Secure Access Custom CA Trust Issues with Firefox and Safari on macOS

Contents

Issue

Users experienced certificate trust errors in macOS browsers (Safari and Firefox) when accessing decrypted internet traffic through Cisco Secure Access. Chrome browser worked correctly, but Safari and Firefox displayed "untrusted certificate" warnings and blocked access to websites and applications.

The complete certificate chain showed:

- Website (such as cnn.com) **> Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA**

Firefox and Safari browsers stopped certificate validation at the Cisco intermediate certificates and failed to chain up to the root CA, while Chrome successfully validated the entire certificate chain.

Environment

- Cisco Secure Access deployment with custom certificate authority for HTTPS decryption
- macOS devices with Safari and Firefox browsers
- Custom CA certificate infrastructure using Microsoft Certificate Authority
- Internet Access policies with decryption and intrusion prevention enabled
- Organization ID: xxxxx

Resolution

The issue was resolved by identifying an encoding mismatch in the certificate chain and switching to the

Cisco Secure Access Root CA for decryption.

Root Cause Analysis

Team identified that the custom certificate authority was created using printable string encoding, which caused incompatibility issues even when leaf certificates were set to UTF8STRING. Firefox and Safari require that all certificates in a chain be in the same format, while Chrome does not have this strict requirement.

Resolution Steps

Switch to Cisco Secure Access Root CA

Alternative Solutions

If using a custom CA is required, these options were identified:

- Rebuild the entire certificate infrastructure using UTF8 encoding (high impact, not recommended)
- Use a different certificate infrastructure that supports UTF8 encoding
- Limitation of Firefox and Safari can not work with the current custom CA setup

Cause

The root cause was an encoding mismatch between the Microsoft Certificate Authority (which uses printablestring encoding by default) and the UTF8 chain used by Cisco Secure Access. Firefox and Safari have stricter certificate validation requirements and need all certificates in the chain to use consistent encoding. the more lenient validation in Chrome allowed it to work with the mixed encoding chain, while Firefox and Safari rejected the inconsistent certificate formats.

The Microsoft CA created certificates using printablestring encoding, but Cisco Secure Access intermediate certificates used UTF8STRING encoding. This mismatch caused Firefox and Safari to fail certificate chain validation at the Cisco intermediate certificate level.

Related Content

- Configure Webex Meeting Access in SWG
- Cisco Technical Support & Downloads