ZTNA Enrollment Failures for Guest Users with Personal Google Accounts in Cisco Secure Access

Contents

Issue

During deployment of Private Access with ZTNA (Zero Trust Network Access), enrollment of a guest user with a personal Google account fails after successful registration in Entra ID and provisioning in Secure Access. The specific symptoms encountered include:

- **Client-based enrollment**: The enrollment process reaches SSO authentication, credentials are provided, but ZTNA displays an "I/O error" and the enrollment process becomes stuck
- **Client-less access**: Returns the error message "Cisco Secure Access Login failure. Check IDP Configuration" along with a transaction ID

These failures prevent access to private resources and impact testing of ZTNA functionality for contractor-style access using non-corporate identities.

Environment

- Cisco Secure Access with ZTNA deployment
- Microsoft Entra ID (formerly Azure AD) as Identity Provider
- Personal Google account (@gmail.com) registered as guest user in Entra ID
- Guest account provisioned and visible in Secure Access
- SAML authentication configured between Entra ID and Cisco Secure Access

Resolution

The enrollment failure was resolved by modifying the SAML attribute mapping configuration in Microsoft Entra ID. The following steps were taken to address the issue:

Step 1: Analyze DART Bundle and Client Behavior

Review the DART bundle to confirm that Cisco Secure Client and ZTA components are operating normally. The analysis should verify that the enrollment flow successfully reaches Cisco Secure Access and that the failure occurs during SAML authentication with the Identity Provider.

Step 2: Examine Entra ID Authentication Logs

Check the Entra ID authentication logs to confirm that the authentication process completes successfully from the Identity Provider perspective. The logs should show successful authentication, but Secure Access rejects the login due to attribute mismatch.

Step 3: Identify SAML Attribute Mapping Issue

Determine that Entra ID is issuing the UPN (User Principal Name) as the SAML claim, which does not match the personal Gmail account identity expected by Secure Access. The asserted IdP attribute does not correspond to the expected user identifier.

Step 4: Modify SAML Attribute Mapping

Change the SAML attribute mapping in Microsoft Entra ID from **UPN** to **Email Address**. This ensures that the email address claim matches the personal Google account identity.

Step 5: Verify Enrollment Success

After implementing the attribute mapping change, retry the ZTNA enrollment process. Cisco Secure Access ZTA should now recognize the Gmail address and allow the enrollment to complete successfully.

Cause

The enrollment failure was caused by a mismatch between the SAML attribute being asserted by Microsoft

Entra ID and the expected user identifier in Cisco Secure Access. Entra ID was configured to send the UPN (User Principal Name) as the SAML claim, but for personal Google accounts (@gmail.com), this UPN did not correspond to the actual email address identity. Cisco Secure Access expected to receive the email address as the identifying attribute to match against the provisioned guest user account, resulting in authentication rejection despite successful IdP authentication.

Related Content

- Cisco Technical Support & Downloads