Configuración de la Autenticación Externa SSO de Microsoft Entra ID para DMP

Contenido

Introducción

Este documento describe cómo configurar el inicio de sesión único de Microsoft Entry ID para autenticarse en el portal Cisco Domain Protection.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

- Protección de dominio de Cisco
- ID de Microsoft Entra
- Certificados SSL X.509 con firma automática o CA firmada (opcional) en formato PEM

Componentes Utilizados

- Acceso de administrador a Cisco Domain Protection
- Acceso de administrador al centro de administración con Microsoft Entra ID

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.

Antecedentes

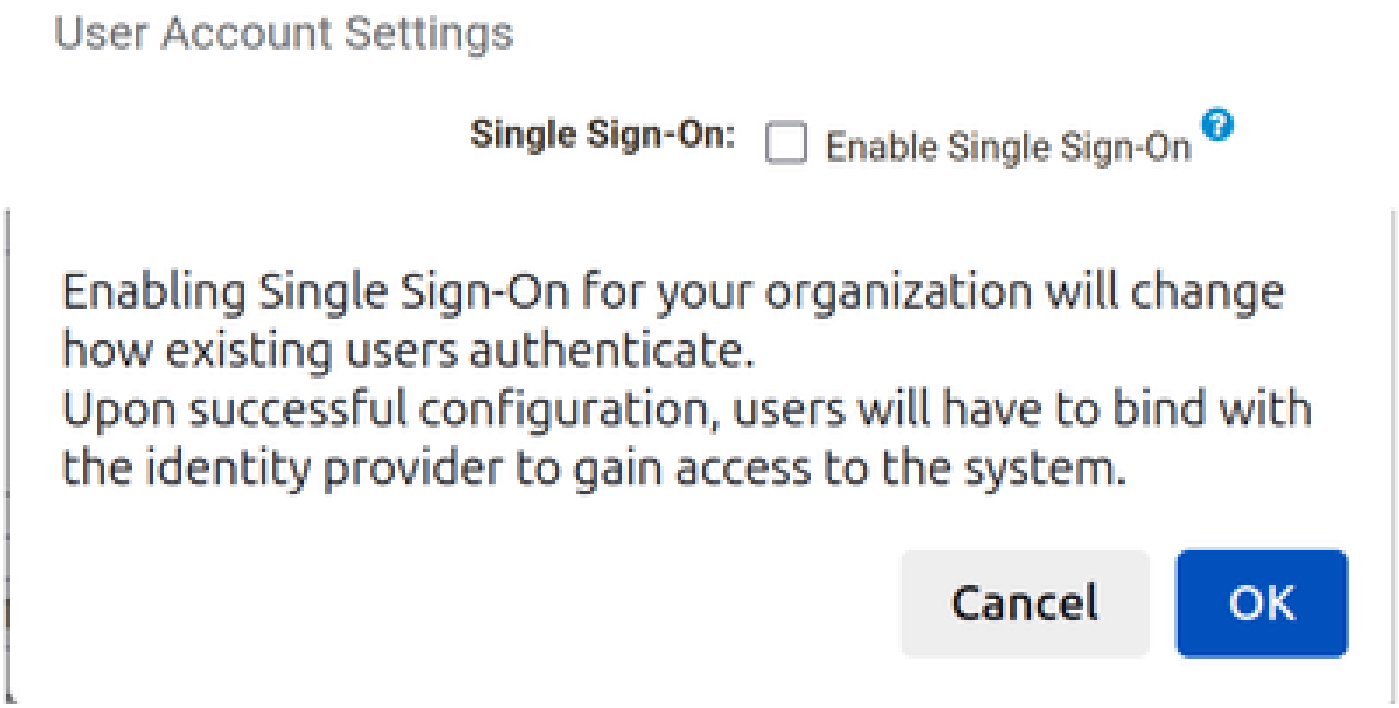
- Cisco Domain Protection habilita el inicio de sesión SSO para usuarios finales a través del protocolo SAML 2.0.
- Microsoft Entra SSO permite y controla el acceso a sus aplicaciones de software como servicio (SaaS), aplicaciones en la nube o aplicaciones en las instalaciones desde cualquier lugar con el inicio de sesión único.
- Cisco Domain Protection se puede establecer como una aplicación de identidad administrada conectada a Microsoft Entry con métodos de autenticación que incluyen autenticación de varios factores, ya que la autenticación de solo contraseña no es segura ni recomendada.
- SAML es un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones sin problemas después de iniciar sesión en una de esas aplicaciones.
- Para obtener más información sobre SAML, consulte: ¿Qué es SAML?

Configurar

Protección de dominios de Cisco (parte 1)

1. Inicie sesión en el portal de administración de Cisco Domain Protection y navegue hasta Admin > Organization. Haga clic en el botón Edit Organization Details, como se muestra en la imagen:

2. Navegue hasta la sección Configuración de la cuenta de usuario y haga clic en la casilla de verificación EnableSingle Sign-On. Aparece un mensaje como se muestra en la imagen:

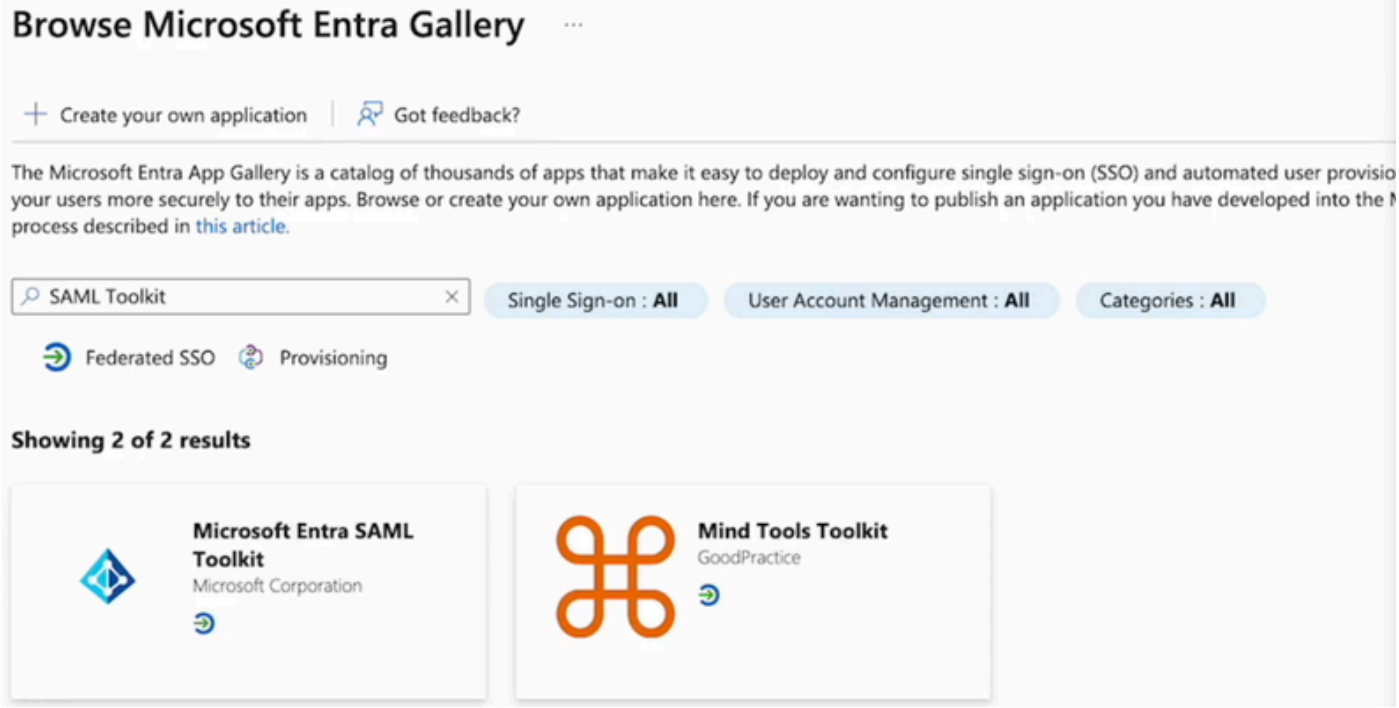


3. Haga clic en el botón Aceptar y copie los parámetros de ID de entidad y URL de servicio de consumidor de aserción (ACS). Estos parámetros se deben utilizar en la autenticación SAML básica de Microsoft Entra ID. Vuelva más tarde para configurar los parámetros Name Identifier Format, SAML 2.0 Endpoint y Public Certificate.

- ID de entidad: dmp.cisco.com
- URL de servicio de consumidor de aserción:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

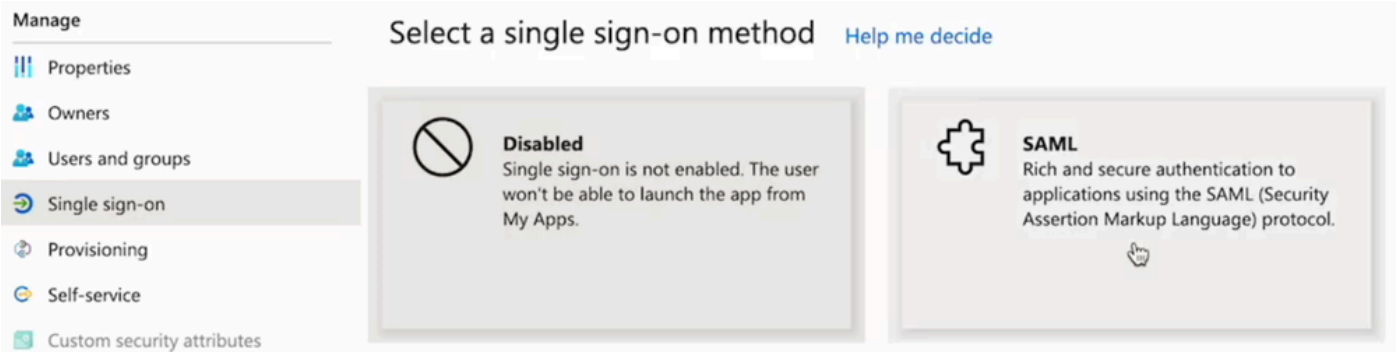
ID de Microsoft Entra

1. Navegue hasta Microsoft Entra ID admin center y haga clic en el botón Add. Seleccione Enterprise Application, y busque Microsoft Entra SAML Toolkit, como se muestra en la imagen:



2. Asígnele un nombre con un valor significativo y haga clic en Crear. Por ejemplo, Inicio de sesión en Protección de dominio.

3. Desplácese al panel lateral izquierdo, en la sección Gestionar. Haga clic en Single sign-on y seleccione SAML.



4. En el panel Configuración básica de SAML, haga clic en Editar y rellene los parámetros:

- Identificador (ID de entidad): dmp.cisco.com
- URL de respuesta (URL de servicio de consumidor de afirmación): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- URL de inicio de sesión: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Click Save.

5. En el panel Atributos y reclamaciones, haga clic en Editar.

En Reclamación necesaria, haga clic en la reclamación Identificador de usuario único (ID de nombre) para editarla.

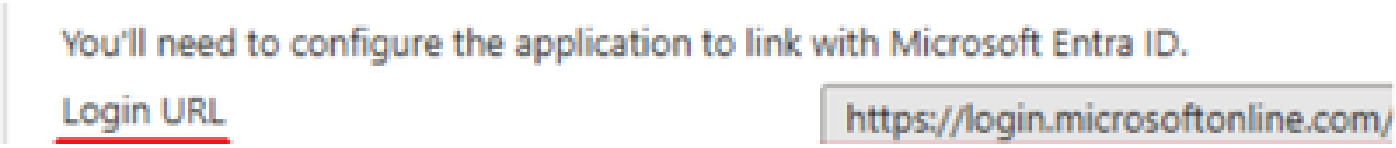
- Establezca el campo del atributo Source en user.userprincipalname. Esto supone que el valor de user.userprincipalname representa una dirección de correo electrónico válida. Si no es así, establezca Source en user.primaryautoritativeemail.
- En el panel Reclamaciones adicionales, haga clic en Editar y cree las asignaciones entre las propiedades de usuario de Microsoft Entry ID y los atributos SAML.

Nombre	Espacio de nombres	Atributo de origen
correo electrónico	Sin valor	user.userprincipalname
nombre	Sin valor	user.givenname
apellido	Sin valor	user.surname

Asegúrese de borrar el campo Namespace para cada reclamación, como se muestra a continuación:

6. Una vez cumplimentadas las secciones Atributos y Reclamaciones, se cumplimenta la última sección Certificado de Firma SAML.

- Guarde la URL de inicio de sesión.

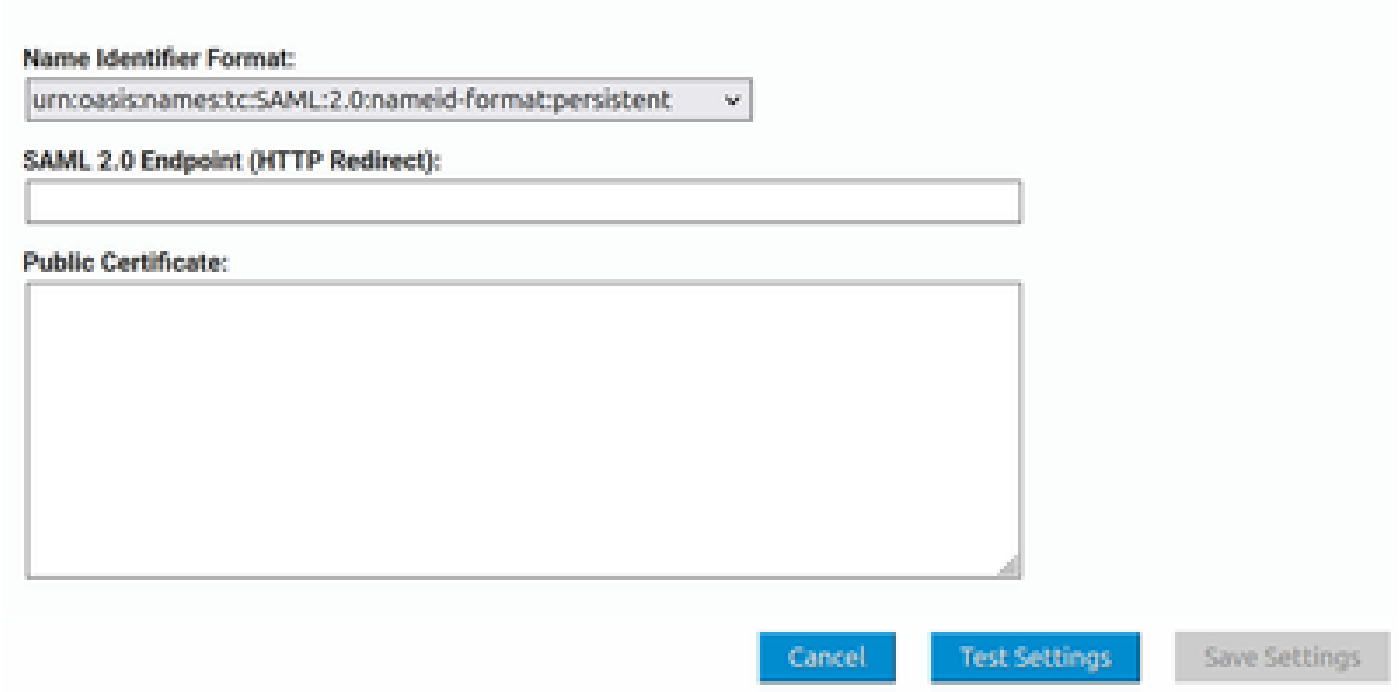


- Guarde el certificado (Base64).

Protección de dominios de Cisco (parte 2)

Vuelva a la sección Cisco Domain Protection > Enable Single Sign-On.

- Formato de identificador de nombre: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- Terminal SAML 2.0 (redirección HTTP): URL de inicio de sesión proporcionada por Microsoft Entra ID
- Certificado público: Certificado (Base64) proporcionado por Microsoft Entra ID



Verificación

Haga clic en Test Settings. Le redirigirá a la página de inicio de sesión de su proveedor de identidad. Inicie sesión con sus credenciales de SSO.

Después de iniciar sesión correctamente, puede cerrar la ventana. Haga clic en Save Settings.

Troubleshoot

```
Error - Error parsing X509 certificate
```

- Asegúrese de que el certificado está en Base64.

```
Error - Please enter a valid URL
```

- Asegúrese de que la URL de inicio de sesión proporcionada por Microsoft Entry ID es correcta.

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).