Endpoint DLP Certificate-Based Auto-Enrollment Failure with SHA1 Hashing Incompatibility

Contents

Issue

Endpoint DLP enrollment fails during certificate-based auto-enrollment with repeated initialization errors. The enrollment process cannot authenticate using the client identity certificate, resulting in continuous retry attempts.

The following error messages are observed in the enrollment logs:

```
[2026-02-05 13:24:58.154989] [info] [AutoEnrollMonitor.cpp:633] Auto-enrollment attempt #5 with enrollm
[2026-02-05 13:24:58.154989] [info] [SSEZtnaEnroller.cpp:185] Processing start event
[2026-02-05 13:24:58.155992] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment
[2026-02-05 13:24:58.398260] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1
[2026-02-05 13:24:58.399259] [error] [SSEZtnaEnroller.cpp:355] None of the 1 user store client certific
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with res
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2241]
Enrollment Stats
================
Authentication type           : certificate
Bootstrap                     : failure (0.251 sec)
----------------
Overall result                : failure (0.251 sec)
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:615] Will retry the enrollment with enrollme
```

Additional TLS-level authentication failures are documented with the error message: "TLS alert received: fatal / bad certificate."

Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Secure Access - Unified Policy (Internet Policies, Private Policies, DLP Policies, RBI, Security Profiles)
- Software Version: ALL

- Authentication Method: Certificate-based auto-enrollment
- Certificate Store: User store client certificates
- Certificate Hashing Algorithm: SHA1 (deprecated)

Resolution

The resolution involves regenerating the identity certificate with a supported hashing algorithm and ensuring proper certificate installation and configuration.

Step 1: Regenerate Identity Certificate with Supported Hashing Algorithm

Generate and reissue the identity certificate using SHA256 or SHA-3 hashing instead of the deprecated SHA1 algorithm. The certificate must be created with the following specifications:

- Hashing algorithm: SHA256 or SHA-3 (SHA1 is not supported)
- Format: PKCS#12 (PFX) format
- Required field: SAN field with RFC822 Name as specified for enrollment

Step 2: Install Updated Certificate in Correct Certificate Store

Install the newly generated certificate in the appropriate certificate store location:

- Certificate store location: User/Machine Personal > Certificates store
- Certificate format: PKCS#12 (PFX)

Step 3: Reboot Endpoint to Re-trigger Authentication

After installing the updated certificate, reboot the endpoint system to re-trigger the authentication process and allow the enrollment mechanism to detect the new certificate.

Step 4: Test Authentication from Non-Corporate Network

To rule out SSL inspection or decryption interference by edge firewalls, test the authentication process from a non-corporate network environment. This helps isolate potential network-level certificate inspection issues that could interfere with the enrollment process.

Step 5: Retry Endpoint DLP Enrollment

After completing the certificate replacement and system reboot, attempt the Endpoint DLP enrollment process again. Monitor the enrollment logs to verify successful authentication and enrollment completion.

Cause

The enrollment failure is caused by the use of SHA1 hashing algorithm in the client identity certificates. SHA1 is a deprecated cryptographic hashing algorithm that is no longer supported by the enrollment policy requirements. The enrollment system specifically requires certificates to be hashed with modern, secure algorithms such as SHA256 or SHA-3 to meet current security standards and policy compliance.

When the enrollment process validates the client certificate against the enrollment choice policy, it rejects certificates that use the deprecated SHA1 hashing algorithm, resulting in the "None of the 1 user store client certificate(s) match the enrollment choice policy" error message and subsequent initialization failure.

Related Content

- Cisco Technical Support & Downloads