Utilizar URL de metadatos fijos de Umbrella para la autenticación SAML de SWG

Contenido

Introducción

Este documento describe cómo utilizar la URL de metadatos fijos de Umbrella para la autenticación SAML de Secure Web Gateway (SWG).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Umbrella SWG.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

URL de metadatos fijos

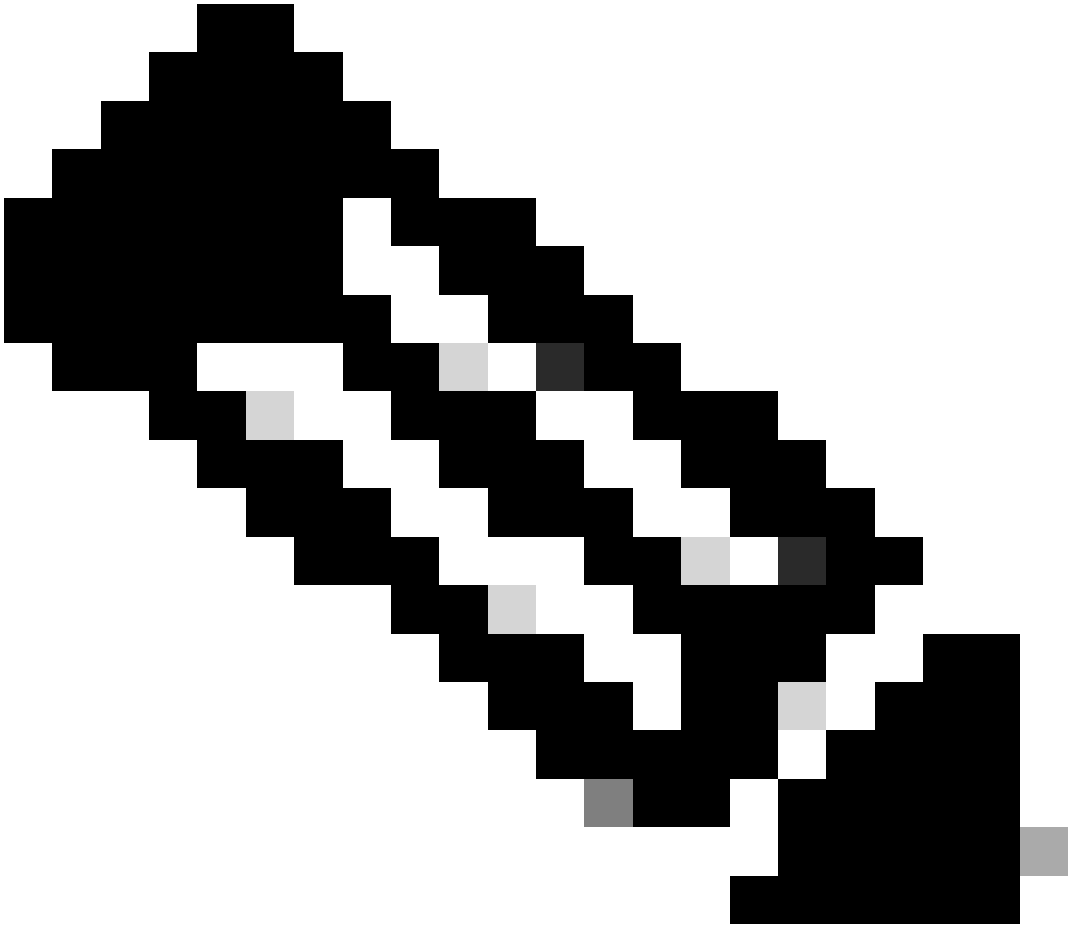
Al utilizar la autenticación SAML para Umbrella SWG, ofrecemos dos opciones para importar nuestra información de certificado a su proveedor de identidad (IdP). Esto es necesario para aquellos IdPs que verifican nuestro certificado de firma de solicitud.

1. Configuración automática mediante URL de metadatos fijos:

https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. Importación manual de nuestro nuevo certificado de firma. Esto debe hacerse cada año a medida que se sustituya el certificado.

La primera opción es ahora el método de configuración preferido para proveedores de identidad (IdP) que admiten actualizaciones automáticas de metadatos basadas en URL. Esto incluye ID populares como Microsoft ADFS y Ping Identity. El beneficio es que el IdP importa automáticamente nuestro nuevo certificado cada año sin intervención manual.



Nota: Muchos IDPs no realizan la validación de las firmas de solicitud SAML y por lo tanto estos pasos no son requeridos. En caso de duda, póngase en contacto con su proveedor de identidades para obtener confirmación.

Requirements

Requisitos para acceder a la URL de metadatos

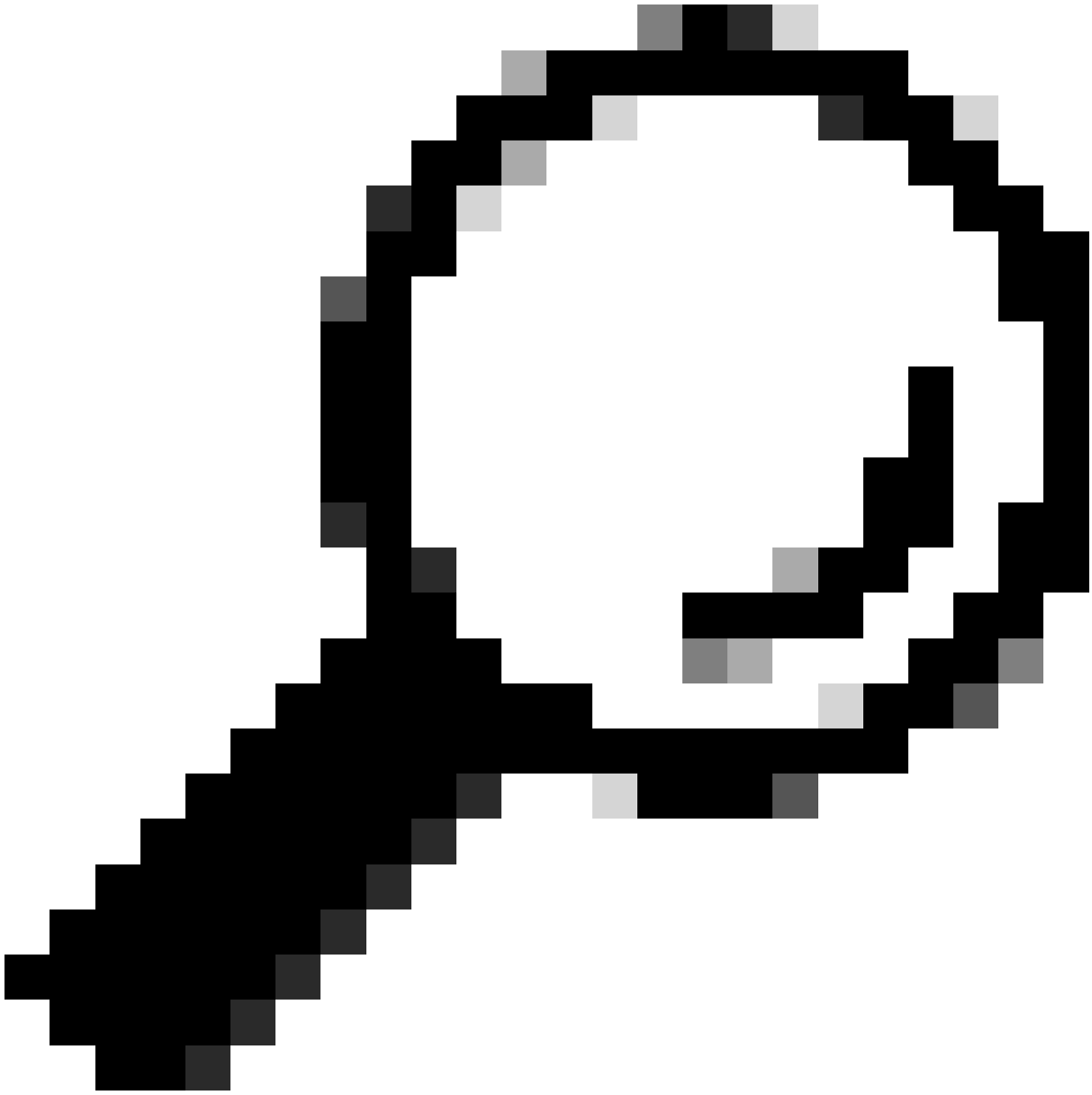
- IdP que admite actualizaciones automáticas de metadatos del proveedor de servicios desde

URL (como ADFS, Ping)
- Su plataforma IdP debe poder acceder a nuestra URL de metadatos así como a las URL asociadas de la Autoridad de Certificación
- Su plataforma IdP también debe poder acceder a las URL de la Autoridad de Certificación para el propio certificado
- Su plataforma IdP debe soportar TLS 1.2 para conectarse a la URL de metadatos de forma segura. Si la aplicación IDP utiliza .NET framework 4.6.1 o anterior, esto podría requerir alguna configuración adicional según la documentación de Microsoft.

Ejemplo: Microsoft ADFS

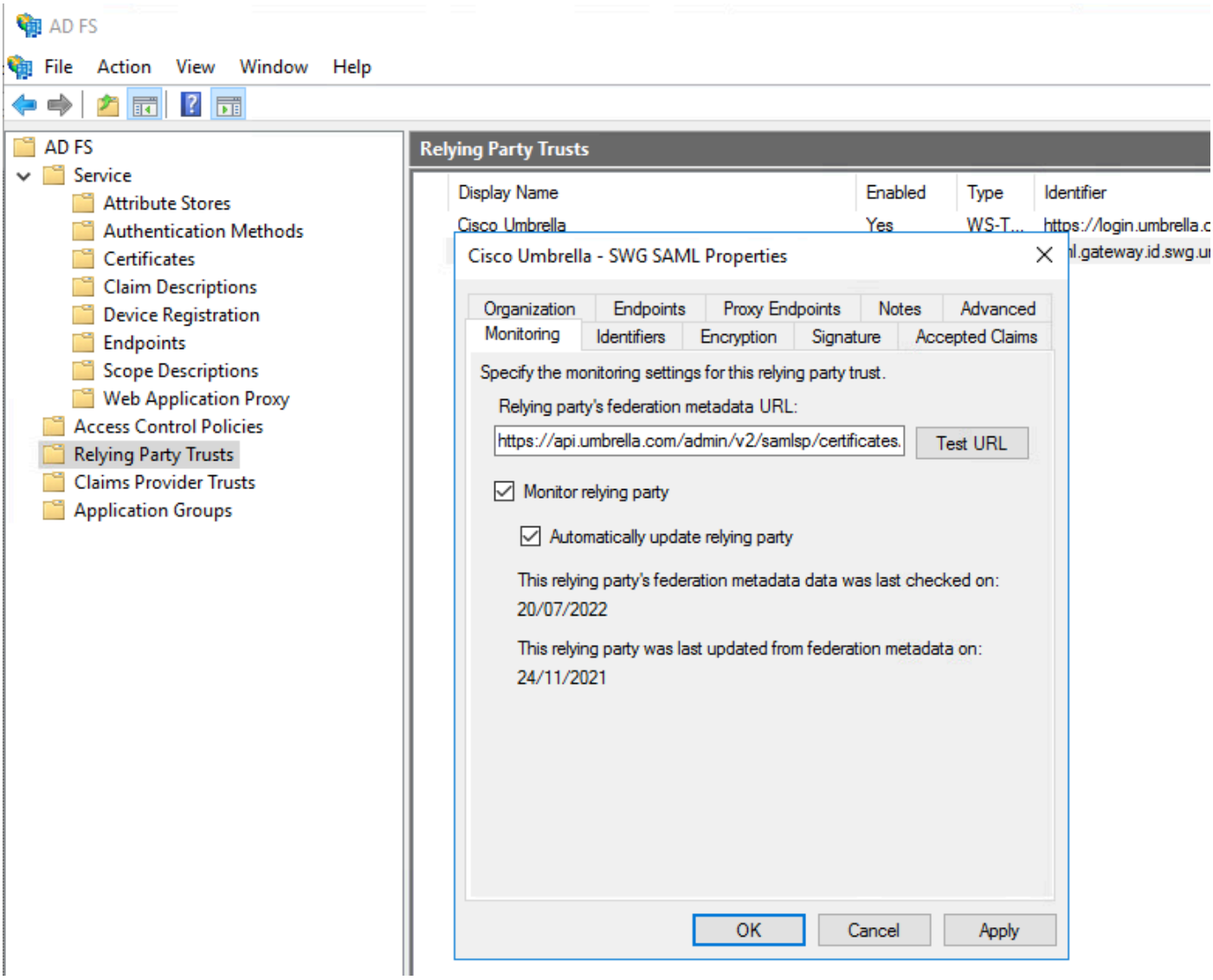
La URL de metadatos fijos se puede configurar editando la configuración de Confianza del usuario de confianza para Umbrella:

1. Vaya a la pestaña Monitoring e introduzca la URL de metadatos.
2. Seleccione Supervisar usuario de confianza y Actualizar automáticamente usuario de confianza.



Consejo: Seleccione el botón Probar URL para verificar que ADFS se pone en contacto con la URL correctamente.

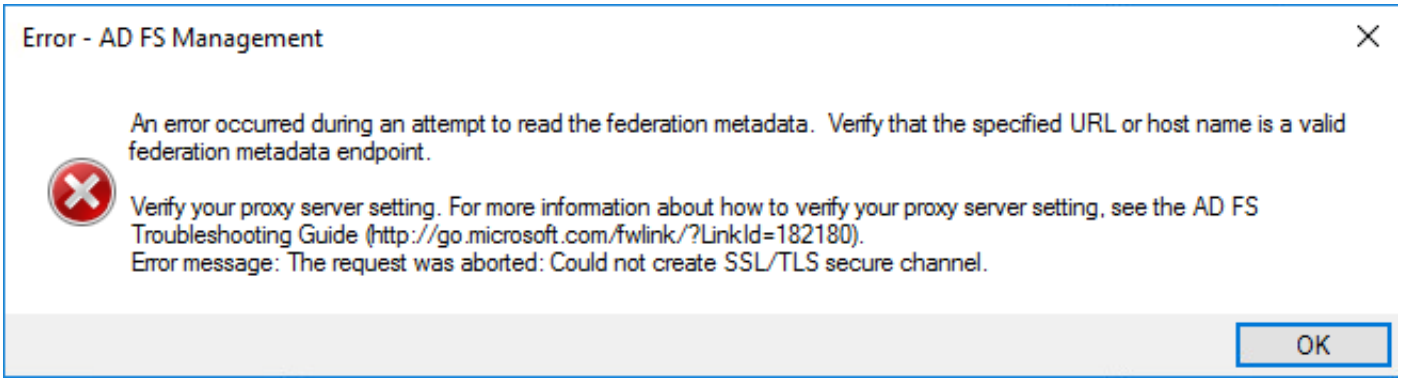
3. Seleccione Aplicar.



ADFS_ConfianzaConfianza.png

Solución de errores

Si recibe el mensaje de error "Se ha producido un error al intentar leer los metadatos de federación. Compruebe que la dirección URL o el nombre de host especificados son un "extremo de metadatos de federación válido" cuando pruebe la dirección URL; esto suele indicar que se requiere un cambio en el Registro para establecer que la versión de .NET Framework utilice cifrado seguro y admita TLS 1.2.



ADFSmetadata_TLS_error.png

Microsoft publica todos los detalles sobre estos cambios en la sección .Net Framework de la documentación de Microsoft.

Normalmente, sin embargo, esto requiere la creación de esta clave y, a continuación, cerrar y volver a abrir la consola de administración de ADFS:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

Limitación: Función EntityID específica de la organización

Si utiliza la función EntityID específica de la organización de Umbrella SAML, no debe utilizar el mecanismo de actualización de metadatos basado en URL. La ID de entidad específica de la organización solo se aplica si tiene varias organizaciones de Umbrella vinculadas al mismo proveedor de identidad. En este escenario, debe agregar manualmente el certificado a cada configuración de IDP.

Importación manual de certificados (alternativa)

Si su IdP no soporta actualizaciones basadas en URL, debe importar manualmente el nuevo certificado de firma de solicitud de Umbrella cada año a su Proveedor de Identidad.

- El certificado se proporciona en nuestro portal de anuncios cada año poco antes de la fecha de vencimiento. Suscríbase al portal para recibir notificaciones
- Agregue el nuevo certificado a la lista de certificados de proveedor de servicios/persona de confianza en su IdP.
    - NO elimine ningún certificado actual. Umbrella sigue firmando con el certificado antiguo hasta el momento de la expiración.
- Si su IdP no contiene la capacidad de importar un certificado de Proveedor de Servicios/Parte Confiadora, esto es una fuerte indicación de que no valida las solicitudes SAML, y no se requiere ninguna otra acción. Póngase en contacto con su proveedor de IdP para confirmar.

Si detecta un error "UPN no está configurado" después de importar el nuevo certificado, esto indica que se ha producido un error. Consulte este artículo para la resolución de problemas: SWG SAML - Error de UPN no configurado

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).