Resolve Cowork (Frontier) Agent Connectivity Issues when Umbrella is Enabled

Contents

Issue

The Cowork (Frontier) agent was not working properly on laptops when Cisco Umbrella was enabled. When Cisco Umbrella was inactive, the agent functioned as expected. Users were unable to use the Cowork agent functionality when Umbrella was active, and no block logs were visible in Cisco Umbrella when users experienced this issue. Error screenshots were provided showing the application failures during Umbrella operation.

Environment

- Cisco Umbrella deployed on enterprise laptops
- Cowork (Frontier) agent application
- SSL/TLS traffic inspection enabled in Cisco Umbrella
- Certificate pinning implemented in the Cowork application

Resolution

The issue was resolved by adding the Cowork application to the Do Not Decrypt (DND) list in Cisco Umbrella. This configuration change allows the Cowork agent to bypass SSL/TLS inspection and maintain its direct encrypted connection to the Cowork servers.

Steps to Configure DND List

Step 1: Access the Cisco Umbrella dashboard and navigate to the **SSL Decryption policy configuration**.

Step 2: Add **Cowork-related domains** and **URLs** to the Do Not Decrypt list to bypass SSL inspection for

this application.

Step 3: Apply the **policy changes** and allow time for the configuration to propagate to all endpoints.

Step 4: Test the **Cowork agent functionality** with Cisco Umbrella enabled to verify proper operation.

Validation

After implementing the DND list configuration, the Cowork application functioned normally with Cisco Umbrella enabled. Internal testing confirmed that the issue did not reoccur over several days of monitoring, and all users were able to access Cowork functionality as expected.

Cause

The Cowork (Frontier) agent uses certificate pinning as a security mechanism. Certificate pinning means the application is hardcoded to only accept and trust its own specific server certificate. When Cisco Umbrella intercepts the traffic and presents the Cisco certificate instead of the original server certificate, the Cowork application detects this change, assumes the connection is not secure, and intentionally drops the connection to protect the data. This is expected behavior for applications that implement certificate pinning security measures.

Related Content

- Create Effective Do Not Decrypt List for Microsoft Applications
- Cisco Technical Support & Downloads