Secure Access Certificate Inspection Posture Check Authentication Failures

Contents

Issue

When attempting to deploy Secure Access with the Endpoint posture profile using the certificate inspection feature, all login attempts fail despite the fact that specific causes of failure cannot be identified in the DART bundle logs.Users are attempting to utilize SAML IDP authentication while also wanting to enforce certificate validation through the posture checking mechanism, but this configuration results in consistent authentication failures even when backend certificate matches are successful.

Environment

- Cisco Secure Access - Secure Client Remote Access (VPN, Posture, Private Resource)
- SAML IDP authentication integration
- Endpoint posture profile with certificate inspection feature enabled
- User certificates with UPN field in SAN matching email addresses
- Secure Access tenant configuration with Users, Groups, and Endpoint devices

Resolution

The certificate endpoint checks in posture are only enforced when using multi-certificate authentication, which requires both user certificate and machine certificate validation. Since the deployment scenario involves users with only user certificates who need to use a single VPN profile, the solution involves implementing SAML + Single certificate authentication instead of relying on posture certificate checking.

Authentication Configuration Steps

Step 1: Configure SAML + Single Certificate Authentication

Configure the authentication method to use SAML authentication combined with single certificate authentication rather than attempting to enforce certificate validation through posture checks.

Step 2: Configure Certificate UPN Matching

Ensure that the UPN field in the certificate's Subject Alternative Name (SAN) contains the user's email address that matches the auth property configured for the user in Secure Access under Users, Groups, and Endpoint devices.

Step 3: Set Primary Authentication Field

Configure the primary field to authenticate using the UPN from the certificate, ensuring it corresponds to the user's email address in the Secure Access user database.

Certificate Structure Requirements

The certificate structure must be configured so that the UPN or secondary value in the certificate matches the auth property for the user in Secure Access. If a user presents a certificate that has a UPN or secondary value that does not match the configured auth property for that user in Secure Access, the authentication will be rejected.

Important Configuration Notes

Multi-certificate authentication (IDP SAML + Multi-Cert Auth) would be required if posture certificate checking enforcement is needed, but this requires both user and machine certificates. For deployments where users only have user certificates and need to use a single VPN profile, SAML + Single certificate authentication provides the appropriate solution while still maintaining certificate-based security controls.

Cause

The certificate endpoint checks in posture are only enforced when multi-certificate authentication is configured. When using SAML authentication with posture certificate checking, the system expects both user and machine certificates to be present for validation. Since the deployment only utilized user certificates with SAML authentication, the posture certificate inspection feature consistently failed authentication attempts despite successful backend certificate matching, as the posture mechanism was not

designed to work with single certificate authentication scenarios.

Related Content

- Cisco Technical Support & Downloads