# AsyncOS 업그레이드 후 TLS 버전 1.0이 비활성화된 이유

## 목차

[소개](#)
[AsyncOS 업그레이드 후 Cisco에서 TLS 버전 1.0을 비활성화하는 이유는 무엇입니까?](#)
[관련 정보](#)

## 소개

이 문서에서는 업그레이드 후 AsyncOS에서 TLS(Transport Layer Security) 버전 1.0을 자동으로 비활성화하는 이유를 설명합니다.

## AsyncOS 업그레이드 후 Cisco에서 TLS 버전 1.0을 비활성화하는 이유는 무엇입니까?

Cisco는 AsyncOS 9.5 릴리스 이후 TLSv1.1 및 v1.2 기능을 도입했습니다. 이전에는 이전 프로토콜이 필요한 환경을 업그레이드한 후 TLSv1.0이 활성화된 상태로 유지되었지만, Cisco에서는 TLSv1.2를 Secure Email 환경의 표준 프로토콜로 전환하는 것이 좋습니다.

Cisco AsyncOS 13.5.1 릴리스 이상에서는 Cisco 보안 정책에 따라 업그레이드할 때 TLS 버전 1.0이 자동으로 비활성화되어 Cisco Secure Email 사용자의 위험을 줄입니다.

이 내용은 13.5.1 GD 릴리즈 노트에 설명되어 있습니다(릴리즈 노트)

| | |
|---|---|
| SSL Configuration Changes | The following are the new changes made to SSL configuration settings:<br>• There is no support for SSLv2 and SSL v3 methods.<br>• There is no support for the TLS v1.0 method if your appliance is in the FIPS mode.<br>• The TLS v1.0 method is disabled by default if your appliance is in the non-FIPS mode.<br>• You can enable the TLS v1.0 method for the TLS client services (LDAP and Updater) in any one of the following ways:<br>– System Administration > SSL Configuration page of the web interface of your appliance. See the "System Administration" section in the user guide<br>– `sslconfig` command in the CLI. See the "CLI Reference Guide for AsyncOS 13.5.1 for Cisco Email Security Appliances."<br>Note If you plan to upgrade from a lower AsyncOS version (for example, 12.x) in non-FIPS mode with TLS v1.0 enabled, to AsyncOS 13.5.1 and later, then TLS v1.0 is disabled by default. You need to enable the TLS v1.0 method on your appliance after upgrade. |

13.5.1 릴리스 이후 버전 릴리스로 업그레이드할 경우 WebUI 및 CLI(명령줄)에도 다음과 같은 경고 메시지가 표시됩니다.

After you upgrade to AsyncOS 13.5.1 and later, TLS v1.1 and v1.2 is enabled by default. - You cannot use TLS v1.0 in FIPS mode. - The appliance disables TLS v1.0 in non-FIPS mode after the upgrade but you can re-enable it if required.

---

> 경고: TLSv1.0을 활성화하면 환경에 잠재적인 보안 위험 및 취약성이 노출됩니다. Cisco는 데이터의 안전한 전송을 위해 사용 가능한 TLSv1.2 및 고속 암호를 활용할 것을 적극 권장합니다.

---

현재 AsyncOS 15.0에서는 Cisco Secure Email AsyncOS를 통해 시스템 관리자가 업그레이드 후 이전 버전 1.0 프로토콜로 인한 잠재적 보안 위험으로 인해 TLSv1.0을 다시 활성화할 수 있습니다.

이러한 유연성을 제공하기 위해서는 이후 릴리스에서 TLSv1.0을 사용하는 옵션을 제거하기 위해 변경될 수 있습니다.

TLSv1.0의 보안 위험 및 취약점:

SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability(BEAST)
SSL/TLSv1.0 범죄 취약성

## 관련 정보

- Cisco Secure Email 릴리스 정보

- 기술 지원 및 문서 – Cisco Systems
- Cisco Secure Email에서 TLSv1.0 활성화

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.