Configurazione di SSO con SAML per più organizzazioni e console MSP in Umbrella

Sommario

Introduzione

In questo documento viene descritto come configurare Single Sign-On (SSO) con SAML per le console MSP e per più organizzazioni in Umbrella.

Limitazioni e ambito di configurazione di SSO

- Questo articolo è specifico per l'integrazione di una console per più organizzazioni o MSP Umbrella con il provider SSO utilizzando SAML.
- In questo articolo non vengono fornite procedure generali di configurazione SAML. Per informazioni generali sulla configurazione, consultare la documentazione relativa all'abilitazione del servizio Single Sign-on.
- La configurazione SSO non è disponibile per gli account utente in STC, MSSP, PPPoV o in qualsiasi console che utilizzi l'accesso Cisco CEC. Gli utenti che accedono con Cisco CEC non possono utilizzare un altro provider SSO.

SSO per la console per più organizzazioni o MSP

Le console per più organizzazioni e MSP non supportano la configurazione SAML direttamente dalla console. L'SSO deve essere abilitato a livello di organizzazione figlio. Per abilitare l'SSO per un amministratore di console, attenersi alla seguente procedura:

1. Creare una nuova organizzazione figlio denominata Single Sign-On. L'organizzazione rimane vuota, ad eccezione degli utenti SSO.

2. Creare un nuovo utente nell'organizzazione Single Sign-On.
    - Questo utente è necessario per la configurazione SAML e deve inoltre esistere nel provider di identità.
    - Non è possibile configurare SAML utilizzando un account MSP o Multi-Org Admin a meno che tale account non venga aggiunto direttamente all'organizzazione figlio.
3. Se vengono visualizzati errori quali "File non trovato", verificare che l'utente attualmente connesso sia un amministratore elencato in Amministrazione > Account sul dashboard dell'organizzazione in cui si sta configurando l'SSO.
4. Accedere a Umbrella Dashboard come utente Single Sign-On.
5. Configurare SSO (SAML) nell'organizzazione Single Sign-On.
6. Invitare gli amministratori esistenti nell'organizzazione "Single Sign On" in sola lettura dal dashboard dell'organizzazione figlio.
    - Una volta accettati, questi utenti diventano membri sia della console di gestione che della singola organizzazione.
    - Questi utenti devono ora accedere tramite SSO e non utilizzare più una password dell'account.

Avviso: Non aggiungere un utente a più di un'organizzazione figlio abilitata per SSO. Se un utente viene aggiunto a più organizzazioni figlio abilitate a SSO,

---

viene bloccato fuori dal dashboard finché un altro amministratore non rimuove l'utente dall'organizzazione abilitata a SSO aggiuntiva.

Domande frequenti

Q: È possibile utilizzare il proprio SSO se si dispone di un portale STC, MSSP o per i partner?

A: No. Devi utilizzare il portale per i partner Cisco IT Okta. L'accesso a Umbrella è determinato dal livello di accesso Okta. Gli account Okta revocati o disabilitati non dispongono dell'accesso Umbrella.

Q: L'SSO in un'organizzazione figlio si applica a tutti gli accessi per l'utente?

A: Sì. L'utente deve accedere tramite SSO e non può accedere ad alcuna organizzazione senza eseguire l'autenticazione con SSO.

Q: È possibile abilitare l'SSO su più organizzazioni figlio?

A: Sì; tuttavia, solo un'organizzazione figlio deve essere configurata per SSO. Aggiungere gli utenti all'organizzazione Single Sign-On in sola lettura per applicare l'SSO per qualsiasi account.

Q: Perché in sola lettura?

A: Non è necessario, ma consente di aggiungere qualsiasi account all'organizzazione senza la possibilità di modificare le impostazioni in questa organizzazione vuota.

Q: Cosa succede se un utente viene aggiunto a una seconda organizzazione con SSO abilitato?

A: L'utente non è più in grado di accedere. Rimuovere l'utente da almeno un'organizzazione SSO o contattare il supporto tecnico per ripristinare l'accesso.

Q: Quando si configura SAML, il test di verifica ha esito negativo e viene visualizzato un errore "FILE NOT FOUND" (FILE NON TROVATO). Perché?

A: Questo si verifica quando si tenta di eseguire la configurazione SAML utilizzando un account MSP o Multi-Org Admin. Eseguire la configurazione SAML utilizzando un account nell'organizzazione Single Sign-On.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).