통해 원활하게 업그레이드됩니다.
- Symantec Endpoint Protection 14.x 클라이언트는 지원되는 운영 체제에 설치된 이전의 모든 12.1 및 11 클라이언트 버전을 통해 원활하게 업그레이드됩니다. 단, 12.1.4 이전의 Mac 클라이언트는 12.1.4 이상으로 업그레이드하거나 제거해야 합니다.

[Symantec Endpoint Protection 14 Migration Considerations\(영문\)](#)

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
- 14.3, 14.3 MP1
- 14.3 RU1

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 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1

NOTE

14.0.1 MP2에서는 Mac용 Symantec Endpoint Protection 클라이언트가 업데이트되지 않았습니다.

Linux 클라이언트**NOTE**

Symantec Agent for Linux 14.3 RU1은 이전 버전의 Linux용 Symantec Endpoint Protection 클라이언트가 검색될 경우 이를 제거하고 신규 설치를 수행합니다. 이전 구성은 유지되지 않습니다.

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 MP10.t로 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
- 14.3, 14.3 MP1
- 14.3 RU1

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 Symantec AntiVirus 및 Symantec Client Security
- 모든 시만텍 Norton 제품
- Windows XP Embedded 5.1용 Symantec Endpoint Protection
- 12.1.4 이전의 모든 Symantec Endpoint Protection for Mac 클라이언트. 또는 12.1.4 이상으로 업그레이드할 수 있습니다.

참고:

- 12.1.x 이전 버전의 경우 Symantec Endpoint Protection 클라이언트 마이그레이션이 지원되지 않습니다.
- Symantec Endpoint Protection Manager 11.0.x 또는 Symantec Endpoint Protection Manager Small Business Edition 12.0.x는 Symantec Endpoint Protection Manager 14의 어떤 버전으로도 직접 업그레이드할 수 없습니다. 최신 릴리스인 14.x로 업그레이드하려면 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.
- 14.0.x에서는 Windows XP, Server 2003 및 Windows XP 기반의 모든 Windows Embedded 운영 체제에 대한 지원이 제외되었습니다. 12.1.x 클라이언트는 수명 종료되었지만 Symantec Endpoint Protection Manager 14.2 RU1에서 이러한 시스템을 기존 12.1.x 클라이언트로 관리할 수 있습니다. 이러한 클라이언트의 경우 이러한 기존 운영 체제를 여전히 지원하는 Data Center Security(DCS) 등의 시만텍 제품을 사용할 수 있습니다.
- 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 마이그레이션하려는 경우 먼저 Symantec Endpoint Protection 14.2.1을 제거해야 합니다.
- 빌드 번호를 알고 있지만 해당하는 릴리스 버전을 모르는 경우 다음을 참조하십시오.

[Endpoint Protection 릴리스 유형 및 버전](#)

추가 정보

다음 표에는 제품 사용에 대한 베스트 프랙티스, 문제 해결 정보와 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"> 최신 릴리스의 제품 설명서(영어) 최신 릴리스의 제품 설명서(기타 언어) 모든 버전의 Symantec Endpoint Protection 14.x 제품 설명서
기술 지원	Endpoint Protection Technical Support(영문) 기술 자료 문서, 제품 릴리스 상세 내역, 업데이트 및 패치, 지원에 대한 문의 옵션이 포함됩니다.
위협 요소 정보 및 업데이트	Symantec Security Center(영문)
교육	교육 서비스 교육 과정, eLibrary 등에 액세스합니다.
Symantec Connect 포럼	Endpoint Protection(영문)

