# シスコクラウドサインオンによるセキュアアクセス移行シングルサインオン認証設定

## 内容

## お問い合わせ内容

UmbrellaからSecure Cloud Controlへの移行中に、管理シングルサインオン(SSO)の動作が予期せず変更されました。以前に設定したMicrosoft Entra IDを認証とMFAに使用する代わりに、管理者はDUOを使用するCisco Cloudサインオンを使用して認証する必要がありました。その結果、管理者は新しいパスワードを設定し、多要素認証のためにDUOに登録するように求められました。

## 環境

- テクノロジー：Secure Access ( 旧称：Umbrella )
- 移行：クラウド制御を保護する包括
- 認証： IDプロバイダーとして構成されたMicrosoft Entra ID (Azure AD)
- Multi-Factor Authentication：以前に設定されたMicrosoft 365 MFA
- 新しい認証方法：Cisco CloudサインオンとDUO

## 解決策

Microsoft Entra IDからCisco Cloudへの認証の移行は、セキュアアクセス移行プロセス中に行われる必須の手順です。SAML UI認証を適切に設定するには、次の手順に従う必要があります。

### 手順1：セキュアアクセスの移行を完了する

Secure AccessでSAML UI認証の設定を試みる前に、Secure Accessの完全移行を完了してください。これにより、すべてのコンポーネントが適切に移行され、認証設定の準備が整います。

### ステップ2:Security Cloud ControlによるSAML認証の設定

SAML UI認証設定は、Secure Access内で直接管理されるのではなく、Security Cloud Control(SCC)インターフェイスで管理されるようになりました。IDプロバイダーの設定オプションにアクセスするには、Security Cloud Control > Authentication Settingsの順に移動します。

### 手順3：アイデンティティプロバイダー設定の確認

Security Cloud Controlページでアイデンティティプロバイダーの設定を確認および検証します。Microsoft Entra ID統合が新しい環境に対して正しく構成されていることを確認します。

## 原因

認証動作の変更は、Umbrellaからセキュアアクセスへの必須の移行プロセスの一部です。この移行中、SAML認証はMicrosoft Entra IDからCisco Cloudのサインオンに自動的に移行します。この移行には、多要素認証にDUOが必要です。これは、認証設定が個々の製品インターフェイス内ではなく、Security Cloud Controlを通じて一元的に管理される新しいSecure Accessプラットフォームで必要とされるアーキテクチャの変更です。

## 関連コンテンツ

- アイデンティティプロバイダーの統合
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。