使用思科云登录的安全访问迁移单点登录身份验证配置

目录

问题

从Umbrella迁移至安全云控制期间，管理单点登录(SSO)行为意外更改。管理员需要使用Cisco Cloud登录和DUO进行身份验证，而不是使用以前配置的Microsoft Entra ID进行身份验证和MFA。这导致管理员被提示设置新密码并注册DUO进行多重身份验证。

环境

- 技术：安全访问（以前称为Umbrella）
- 迁移：Umbrella用于保护云控制
- 身份验证:Microsoft Entra ID(Azure AD)配置为身份提供程序
- 多重身份验证：Microsoft 365 MFA以前配置
- 新的身份验证方法：使用DUO的Cisco Cloud登录

分辨率

从Microsoft Entra ID到思科云登录的身份验证迁移是安全访问迁移过程中必须执行的步骤。要正确配置SAML UI身份验证，应执行以下步骤：

步骤 1：完成安全访问迁移

尝试在安全访问中配置SAML UI身份验证之前，请完成完全的安全访问迁移。这可确保所有组件都正确迁移并做好身份验证配置的准备。

步骤 2：通过安全云控制配置SAML身份验证

SAML UI身份验证配置现在通过安全云控制(SCC)界面管理，而不是直接在安全访问中管理。导航到安全云控制>身份验证设置以访问身份提供程序配置选项。

步骤 3：检查身份提供程序配置

在安全云控制(Security Cloud Control)页面中查看和验证身份提供程序配置。确保为新环境正确配置了Microsoft Entra ID集成。

原因

身份验证行为更改是从Umbrella到Secure Access的强制性迁移过程的一部分。在此迁移期间，SAML身份验证自动从Microsoft Entra ID转换到Cisco Cloud登录，这需要DUO进行多重身份验证。这是新安全访问平台中所需的架构更改，在此平台中，身份验证设置通过安全云控制集中管理，而不是在单个产品界面中管理。

相关内容

- 集成身份提供程序
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。