使用思科雲登入的安全訪問遷移單點登入身份驗證配置

目錄

問題

從Umbrella遷移至安全雲控制期間，管理單一登入(SSO)行為意外更改。管理員需要使用Cisco Cloud登入和DUO進行身份驗證，而不是使用以前配置的Microsoft Entra ID進行身份驗證和MFA。這導致管理員被提示設定新密碼並註冊DUO進行多重身份驗證。

環境

- 技術：安全存取（前身為Umbrella）
- 遷移：Umbrella保護雲控制
- 驗證:配置為身份提供程式的Microsoft Entra ID(Azure AD)
- 多重身份驗證：Microsoft 365 MFA先前已配置
- 新的身份驗證方法：使用DUO的Cisco Cloud登入

解析

從Microsoft Entra ID到思科雲登入的身份驗證遷移是安全訪問遷移過程中必須執行的步驟。要正確配置SAML UI身份驗證，應遵循以下步驟：

步驟 1:完成安全訪問遷移

嘗試在Secure Access中配置SAML UI身份驗證之前，請完成完整的Secure Access遷移。這可確保所有元件都正確遷移並做好身份驗證配置的準備。

步驟 2:通過安全雲控制配置SAML身份驗證

SAML UI身份驗證配置現在通過安全雲控制(SCC)介面管理，而不是直接在安全訪問中管理。導航到安全雲控制>身份驗證設定以訪問身份提供程式配置選項。

步驟 3:檢視身份提供程式配置

在Security Cloud Control頁面中檢視和驗證身份提供程式配置。確保已針對新環境正確配置Microsoft Entra ID整合。

原因

身份驗證行為更改是從Umbrella到Secure Access的強制遷移過程的一部分。在此遷移過程中，SAML身份驗證會自動從Microsoft Entra ID轉換到Cisco Cloud登入，這要求DUO進行多重身份驗證。這是新安全訪問平台中所需的架構更改，在該平台中，身份驗證設定通過安全雲控制集中管理，而不是在單個產品介面內管理。

相關內容

- 整合身份提供程式
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。