Configuration de l'authentification externe SSO Microsoft Entra ID pour DMP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Cisco Domain Protection (Partie 1)
  - ID d'entrée Microsoft
  - Cisco Domain Protection (Partie 2)
- Vérifier
- Dépannage

Introduction

Ce document décrit comment configurer l'authentification unique Microsoft Entra ID pour l'authentification auprès du portail Cisco Domain Protection.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Protection du domaine Cisco
- ID d'entrée Microsoft
- Certificats SSL X.509 auto-signés ou CA signés (facultatif) au format PEM

Composants utilisés

- Accès administrateur Cisco Domain Protection
- 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

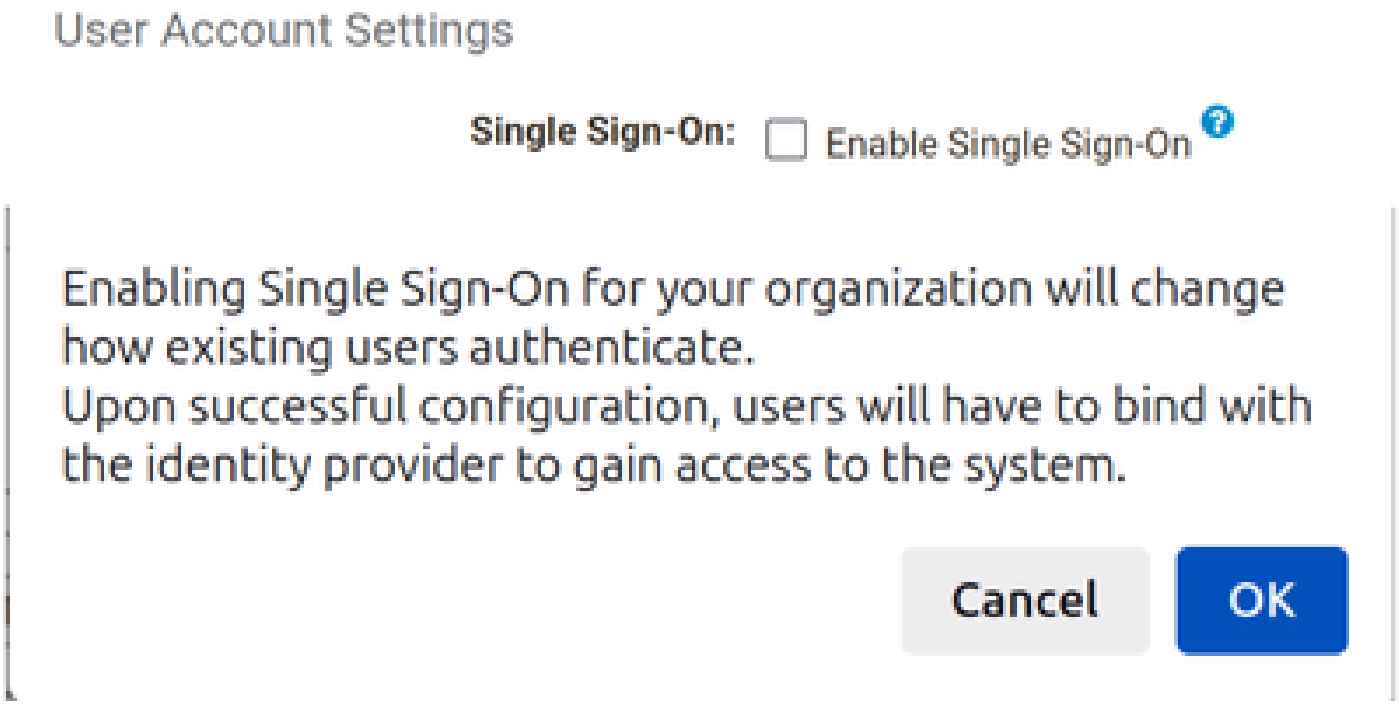
- Cisco Domain Protection active la connexion SSO pour les utilisateurs finaux via le protocole SAML 2.0.
- Microsoft Entra SSO permet et contrôle l'accès à vos applications SaaS (Software as a Service), applications cloud ou applications sur site depuis n'importe quel endroit avec l'authentification unique.
- Cisco Domain Protection peut être défini en tant qu'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

Cisco Domain Protection (Partie 1)

1. Connectez-vous au portail d'administration de Cisco Domain Protection et accédez à Admin > Organization. Cliquez sur le bouton Edit Organization Details, comme illustré dans l'image :

2. Accédez à la section Paramètres du compte d'utilisateur et cliquez sur Activer l'authentification unique. Un message s'affiche comme illustré dans l'image :

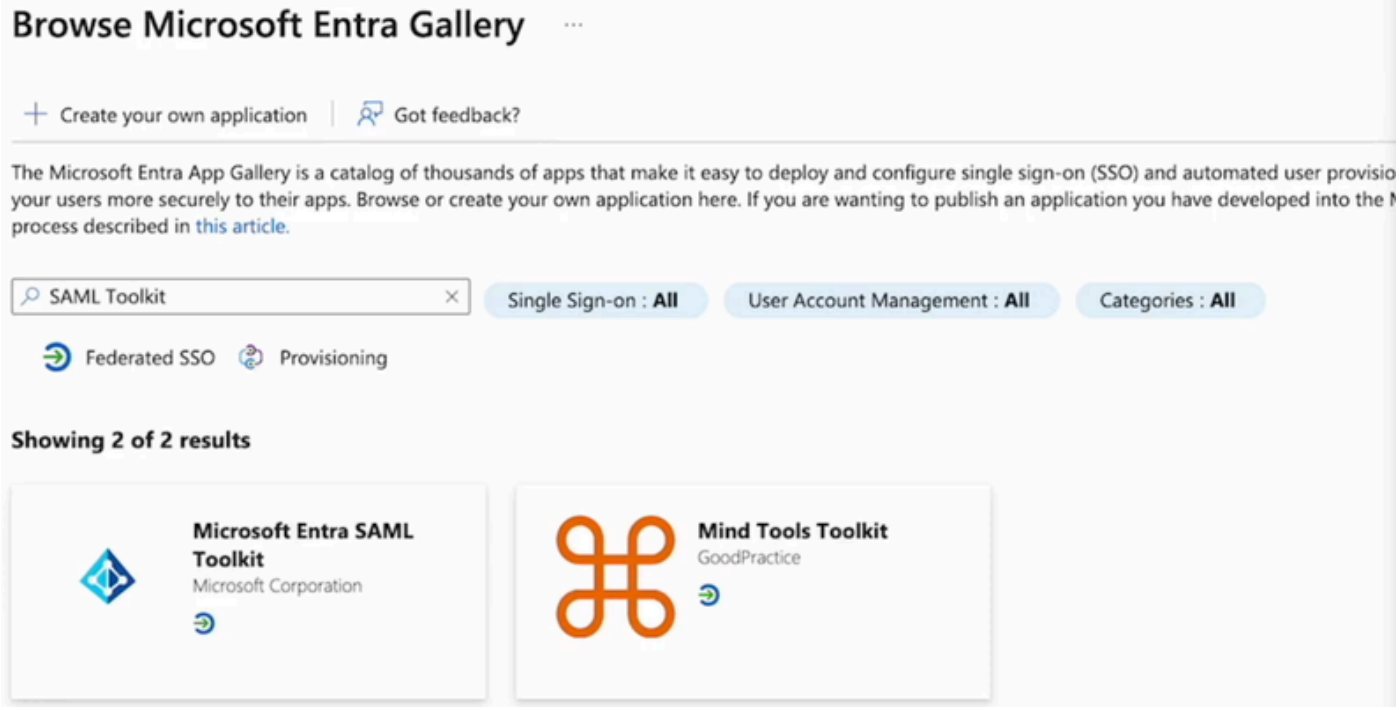


3. Cliquez sur le bouton OK et copiez les paramètres ID d'entité et URL ACS (Assertion Consumer Service). Ces paramètres doivent être utilisés dans l'authentification SAML Microsoft Entra ID Basic. Retournez ultérieurement pour configurer les paramètres Name Identifier Format, SAML 2.0 Endpoint et Public Certificate.

- ID d'entité : dmp.cisco.com
- URL du service client d'assertion : https://<dmp_id>.dmp.cisco.com/auth/saml/callback

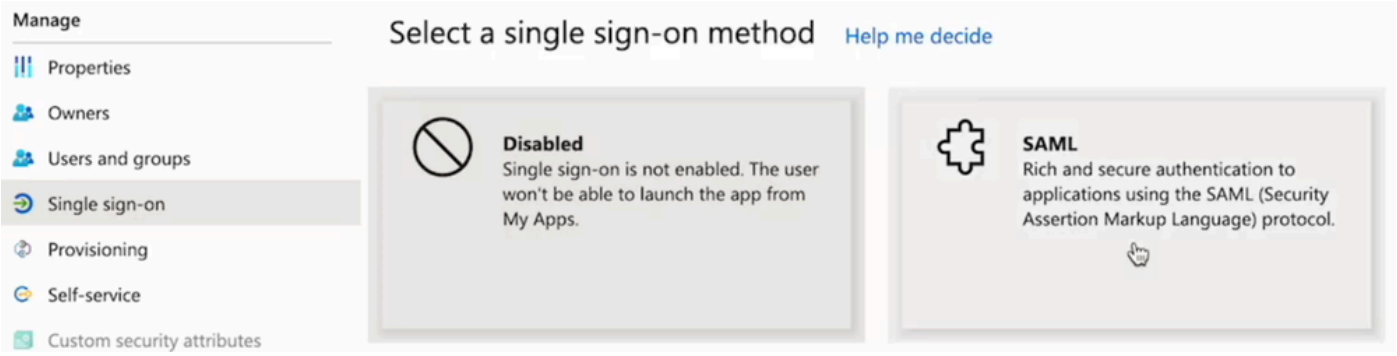
ID d'entrée Microsoft

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



2. Nommez-le avec une valeur significative et cliquez sur Créer. Par exemple, Connexion à la protection du domaine.

3. Accédez au panneau latéral 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 paramètres :

- Identifiant (ID d'entité) : dmp.cisco.com
- URL de réponse (URL du service client d'assertion) : https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- URL de connexion : https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 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.

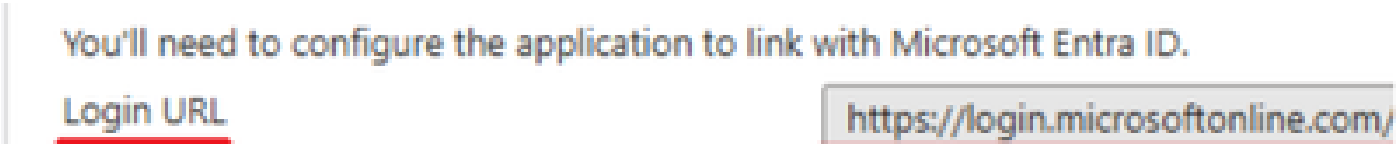
- Définissez le champ d'attribut Source sur user.userprincipalname. Cela suppose que la valeur de user.userprincipalname représente une adresse e-mail valide. Si ce n'est pas le cas, définissez Source sur user.primaryautoritativeemail.
- Dans le panneau Revendications supplémentaires, cliquez sur Modifier 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 l'URL de connexion.

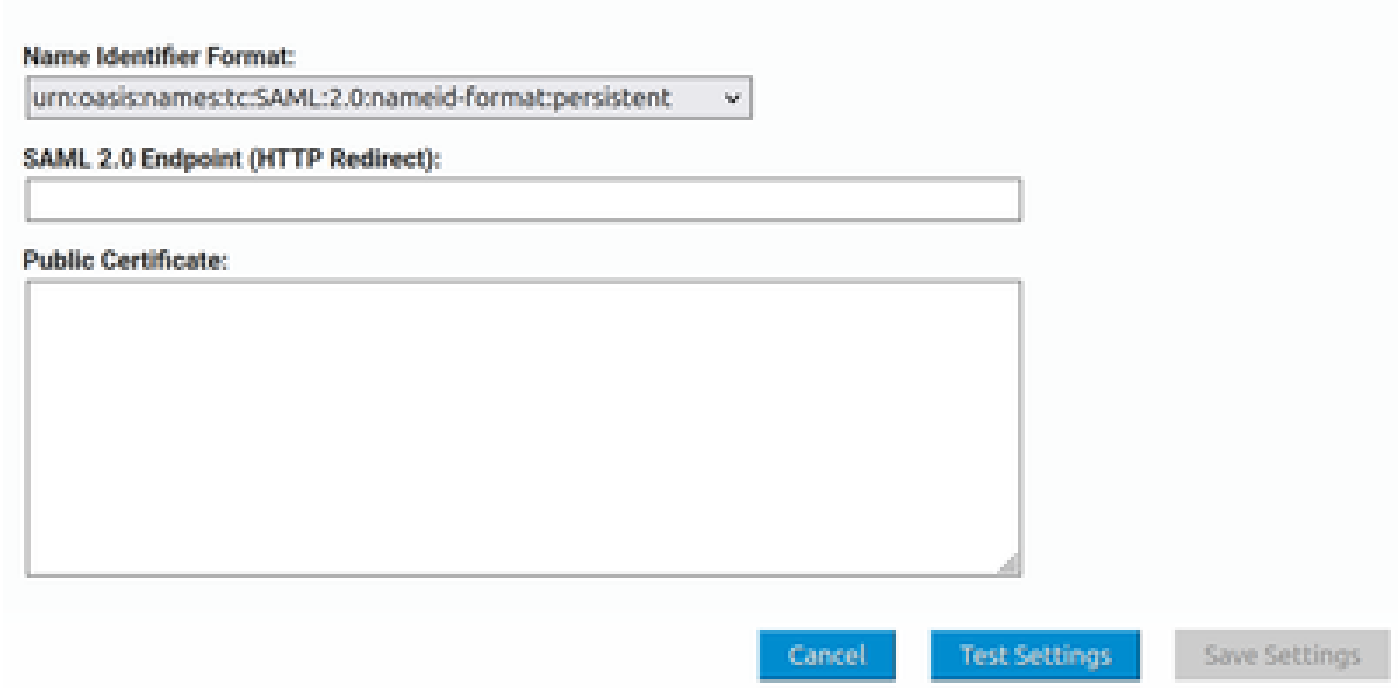


- Enregistrez le certificat (Base64).

Cisco Domain Protection (Partie 2)

Revenez à la section Cisco Domain Protection > Enable Single Sign-On.

- Format d'identificateur de nom : urn : oasis : names : tc : SAML : 2.0 : nameid-format : persistent
- Point de terminaison SAML 2.0 (redirection HTTP) : URL de connexion fournie par Microsoft Entra ID
- Certificat public : Certificat (Base64) fourni par Microsoft Entra ID



Vérifier

Cliquez sur Paramètres de test. Il vous redirige vers la page de connexion de votre fournisseur d'identité. Connectez-vous avec vos identifiants SSO.

Une fois la connexion établie, vous pouvez fermer la fenêtre. Cliquez sur Save Settings.

Dépannage

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

- Vérifiez que le certificat est en Base64.

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

- Assurez-vous que l'URL de connexion fournie par l'ID Microsoft Entra est correcte.

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.