

Troubleshoot Secure Access Error "TLS Error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER"

Contents

[Introduction](#)

[Problem](#)

[Solution](#)

[Additional Details](#)

[Related Information](#)

Introduction

This document describes a way to resolve the Secure Access error: "TLS error: 268435703:SSL routines:OPENSSL_internal:WRONG_VERSION_NUMBER".

Problem

When a user tries to open a Private Resource using Browser-Based Zero Trust Access, using the public URL for the resource (for example **https://<app-name>.ztna.sse.cisco.io**), the application does not load in the browser and the error is seen:

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**

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

Secure Client Error

Solution

Make sure you configure a proper Protocol under the Endpoint Connection Method in the Private Resource Section:

- If the private application is available over HTTP only, you must select HTTP.
- If the private application is available over HTTPS only, you must select HTTPS.
- If the private application is available over HTTP or HTTPS, this error must never be seen.

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 [Server Name Indication \(SNI\) \(optional\)](#)

Validate Application Certificate

VPN connections

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

Private Resource Configuration

Additional Details

The Secure Access proxy engine tries to establish a connection to the Private Resource using the Protocol specified in the dashboard.

If the proxy is unable to establish HTTPs channel with the private application (due to misconfiguration on either side), you can see OpenSSL-related errors in the browser when trying to access Private Resources via the Browser-based connection.

Related Information

- [Secure Access User Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)