# Löschen eines nicht vertrauenswürdigen Zugriffsprofils, das zu einem Verlust des Benutzerzugriffs führt

## Inhalt

## Problem

Nach dem Löschen eines Zero Trust Access (ZTA)-Profils, von dem angenommen wurde, dass es nicht verwendet wurde, erlitten alle Benutzer mit dem ZTNA-Modul einen vollständigen Verlust des Zugriffs auf private Ressourcen und die Internetnavigation. Die Löschung dieses Profils führte zu einer sofortigen Unterbrechung des Service für alle ZTNA-Benutzer und hinderte sie daran, über die Zero Trust Network Access-Infrastruktur auf Ressourcen zuzugreifen.

Die betroffenen Benutzer konnten keine Verbindungen herstellen zu:

- Private interne Ressourcen
- Internetnavigation durch das ZTNA-Modul

## Umwelt

- Sicherer Zugriff (Netzwerkzugriff ohne Vertrauen)
- ZTNA-Modul mit mehreren Benutzerprofilen bereitgestellt
- Standardrichtlinie mit ZTNA-Kontrolle konfiguriert
- Mehrere ZTA-Profile für die Benutzerzugriffsverwaltung konfiguriert

## Auflösung

## Verstehen der Logik der ZTA-Profilzuordnung

Profile mit nicht vertrauenswürdigem Zugriff werden basierend auf einer bestimmten Abgleichsreihenfolge und Logik angewendet:

- Profilzuordnung: ZTA-Profile werden der Reihe nach anhand von Kriterien für die Benutzer- und Zielzuordnung ausgewertet.
- Standardprofilverhalten: Wenn kein bestimmtes Profil den Benutzer- oder Zielkriterien entspricht, wird das Standardprofil verwendet.
- Profilabhängigkeiten: Das Löschen eines Profils, das als effektiver Standard dient, kann zu Serviceunterbrechungen führen, auch wenn es nicht verwendet wird.

Das gelöschte Profil hat wahrscheinlich als effektives Standardprofil für die Benutzerzuordnung funktioniert, obwohl es in der Konfigurationsschnittstelle nicht verwendet wurde. Beim Entfernen dieses Profils haben die Benutzer ihren primären Zugriffspfad über die ZTNA-Infrastruktur verloren.

## Validierungsschritte

Um ähnliche Probleme in Zukunft zu vermeiden, muss dieser Validierungsansatz implementiert werden:

1.- Überprüfen Sie vor dem Löschen alle konfigurierten ZTA-Profile und die entsprechenden Kriterien.

2.- Bestimmen Sie, welches Profil als effektiver Standard für den Benutzerzugriff dient.

3.- Überprüfen Sie die Zuordnung von Benutzer zu Profil mithilfe von Konfigurations-Screenshots und der Richtlinienüberprüfung.

4.- Testprofil ändert sich kontrolliert, bevor es auf die Produktion angewendet wird.

# Ursache

Die Ursache war das Löschen eines ZTA-Profils, das als effektives Standardprofil für den ZTA-Benutzerzugriff fungierte, obwohl es in der Konfigurationsschnittstelle nicht verwendet wurde. Beim Entfernen dieses Profils gingen die primären Zuordnungskriterien für den Benutzerzugriff verloren, sodass alle ZTNA-Benutzer keine Verbindung mehr zu privaten Ressourcen und zur Internetnavigation hatten. Die Logik der Profilzuordnung hängt davon ab, ob ein gültiges Standardprofil für den Fallback verfügbar ist, wenn bestimmte Benutzer- oder Zielkriterien von anderen konfigurierten Profilen nicht erfüllt werden.

## 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.