MacOS Internet Access Issues After Importing Secure Access Certificate

Contents

Issue

MacOS users experience inability to access internet resources through Cisco Secure Access after importing the internet certificate from the portal.

The affected services include:

- Microsoft Outlook (send and receive functionality)
- Google.com
- AI websites
- Other web destinations

Windows users with the same configuration are not impacted and continue to function normally. The issue specifically affects MacOS clients' access to email and general internet browsing capabilities after certificate import.

Environment

- Cisco Secure Access with Unified Policy configuration
- MacOS clients with imported internet certificate from Cisco Secure Access portal
- Windows clients with same configuration (unaffected)
- Internet Policies, Private Policies, DLP Policies, RBI, and Security Profiles in use
- Mixed operating system environment with differential behavior between MacOS and Windows

Resolution

The resolution involves adding specific Microsoft Outlook endpoints and applications to the Do Not Decrypt (DND) list to bypass SSL inspection for these services.

Step 1: Add Outlook Endpoints to DND List

Add the endpoints or applications described in the next sections to the Do Not Decrypt (DND) configuration to resolve the Outlook access issues.

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
smtp.office365.com
```

Step 2: Validate Resolution

After adding the Outlook-related endpoints to the DND list, verify that the affected MacOS clients can now access:

- Microsoft Outlook send and receive functionality
- Other previously affected internet resources

The user confirmed that after implementing these DND entries, the Outlook applications continue to function normally on MacOS devices.

Cause

The issue was caused by SSL/TLS encryption inspection interfering with MacOS clients' ability to establish secure connections to internet resources, particularly Microsoft Outlook services. The encryption inspection process was preventing proper certificate validation or connection establishment specifically on MacOS platforms, while Windows clients were unaffected by the same inspection policies. Adding the affected endpoints to the Do Not Decrypt list bypasses the inspection for these specific services, allowing normal connectivity to resume.

Related Content

- Cisco Technical Support & Downloads