Endpoint DLP Enrollment Fails Due to TLS Certificate Issues

Issue

Endpoint enrollment into Secure Access Endpoint DLP fails with a TLS fatal or bad certificate error during the certificate-based TLS handshake. The enrollment process cannot complete despite the endpoint having valid user and machine certificates issued by a Certificate Authority (CA) that has been uploaded to the Secure Access Portal. This failure prevents Endpoint DLP onboarding and impacts the ability to enable data loss prevention capabilities on endpoints.

Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Secure Access
- Product Family: SECACCS
- Endpoint has user certificate and machine certificate issued by CA
- Certificate Authority uploaded into Secure Access Portal
- Endpoint attempting DLP enrollment

Resolution

Check the Logs located at **C > Program Data > Cisco > Cisco Secure client > EDLP > csc_edlpenroll.log**:

[2026-03-11 14:57:18.244870] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment[1]

[2026-03-11 14:57:18.244870] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1

[2026-03-
11 14:57:18.244870] [info] [SSEZtnaEnroller.cpp:360] 1 of 1 user store client certificate(s) match the enrollment ch

[2026-03-
11 14:57:18.244870] [info] [SSEZtnaEnroller.cpp:470] **Using client certificate cert=subject=/CN=x@cisco.com** issuer=/CN=EDLPRootLab chainLen=2

[2026-03-11 14:57:18.244870]

[2026-03-
11 14:57:18.402611] [info] [OpenSSLClientCertAuth.cpp:132] invoking SSL_CTX_set1_client_sigalgs_list: RSA+
PSS+SHA256

**[2026-03-
11 14:57:18.450140] [info] [OpenSSLClientCertAuth.cpp:470] TLS alert received: fatal / bad certificate**

[2026-03-11 14:57:18.450140] [info] [HttpClient.cpp:315] missing HttpConnection

[2026-03-11 14:57:18.450140] [info] [HttpClient.cpp:534] request complete for url=https://orgid-edlp.enroll.ztna.sse.cisco.com/enrollInit/edlp res=56 error=Failure when receiving data from the peer

[2026-03-11 14:57:18.450140] [error] [CurlSocketManager.cpp:72] unknown sockfd: 1808

To resolve the TLS certificate error during Endpoint DLP enrollment, follow these steps.

1. Regenerate the certificate with proper key length. Regenerate the affected certificate using a 2048-
bit public key. This addresses potential issues with certificate key length that could be causing the TLS handshake fa

2.Test endpoint DLP enrollment. After regenerating the certificate with the 2048-
bit public key, attempt the Endpoint DLP enrollment process again to verify if the TLS certificate error has been reso

Check the Logs located at **C > Program Data > Cisco > Cisco Secure client > EDLP > csc_edlpenroll.log**:

2026-02-27 11:21:04.032108] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment[a01121f1-cab2-47fb-
927a-e512ba4df752]

[2026-02-27 11:21:04.032108] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1

**[2026-02-
27 11:21:04.032108] [info] [SSEZtnaEnroller.cpp:360] 1 of 1 user store client certificate(s) match the enrollme**

**[2026-02-
27 11:21:04.032108] [info] [SSEZtnaEnroller.cpp:470] Using client certificate: alias= cert=subject=/CN=x@ci**

[2026-02-27 11:21:04.032108] [info] [HttpClient.cpp:52] start request: method=POST url=https://orgid-edlp.enroll.ztna.sse.cisco.com/enrollInit/edlp

[2026-02-
27 11:21:04.032108] [info] [SSEZtnaEnroller.cpp:483] Initiated HTTP request method=POST url=https://orgid-edlp.enroll.ztna.sse.cisco.com/enrollInit/edlp with headers

[2026-02-
27 11:21:04.032108] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to Pending for Enrolln

**[2026-02-
27 11:21:07.785803] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with result: Success**

[2026-02-27 11:21:07.785803] [info] [SSEZtnaEnroller.cpp:2241]

Enrollment Stats

==========

Authentication type : certificate

Bootstrap : success (0.728 sec)

DeviceRegistration : success (1.312 sec)

DHARegistration : success (0.220 sec)

ACMEEnrollment : success (1.291 sec)

PersistEnrollment : success (0.210 sec)

Overall result : success (3.761 sec)

[2026-02-27 11:21:07.785803] [info] [ZtnaEnrollmentService.cpp:510] Updating cert data for Enrollment

Cause

The TLS fatal / bad certificate error during Endpoint DLP enrollment is likely caused by certificate key length issues or certificate compatibility problems during the TLS handshake process. The certificate potentially does not meet the required specifications for the Secure Access Endpoint DLP enrollment process, despite being issued by a valid Certificate Authority that has been properly uploaded to the Secure Access Portal.

Related Content

- Cisco Technical Support & Downloads