在Umbrella中为多组织和MSP控制台配置SAML的SSO

目录

简介

本文档介绍如何使用SAML在Umbrella中为多组织和MSP控制台配置单点登录(SSO)。

SSO配置范围和限制

- 本文专门介绍如何使用SAML将多组织或MSP Umbrella控制台与您的SSO提供商集成。
- 本文不提供一般SAML配置步骤。有关常规配置，请参阅启用单点登录文档。
- SSO配置不可用于STC、MSSP、PPoV或任何使用Cisco CEC登录的控制台中的用户帐户。使用思科CEC登录的用户无法使用其他SSO提供程序。

多组织或MSP控制台的SSO

多组织和MSP控制台不支持直接从控制台进行SAML配置。必须在子组织级别启用SSO。要为控制台管理员启用SSO，请完成以下步骤：

1. 创建名为"单一登录"的新子组织。除SSO用户外，此组织保持为空。
2. 在单一登录组织中创建新用户。
    - 此用户是SAML配置所必需的，并且必须存在于您的身份提供程序中。
    - 无法使用MSP或多组织管理员帐户配置SAML，除非管理员也直接添加到子组织。
3. 如果出现"File Not Found"之类的错误，请确保当前登录的用户是您在配置SSO的组织控制面板上Admin > Accounts下列出的管理员。
4. 以Single Sign On用户身份登录到Umbrella控制面板。
5. 在单点登录组织中配置SSO(SAML)。
6. 从子组织控制面板以只读方式邀请现有管理员加入"单一登录"组织。

- 接受后，这些用户将成为管理控制台和此单一组织的成员。
- 这些用户现在必须通过SSO登录，并且不再使用帐户密码。

警告：请勿向多个启用SSO的子组织添加用户。如果用户被添加到多个启用SSO的子组织，该用户将被锁定在控制面板之外，直到其他管理员将该用户从其他启用SSO的组织中删除。

常见问题解答

问:如果我有STC、MSSP或合作伙伴门户，可以使用自己的SSO吗？

A：不可以。您必须使用思科IT Okta合作伙伴门户。对Umbrella的访问取决于Okta访问级别。已撤销或已禁用的Okta帐户没有Umbrella访问权限。

问:一个子组织中的SSO是否适用于该用户的所有登录？

A：Yes.用户必须通过SSO登录，在未通过SSO进行身份验证之前，无法访问任何组织。

问:是否可以在多个子组织上启用SSO?

A：Yes;但是，只能为SSO配置一个子组织。将用户以只读方式添加到单一登录组织，以对任何帐户实施SSO。

问:为什么是只读的？

A：这并不是必需的，但可使任何帐户添加到组织中，而无需更改此空组织中的任何设置。

问:如果用户添加到启用了SSO的第二个组织，会发生什么情况？

A：用户无法登录。从至少一个SSO组织中删除用户，或与支持人员联系以恢复访问权限。

问:配置SAML时，验证测试失败，并出现“FILE NOT FOUND”（未找到文件）错误。为什么？

A：当使用MSP或多组织管理员帐户尝试SAML配置时，会出现这种情况。使用单点登录组织中的帐户执行SAML配置。

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）。