Configurer l'authentification externe SSO Microsoft Entra ID pour CRES

Table des matières

Introduction

Ce document décrit comment configurer l'authentification unique Microsoft Entra ID pour l'authentification auprès du service Cisco Secure Email Encryption Service.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Service de cryptage sécurisé des e-mails (recommandé)
- ID d'entrée Microsoft
- Certificats SSL X.509 auto-signés ou CA signés (facultatif) au format PEM

Composants utilisés

- Accès administrateur au service de cryptage de messagerie électronique sécurisé (recommandé)
- Accès administrateur au centre d'administration Microsoft Entra ID

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

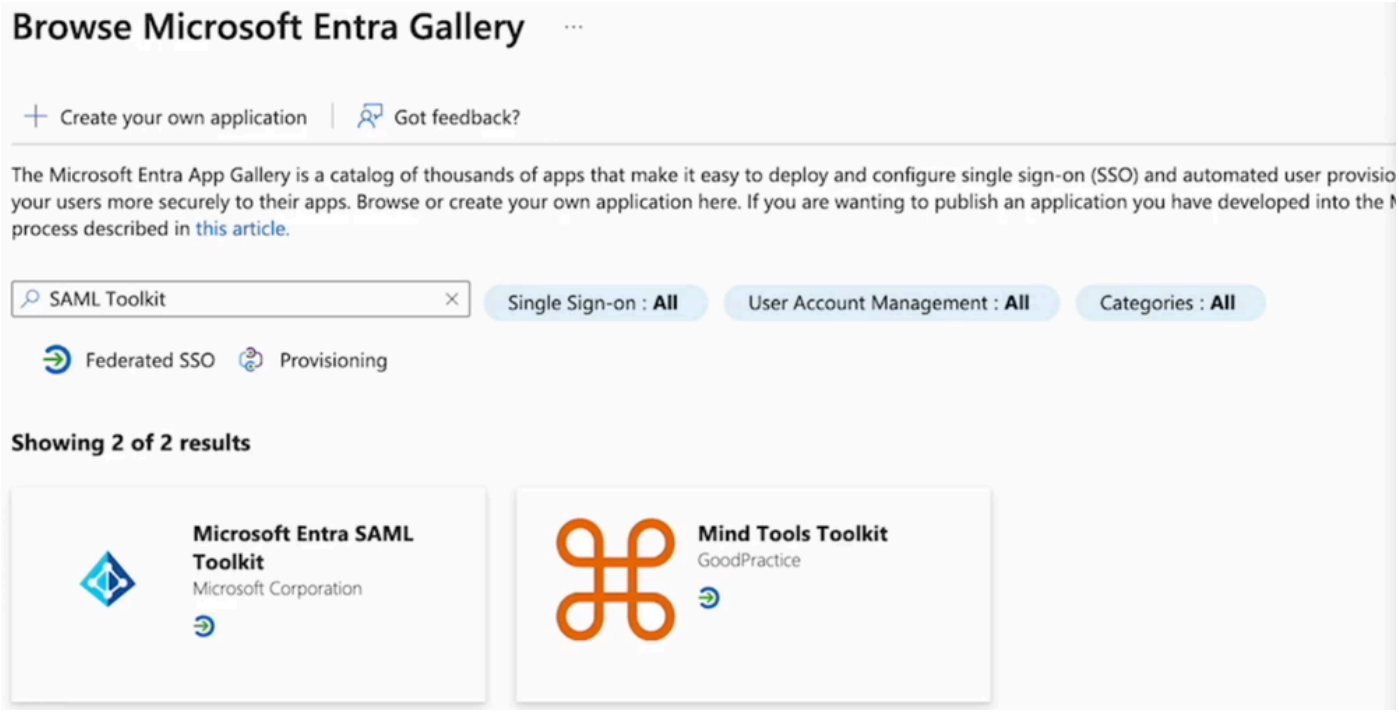
Informations générales

- Le recommandé permet aux utilisateurs finaux qui utilisent SAML d'ouvrir une session SSO.
- Microsoft Entra SSO permet et contrôle l'accès à vos applications SaaS (Software as a Service), applications cloud ou applications sur site depuis n'importe quel endroit avec l'authentification unique.
- Le recommandé peut être défini comme une application d'identité gérée connectée à Microsoft Entra avec des méthodes d'authentification qui incluent l'authentification multifacteur car l'authentification par mot de passe uniquement n'est ni sûre ni recommandée.
- SAML est un format de données standard ouvert basé sur XML qui permet aux administrateurs d'accéder à un ensemble défini d'applications de manière transparente après la connexion à l'une de ces applications.
- Pour en savoir plus sur le langage SAML, reportez-vous à : Qu'est-ce que SAML ?

Configurer

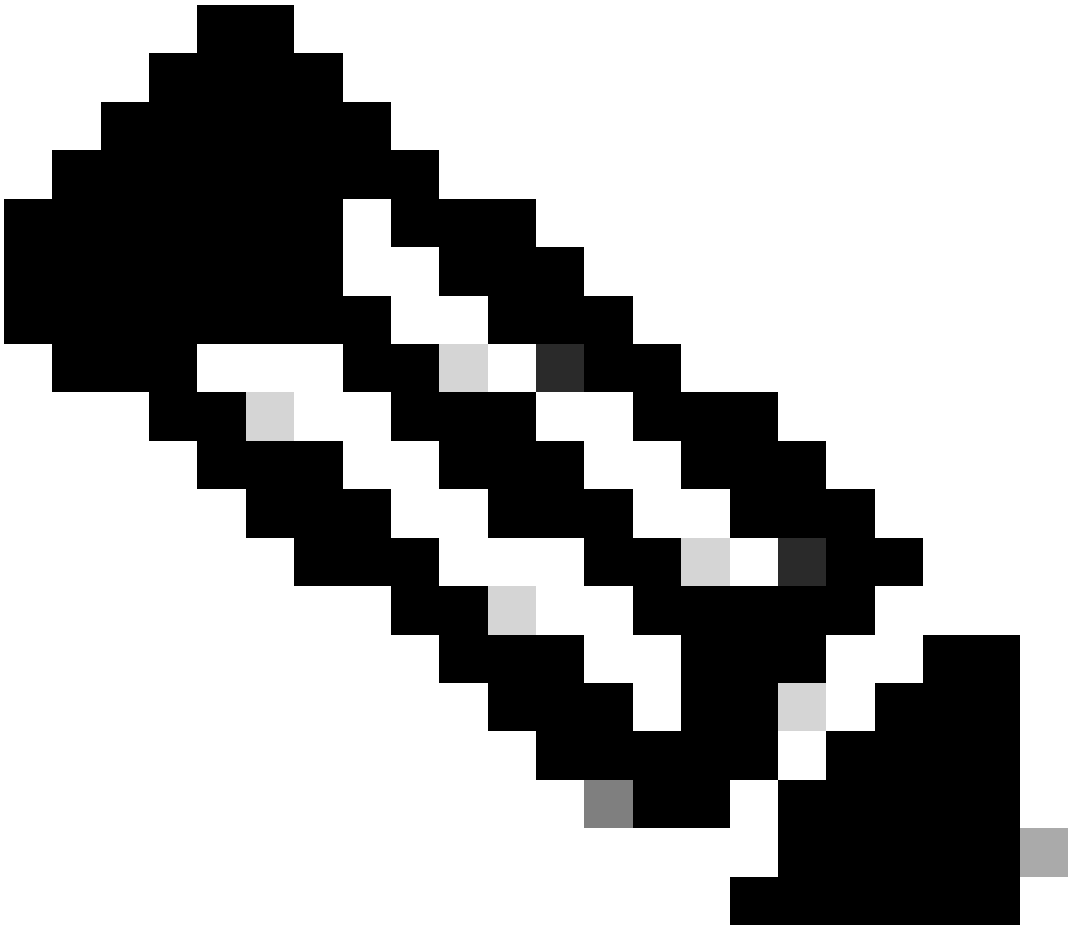
ID d'entrée Microsoft

1. Accédez au Centre d'administration Microsoft Entra ID et cliquez sur le bouton Ajouter. Sélectionnez Application d'entreprise et recherchez Microsoft Entra SAML Toolkit, comme illustré dans l'image :



Parcourir Microsoft Entra Gallery

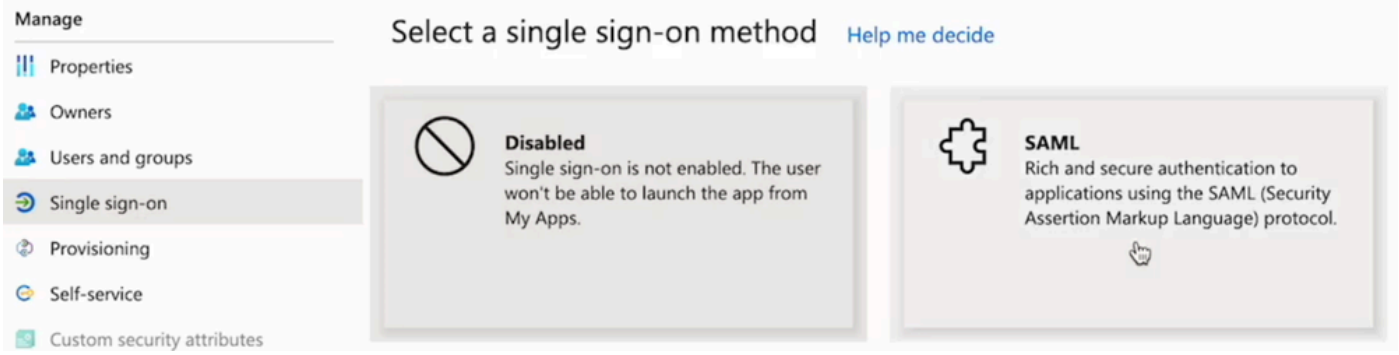
2. Nommez-le avec une valeur significative et cliquez sur Créer. Par exemple, Connexion unique CRES.



> Remarque : Pour permettre à tous les utilisateurs de se connecter au portail CRES, vous devez désactiver manuellement Required Assignment sous les propriétés CRES Sign On (SAML toolkit) et sélectionner No pour Assignment Required.

---

3. Accédez au panneau de gauche, sous la section Gérer, cliquez sur Authentification unique, puis sélectionnez SAML.



4. Dans le panneau Configuration SAML de base, cliquez sur Modifier, et renseignez les attributs comme suit :

- Identificateur (ID d'entité) : https://res.cisco.com/
- URL de réponse (Assertion Consumer Service URL) : https://res.cisco.com/websafe/ssourl
- URL de connexion : https://res.cisco.com/websafe/ssourl
- Cliquez sur Save.

5. Dans le panneau Attributs et revendications, cliquez sur Modifier.

Sous Requis, cliquez sur la revendication Identificateur d'utilisateur unique (ID de nom) pour la modifier.

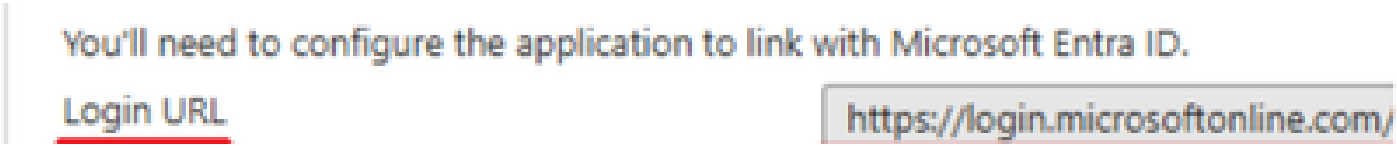
- Définissez le champ d'attribut Source sur user.userprincipalname. Cela suppose que la valeur de user.userprincipalname représente une adresse e-mail valide. Si ce n'est pas le cas, définissez Source sur user.primaryautoritativeemail.
- Dans le panneau Revendications supplémentaires, cliquez sur Modifier et créez les mappages entre les propriétés utilisateur Microsoft Entra ID et les attributs SAML.

Nom	Espace de noms	Attribut source
adresse e-mail	Aucune valeur	user.userprincipalname
Prénom	Aucune valeur	user.givenname
nom	Aucune valeur	user.surname

Assurez-vous d'effacer le champ Namespace pour chaque revendication, comme indiqué ci-dessous :

6. Une fois les sections Attributs et Réclamations remplies, la dernière section Certificat de signature SAML est remplie. Enregistrez les valeurs suivantes telles qu'elles sont requises dans le portail CRES :

- Enregistrez l'URL de connexion.



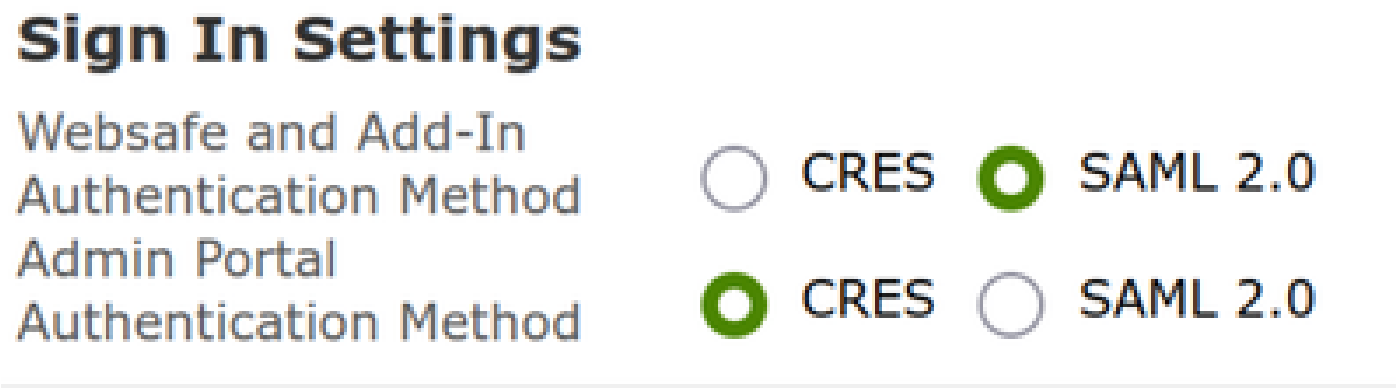
- Cliquez sur le lien Certificate (Base64) Download.

Service de cryptage de messagerie Cisco

1. Connectez-vous au portail d'organisation Secure Email Encryption Service en tant qu'administrateur.

2. Dans l'onglet Comptes, sélectionnez l'onglet Gérer les comptes et cliquez sur votre numéro de compte.

3. Dans l'onglet Détails, faites défiler jusqu'à Authentication Method et sélectionnez SAML 2.0.



4.- Complétez les attributs comme suit :

- Nom de l'attribut de courrier électronique secondaire SSO : adresse e-mail
- ID d'entité du fournisseur de services SSO* : https://res.cisco.com/
- URL du service client SSO* : Ce lien est fourni par Entra ID, sous
- URL de déconnexion SSO : laissez le champ vide

5.- Cliquez sur Activer SAML.

Vérifier

Une nouvelle fenêtre s'affiche pour confirmer que l'authentification SAML a été activée après une connexion réussie. Cliquez sur Next (Suivant). Elle vous redirige vers la page de connexion de votre fournisseur d'identité. Connectez-vous à l'aide de vos informations d'identification SSO. Une

fois connecté, vous pouvez fermer la fenêtre. Cliquez sur Save.

Dépannage

Si la fenêtre ne vous a pas redirigé vers la page de connexion de votre fournisseur d'identité, un retour en arrière est renvoyé pour vous fournir l'erreur. Vérifiez les Attributs et les Revendications, assurez-vous qu'il est configuré avec le même nom que dans la section Méthode d'authentification CRES. L'adresse de messagerie de l'utilisateur utilisée dans la connexion SAML doit correspondre à l'adresse de messagerie dans CRES. N'utilisez pas d'alias.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.