

# 보안 액세스 오류 트러블슈팅 "TLS 오류: 268435703:SSL 루틴 :OPENSSL\_internal:WRONG\_VERSION\_NUMBER"

## 목차

---

[소개](#)

[문제](#)

[솔루션](#)

[추가 세부 정보](#)

[관련 정보](#)

---

## 소개

이 문서에서는 보안 액세스 오류를 해결하는 방법에 대해 설명합니다. "TLS error: 268435703:SSL routes:OPENSSL\_internal:WRONG\_VERSION\_NUMBER".

## 문제

사용자가 리소스에 대한 공용 URL(예: <https://<app-name>.ztna.sse.cisco.io>)을 사용하여 브라우저 기반 제로 트러스트 액세스를 사용하여 프라이빗 리소스를 열려고 하면 응용 프로그램이 브라우저에 로드되지 않고 오류가 표시됩니다.

응용 프로그램에 연결할 수 없습니다.

관리자에게 문의하십시오.

업스트림 연결 오류 또는 헤더 전 연결 끊기/재설정 이유 재설정: 연결 실패, 전송 실패 이유: TLS 오류: 268435703:SSL 루틴:OPENSSL\_internal:WRONG\_VERSION\_NUMBER

# Cisco Secure Access

---



**Application is unreachable**

**Please contact your administrator**

upstream connect error or disconnect/reset before headers. reset reason: connection failure, transport failure reason: TLS error: 268435703:SSL routines:OPENSSL\_internal:WRONG\_VERSION\_NUMBER

---

보안 클라이언트 오류

## 솔루션

Private Resource(프라이빗 리소스) 섹션의 Endpoint Connection Method(엔드포인트 연결 방법) 아래에서 적절한 프로토콜을 구성해야 합니다.

- 프라이빗 애플리케이션을 HTTP에서만 사용할 수 있는 경우 HTTP를 선택해야 합니다.
- 프라이빗 애플리케이션이 HTTP를 통해서만 사용 가능한 경우 HTTP를 선택해야 합니다.
- 프라이빗 애플리케이션을 HTTP 또는 HTTPS를 통해 사용할 수 있는 경우 이 오류는 표시되지 않아야 합니다.

## Endpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices can access the resource.

### Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

### Client-based connection

Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

+ FQDN or IP Address

### Browser-based connection

Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not

Public URL for this resource ⓘ

https://   ⓘ

Protocol

Validate Application Certificate ⓘ

### VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

프라이빗 리소스 구성

## 추가 세부 정보

보안 액세스 프록시 엔진은 대시보드에 지정된 프로토콜을 사용하여 프라이빗 리소스에 대한 연결을 설정하려고 시도합니다.

프록시에서 프라이빗 애플리케이션과의 HTTPs 채널을 설정할 수 없는 경우(양쪽의 잘못된 컨피그레이션 때문에), 브라우저 기반 연결을 통해 프라이빗 리소스에 액세스하려고 시도할 때 브라우저에서 OpenSSL 관련 오류를 볼 수 있습니다.

## 관련 정보

- [Secure Access 사용 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.