Cisco Secure Access - Renovación de certificado SAML con IDP(Microsoft Entra ID)

Contenido

Problema

Cuando se utiliza la autenticación SSO con Microsoft Entra ID SAML como proveedor de identidad (IdP) para Cisco Secure Access, los certificados de verificación SAML están a punto de caducar.

Las organizaciones deben comprender el proceso de renovación de certificados correcto para evitar interrupciones en la autenticación y determinar si se debe crear una nueva configuración de inicio de sesión único en Secure Access al renovar los certificados SAML de ID de entrada.

Entorno

- Cisco Secure Access con autenticación SSO configurada
- Microsoft Entra ID SAML como proveedor de identidad
- Certificados de verificación SAML con fechas de vencimiento próximas
- Configuración de SSO existente para SWG (gateway web seguro) y ZTNA (acceso a red sin confianza)

Resolución

Paso 1 - Detectar renovación de certificados

- El proveedor de identidad (IdP) renueva o gira su certificado de firma SAML.
- Esto suele suceder cuando el certificado se acerca a la expiración.

Paso 2 - Obtener metadatos actualizados de IdP

- Exporte el nuevo XML de metadatos IdP o el nuevo certificado de firma desde el IdP.

Paso 3 - Verificar cambio de certificado

Confirme que el certificado ha cambiado realmente.

Comprobar:

- Huella digital
- Fecha de vencimiento
- Emisor

Esto garantiza que el SP esté actualizado con el certificado correcto

Actualizar configuración del proveedor de servicios

Inicie sesión en el panel de Cisco Secure Access y actualice la configuración.

Desplácese hasta Conectar: usuario y grupos.

Haga clic en Gestión de configuración

En Autenticación de SSO: edite el perfil de autenticación de SSO; cargue el archivo de metadatos mediante el nuevo certificado o cargue el certificado si se realiza una configuración manual.

Paso 5: Guardar y aplicar la configuración

- Guardar la configuración actualizada

Paso 6 - Validación de la Autenticación SSO

Realice una prueba de inicio de sesión SSO.

Causa

El proveedor de servicios utiliza el certificado de firma del proveedor de identidad (IdP) para comprobar la firma de afirmación SAML y, cuando el IdP renueva el certificado, el SP debe actualizar su certificado de confianza para continuar validando las solicitudes de autenticación

Contenido relacionado

- Cisco Secure Access - Descripción general y configuración de SAML Single Sign-On
- Configuración de SSO de SAML para Cisco Secure Access (ejemplo de Microsoft Entra ID)
- 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).