Configurer le flux de connexion administrateur ISE 3.1 via SAML SSO avec Azure AD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Conditions
  - SAML
  - Assertion SAML
- Diagramme de flux général
- Configurer l'intégration SSO SAML avec Azure AD
  - Étape 1 : configuration du fournisseur d'identité SAML sur ISE
  - Étape 2 : configuration des paramètres du fournisseur d'identité Azure AD
  - Étape 3. Télécharger des métadonnées d'Azure Active Directory vers ISE
  - Étape 4 : configuration des groupes SAML sur ISE
  - (Facultatif) Étape 5 : configuration des stratégies RBAC
- Vérifier
- Dépannage
  - Problèmes courants
  - Dépannage d'ISE
    - Journaux avec nom de connexion SAML et nom de revendication de groupe incompatible

Introduction

Ce document décrit comment configurer l'intégration SSO SAML de Cisco ISE 3.1 avec un fournisseur d'identité externe tel qu'Azure Active Directory (AD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

1. Cisco ISE 3.1
2. Déploiements SAML SSO
3. Azure AD

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

1. Cisco ISE 3.1
2. Azure AD

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

Conditions

Fournisseur d'identités (IdP) : Autorité Azure AD qui vérifie et affirme une identité d'utilisateur et des privilèges d'accès à une ressource demandée (le fournisseur de services).

Fournisseur de services : ressource ou service hébergé auquel l'utilisateur a l'intention d'accéder (le serveur d'applications ISE).

SAML

Le langage SAML (Security Assertion Markup Language) est une norme ouverte qui permet au fournisseur d'identité de transmettre des informations d'identification d'autorisation au fournisseur de services.

Les transactions SAML utilisent le langage XML (Extensible Markup Language) pour les communications normalisées entre le fournisseur d'identité et les fournisseurs de services.

SAML est le lien entre l'authentification d'une identité d'utilisateur et l'autorisation d'utiliser un service.

Assertion SAML

Une assertion SAML est le document XML que le fournisseur d'identité envoie au fournisseur de services qui contient l'autorisation utilisateur.

Il existe trois types différents d'assertions SAML : l'authentification, l'attribut et la décision d'autorisation.

- Les assertions d'authentification prouvent l'identification de l'utilisateur et indiquent l'heure à laquelle l'utilisateur s'est connecté et la méthode d'authentification qu'il a utilisée (Kerberos, à deux facteurs, à titre d'exemples)
- L'assertion d'attribution transmet les attributs SAML, des données spécifiques qui

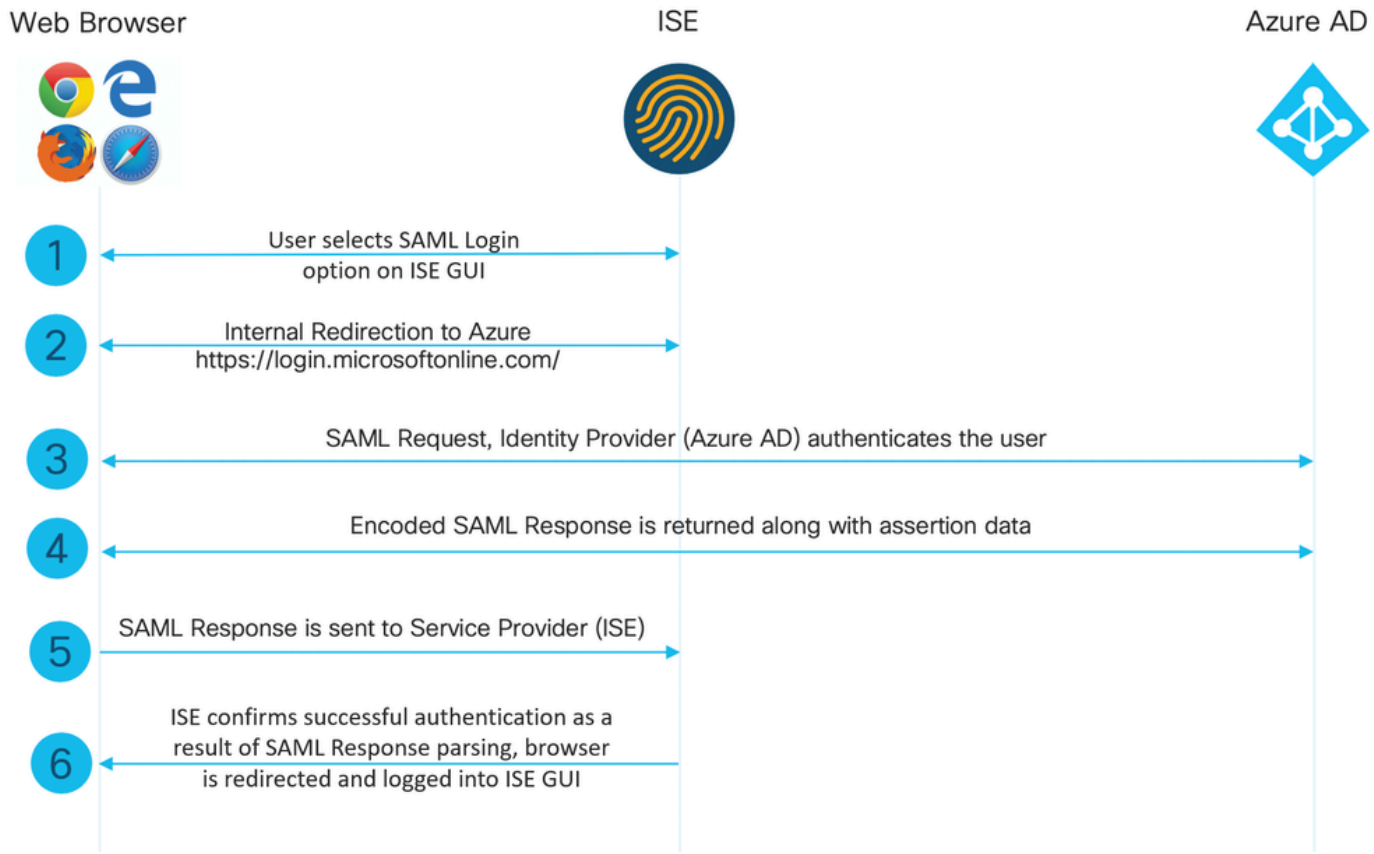
fournissent des informations sur l'utilisateur, au fournisseur de services.
- Une assertion de décision d'autorisation déclare si l'utilisateur est autorisé à utiliser le service ou si le fournisseur d'identification a refusé sa demande en raison d'un défaut de mot de passe ou d'un manque de droits sur le service.

Diagramme de flux général

SAML fonctionne en transmettant des informations sur les utilisateurs, les connexions et les attributs entre le fournisseur d'identité, Azure AD, et le fournisseur de services, ISE.

Chaque utilisateur se connecte une fois à une authentification unique (SSO) avec le fournisseur d'identité, puis le fournisseur Azure AD transmet les attributs SAML à ISE lorsque l'utilisateur tente d'accéder à ces services.

ISE demande l'autorisation et l'authentification à partir d'Azure AD, comme indiqué dans l'image :



Configurer l'intégration SSO SAML avec Azure AD

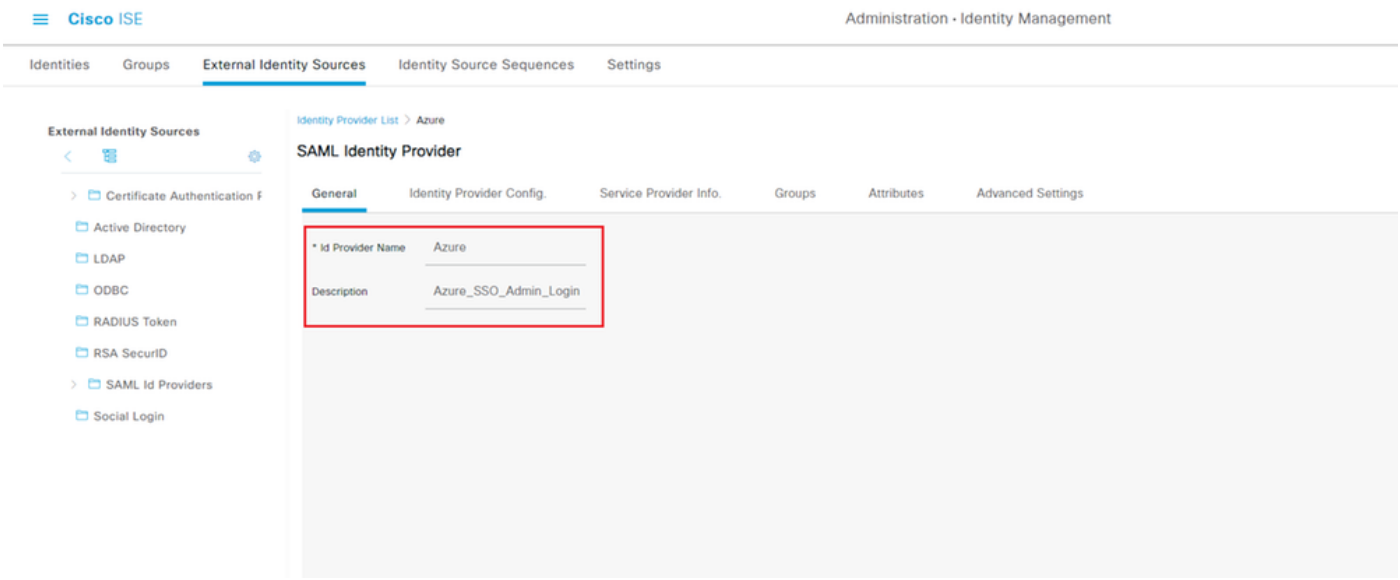
Étape 1 : configuration du fournisseur d’identité SAML sur ISE

1. Configurez Azure AD en tant que source d'identité SAML externe :

Sur ISE, accédez à Administration > Identity Management > External Identity Sources > SAML Id

Providers et cliquez sur le bouton Add.

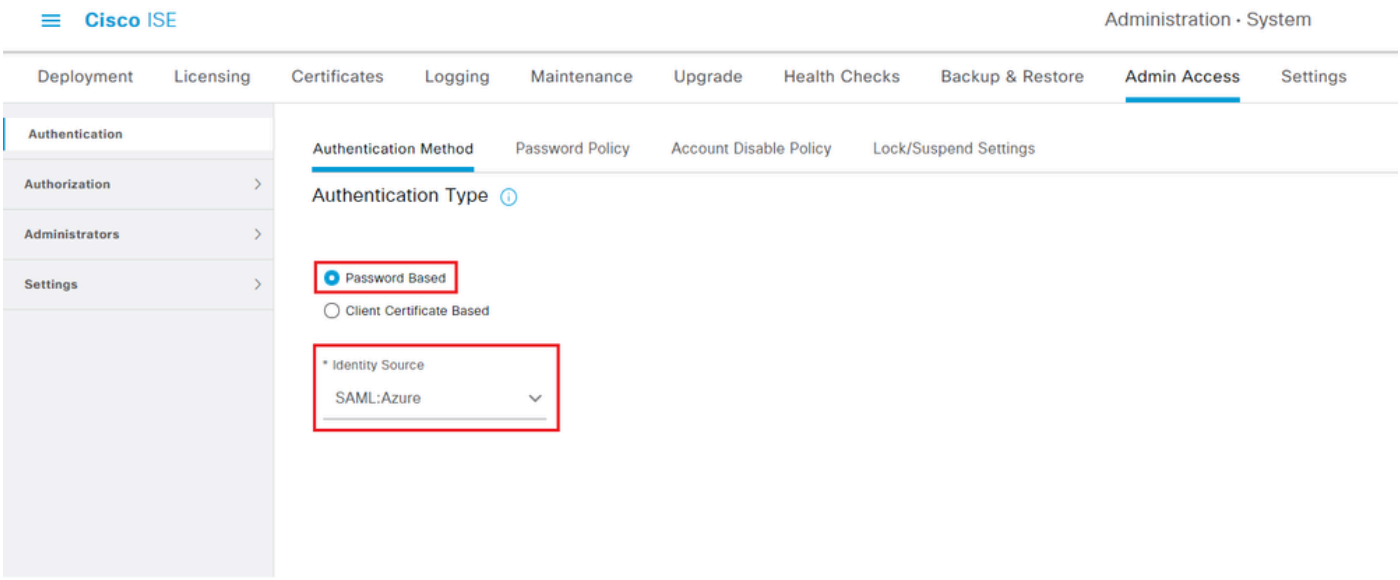
Entrez l'ID Provider Name et cliquez sur Submit afin de l'enregistrer. Le nom du fournisseur d'ID est significatif uniquement pour ISE, comme indiqué dans l'image.



2. Configurez la méthode d'authentification ISE :

Accédez à Administration > System > Admin Access > Authentication > Authentication Method et sélectionnez la case d'option Password Based.

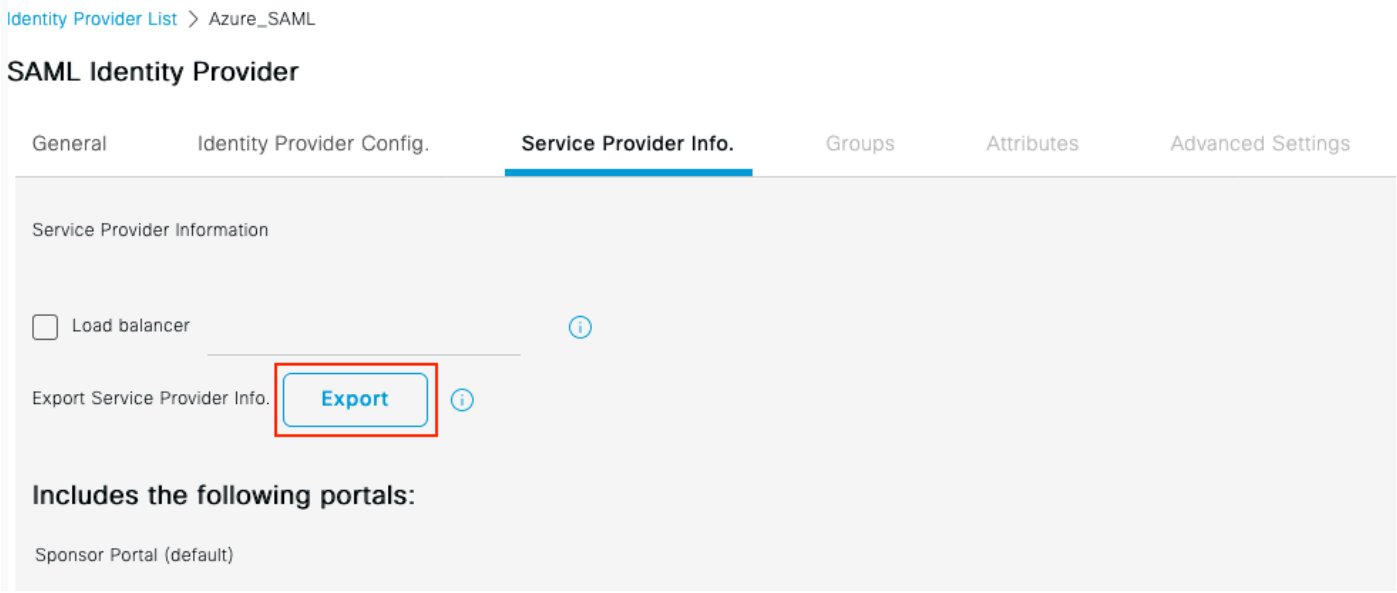
Sélectionnez le nom du fournisseur d'ID requis créé précédemment dans la liste déroulante Source d'identité, comme illustré dans l'image.



3. Exporter les informations du fournisseur de services :

Accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].

Basculez l'onglet vers Service Provider Info. et cliquez sur le bouton Exporter comme illustré dans l'image.



Téléchargez le fichier .xml et enregistrez-le. Notez l'URL de l'emplacement et la valeur entityID.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasi
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSig
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMS0xOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1opO1qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzFO38ciQqlmOsqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe79OR5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV8OmN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4HOvdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wkOBLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMcOaS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
```

```
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

</md:SPSSODescriptor>
</md:EntityDescriptor>
```

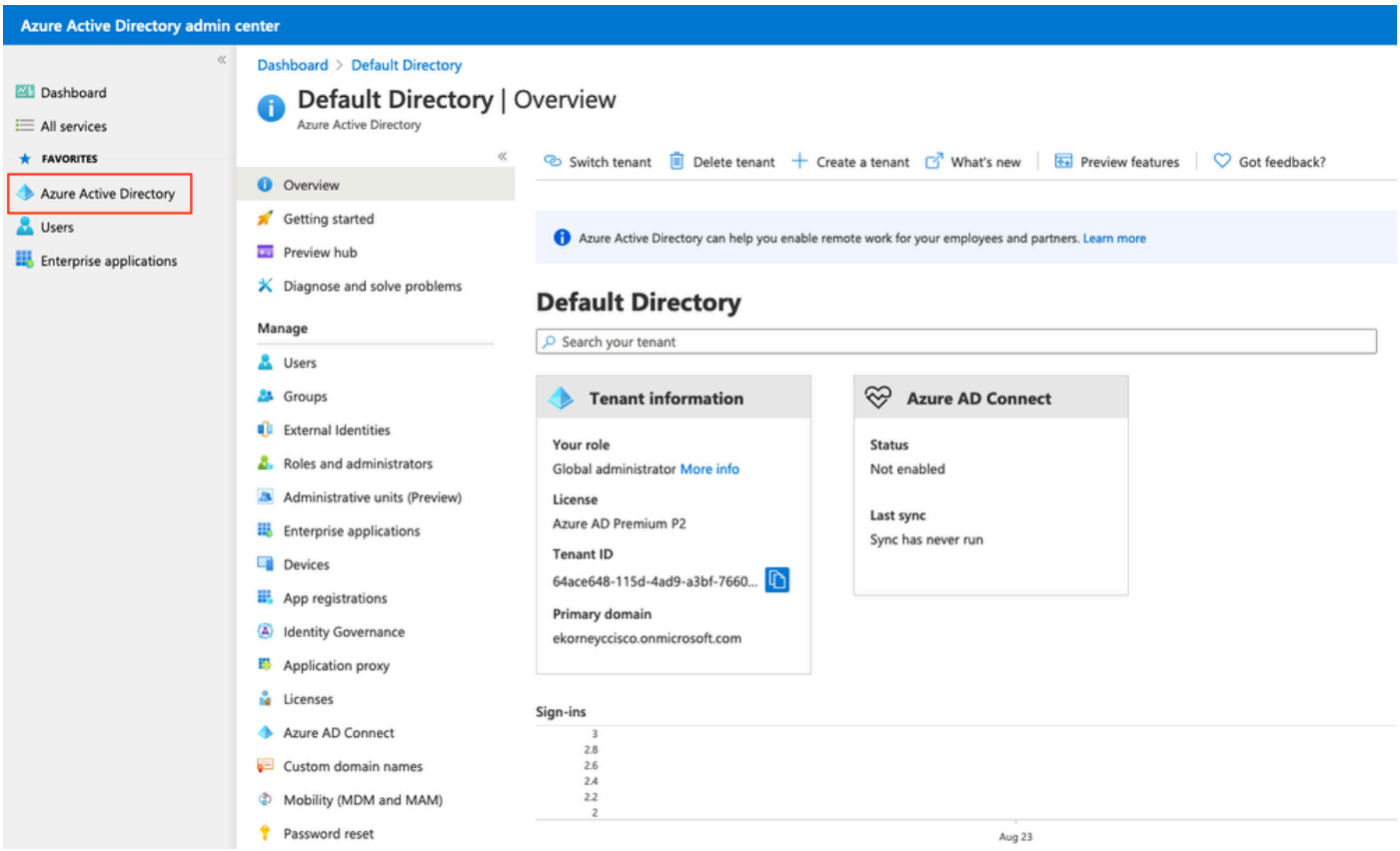
Attributs intéressants du fichier XML :

- entityID="http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2"
- AssertionConsumerService Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action"
- AssertionConsumerService Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action"

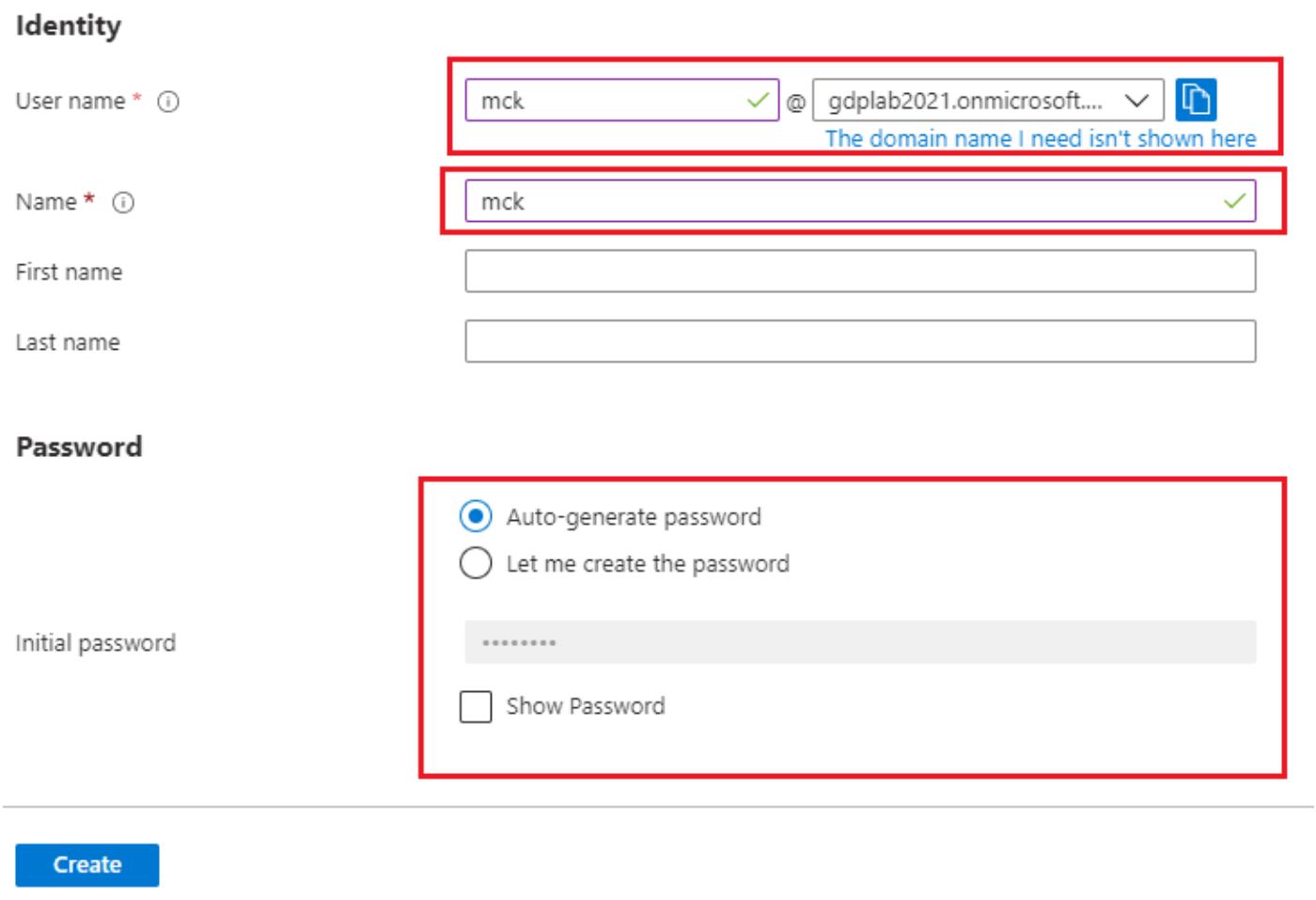
Étape 2 : configuration des paramètres du fournisseur d'identité Azure AD

1. Créez un utilisateur Azure AD :

Connectez-vous au tableau de bord du centre d'administration Azure Active Directory et sélectionnez votre AD comme indiqué dans l'image.

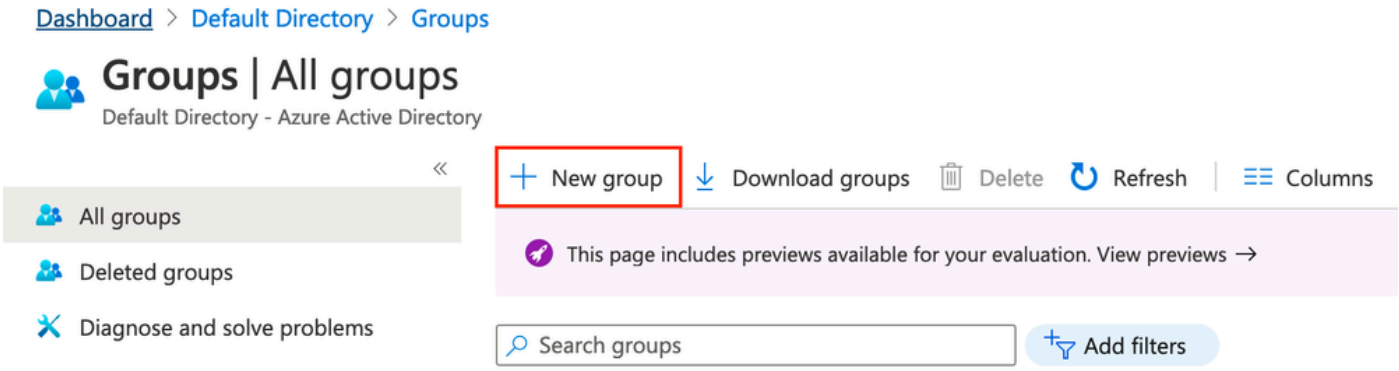


Sélectionnez Users, cliquez sur New User, configurez le nom d'utilisateur, le nom et le mot de passe initial selon les besoins. Cliquez sur Create comme indiqué dans l'image.

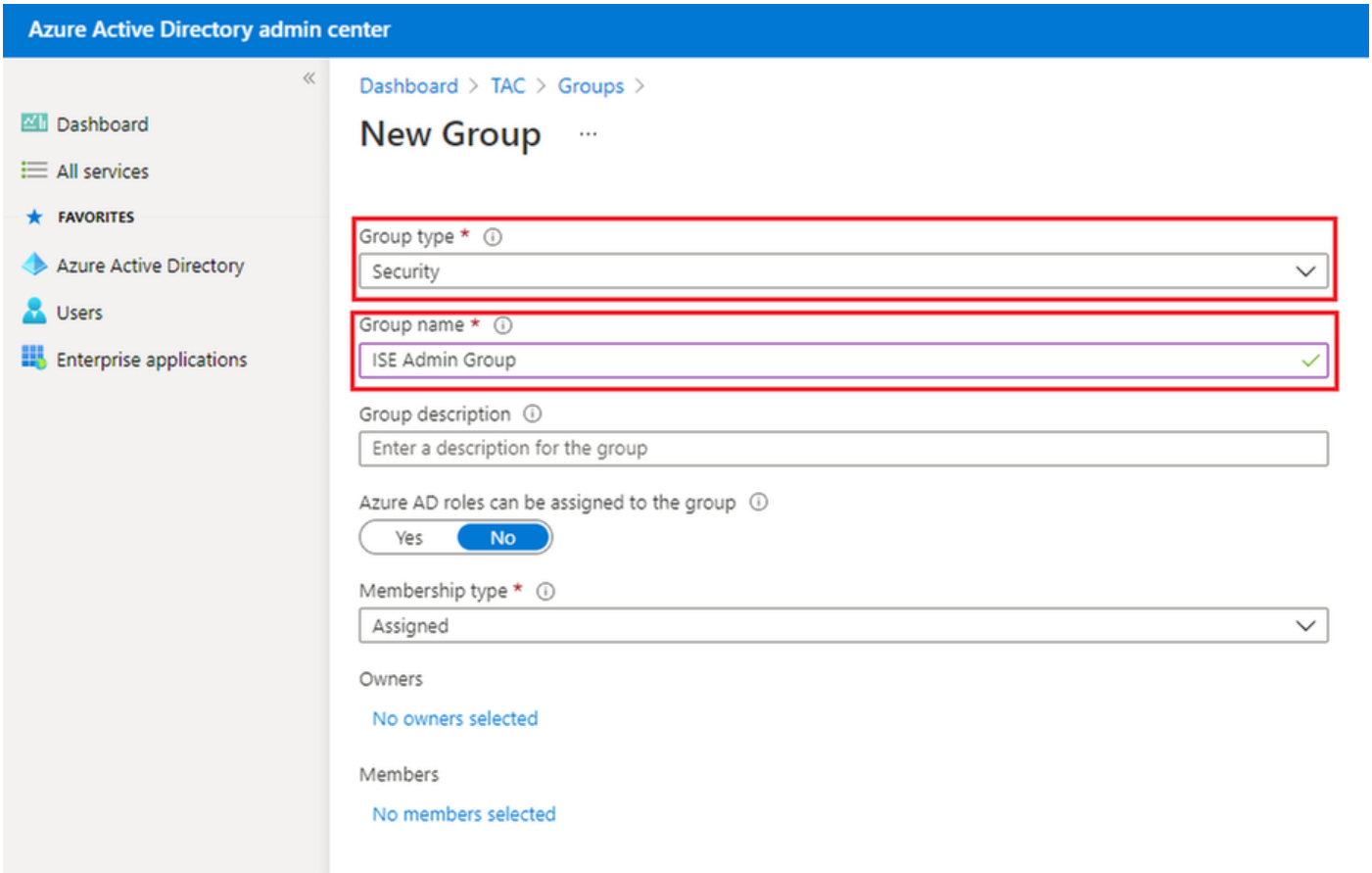


2. Créez un groupe Azure AD :

Sélectionnez Groupes. Cliquez sur Nouveau groupe.

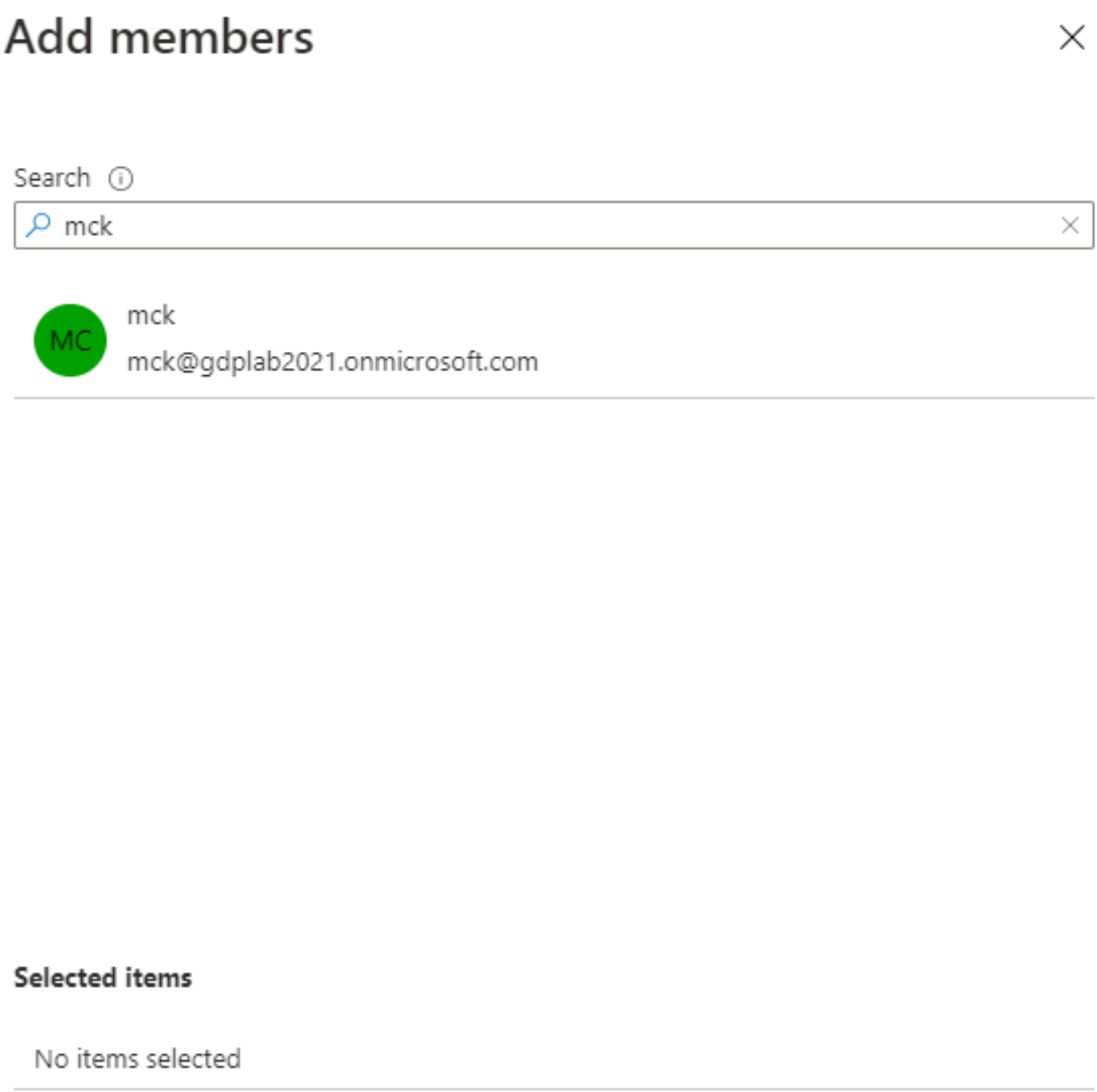


Conservez le type de groupe Sécurité. Configurez le nom du groupe comme indiqué dans l'image.

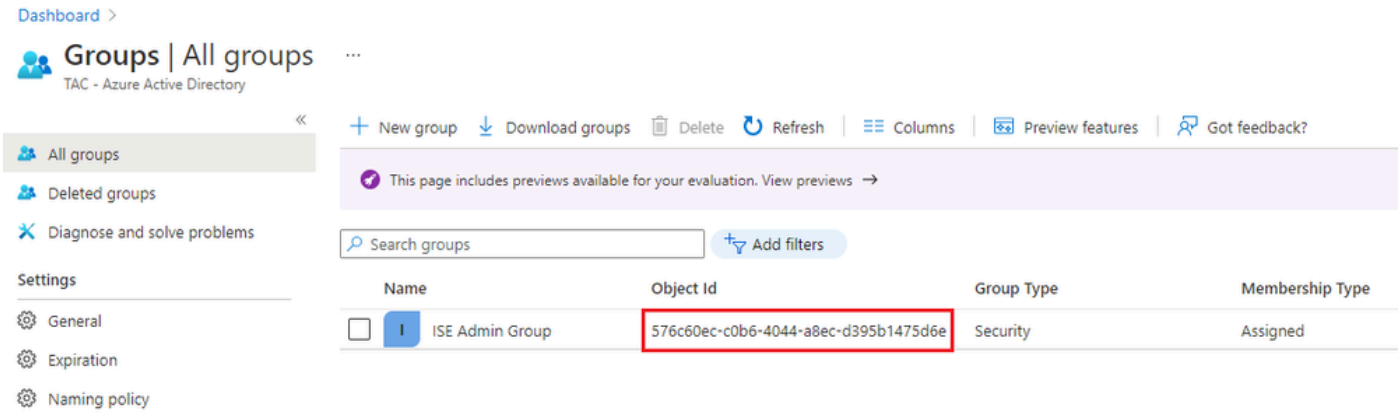


3. Affectez un utilisateur Azure AD au groupe :

Cliquez sur Aucun membre sélectionné. Choisissez l'utilisateur et cliquez sur Sélectionner. Cliquez sur Create afin de créer le groupe avec un utilisateur qui lui est assigné.

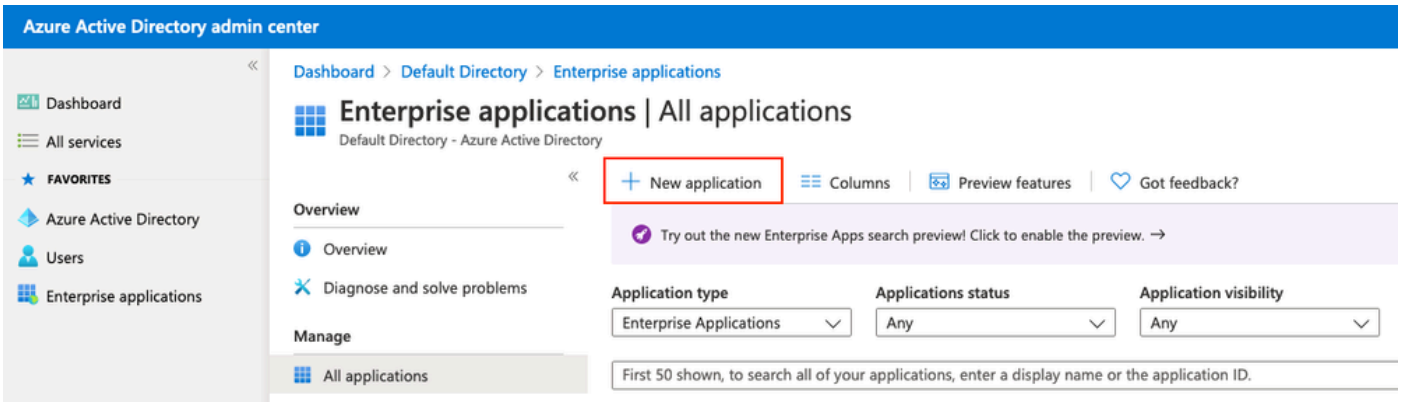


Notez l'ID d'objet de groupe, dans cet écran, il s'agit de 576c60ec-c0b6-4044-a8ec-d395b1475d6e pour le groupe d'administration ISE comme illustré dans l'image.

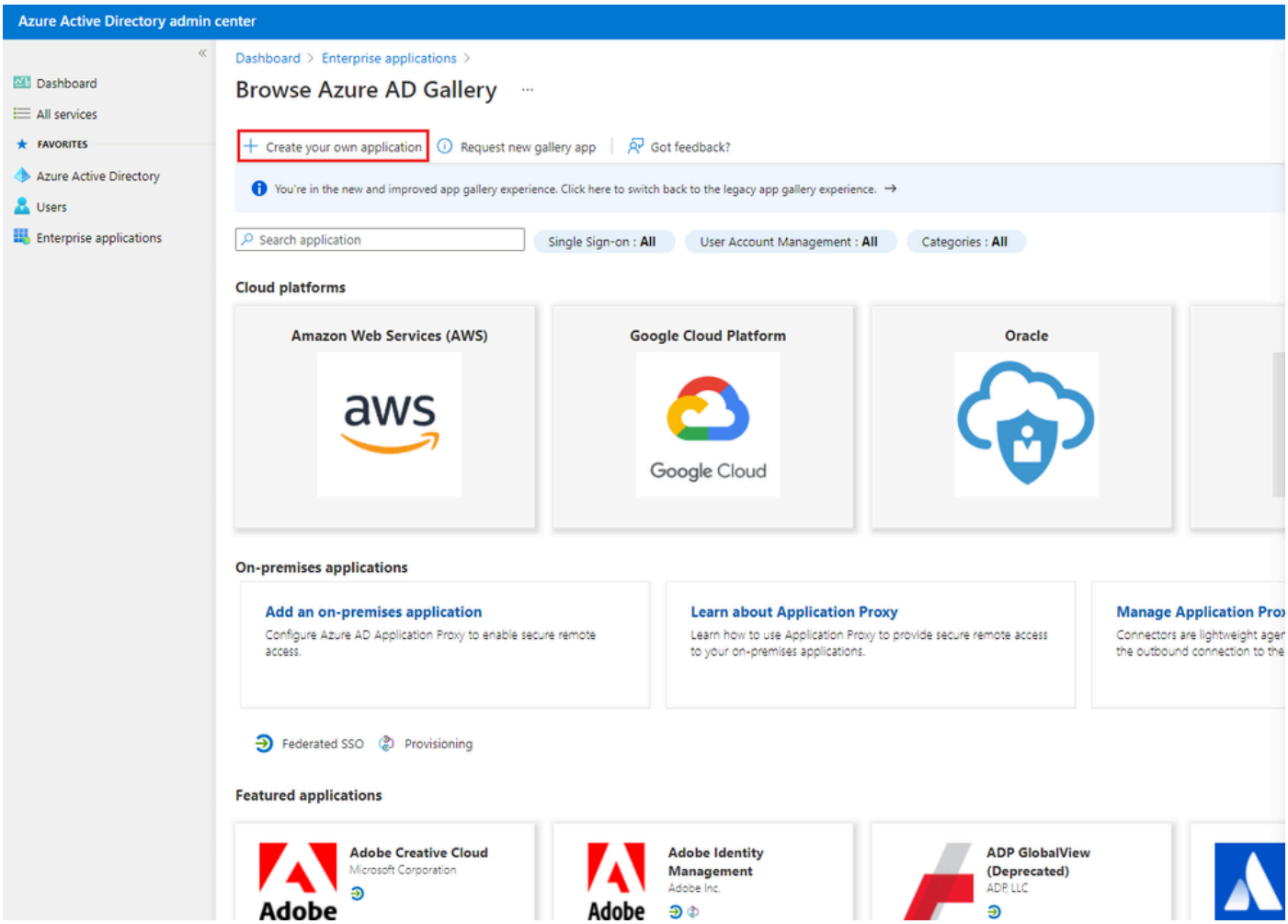


4. Créez une application Azure AD Enterprise :

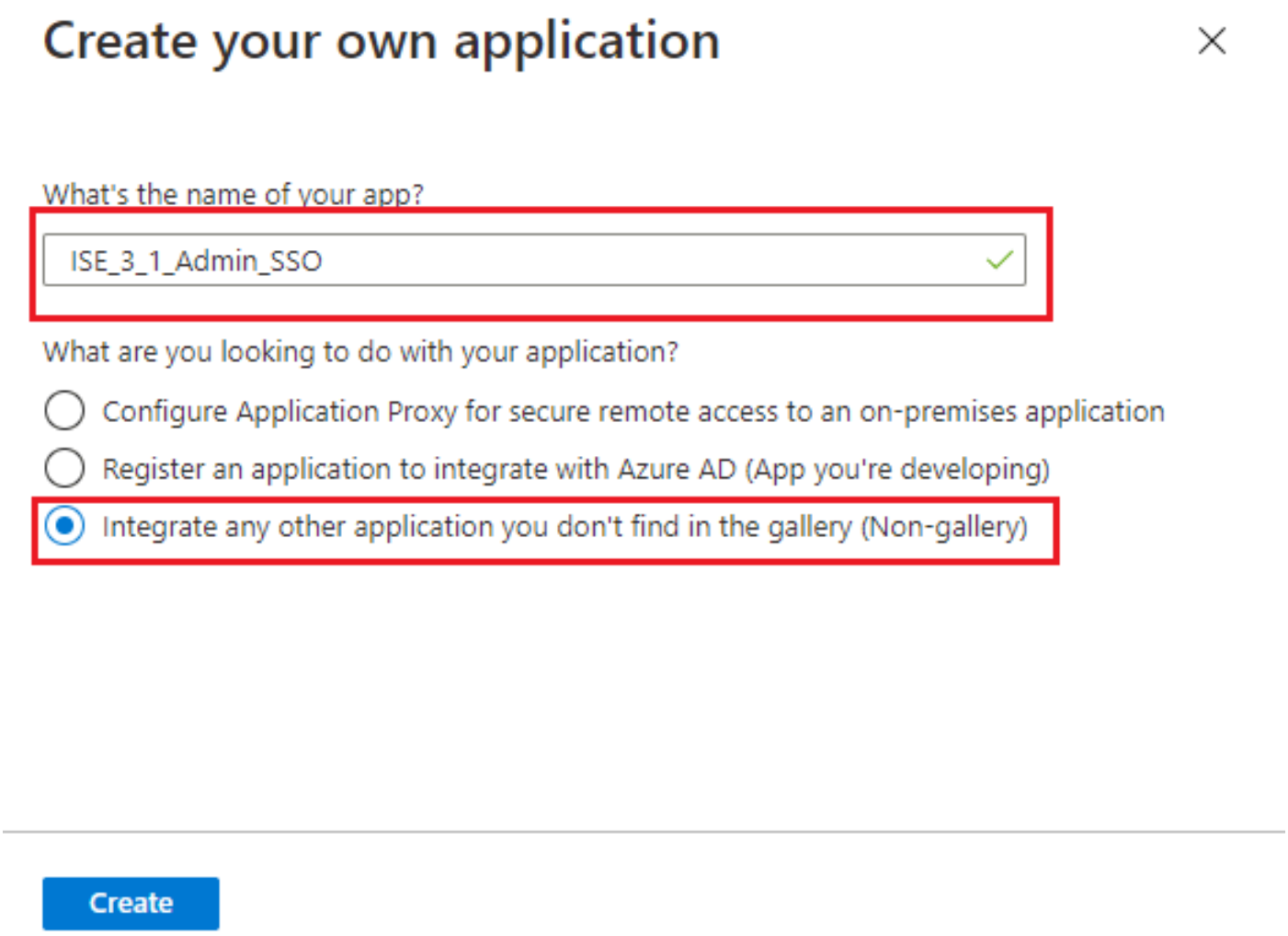
Sous AD, sélectionnez Applications d'entreprise et cliquez sur Nouvelle application.



Sélectionnez l'option Créer votre propre application.

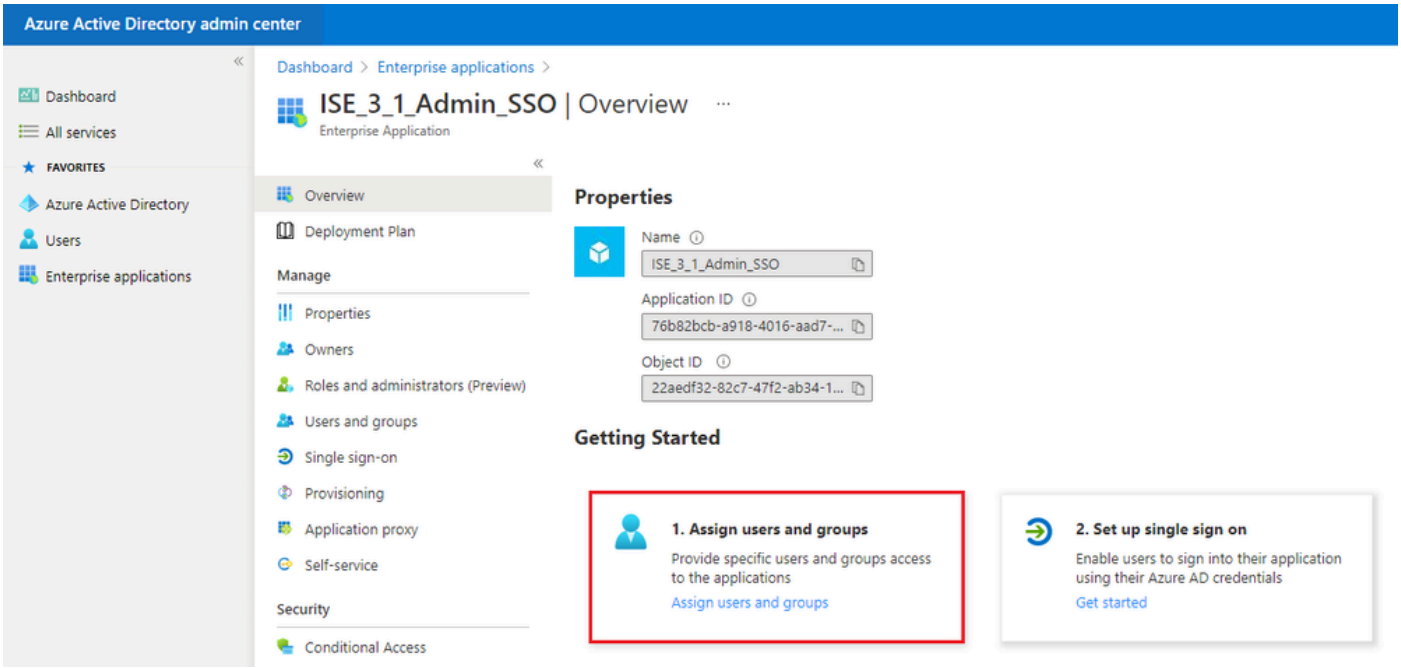


Entrez le nom de votre application et sélectionnez le bouton radio Intégrer toute autre application que vous ne trouvez pas dans la galerie (Non-galerie) et cliquez sur le bouton Créer comme indiqué dans l'image.

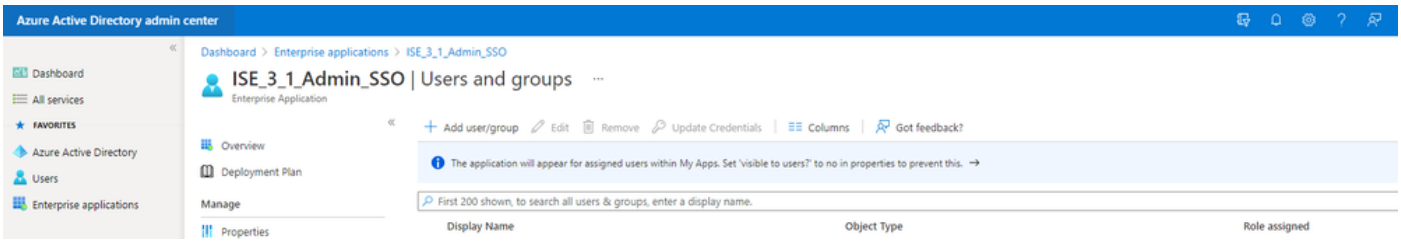


5. Ajoutez un groupe à l'application :

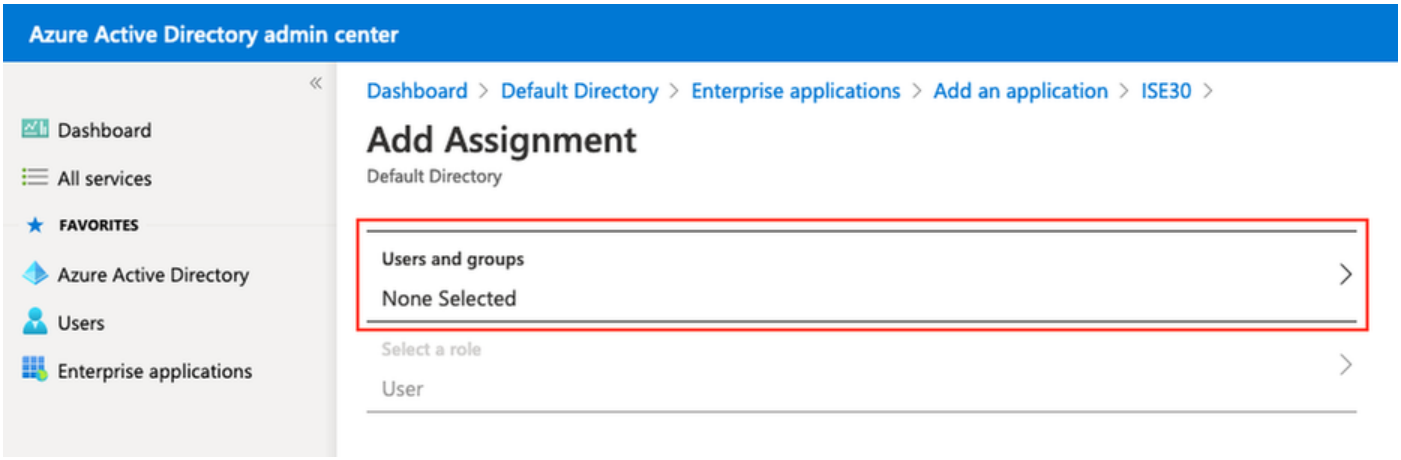
Sélectionnez Affecter des utilisateurs et des groupes.



Cliquez sur Ajouter un utilisateur/groupe.

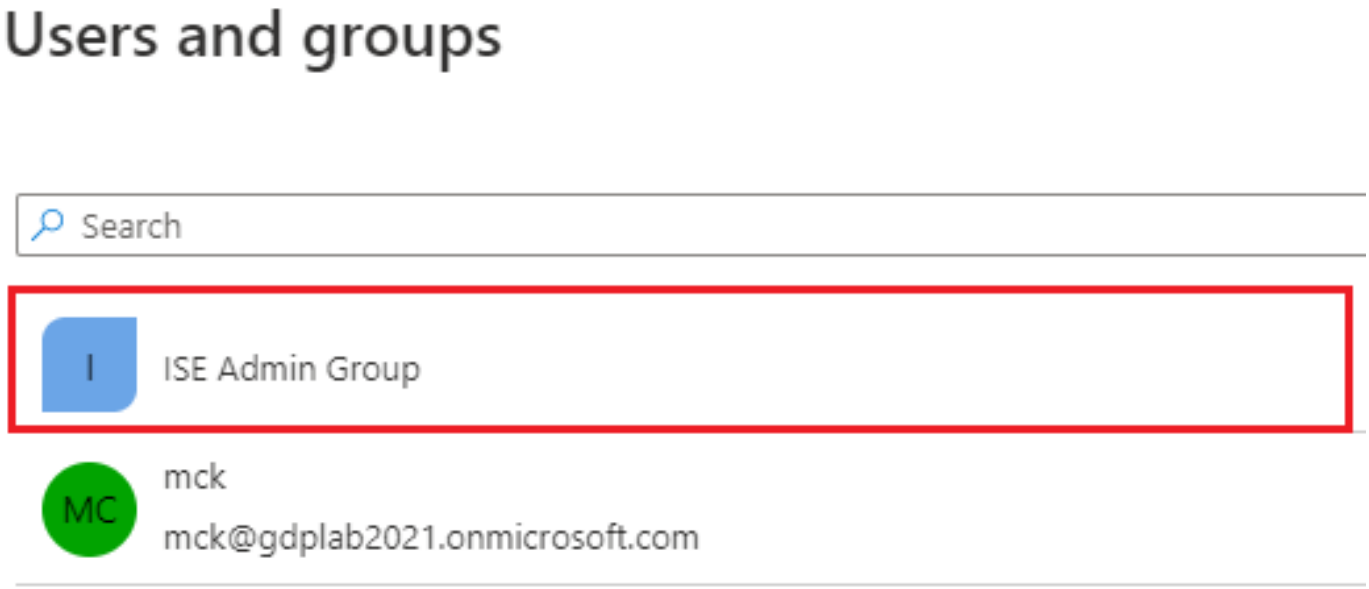


Cliquez sur Utilisateurs et groupes.

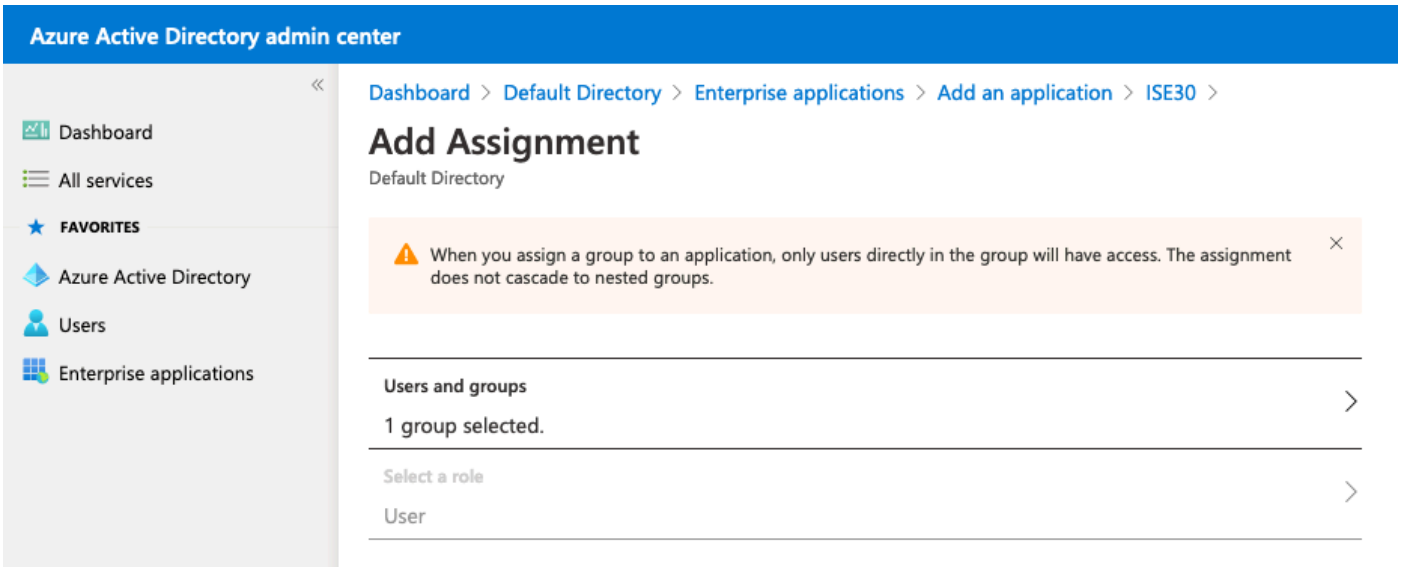


Choisissez le groupe configuré précédemment et cliquez sur Sélectionner.

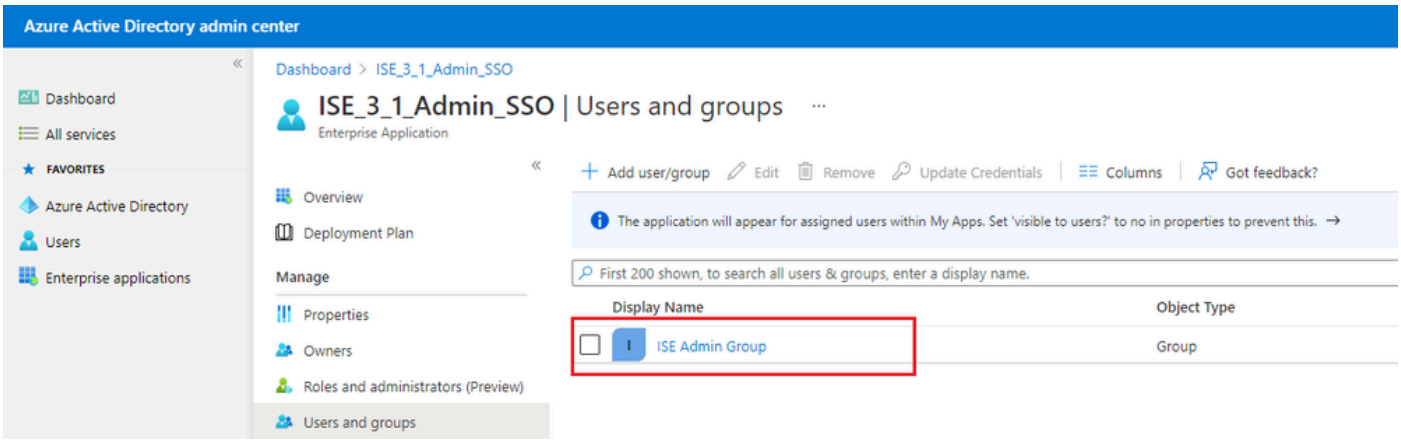
Remarque : Sélectionnez l'ensemble d'utilisateurs ou de groupes qui obtiennent l'accès voulu, car les utilisateurs et les groupes mentionnés ici ont accès à l'ISE une fois la configuration terminée.



Une fois le groupe sélectionné, cliquez sur Assign.

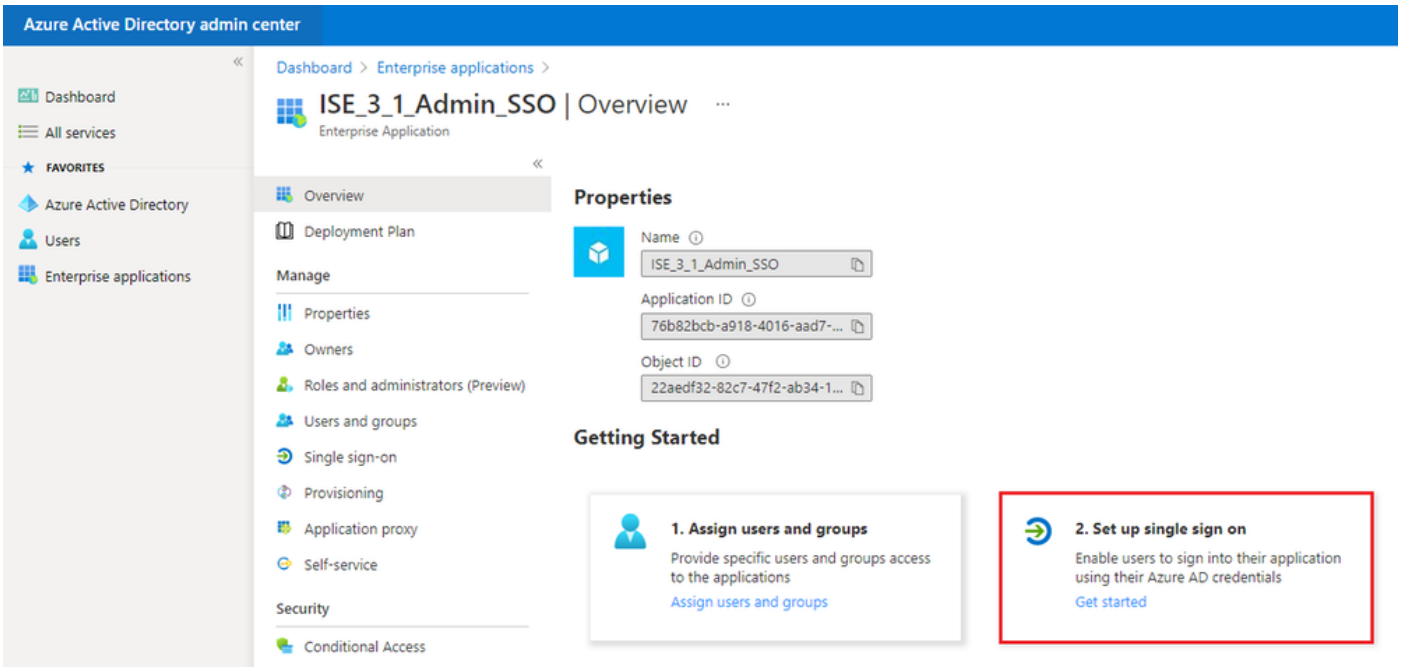


Par conséquent, le menu Utilisateurs et groupes de l'application configurée est renseigné avec le groupe sélectionné.

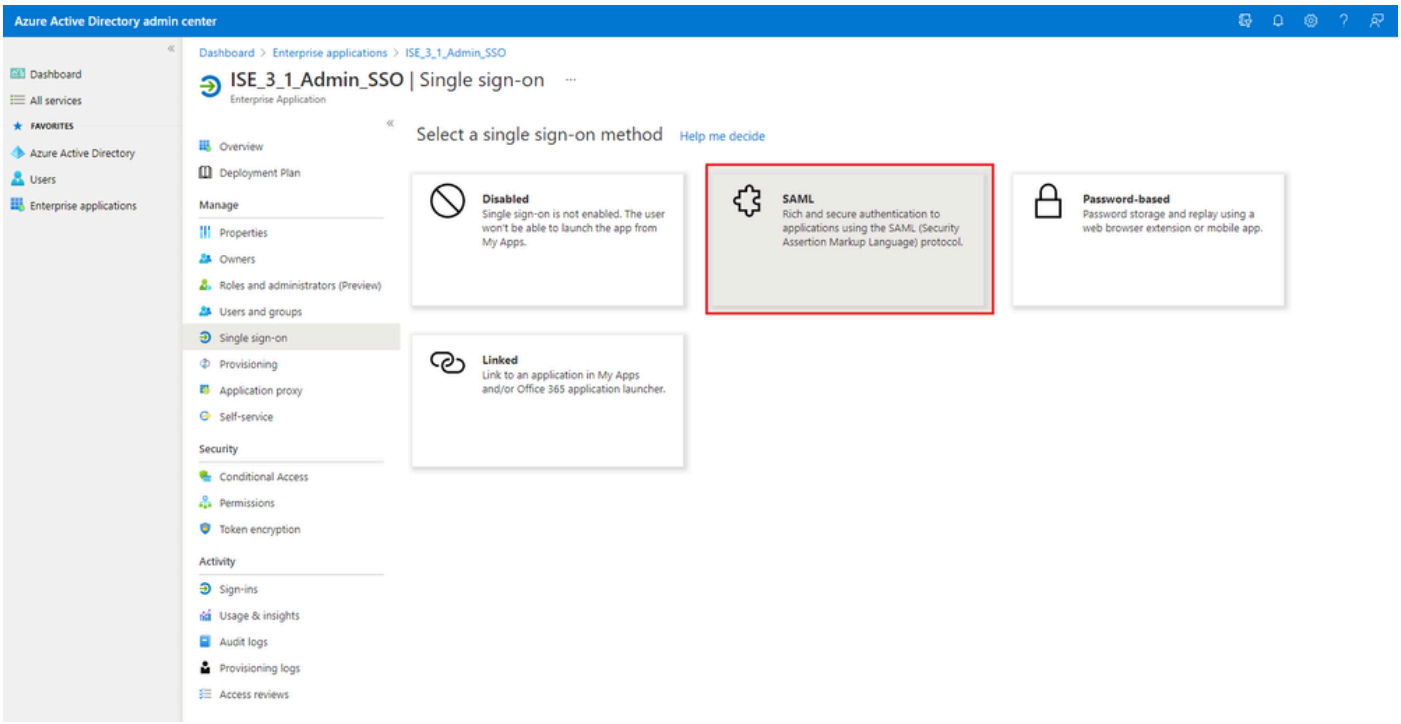


6. Configurez une application Azure AD Enterprise :

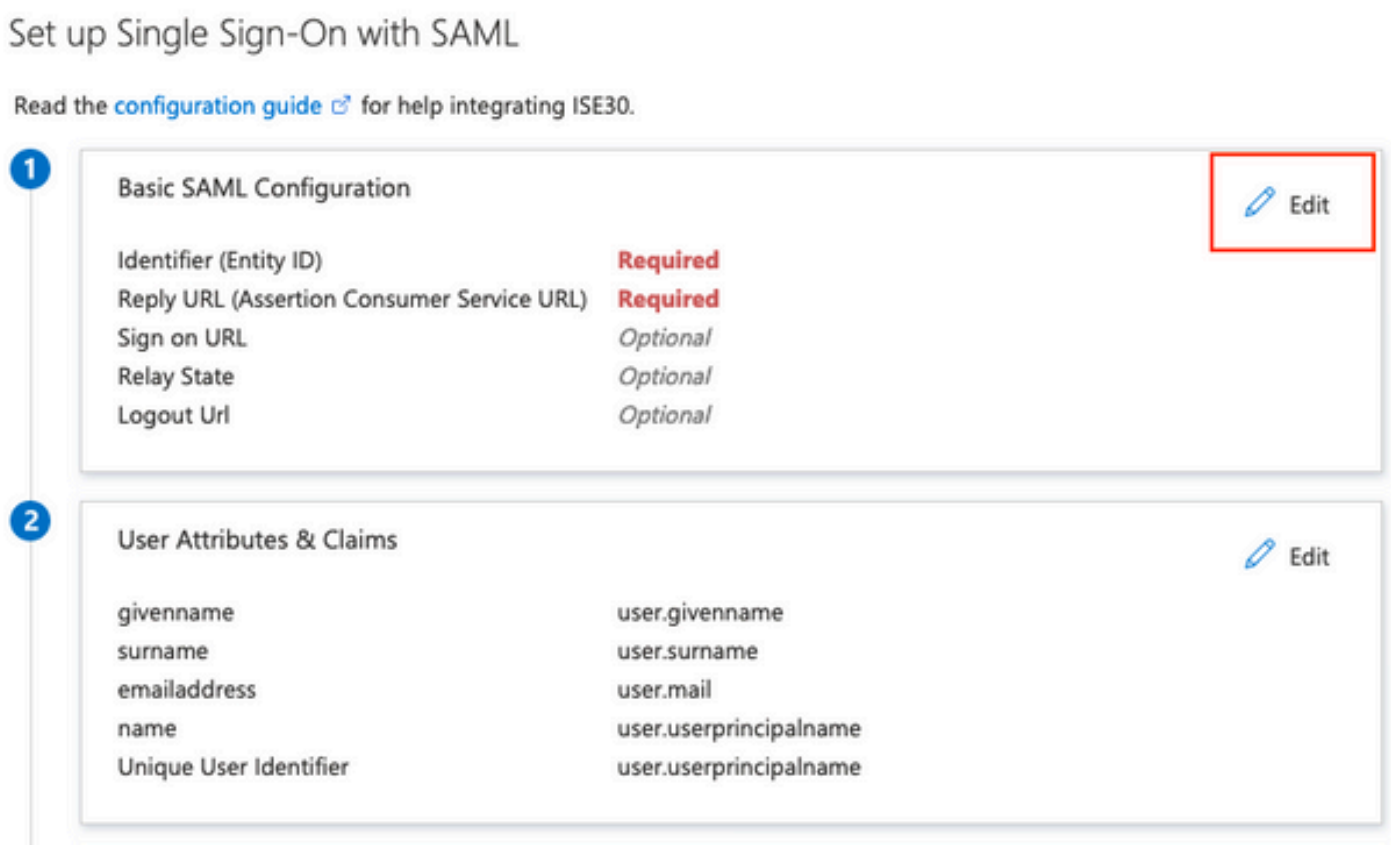
Revenez à votre application et cliquez sur Configurer l'authentification unique.



Sélectionnez SAML sur l'écran suivant.

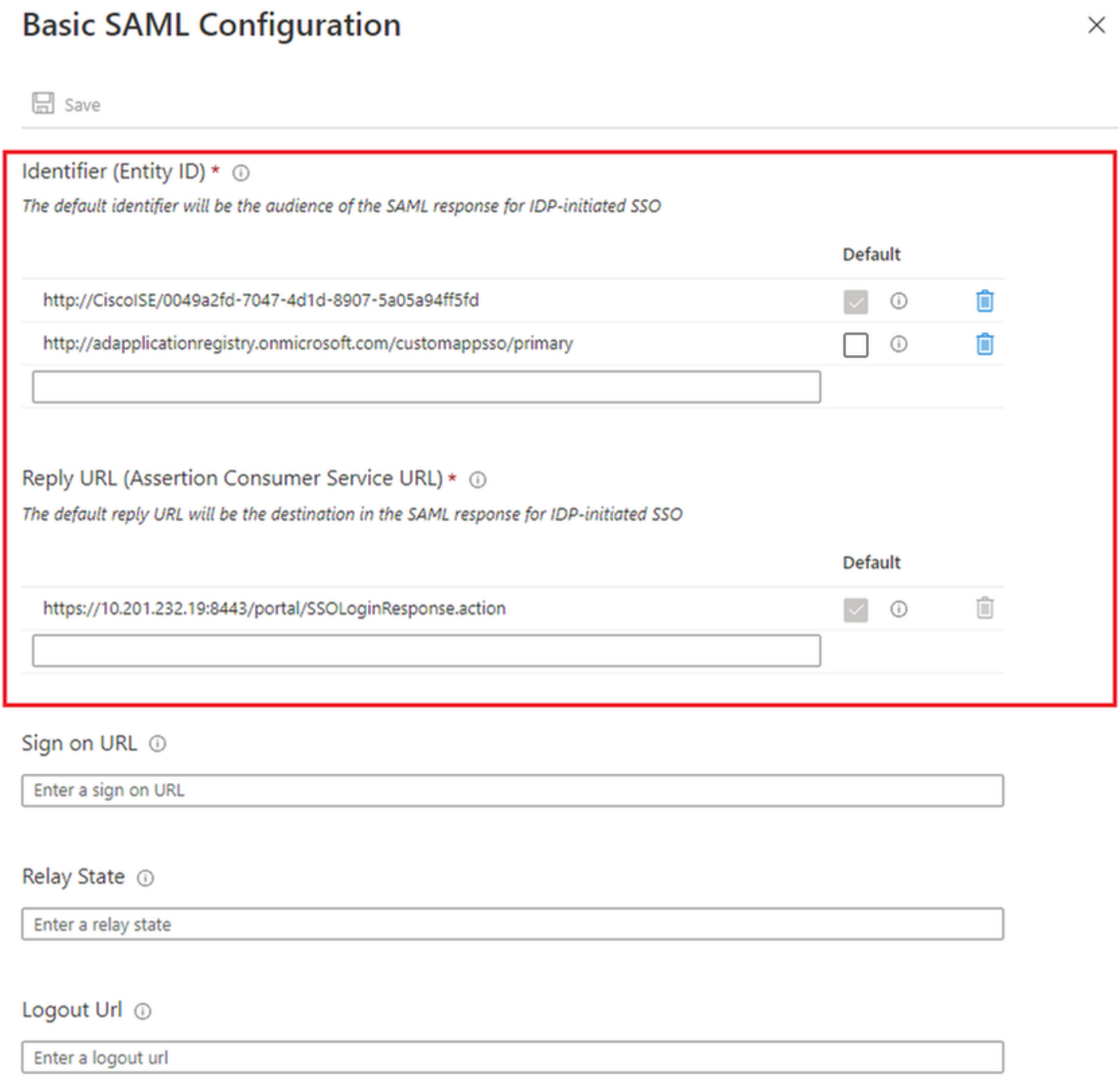


Cliquez sur Edit en regard de Basic SAML Configuration.



Renseignez Identifier (ID d'entité) avec la valeur entityID du fichier XML de l'étape Exporter les informations du fournisseur de services. Renseignez l'URL de réponse (URL du service consommateur d'assertions) avec la valeur Emplacements de AssertionConsumerService. Cliquez sur Enregistrer.

Remarque : L'URL de réponse agit comme une liste de passage, ce qui permet à certaines URL d'agir en tant que source lorsqu'elles sont redirigées vers la page du fournisseur d'identité.

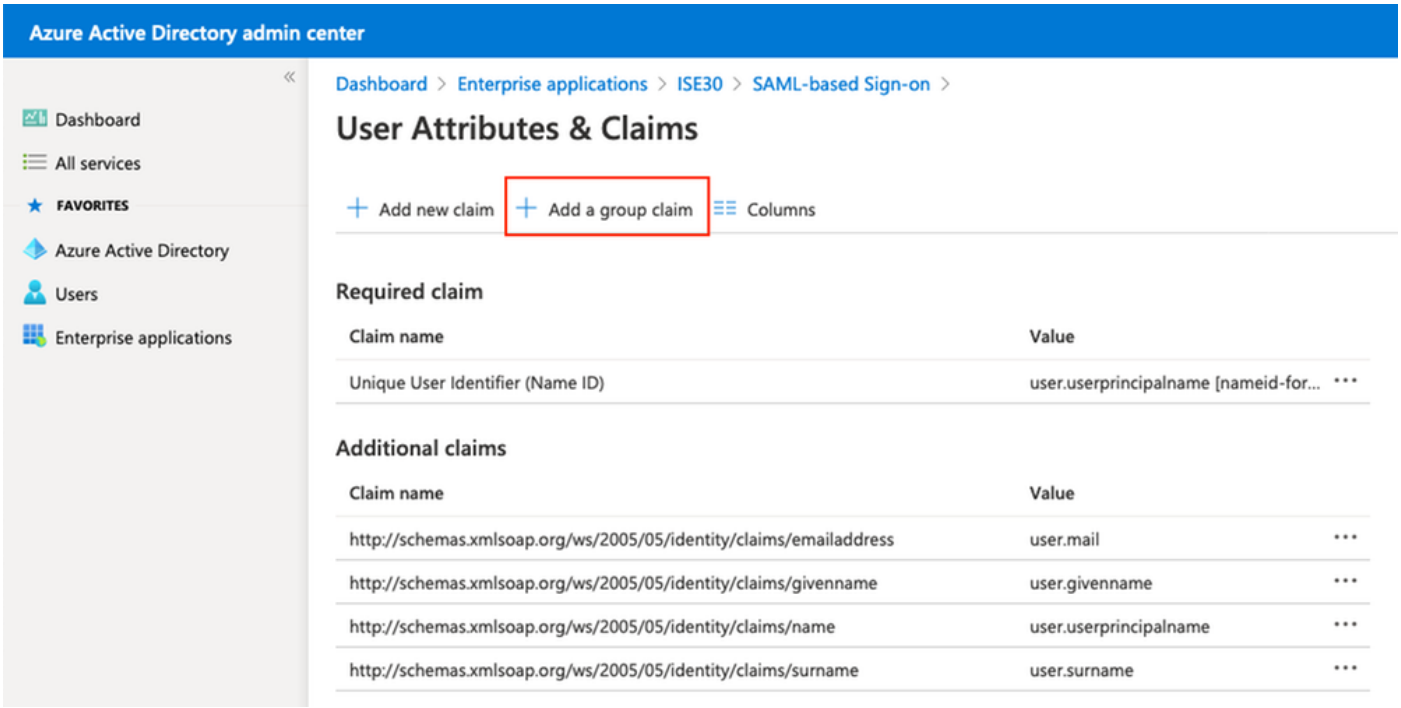


7. Configurez l'attribut Groupe Active Directory :

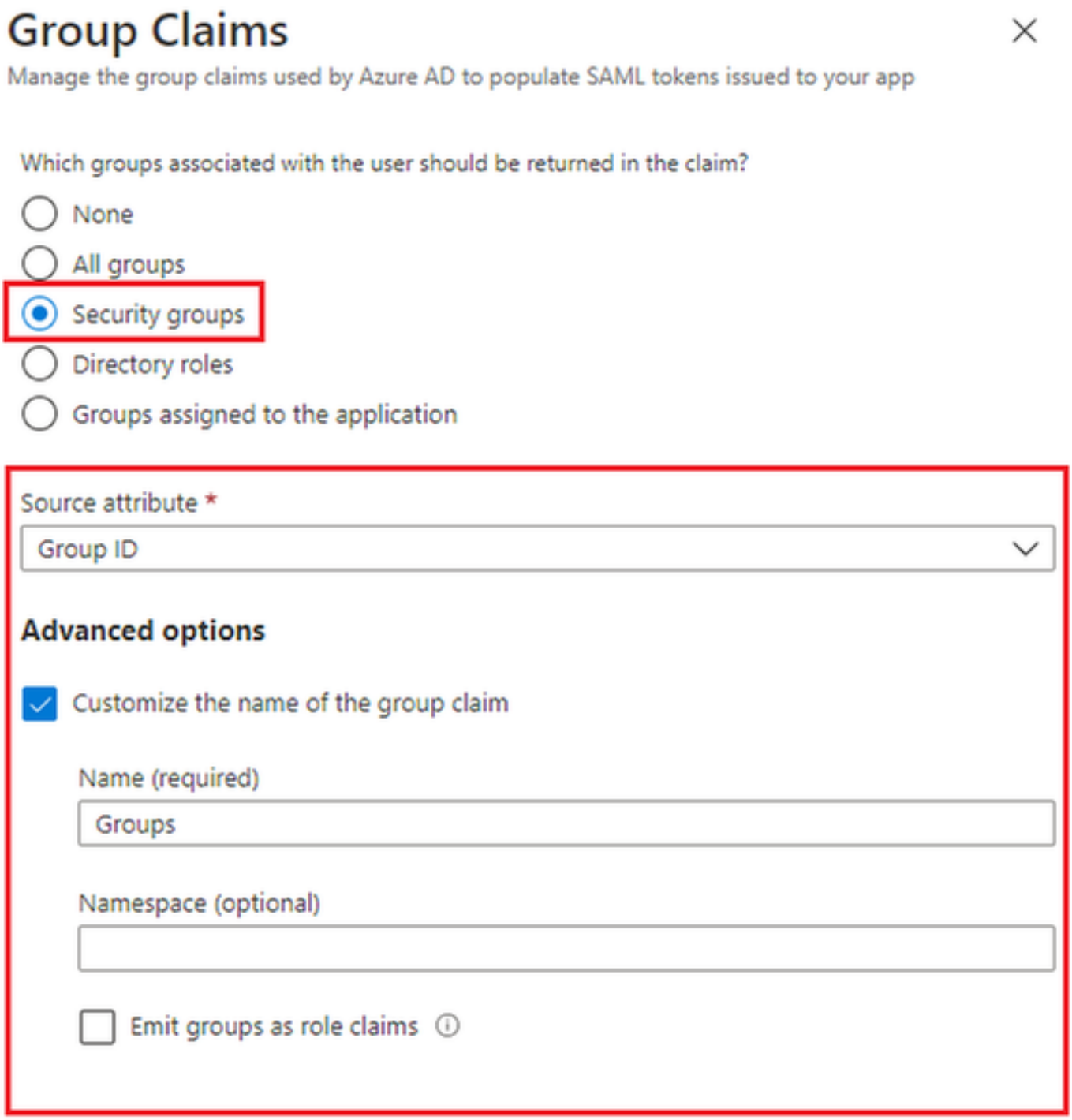
Afin de retourner la valeur d'attribut de groupe configurée précédemment, cliquez sur Edit à côté de User Attributes & Claims.



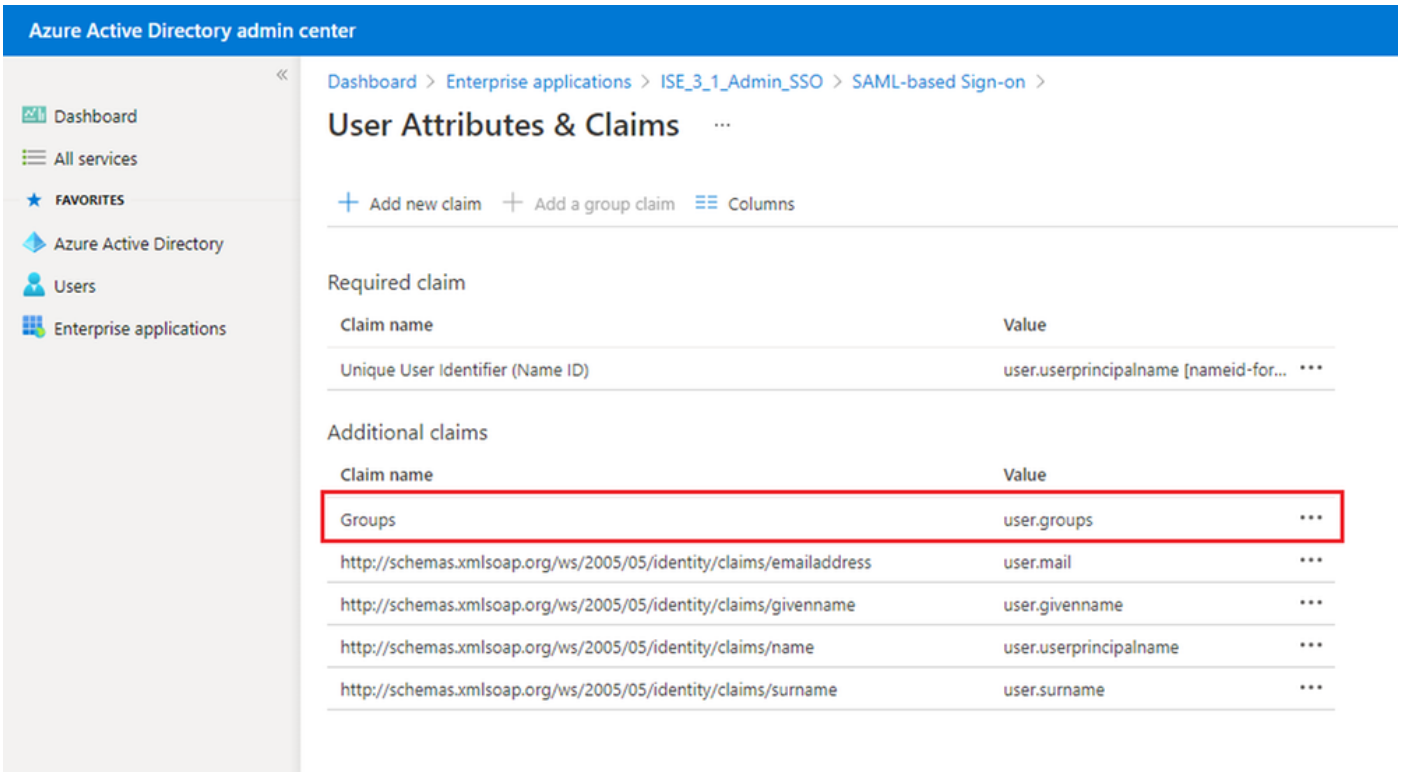
Cliquez sur Ajouter une revendication de groupe.



Sélectionnez Groupes de sécurité et cliquez sur Enregistrer. Sélectionnez ID de groupe dans le menu déroulant de l'attribut Source. Cochez la case pour personnaliser le nom de la revendication de groupe et entrez le nom Groupes.

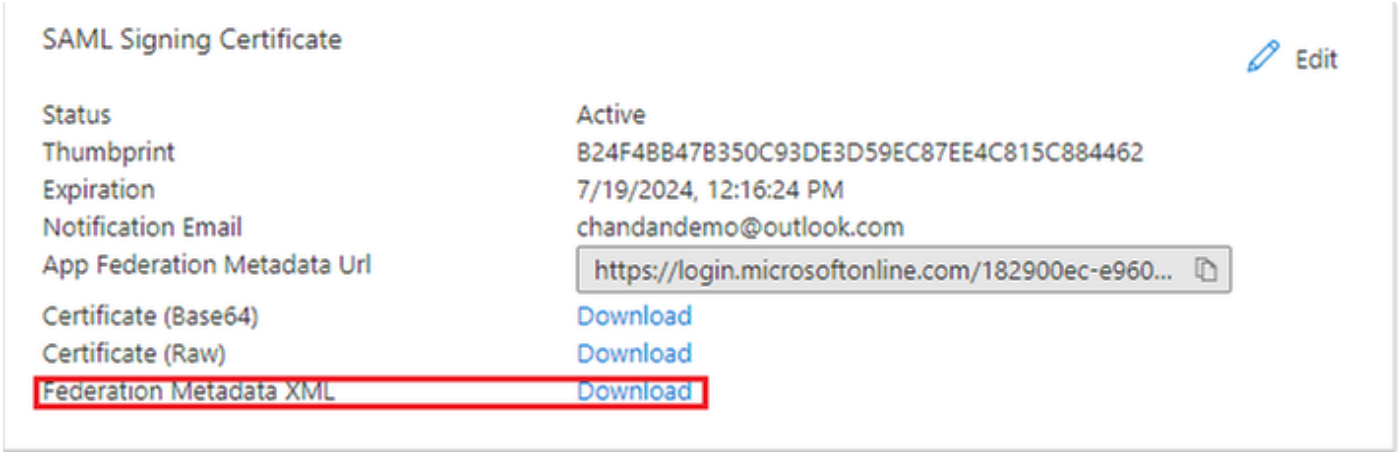


Notez le nom de la demande pour le groupe. Dans ce cas, il s'agit de Groupes.



8. Téléchargez le fichier XML de métadonnées Azure Federation :

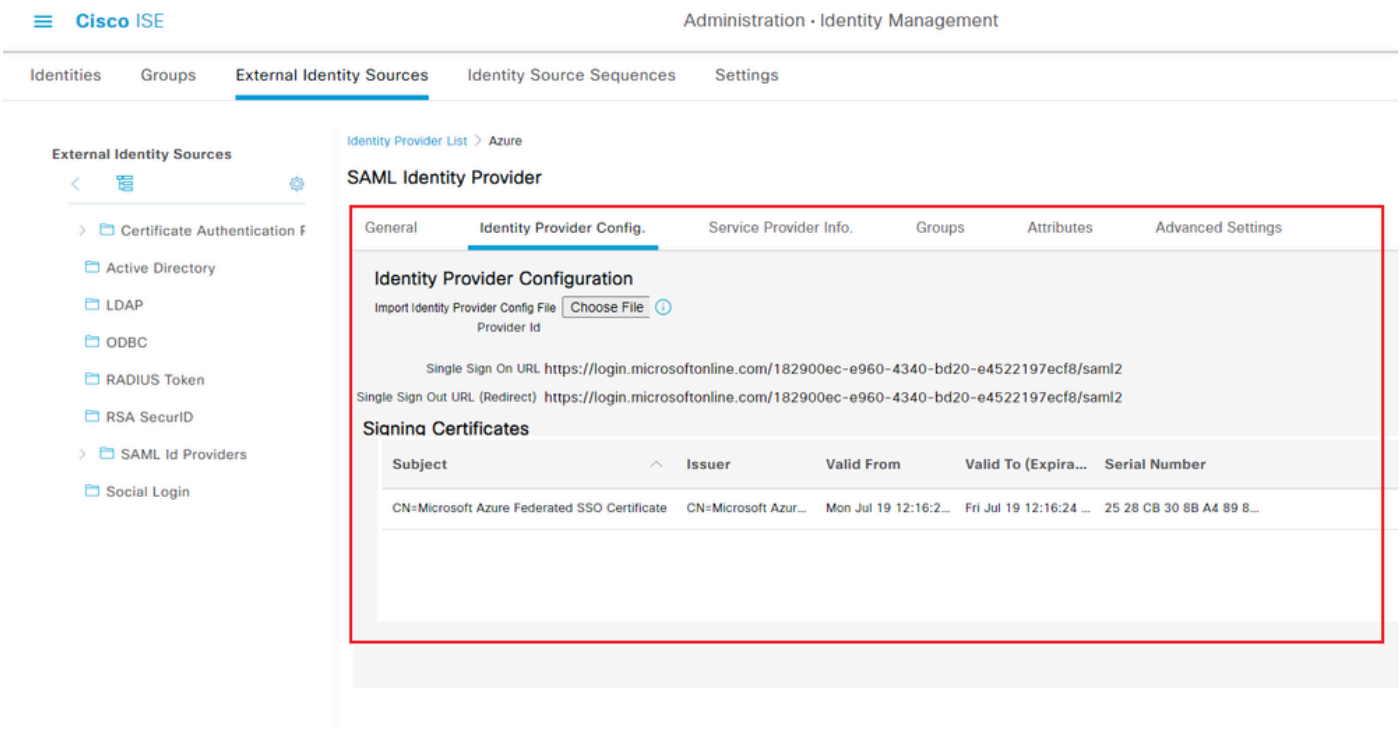
Cliquez sur Télécharger par rapport au XML de métadonnées de fédération dans le certificat de signature SAML.



Étape 3. Télécharger des métadonnées d'Azure Active Directory vers ISE

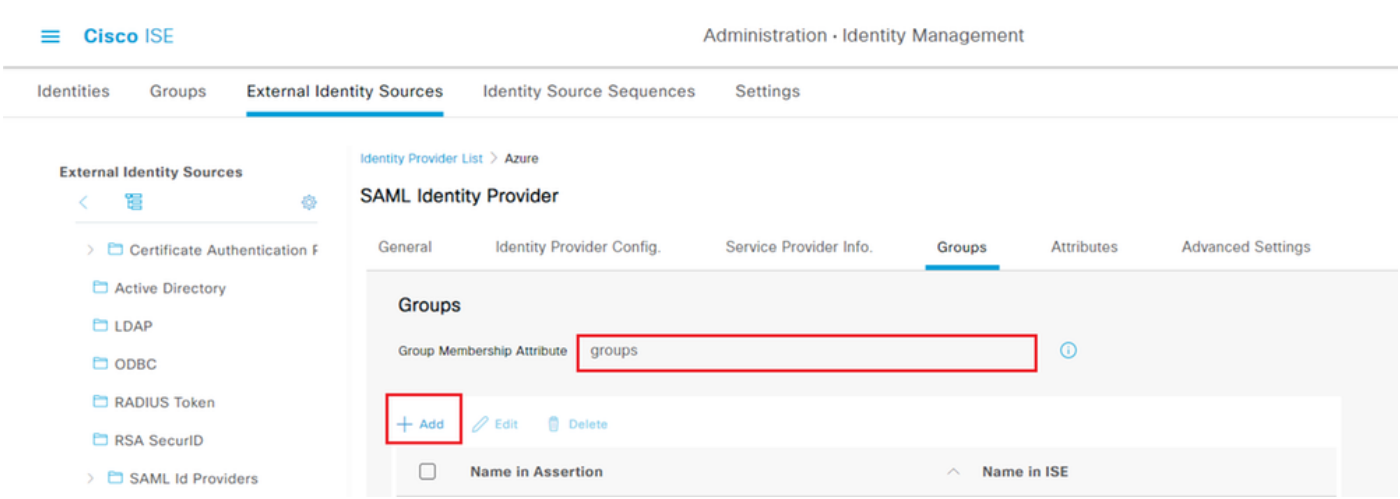
Accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].

Basculez l'onglet vers Identity Provider Config. et cliquez sur Browse. Sélectionnez le fichier XML de métadonnées de fédération à l'étape Télécharger le XML de métadonnées de fédération Azure et cliquez sur Enregistrer.



Étape 4 : configuration des groupes SAML sur ISE

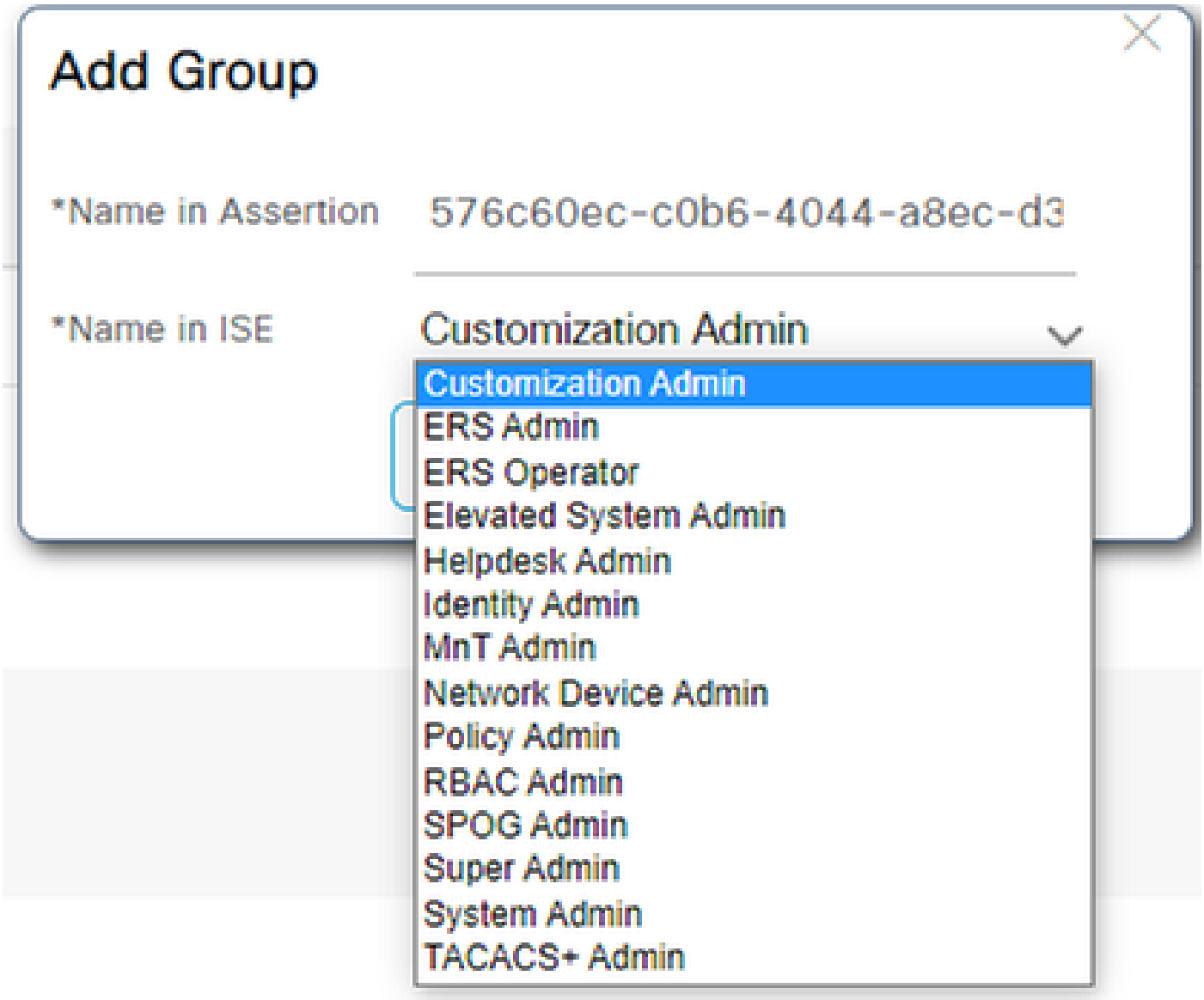
Basculez vers l'onglet Groupes et collez la valeur du nom de la revendication de l'attribut Configurer le groupe Active Directory dans l'attribut d'appartenance au groupe.



Cliquez sur Ajouter. Renseignez Name dans Assertion avec la valeur de Group Object id du groupe ISE Admin Group capturé dans Assign Azure Active Directory User to the Group.

Configurez Name dans ISE avec la liste déroulante et sélectionnez le groupe approprié sur ISE. Dans cet exemple, le groupe utilisé est Super Admin. Click OK. Cliquez sur Save.

Ceci crée un mappage entre le groupe dans Azure et le nom du groupe sur ISE.

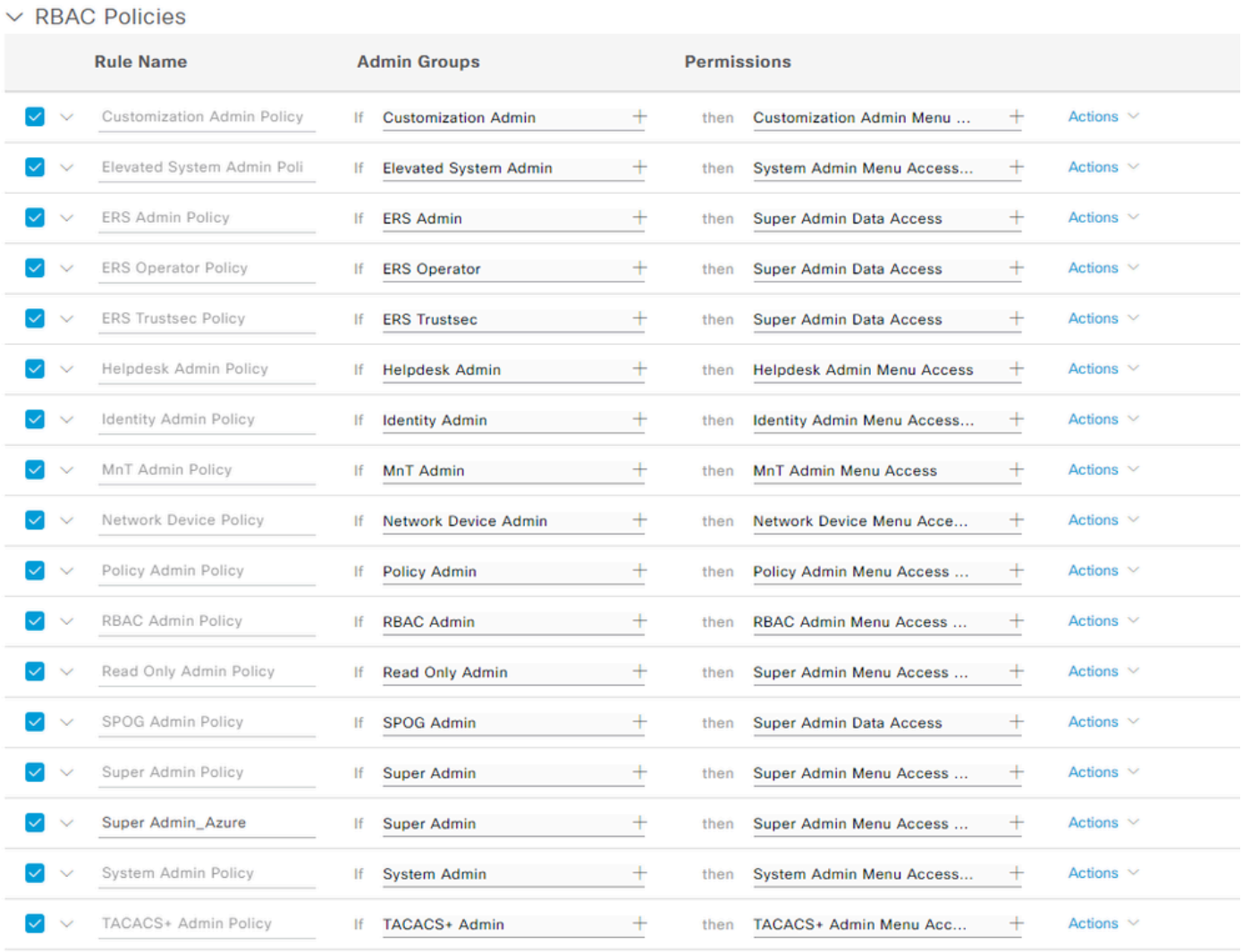


(Facultatif) Étape 5 : configuration des stratégies RBAC

De l'étape précédente, il existe différents types de niveaux d'accès utilisateur qui peuvent être configurés sur ISE.

Pour modifier les politiques de contrôle d'accès basées sur les rôles (RBAC), accédez à Administration > System > Admin Access > Authorization > Permissions > RBAC Policies et configurez-les si nécessaire.

Cette image est une référence à l'exemple de configuration.



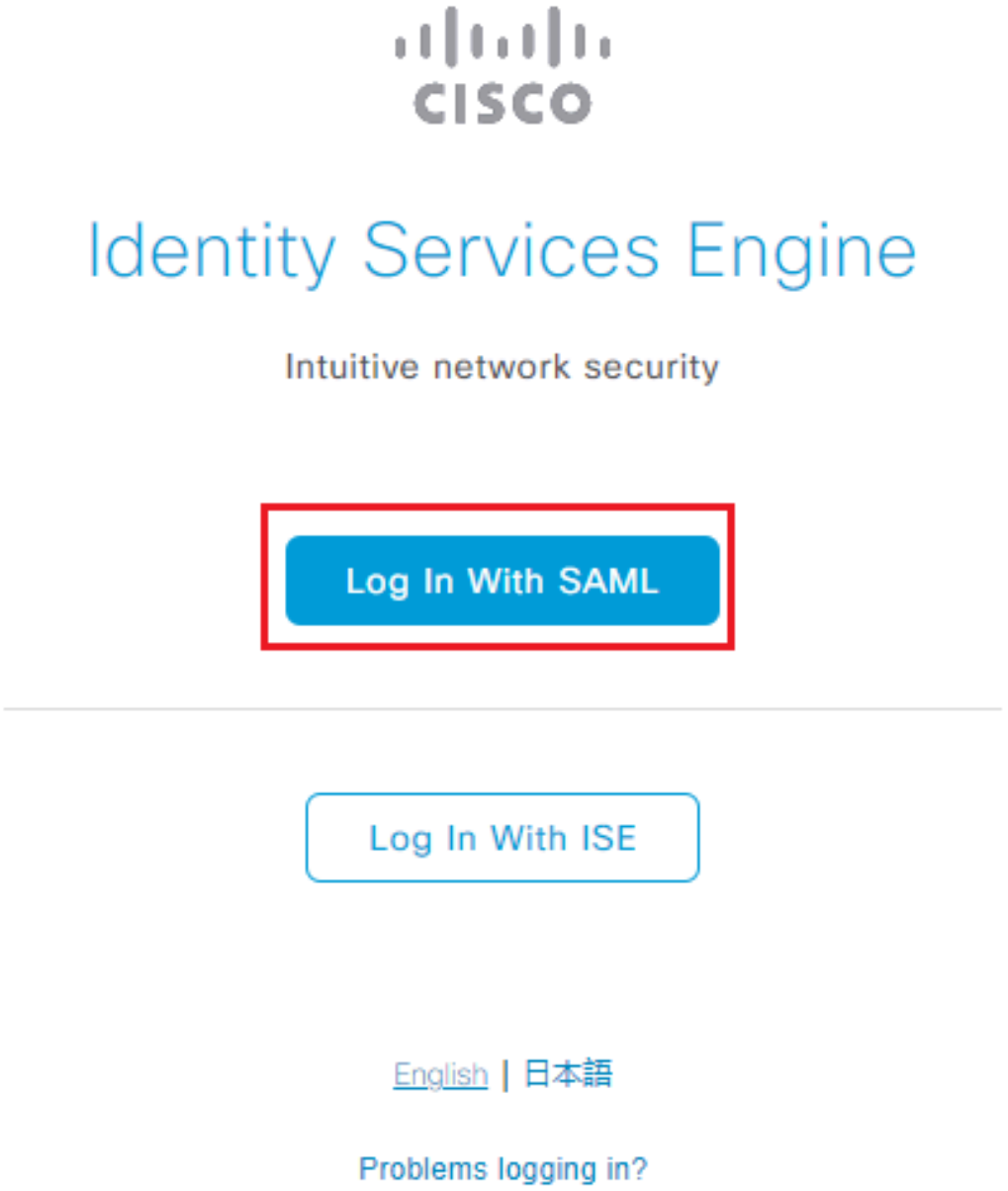
Vérifier

Vérifiez que votre configuration fonctionne correctement.

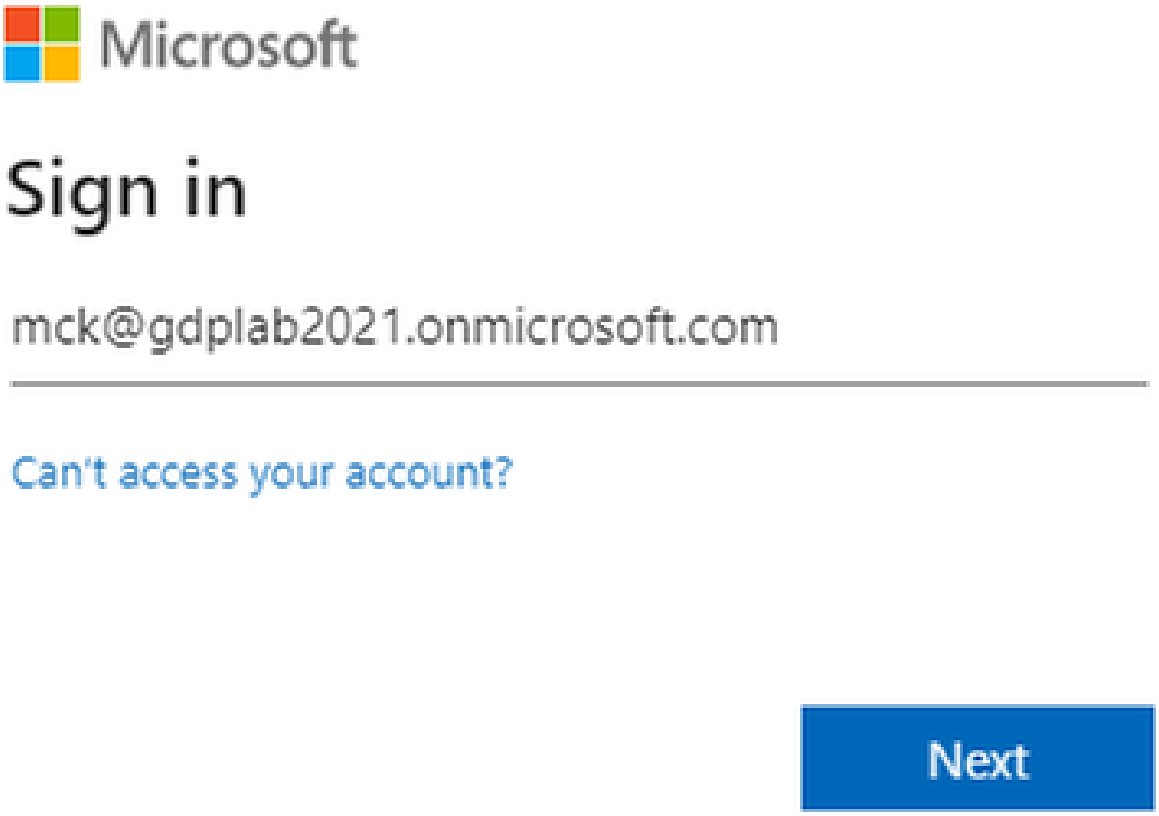
Remarque : Le test de connexion SAML SSO de la fonctionnalité de test Azure ne fonctionne pas. La demande SAML doit être initiée par ISE pour que l'authentification unique SAML Azure fonctionne correctement.

Ouvrez l'écran d'invite de connexion à l'interface ISE. Une nouvelle option vous est présentée pour vous connecter avec SAML.

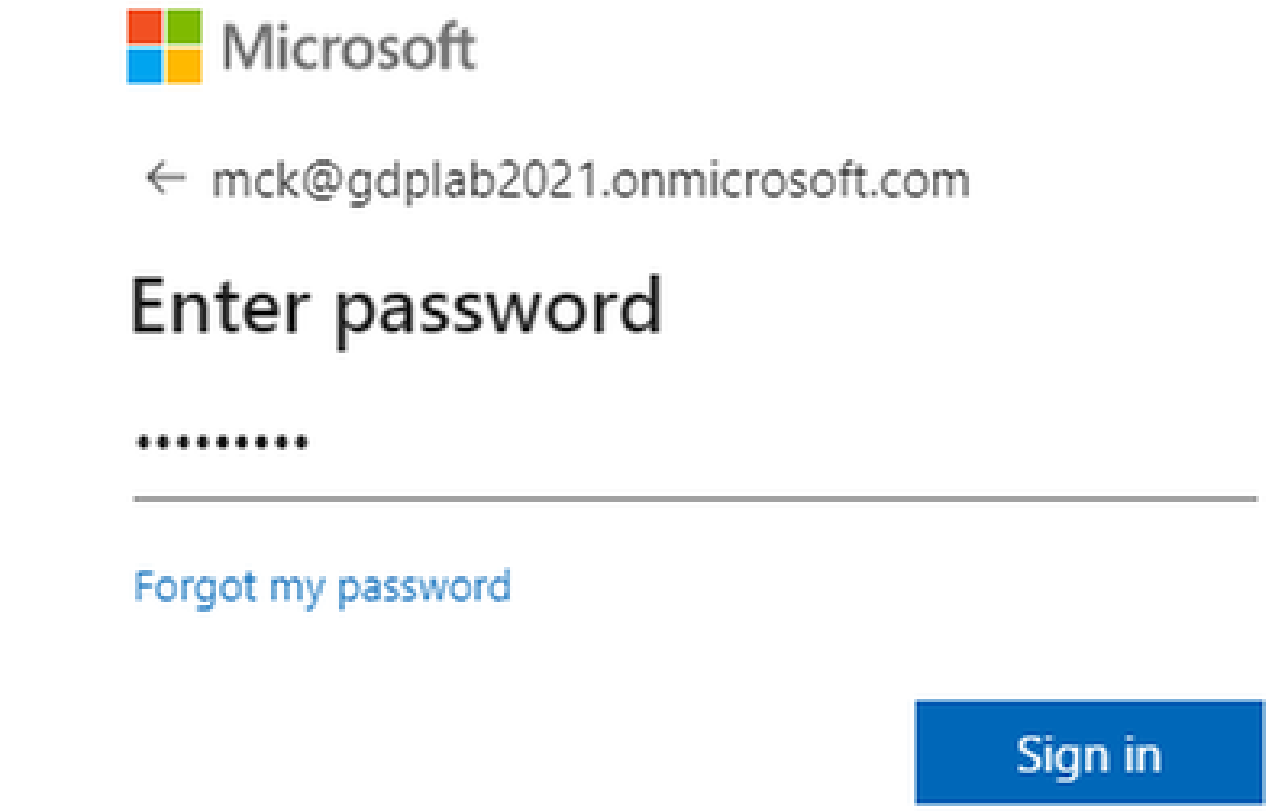
1. Accédez à la page de connexion à l'interface utilisateur graphique ISE et cliquez sur Log In with SAML.



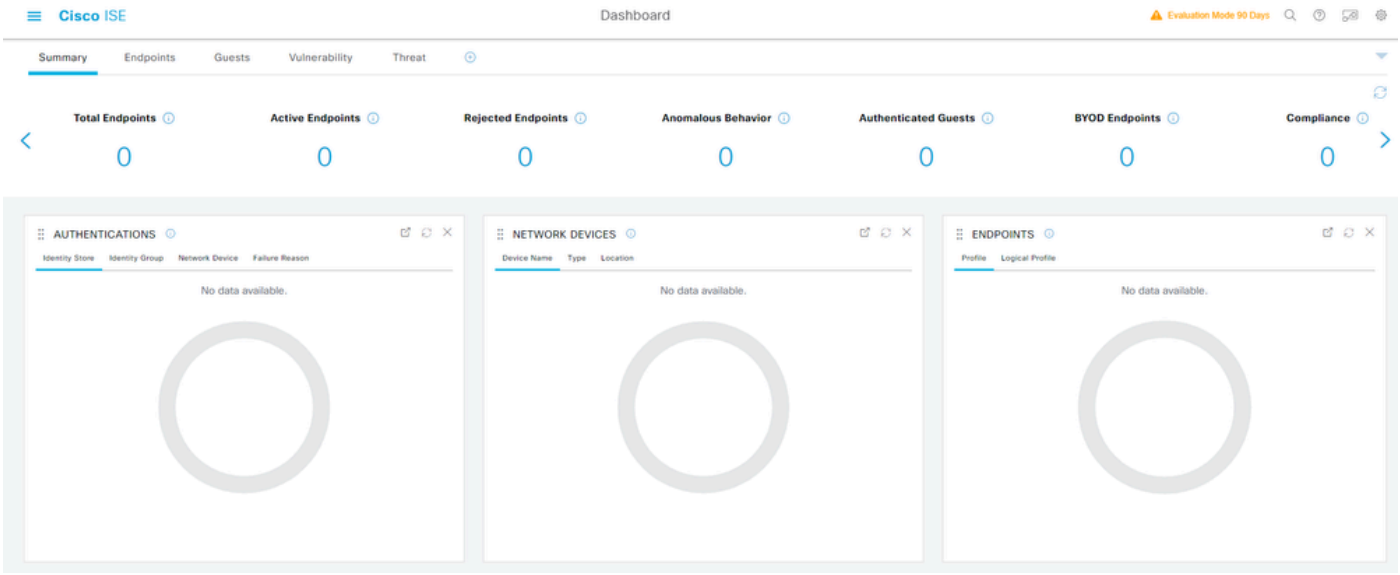
2. Vous êtes redirigé vers l'écran de connexion Microsoft. Entrez vos identifiants de nom d'utilisateur d'un compte dans un groupe mappé à ISE comme indiqué ici et cliquez sur Next comme indiqué dans l'image.



3. Entrez votre mot de passe pour l'utilisateur et cliquez sur Connexion.



4. Vous êtes à présent redirigé vers le tableau de bord de l'application ISE avec les autorisations appropriées configurées en fonction du groupe ISE configuré précédemment comme indiqué dans l'image.



Dépannage

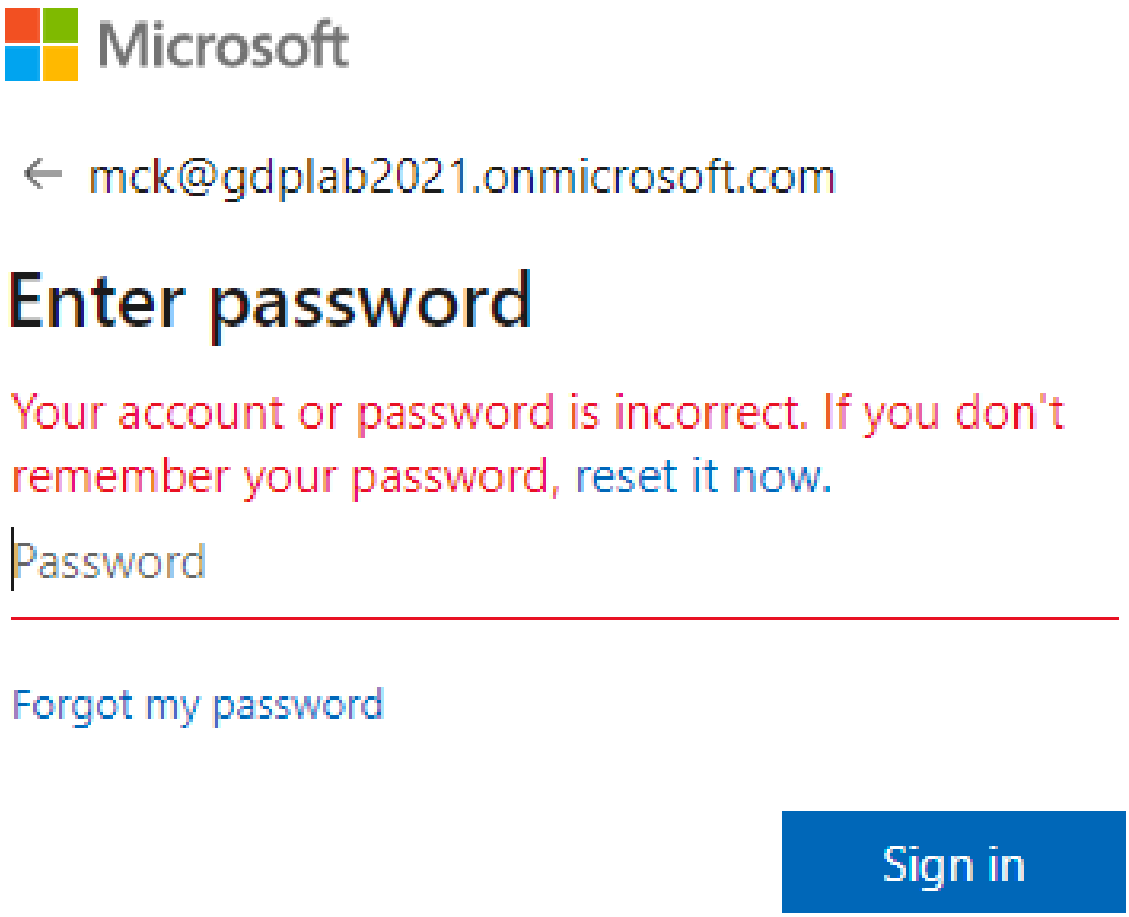
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Problèmes courants

Il est essentiel de comprendre que l'authentification SAML est gérée entre le navigateur et Azure Active Directory. Par conséquent, vous pouvez obtenir des erreurs liées à l'authentification directement auprès du fournisseur d'identité (Azure) où l'engagement ISE n'a pas encore commencé.

Problème 1. L'erreur « Votre compte ou votre mot de passe est incorrect » s'affiche une fois que vous avez entré les informations d'identification. Ici, les données utilisateur ne sont pas encore reçues par ISE et le processus à ce stade reste avec IdP (Azure).

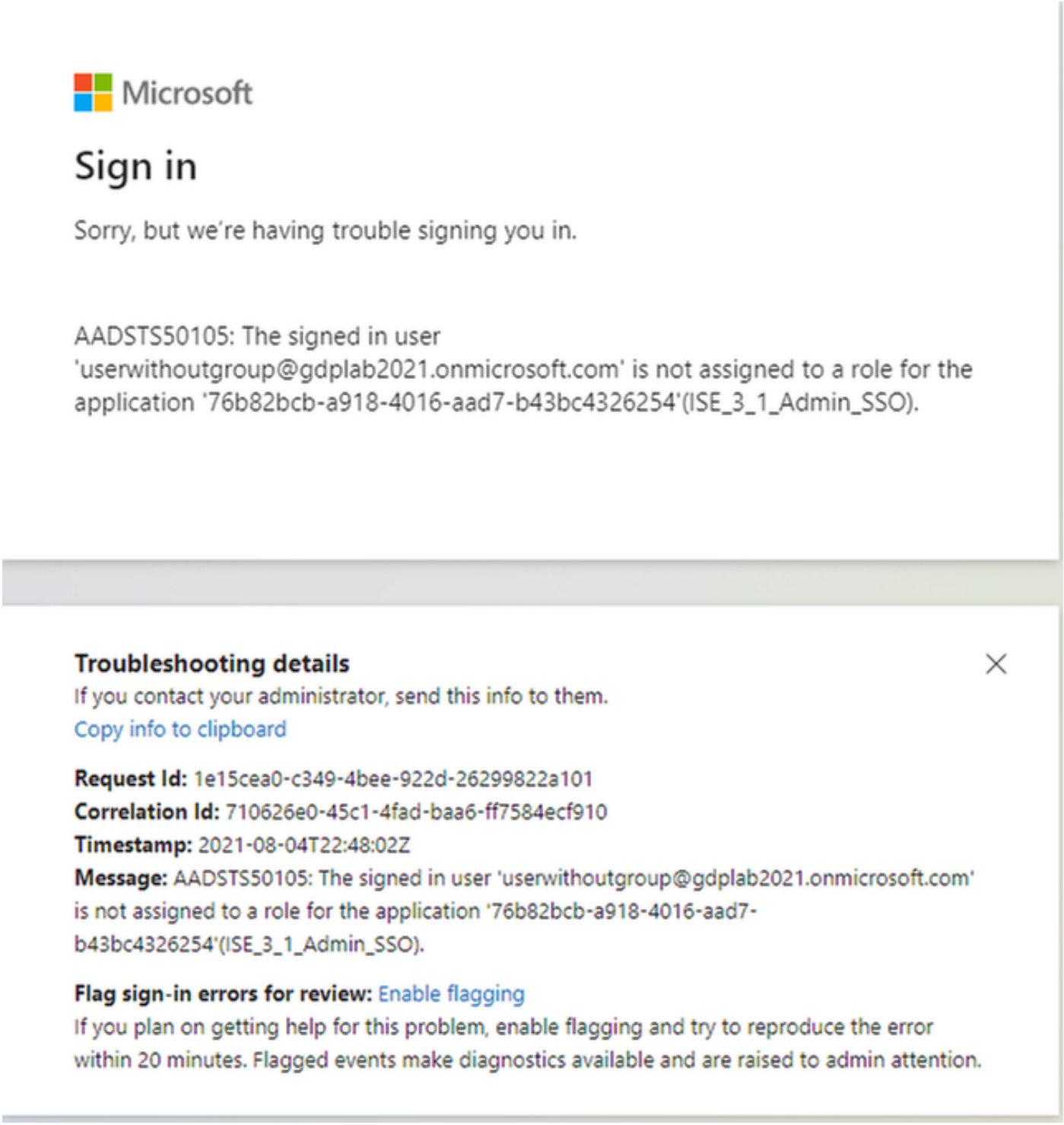
La raison la plus probable est que les informations de compte sont incorrectes ou que le mot de passe est incorrect. Afin de fixer : réinitialisez le mot de passe ou fournissez le mot de passe correct pour ce compte, comme indiqué dans l'image.



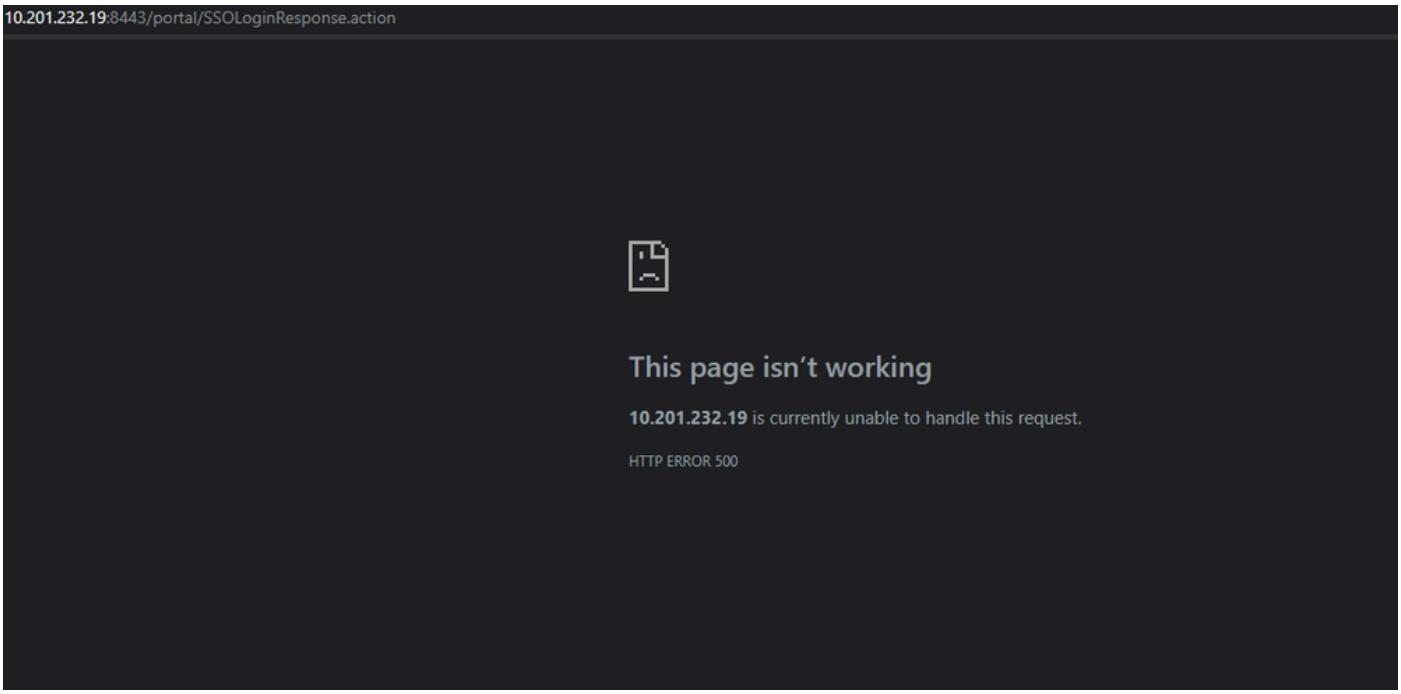
Problème 2. L'utilisateur ne fait pas partie du groupe qui est censé être autorisé à accéder à SAML SSO. Comme dans le cas précédent, les données utilisateur ne sont pas encore reçues par

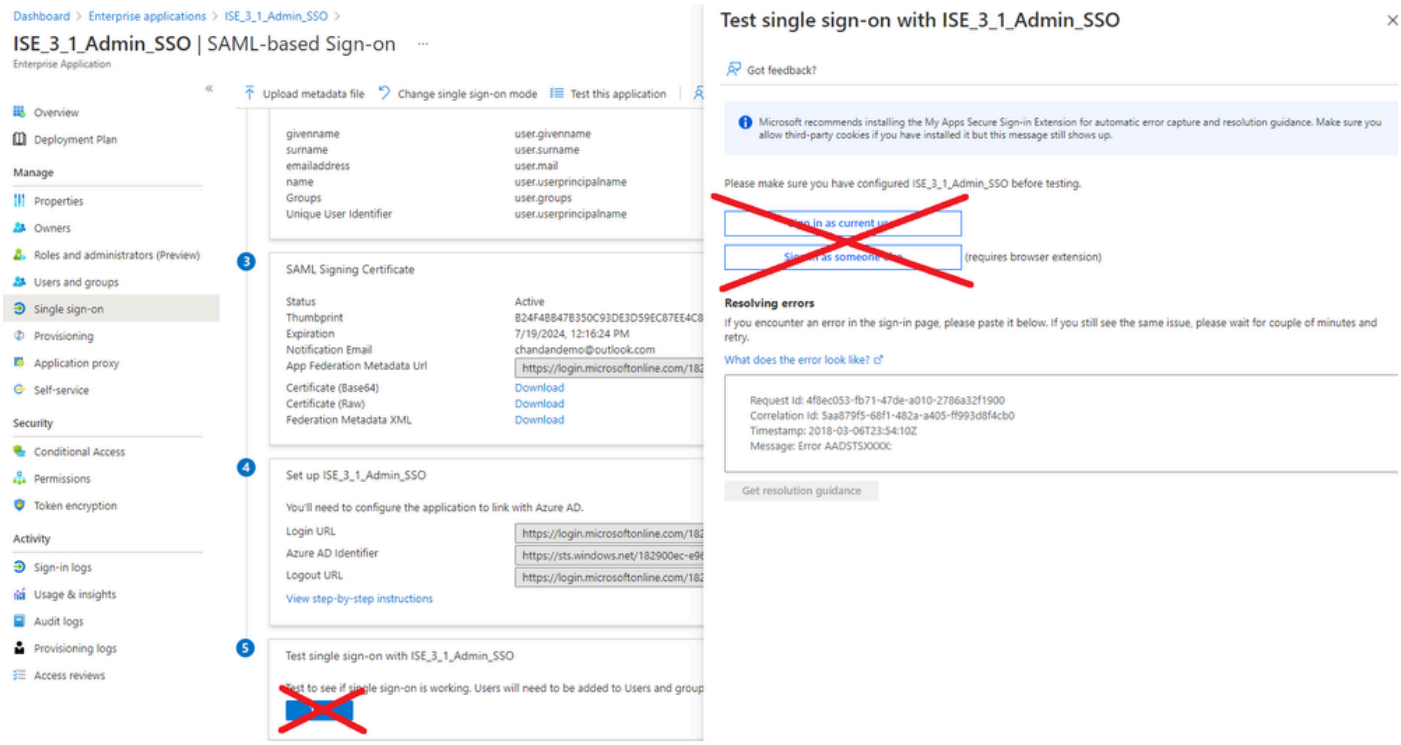
ISE et le processus reste à ce stade avec IdP (Azure).

Solution : vérifiez que l'étape Add group to the Application configuration est correctement exécutée comme indiqué dans l'image.



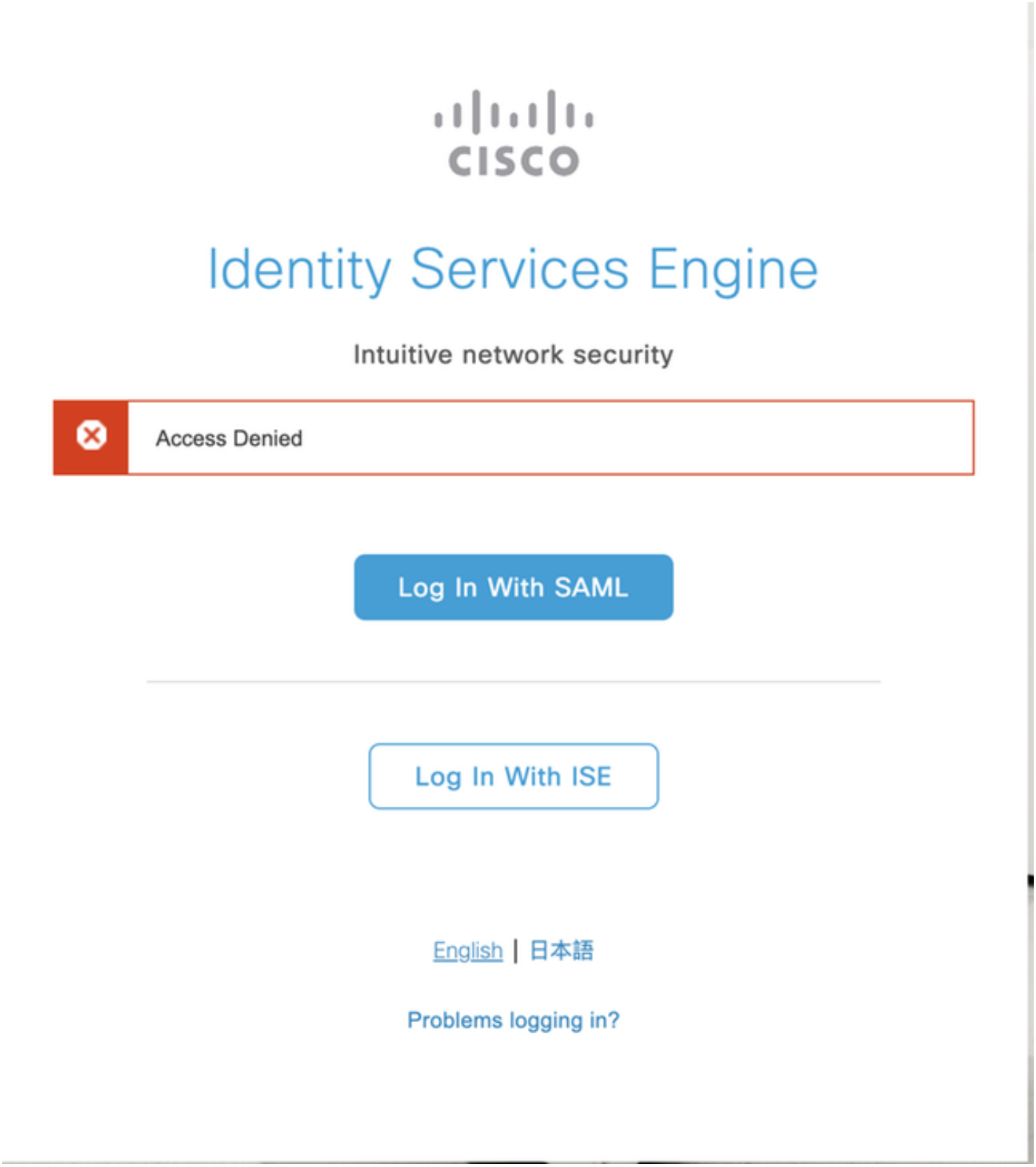
Problème 3. Le serveur d'applications ISE ne peut pas traiter les demandes de connexion SAML. Ce problème se produit lorsque la demande SAML est initiée à partir du fournisseur d'identité Azure, au lieu du fournisseur de services ISE. Le test de la connexion SSO à partir d'Azure AD ne fonctionne pas car ISE ne prend pas en charge les requêtes SAML initiées par le fournisseur d'identité.





Problème 4. ISE affiche l'erreur « Accès refusé » après une tentative de connexion. Cette erreur se produit lorsque le nom de la revendication du groupe créé précédemment dans l'application Entreprise Azure ne correspond pas dans ISE.

Solution : assurez-vous que le nom de la revendication de groupe dans Azure et ISE sous l'onglet Groupes du fournisseur d'identité SAML sont identiques. Référez-vous aux étapes 2.7. et 4. sous la section Configurer SSO SAML avec Azure AD de ce document pour plus de détails.



Dépannage d'ISE

Le niveau de consignation des composants doit être modifié sur ISE. Accédez à Operations > Troubleshoot > Debug Wizard > Debug Log Configuration.

Nom du composant	Niveau de consignation	Nom du fichier journal

portail	DÉBOGUER	guest.log
ouvert	DÉBOGUER	ise-psc.log
petit	DÉBOGUER	ise-psc.log

Journaux avec nom de connexion SAML et nom de revendication de groupe incompatible

Ensemble de débogages affichant un scénario de dépannage de non-correspondance de nom de revendication au moment de l'exécution du flux (ise-psc.log).

Remarque : Gardez un oeil sur les éléments en gras. Les journaux ont été raccourcis pour des raisons de clarté.

---

1. L'utilisateur est redirigé vers l'URL IdP depuis la page d'administration ISE.

<#root>

```
2021-07-29 13:48:20,709 INFO   [admin-http-pool46][] api.services.persistance.dao.DistributionDAO -::::
2021-07-29 13:48:20,712 INFO   [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -::
```

forwardStr for: https://10.201.232.19/admin/LoginAction.do

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

IDP URL: https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

SAML request - spUrlToReturnTo:https://10.201.232.19:8443/portal/SSOLoginResponse.action

```
2021-07-29 13:48:20,844 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

2. Une réponse SAML est reçue du navigateur.

<#root>

```
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

```
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA

-:::::- Decoded SAML relay state of: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a

2021-07-29 13:48:27,177 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode

-:::::- Decoded SAML message

2021-07-29 13:48:27,182 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.dec
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::::- Intended message destination endpoint: h
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de

2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
```

3. L'analyse des attributs (assertions) est démarrée.

<#root>

```
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA

2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA

[parseAttributes] Set on IdpResponse object  - attribute<http://schemas.xmlsoap.org/ws/2005/05/identity/

2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

4. L'attribut Group est reçu avec la valeur 576c60ec-c0b6-4044-a8ec-d395b1475d6e, validation

de signature.

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
        IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
        SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
        Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOLoginResponse.action
        Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-89
        Client Address: 10.24.226.171
        Load Balancer: null
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,358 INFO   [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp
```

5. Validation des autorisations RBAC.

<#root>

```
**************************Rbac Log Summary for user samlUser***************************
2021-07-29 13:48:27,360 INFO   [admin-http-pool50][] com.cisco.ise.util.RBACUtil -::::- Populating cach

2021-07-29 13:48:27,368 ERROR  [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::

java.lang.NullPointerException

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login
```

```
2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login

2021-07-29 13:48:27,369 ERROR  [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- Can't sav

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -::

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

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.