Configuración de la autenticación externa SSO de Microsoft Entra ID para CRES

Contenido

Introducción

Este documento describe cómo configurar Microsoft Entra ID Single Sign-on para autenticarse en Cisco Secure Email Encryption Service.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicio de cifrado de correo electrónico seguro (sobre registrado)
- ID de Microsoft Entra
- Certificados SSL X.509 con firma automática o CA firmada (opcional) en formato PEM

Componentes Utilizados

- Acceso de administrador al servicio de cifrado de correo electrónico seguro (sobre registrado)
- 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.

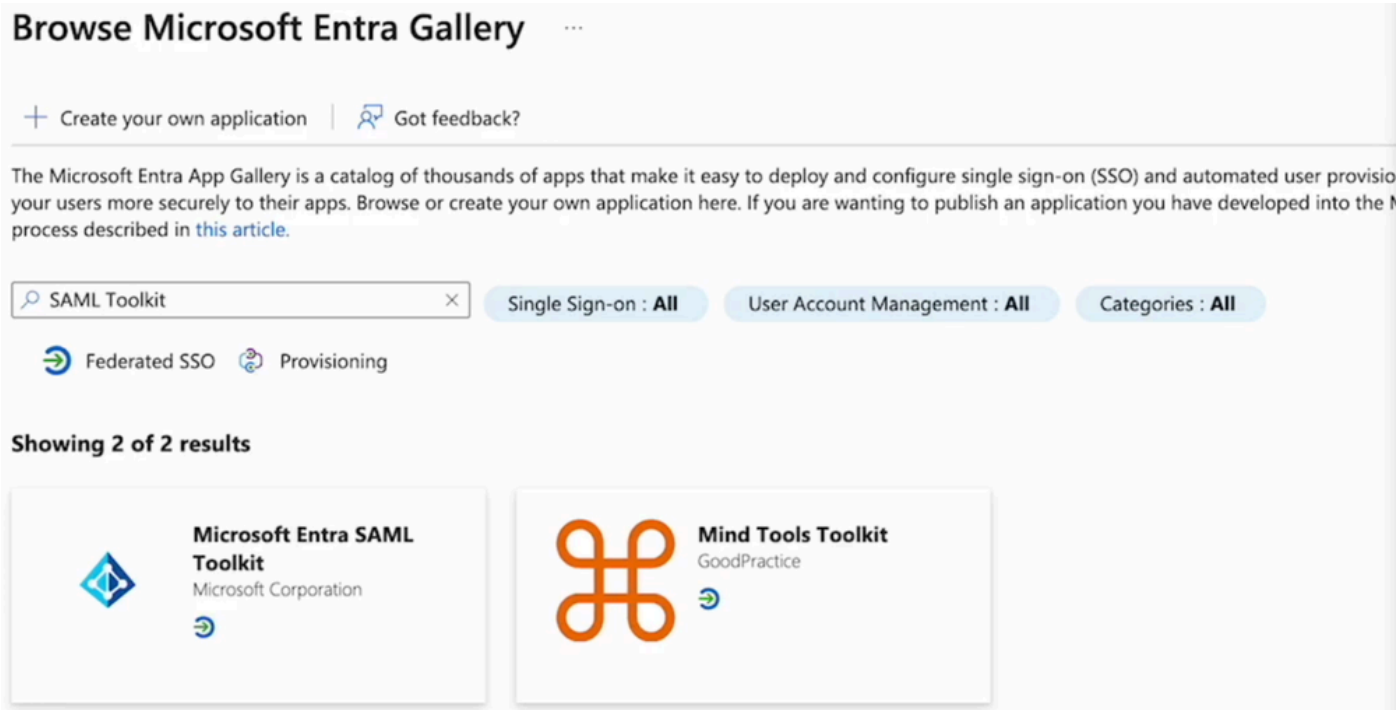
Antecedentes

- El sobre registrado permite iniciar sesión en SSO para los usuarios finales que utilizan SAML.
- 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.
- El sobre registrado 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

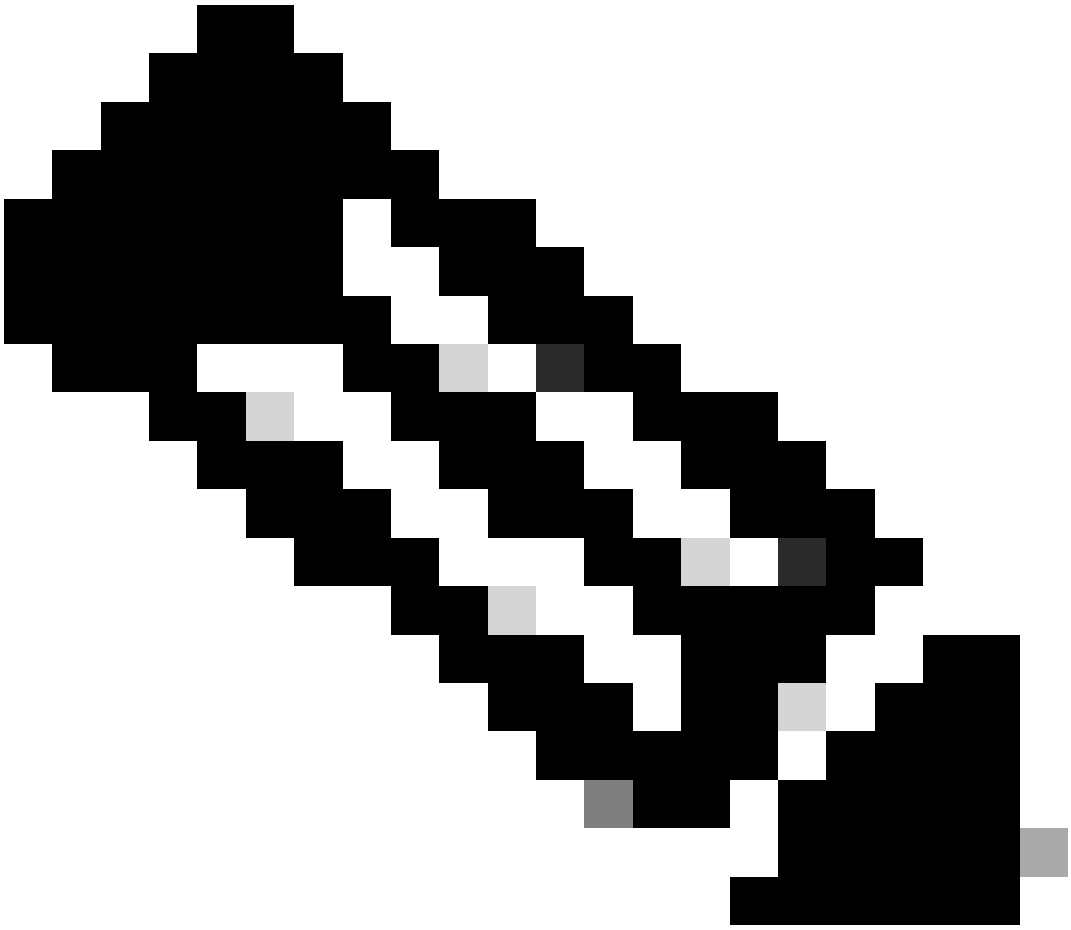
ID de Microsoft Entra

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



Examinar la Galería de Microsoft Entra

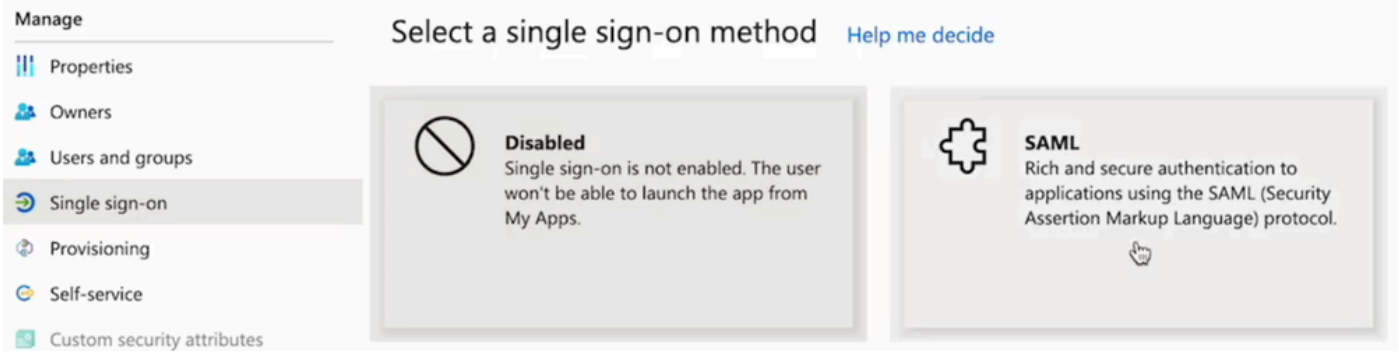
2. Asígnele un nombre con un valor significativo y haga clic en Crear. Por ejemplo, Inicio de sesión único de CRES.



Nota: Para permitir que todos los usuarios inicien sesión en el portal de CRES, debe deshabilitar manualmente Asignación necesaria en Propiedades del kit de herramientas de inicio de sesión de CRES (SAML)y, para Asignación necesaria, seleccionar No.

---

3. Desplácese hasta el panel izquierdo, en la sección Administrar, haga clic en Inicio de sesión único y seleccione SAML.



4. En el panel Configuración básica de SAML, haga clic en Editar y rellene los atributos de la siguiente manera:

- Identificador (Id. de entidad): https://res.cisco.com/
- URL de respuesta (URL de servicio al consumidor de aserción): https://res.cisco.com/websafe/ssourl
- URL de inicio de sesión: https://res.cisco.com/websafe/ssourl
- 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 de 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.

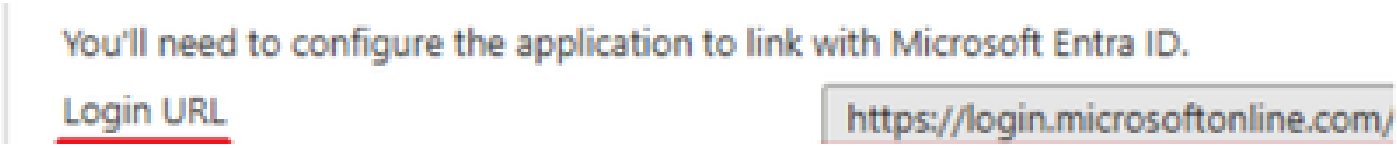
Nombre	Espacio de nombres	Atributo de origen
correo electrónico	Sin valor	user.userprincipalname
nombre	Sin valor	user.givenname
apellido	Sin valor	user.surname

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 los siguientes valores tal y como se requieren en el

portal de CRES:

- Guarde la URL de inicio de sesión.



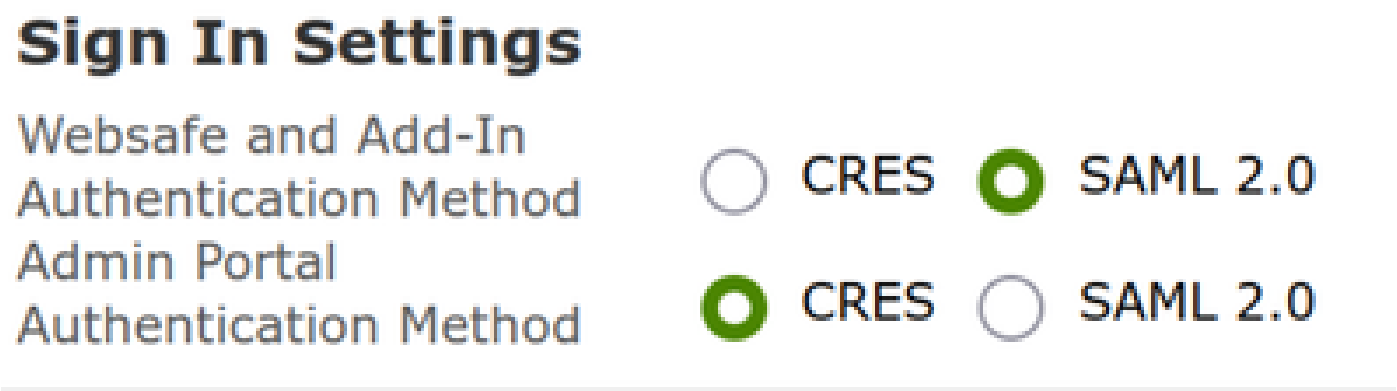
- Seleccione el enlace Descarga del certificado (Base64).

Servicio Cisco Email Encryption

1. Inicie sesión en el portal de la organización de Secure Email Encryption Service como administrador.

2. En la pestaña Cuentas, seleccione la pestaña Administrar cuentas y haga clic en su Número de cuenta.

3. En la pestaña Detalles, desplácese al Método de Autenticación y seleccione SAML 2.0.



4.- Rellenar los atributos de la siguiente manera:

- Nombre alternativo de atributo de correo electrónico SSO: correo electrónico
- ID de entidad del proveedor de servicios SSO*: https://res.cisco.com/
- URL de servicio al cliente de SSO*: Este enlace lo proporciona Entra ID, en
- URL de cierre de sesión de SSO: déjelo en blanco

5.- Haga clic en Activar SAML.

Verificación

Aparece una nueva ventana que confirma que, tras un inicio de sesión correcto, se ha activado la

autenticación SAML. Haga clic en Siguiente. Le redirige 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. Click Save.

Troubleshoot

Si la ventana no le ha redirigido a la página de inicio de sesión de su proveedor de identidad, se devuelve un rastreo de retorno que le proporciona el error. Revise los Atributos y reclamaciones, asegúrese de que esté configurado con el mismo nombre que en la sección Método de autenticación de CRES. La dirección de correo electrónico del usuario utilizada en el inicio de sesión de SAML debe coincidir con la dirección de correo electrónico de CRES. No utilice alias.

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).