Secure Access RAVPN Authentication Failed with Duo SAML Integration

Contents

Issue

When attempting to connect to Cisco Secure Access Remote Access VPN (RAVPN) using Duo as the Identity Provider (IDP) with Active Directory integration in the background, users experience authentication failures despite successful authentication at the Duo portal level.

The specific symptoms include:

- Duo portal displays a success message for authentication.
- Cisco SecureClient displays an "Authentication failed" error message immediately after the Duo success.
- Duo logs show "access granted" status.
- Cisco Secure Access portal logs show "AAA failure" status.

This creates a disconnect where the external identity provider confirms successful authentication, but the VPN client cannot establish the connection due to authentication validation failures within the Secure Access infrastructure.

Environment

- Cisco Secure Access RAVPN deployment
- Duo Security as SAML Identity Provider
- Active Directory integration with Duo
- Cisco SecureClient for VPN connectivity
- SAML-based authentication flow

Resolution

The authentication failure was resolved by correcting the user attribute mapping between Duo and Cisco Secure Access. The steps outlined in the next sections were taken to identify and resolve the issue.

Step 1: Check Activity Search

1.- Log in to Cisco Secure Access Dashboard. Click **Monitor> Remote Access Logs**.

2.- Check for the username field under the authorization check failure messages.

3.- Match it against UPN value under **Connect > User and Groups**.

Cisco Secure Access looks at User Principal Name value for Authorization check.

User Principal Name being passed from Duo did not match the user principal name value for that user under **User and Groups**.

The investigation showed:

- **User email addres**s: user@gmail.com
- **User Principal Name (UPN** username

Step 2: Duo Configuration Adjustment

The resolution involved modifying the Duo SAML configuration to ensure proper user attribute mapping:

- Access the Duo Admin Panel.
- Navigate to the SAML application configuration for Cisco Secure Access.
- Modify the user attribute mapping to send the email address which must match User Principal Name value for that user under User and Groups.
- Save the configuration changes.

Step 4: Verification

After adjusting the Duo configuration, the authentication flow was tested and verified successful. The user was able to connect using Remote Access VPN without authentication failures.

Cause

The root cause of the authentication failure was a user attribute mapping mismatch between Duo SAML assertions and Cisco Secure Access expectations. Duo was configured to send the username under User Principal Name (UPN) in SAML assertions, while Cisco Secure Access was configured to expect the user email address This mismatch caused the authentication to fail at the Secure Access level despite successful authentication at the Duo IDP level, resulting in the "AAA failure" logged in Secure Access while Duo logs showed "access granted."

Related Content

- Cisco Technical Support & Downloads