

RAVPN-Authentifizierung für sicheren Zugriff fehlgeschlagen mit Duo SAML-Integration

Inhalt

Problem

Bei dem Versuch, eine Verbindung mit dem Cisco Secure Access Remote Access VPN (RAVPN) herzustellen, bei dem Duo als Identity Provider (IDP) mit Active Directory-Integration im Hintergrund verwendet wird, treten trotz erfolgreicher Authentifizierung auf Duo-Portalebene Authentifizierungsfehler auf.

Zu den spezifischen Symptomen gehören:

- Das Duo Portal zeigt eine Erfolgsmeldung für die Authentifizierung an.
- Cisco SecureClient zeigt die Fehlermeldung "Authentication failed" (Authentifizierung fehlgeschlagen) unmittelbar nach dem Erfolg von Duo an.
- Duo-Protokolle zeigen den Status "Zugriff gewährt" an.
- Die Protokolle des Cisco Secure Access-Portals zeigen den Status "AAA-Fehler" an.

Dadurch wird die Verbindung getrennt, und der externe Identitätsanbieter bestätigt die erfolgreiche Authentifizierung. Der VPN-Client kann die Verbindung jedoch aufgrund von Fehlern bei der Authentifizierung in der Infrastruktur für sicheren Zugriff nicht herstellen.

Umwelt

- Cisco Secure Access RAVPN-Bereitstellung
- Duo Security als SAML Identity Provider
- Active Directory-Integration mit Duo

- Cisco SecureClient für VPN-Verbindungen
- SAML-basierter Authentifizierungsablauf

Auflösung

Der Authentifizierungsfehler wurde durch Korrigieren der Benutzerattributzuordnung zwischen Duo und Cisco Secure Access behoben. Die in den nächsten Abschnitten beschriebenen Schritte wurden durchgeführt, um das Problem zu identifizieren und zu lösen.

Schritt 1: Aktivitätssuche überprüfen

1.- Melden Sie sich beim Cisco Secure Access Dashboard an. Klicken Sie auf Überwachen > RAS-Protokolle.

2.- Suchen Sie in den Fehlermeldungen für die Autorisierungsprüfung nach dem Feld "Benutzername".

3.- Ordnen Sie es dem UPN-Wert unter Verbinden > Benutzer und Gruppen zu.

Cisco Secure Access prüft den Wert des Benutzerprinzipalnamens für die Autorisierungsprüfung.

Der von Duo übergebene Benutzer-Prinzipalname stimmt nicht mit dem Wert des Benutzer-Prinzipalnamens für diesen Benutzer unter Benutzer und Gruppen überein.

Die Untersuchung ergab Folgendes:

- E-Mail-Adresse des Benutzers: user@gmail.com
- Benutzerprinzipalname (UPN-Benutzername)

Phase 2: Duo Konfigurationseinstellung

Die Auflösung umfasste die Änderung der Duo SAML-Konfiguration, um eine korrekte Zuordnung der Benutzerattribute sicherzustellen:

- Zugriff auf den Duo-Administrationsbereich
- Navigieren Sie zur SAML-Anwendungskonfiguration für Cisco Secure Access.
- Ändern Sie die Zuordnung des Benutzerattributs, um die E-Mail-Adresse zu senden, die mit dem Wert für den Benutzerprinzipalnamen für diesen Benutzer unter Benutzer und Gruppen übereinstimmen muss.
- Speichern Sie die Konfigurationsänderungen.

Schritt 4: Verifizierung

Nach der Anpassung der Duo-Konfiguration wurde der Authentifizierungsfluss getestet und erfolgreich verifiziert. Der Benutzer konnte ohne Authentifizierungsfehler über das Remote Access VPN eine Verbindung herstellen.

Ursache

Die Hauptursache für den Authentifizierungsfehler war eine falsche Zuordnung der Benutzerattribute zwischen den Duo SAML-Assertionen und den Erwartungen an Cisco Secure Access. Duo wurde so konfiguriert, dass der Benutzername unter User Principal Name (UPN) in SAML Assertionen gesendet wurde, während Cisco Secure Access so konfiguriert wurde, dass die E-Mail-Adresse des Benutzers erwartet wurde. Diese Diskrepanz führte dazu, dass die Authentifizierung auf Secure Access-Ebene trotz erfolgreicher Authentifizierung auf Duo IDP-Ebene fehlschlug. Das Ergebnis war der "AAA-Fehler" bei Secure Access, während in Duo-Protokollen der "Zugriff gewährt" angezeigt wurde.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.