Secure Client Umbrella Module SSL/TLS Trust Failure During Device Registration

Contents

Issue

During rollout of Cisco Secure Client with the Umbrella module, devices stopped syncing with the Dashboard and reported as "Inactive." The affected clients experienced SSL/TLS trust failures when attempting to register to devices.api.sse.cisco.com, preventing successful device registration and protection coverage.

The UI showed Umbrella as inactive with these status messages:

- Umbrella is inactive.
- You are not currently protected by secure web gateway.
- The secure web gateway is not licensed / is disabled.

Diagnostic findings revealed a consistent SSL/TLS Trust Failure during registration with this error message in the Secure Client logs:

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

Environment

- Cisco Secure Client with Umbrella module deployment across 2,000+ endpoints
- SD-WAN infrastructure with route policies
- Legacy Umbrella tunnels in place
- Network configuration allowing all required destinations per Cisco documentation
- No SSL decryption active for Cisco destinations on perimeter

Resolution

The resolution involved identifying and correcting a routing configuration issue that was causing device registration traffic to be misdirected through legacy Umbrella tunnels.

Root Cause Identification

Analysis of packet capture data revealed that the TLS certificate presented for the API connection was a Cisco Umbrella certificate rather than the expected Cisco Secure Access/Let's Encrypt certificate. Identify the IP address for devices.api.sse.cisco.com.

Further investigation identified an SD-WAN route policy that matched the 146.112.0.0/16 subnet, causing traffic to devices.api.sse.cisco.com to be routed into legacy Umbrella tunnels instead of the intended destination.

Configuration Changes

These steps were taken to resolve the issue:

- Step 1: Remove the problematic static routes. Static routes pointing 146.112.0.0/16 to the legacy Umbrella tunnels were removed from the SD-WAN configuration.
- Step 2: Validate connectivity. After removing the static routes, affected clients were tested to ensure they could successfully connect and register to devices.api.sse.cisco.com.

Verification

The expected certificate chain for devices.api.sse.cisco.com ought to appear as shown:

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
```

```
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

After implementing the configuration changes, affected clients successfully connected and registered, and the deployment was completed successfully.

Cause

The root cause was an SD-WAN route policy that matched the 146.112.0.0/16 subnet, causing device registration traffic destined for devices.api.sse.cisco.com (146.112.59.104) to be incorrectly routed through legacy Umbrella tunnels. This resulted in the presentation of an incorrect TLS certificate (Cisco Umbrella certificate instead of the expected Cisco Secure Access/Let's Encrypt certificate), leading to SSL/TLS trust failures during the device registration process.

Related Content

- Cisco Secure Client Network Requirements Documentation
- Cisco Technical Support & Downloads