

# Configurazione dell'autenticazione Single Sign-On per la migrazione ad accesso sicuro con Cisco Cloud Sign-On

## Sommario

---

---

## Problema

Durante la migrazione da Umbrella a Secure Cloud Control, il comportamento amministrativo Single Sign-On (SSO) è cambiato in modo imprevisto. Anziché utilizzare l'ID Microsoft Entra configurato in precedenza per l'autenticazione e l'autenticazione a più fattori, agli amministratori è stato richiesto di eseguire l'autenticazione utilizzando Cisco Cloud Sign-On con DUO. Di conseguenza, agli amministratori viene richiesto di impostare nuove password e di registrarsi a DUO per l'autenticazione a più fattori.

## Ambiente

- Tecnologia: Secure Access (in precedenza Umbrella)
- Migrazione: Umbrella per il controllo sicuro del cloud
- Autenticazione: ID Entra Microsoft (Azure AD) configurato come provider di identità
- Multi-Factor Authentication: Microsoft 365 MFA precedentemente configurato
- Nuovo metodo di autenticazione: Cisco Cloud sign-on con DUO

## Risoluzione

La migrazione dell'autenticazione da Microsoft Entra ID a Cisco Cloud Sign-On è un passaggio obbligatorio che si verifica durante il processo di migrazione di Secure Access. Per configurare correttamente l'autenticazione dell'interfaccia utente SAML, effettuare le operazioni riportate di seguito.

## Passaggio 1: Completare la migrazione Secure Access

Completare la migrazione di Accesso sicuro completa prima di tentare di configurare l'autenticazione dell'interfaccia utente SAML in Accesso sicuro. In questo modo tutti i componenti vengono correttamente migrati e sono pronti per la configurazione dell'autenticazione.

## Passaggio 2: Configurazione dell'autenticazione SAML tramite il controllo del cloud di sicurezza

La configurazione dell'autenticazione dell'interfaccia utente SAML viene ora gestita tramite l'interfaccia SCC (Security Cloud Control) anziché direttamente all'interno di Secure Access. Passare a Controllo cloud di sicurezza > Impostazioni di autenticazione per accedere alle opzioni di configurazione del provider di identità.

## Passaggio 3: Verifica configurazione provider di identità

Esaminare e convalidare la configurazione del provider di identità nella pagina Controllo cloud di sicurezza. Verificare che l'integrazione di Microsoft Entra ID sia configurata correttamente per il nuovo ambiente.

## Causa

La modifica del comportamento di autenticazione fa parte del processo di migrazione obbligatorio da Umbrella a Secure Access. Durante questa migrazione, l'autenticazione SAML passa automaticamente da Microsoft Entra ID a Cisco Cloud Sign-On, che richiede DUO per l'autenticazione a più fattori. Si tratta di una modifica dell'architettura necessaria nella nuova piattaforma Secure Access, in cui le impostazioni di autenticazione vengono gestite centralmente tramite Security Cloud Control anziché all'interno delle singole interfacce di prodotto.

## Contenuto correlato

- [Integrazione dei provider di identità](#)
- [Supporto tecnico Cisco e download](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).