Richiesta di autenticazione SAML Cisco Secure Client a ogni tentativo con Microsoft Entra ID SSO

Sommario

Problema

Cisco Secure Client (AnyConnect) integrato con Microsoft Entra ID per l'autenticazione SAML ha riscontrato più problemi relativi all'autenticazione che hanno causato l'interruzione della funzionalità Single Sign-On (SSO):

- Agli utenti veniva richiesta l'autenticazione per ogni tentativo di connessione VPN, anche quando nel browser era presente una sessione Entra ID attiva
- Il client stava avviando il browser incorporato al posto del browser esterno/di sistema, nonostante l'autenticazione del browser esterno fosse esplicitamente abilitata per SAML
- Gli utenti hanno riscontrato spesso l'errore: "Errore di autenticazione dovuto a un problema di reindirizzamento all'URL SSO"
- Il comportamento dell'SSO era cambiato rispetto al precedente stato di funzionamento in cui gli utenti potevano connettersi alla VPN semplicemente facendo clic su Connetti senza richieste di autenticazione

Ambiente

- Prodotto: Cisco Secure Client (AnyConnect)
- Tecnologia: VPN ad accesso sicuro con autenticazione SAML
- Provider di identità: ID Entra Microsoft (Azure AD)
- Metodo di autenticazione: Integrazione SAML SSO
- Autenticazione del browser esterno abilitata per SAML

Risoluzione

La risoluzione ha comportato la risoluzione dei problemi di stato di aggiunta del dispositivo Azure AD sottostante e di configurazione del browser che hanno causato i problemi di autenticazione:

Passaggio 1: Esegui diagnosi stato di aggiunta ad Azure AD

Eseguire il comando seguente per verificare lo stato corrente di aggiunta ad Azure AD del dispositivo interessato:

```
dsregcmd /status
```

Controllare l'output per verificare se il dispositivo mostra AzureAdJoined = NO, che indica uno stato di aggiunta ad Azure AD non corretto.

Passaggio 2: Correggi stato di aggiunta ad Azure AD

Eseguire il comando dsregcmd per correggere lo stato di partecipazione ad Azure AD nel dispositivo interessato. Dopo aver eseguito le operazioni dsregcmd appropriate,

```
dsregcmd /status
dsregcmd /leave
dsregcmd /join`
```

Verificare che lo stato del dispositivo indichi:

```
AzureAdJoined = YES
```

Questa correzione risolve il problema dello stato di autenticazione sottostante che stava causando la richiesta delle credenziali da parte di Cisco Secure Client su ciascuna connessione.

Passaggio 3: Reimposta applicazioni browser predefinite

Per risolvere il problema relativo al comportamento del browser esterno rispetto a quello del browser incorporato:

Ripristinare le impostazioni predefinite delle applicazioni del dispositivo per garantire che Cisco Secure Client avvii correttamente il browser esterno/di sistema per l'autenticazione SAML anziché il browser incorporato.

```
Settings → Apps → Default apps → Reset
```

Passaggio 4: Verifica

Dopo aver implementato le modifiche precedenti, verificare i seguenti comportamenti:

- Cisco Secure Client non richiede più l'autenticazione tramite password o Windows Hello su ciascuna connessione VPN
- Il client avvia correttamente il browser esterno per l'autenticazione SAML anziché il browser incorporato
- La funzionalità SSO viene ripristinata, consentendo agli utenti di connettersi senza più richieste di autenticazione quando esiste una sessione Entra ID attiva
- L'errore "Errore di autenticazione dovuto a un problema di reindirizzamento all'URL SSO" non si verifica più

Causa

I problemi di autenticazione sono stati causati da uno stato di partecipazione ad Azure AD non corretto nel dispositivo interessato, in cui il dispositivo visualizzava AzureAdJoined = NO anziché lo stato AzureAdJoined = YES richiesto. Questo stato di join non corretto ha impedito la convalida del token SSO e ha forzato Cisco Secure Client a richiedere l'autenticazione per ogni tentativo di connessione.

Inoltre, le impostazioni predefinite dell'applicazione del dispositivo non sono state configurate correttamente, causando l'avvio del browser incorporato da parte di Cisco Secure Client anziché del browser esterno per l'autenticazione SAML, nonostante l'abilitazione dell'impostazione del browser esterno nella configurazione del client.

Contenuto correlato

- Supporto tecnico Cisco e download

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).