Configure SSO with SAML for Multi-Org and MSP Consoles in Umbrella

Contents

Introduction

This document describes how to configure Single Sign-on (SSO) with SAML for Multi-Org and MSP consoles in Umbrella.

SSO Configuration Scope and Restrictions

- This article is specific to integrating a Multi-Org or MSP Umbrella console with your SSO provider using SAML.
- This article does not provide general SAML configuration steps. For general configuration, refer to the documentation Enable Single Sign-On.
- SSO configuration is not available for user accounts in STC, MSSP, PPoV, or any console using the Cisco CEC login. Users who log in using Cisco CEC cannot use another SSO provider.

SSO for the Multi-Org or MSP Console

The Multi-Org and MSP consoles do not support SAML configuration directly from the console. SSO must be enabled at the child organization level. To enable SSO for a console administrator, complete these steps:

1. Create a new child organization named **Single Sign On**. This organization remains empty except for SSO users.
2. Create a new user in the **Single Sign On** organization.
    - This user is required for SAML configuration and must also exist in your identity provider.
    - SAML cannot be configured using an MSP or Multi-Org Admin account unless that admin is also added directly to the child organization.
3. If errors such as "File Not Found" appear, ensure the currently logged-in user is an admin listed under **Admin > Accounts** on the dashboard of the organization where you are configuring SSO.
4. Log in to the Umbrella Dashboard as the **Single Sign On user**.
5. Configure SSO (SAML) in the **Single Sign On organization**.

6. Invite existing administrators into the "Single Sign On" organization as read only from the child organization dashboard.
    - Once accepted, these users become members of both the management console and this single organization.
    - These users must now sign in via SSO and no longer use an account password.

Warning: Do not add a user to more than one SSO-enabled child organization. If a user is added to multiple SSO-enabled child organizations, the user becomes locked out of the dashboard until another admin removes the user from the additional SSO-enabled organization.

Frequently Asked Questions

Q: Can I use my own SSO if I have an STC, MSSP, or Partner portal?

A: No. You must use the Cisco IT Okta partner portal. Access to Umbrella is determined by Okta access level. Revoked or disabled Okta accounts do not have Umbrella access.

Q: Does the SSO in one child organization apply to all logins for the user?

A: Yes. The user must sign in via SSO and cannot access any organizations without authenticating with

SSO.

Q: Can I enable SSO on multiple child organizations?

A: Yes; however, only one child organization must be configured for SSO. Add users to the Single Sign On organization as read only to enforce SSO for any account.

Q: Why read only?

A: This is not required, but enables any account to be added to the organization without the ability to change any settings in this empty organization.

Q: What happens if a user is added to a second organization with SSO enabled?

A: The user becomes unable to sign in. Remove the user from at least one SSO organization or contact support to restore access.

Q: When configuring SAML, the verification test fails and a "FILE NOT FOUND" error appears. Why?

A: This occurs when SAML configuration is attempted using an MSP or Multi-Org Admin account. Perform SAML configuration using an account in the **Single Sign On organization**.