ZTNA Client - Network Interceptor Error

Contents

Issue

Users experiencing network interceptor errors when attempting to access private resources through Cisco Secure Access Zero Trust Access (ZTNA). The error prevents successful connection to any private resources configured within the Zero Trust Access environment, resulting in complete loss of access to internal applications and services.

Environment

- Technology: Cisco Secure Access - Zero Trust Access (ZTNA)
- Software Version: 5.1.14
- Product Family: SECACCS
- Error Type: Network interceptor error
- Impact: Critical - Complete loss of access to private resources
- Recent Changes: None reported

Resolution

This can be seen in the Dart logs:

++ The following logs were found:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() IZtnaApi::SetParameters failed with error co

2026-03-
02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 Ztna

2026-03-
02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] I/ ZtnaConfigEnforcer.cpp:145 ZtnaC

in the Cached config from DART

A trailing white space is introduced - **cisco.com** - causing this issue.

- After further testing, it became evident that selecting the remotely reachable address option for private resourc
- However, it looks like when the remotely reachable address field was checked, there was an extra whitespace
- As the default zero-trust profile was in-
  use, meaning that any newly created or existing private resource configuration is pushed down to every user in
- To remedy this issue for the time being,go to the private resources and ensure whitespaces are not present in th

Cause

The network interceptor error in Cisco Secure Access Zero Trust Access is typically caused by misconfigured or pro

Related Content

- Cisco Technical Support & Downloads