Solicitud de autenticación SAML de Cisco Secure Client en cada intento con SSO de Microsoft Entra ID

Contenido

Problema

Cisco Secure Client (AnyConnect) integrado con Microsoft Entra ID para la autenticación SAML estaba experimentando varios problemas relacionados con la autenticación que afectaron a la funcionalidad de inicio de sesión único (SSO):

- Se solicitaba a los usuarios la autenticación en cada intento de conexión VPN, incluso cuando existía una sesión de Entra ID activa en el navegador
- El cliente estaba iniciando el explorador integrado en lugar del explorador externo/del sistema, a pesar de que la autenticación del explorador externo estaba habilitada explícitamente para SAML
- Los usuarios encontraron con frecuencia el error: "Error de autenticación debido a un problema con el redireccionamiento a la URL de SSO"
- El comportamiento de SSO ha cambiado con respecto al estado de funcionamiento anterior, en el que los usuarios se podían conectar a VPN simplemente haciendo clic en Conectar sin mensajes de autenticación

Entorno

- Producto: Cisco Secure Client (AnyConnect)
- Tecnología: VPN de acceso seguro con autenticación SAML
- Proveedor de identidad: ID de Microsoft Entry (Azure AD)
- método de autentificación: Integración de SSO de SAML

- Autenticación de explorador externo habilitada para SAML

Resolución

La resolución implicaba la resolución de los problemas de configuración de estado y explorador de unión del dispositivo Azure AD subyacente que causaban los problemas de autenticación:

Paso 1: Diagnosticar estado de unión a Azure AD

Ejecute el siguiente comando para comprobar el estado actual de unión a Azure AD del dispositivo afectado:

```
dsregcmd /status
```

Revise el resultado para identificar si el dispositivo muestra AzureAdJoined = NO, que indica un estado de unión de Azure AD incorrecto.

Paso 2: Estado de unión a Azure AD correcto

Ejecute el comando dsregcmd para corregir el estado de unión de Azure AD en el dispositivo afectado. Después de ejecutar las operaciones dsregcmd apropiadas,

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

Verifique que el estado del dispositivo muestre:

```
AzureAdJoined = YES
```

Esta corrección resuelve el problema de estado de autenticación subyacente que causaba que Cisco Secure Client solicitara credenciales en cada conexión.

Paso 3: Restablecer aplicaciones de explorador predeterminadas

Para solucionar el problema del navegador externo frente al comportamiento del navegador integrado:

Restablezca la configuración predeterminada de las aplicaciones del dispositivo para asegurarse de que Cisco Secure Client inicia correctamente el explorador externo/del sistema para la autenticación SAML en lugar del explorador integrado.

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

Paso 4: Verificación

Después de implementar los cambios anteriores, verifique los siguientes comportamientos:

- Cisco Secure Client ya no solicita contraseña ni autenticación de Windows Hello en cada conexión VPN
- El cliente inicia correctamente el explorador externo para la autenticación SAML en lugar del explorador integrado
- Se restaura la funcionalidad de SSO, lo que permite a los usuarios conectarse sin peticiones de autenticación repetidas cuando existe una sesión de Entra ID activa
- Ya no se produce el error "Error de autenticación debido a un problema con el redireccionamiento a la URL de SSO"

Causa

Los problemas de autenticación fueron causados por un estado de unión a Azure AD incorrecto en el dispositivo afectado, donde el dispositivo mostraba AzureAdJoined = NO en lugar del estado

AzureAdJoined = YES requerido. Este estado de unión incorrecto impidió una validación de token de SSO adecuada y obligó a Cisco Secure Client a solicitar autenticación en cada intento de conexión.

Además, la configuración predeterminada de la aplicación del dispositivo estaba mal configurada, lo que provocó que Cisco Secure Client iniciara el explorador integrado en lugar del explorador externo para la autenticación SAML, a pesar de que la configuración del explorador externo estaba habilitada en la configuración del cliente.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).