使用SAML為Umbrella中的多組織和MSP控制檯配置SSO

目錄

簡介

本文檔介紹如何使用SAML在Umbrella中為多組織和MSP控制檯配置單一登入(SSO)。

SSO配置範圍和限制

- 本文專門介紹如何使用SAML將多組織或MSP Umbrella控制檯與SSO提供商整合。
- 本文不提供一般SAML配置步驟。有關一般配置，請參閱啟用單一登入文檔。
- 對於使用Cisco CEC登入的STC、MSSP、PPoV或任何控制檯中的使用者帳戶，SSO配置不可用。使用Cisco CEC登入的使用者無法使用其他SSO提供程式。

多組織或MSP控制檯的SSO

Multi-Org和MSP控制檯不支援直接從控制檯進行SAML配置。必須在子組織級別啟用SSO。要為控制檯管理員啟用SSO，請完成以下步驟：

1. 建立一個名為Single Sign On的新子組織。除SSO使用者外，此組織保持為空。
2. 在單一登入組織中建立新用戶。
    - 此使用者是SAML配置所必需的，並且必須存在於您的身份提供程式中。
    - 無法使用MSP或多組織管理員帳戶配置SAML，除非該管理員還直接新增到子組織。
3. 如果出現「File Not Found（未找到檔案）」之類的錯誤，請確保當前登入的使用者是組織（在其中配置SSO）的控制面板上Admin > Accounts下列出的管理員。
4. 以Single Sign On使用者身份登入Umbrella控制面板。
5. 在單一登入組織中配置SSO(SAML)。
6. 從子組織儀表板以只讀方式邀請現有管理員加入「單一登入」組織。

- 接受後，這些使用者將成為管理控制檯和此單一組織的成員。
- 這些使用者現在必須通過SSO登入且不再使用帳戶密碼。

警告：不要將使用者新增到多個啟用了SSO的子組織。如果將使用者新增到多個啟用SSO的子組織，則使用者將被鎖定在儀表板外，直到另一個管理員將該使用者從其他啟用SSO的組織中刪除。

常見問題

Q:如果我有STC、MSSP或合作夥伴門戶，是否可以使用自己的SSO?

A:不能。您必須使用思科IT合作夥伴門戶。對Umbrella的訪問由Okta訪問級別決定。已撤銷或已禁用的Okta帳戶沒有Umbrella訪問許可權。

Q:一個子組織中的SSO是否應用於該使用者的所有登入？

A:會。使用者必須通過SSO登入，且在未通過SSO進行身份驗證之前無法訪問任何組織。

Q:是否可以在多個子組織上啟用SSO?

A:是;但是，只能為SSO配置一個子組織。將使用者以只讀方式新增到單一登入組織，以強制實施任何帳戶的SSO。

Q:為什麼是只讀的？

A:這不是必需的，但允許將任何帳戶新增到組織，而無需更改此空組織中的任何設定。

Q:如果使用者新增到啟用SSO的第二個組織，會發生什麼情況？

A:使用者無法登入。將使用者從至少一個SSO組織或聯絡支援人員以恢復訪問許可權。

Q:配置SAML時，驗證測試失敗，並顯示「FILE NOT FOUND」錯誤。為什麼？

A:當使用MSP或多組織管理員帳戶嘗試SAML配置時會發生這種情況。使用單一登入組織中的帳戶執行SAML配置。

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）。