

- Authentification unique Eurécia - SAML Google



Date/Version	Contenu	Etat
30/06/2016	Création du document	Diffusable

But du document : Ce document constitue un guide des étapes à suivre pour mettre en place une fédération d'identité à partir de Google.

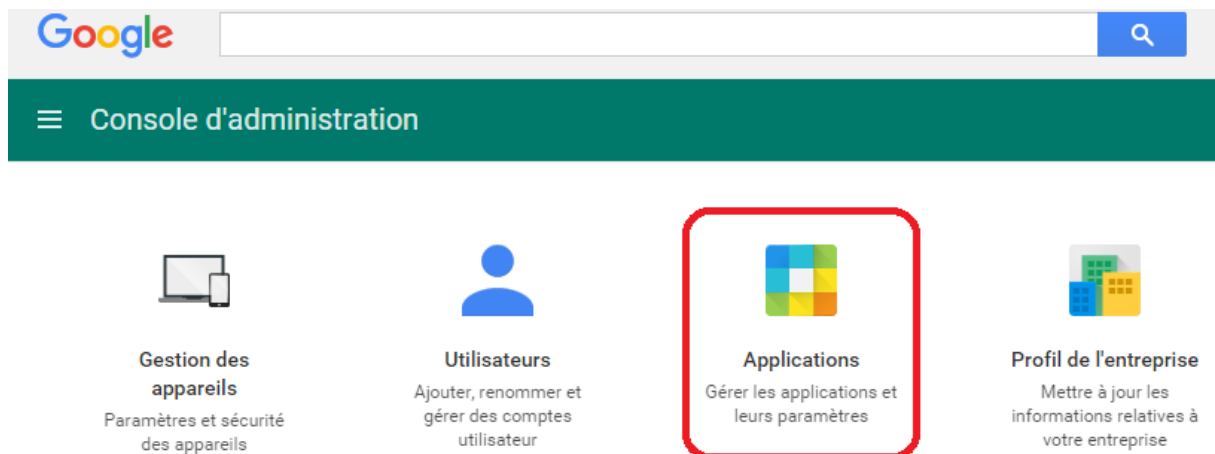
Le serveur de fédération publie les informations nécessaires à la connexion par l'utilisateur à l'application Eurécia

Etape 1 : Création d'une application SAML

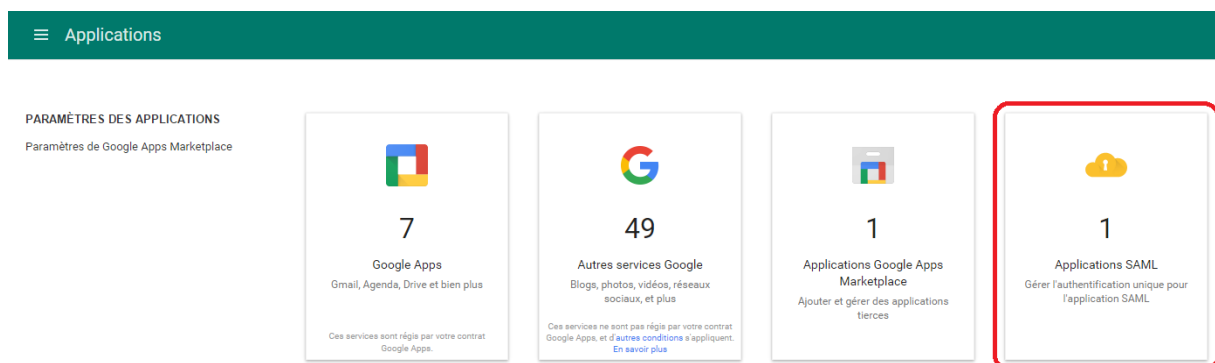
Prérequis :

Vous devez disposer d'un compte Google disposant des droits administrateur sur l'entreprise.

La création d'une application SAML se fait depuis la console d'administration Google (<https://admin.google.com>) dans le menu 'Applications' :



Un menu est présent pour ajouter une application SAML :



Un bouton 'plus' apparaît en bas à droite de la fenêtre et permet d'ajouter une application SAML :

Activer l'authentification unique pour une application SAML



Etape 2 : Configuration de l'application SAML

- Google propose un large choix de services préconfigurés, dans le cas d'Eurécia choisir de configurer une application personnalisée :

Étape 1 ×

Activer l'authentification unique pour l'application SAML

Sélectionnez le service ou l'application pour lequel vous souhaitez configurer l'authentification unique.

- Amazon Web Services >
- BlueJeans >
- Box >
- Cigna >
- Citrix GotoMeeting >
- Concur >
- Coupa >

CONFIGURER MON APPLICATION PERSONNALISÉE

- 📄 Télécharger le fichier de métadonnées IDP.
Il s'agit d'un fichier XML qui devra pas la suite être transmis à Eurécia.

Ces métadonnées permettront à Eurécia d'interpréter la demande de connexion initiée par Google.

Étape 2 sur 5 ✕

Informations sur Google IdP

Choisissez l'une ou l'autre des options pour configurer Google en tant que fournisseur d'identité. Ajoutez des informations relatives au fournisseur de services dans la configuration de l'authentification unique. [En savoir plus](#)

Option n° 1

URL d'authentification unique	https://accounts.google.com/o/saml2/idp?idpid=C00gkzzle
ID d'entité	https://accounts.google.com/o/saml2?idpid=C00gkzzle

Certificat ↓ TÉLÉCHARGEMENT

----- OU -----

Option n°2

Métadonnées IDP	↓ TÉLÉCHARGEMENT
-----------------	------------------

PRÉC. ANNULER SUIVANT

👉 Donner un nom explicite à l'application :

Étape 3 sur 5 ✕

Informations générales sur votre application personnalisée

Veillez fournir les informations générales requises pour configurer votre application personnalisée. Elles seront consultables par les utilisateurs finaux de l'application.

Nom de l'application *	EURECIA	id-appli : eurecia
Description	Application <u>SAML</u> pour Eurécia	
Importer un logo	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">📎 SÉLECTIONNER UN FICHIER</div> Logo_200px.jpg 29.6 KB	

Ce logo sera visible par tous les utilisateurs autorisés à accéder à cette application. Veuillez importer une image .png ou .gif de 256 x 256 pixels.

PRÉC. ANNULER SUIVANT

Ps : un logo peut être chargé et sera utilisé pour tous les utilisateurs.

Vous pouvez télécharger celui de Eurécia ici :

http://www.eurecia.com/profiles/eurecia/themes/eurecia_theme/logo.png

👉 Détails relatifs au fournisseur de services -> Eurécia

Reproduire la configuration suivante :

Étape 4 sur 5 ✕

Détails relatifs au fournisseur de services

Veillez fournir les détails relatifs au fournisseur de services pour configurer l'authentification unique pour votre application personnalisée. L'URL ACS et l'ID d'entité sont obligatoires.

URL ACS *	<input type="text" value="https://plateforme.eurecia.com/Shibboleth.sso/SAM"/>	
ID d'entité *	<input type="text" value="https://plateforme.eurecia.com/shibboleth"/>	
URL de démarrage	<input type="text" value="https://plateforme.eurecia.com/secureshib"/>	
Réponse signée	<input type="checkbox"/>	
Identifiant du nom	<input type="text" value="Informations générales"/>	<input type="text" value="Adresse e-mail principale"/>
Format de l'ID du nom	<input type="text" value="EMAIL"/>	

PRÉC. ANNULER SUIVANT

Pour l'environnement de production =>

URL ACS => <https://plateforme.eurecia.com/Shibboleth.sso/SAML2/POST>

ID d'entité => <https://plateforme.eurecia.com/shibboleth>

URL de démarrage => <https://plateforme.eurecia.com/secureshib>

Format de l'ID du nom => EMAIL


Pour l'environnement de démo =>

URL ACS => <https://demo.eurecia.com/Shibboleth.sso/SAML2/POST>

ID d'entité => <https://demo.eurecia.com/shibboleth>

URL de démarrage => <https://demo.eurecia.com/secureshib>

Format de l'ID du nom => EMAIL

 Ajouter un nouveau mappage :

AJOUTER UN NOUVEAU MAPPAGE

Reproduire la configuration suivante :

Étape 5 sur 5 ×

Mappage des attributs

Fournir les mappages des attributs de fournisseur de service pour les champs disponibles du profil d'utilisateur

<u>http://schemas.xmlsoap.org/w</u>	Informations générales ▼	Adresse e-mail principale ▼
-------------------------------------	-----------------------------	--------------------------------

AJOUTER UN NOUVEAU MAPPAGE

PRÉC. ANNULER TERMINER

Attribut de l'application => <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

🌿 Si les données renseignées sont correctes, le panneau suivant apparaît :

Configuration de l'authentification unique pour EURECIA ✕

- ✓ Détails relatifs à l'application enregistrés.
- ✓ Le mappage d'attributs obligatoire a bien été configuré.

👉 Vous devrez importer les données IDP de Google dans le panneau d'administration de EURECIA pour terminer le processus de configuration SAML.

OK

🌿 Etape 3 : Mise à disposition de l'application pour tous les utilisateurs

L'application EURECIA est désormais créée et apparaît dans le menu 'Applications SAML' :

The screenshot shows a navigation bar with 'Applications > Applications SAML'. Below it, a table lists applications. The 'EURECIA' application is shown with the status 'Désactivé'.

Services	État
EURECIA	Désactivé

L'application n'est pour autant pas accessible par les utilisateurs.

Pour cela, il faut activer l'application pour tout le monde :

The screenshot shows the 'EURECIA' application row with the status 'Désactivé'. A dropdown menu is open, showing three options: 'Activé pour tout le monde' (selected), 'Activé pour certaines organisations', and 'Désactivé'.

EURECIA	Désactivé	<ul style="list-style-type: none">Activé pour tout le mondeActivé pour certaines organisationsDésactivé
---------	-----------	---

Ps : L'activation peut prendre plusieurs heures avant d'être effective !

Etape 4 : Envoi du fichier de métadonnées à Eurécia

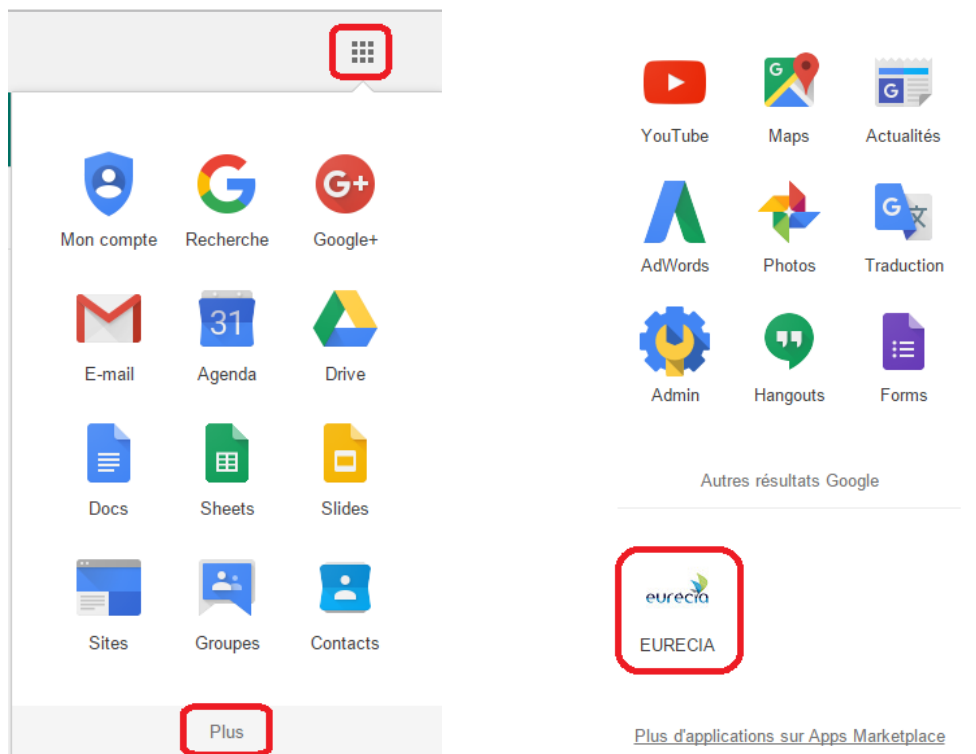
Afin que la connexion SSO puisse être initiée avec Eurécia, les données IDP de Google doivent être importées dans Eurécia.

Le fichier XML téléchargé au départ de la configuration doit être envoyé au service client Eurécia, Soit directement à votre consultant référent, soit au service support via l'adresse support@eurecia.com.

Etape 5 : Tests de fonctionnement

Une fois l'application déployée dans Google et le fichier de métadonnées intégré à Eurécia, vous pouvez vous connecter en SSO.

Lorsque vous êtes connecté à Google, le bouton permettant d'accéder aux applications (en haut à droite) vous donne accès à l'application SAML créée (généralement sous le bouton « plus ») :



Un simple clic sur cette application depuis un compte Google de votre société doit permettre de se connecter à Eurécia sur le compte utilisateur correspondant.

Ps : l'adresse email faisant office d'identifiant, la connexion ne peut se faire que si un compte utilisateur existe dans Eurécia et dispose de la même adresse email que celle configurée dans Google !