Configurer le portail des sponsors ISE avec Microsoft Entra ID SAML SSO

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Diagramme D'Écoulement De Haut Niveau
- Configurer
  - Étape 1 : configuration du fournisseur d'identité SAML et du portail de sponsor sur ISE
    - Ajouter le fournisseur d'identité SAML
    - Configurer le portail de sponsor sur l'idP
    - Exporter les informations du fournisseur de services
  - Étape 2 : configuration de l'identifiant Microsoft Entra ID
    - Créer un utilisateur Azure AD
    - 2. Créez un groupe et ajoutez l'utilisateur
    - 3. Créer une application Entreprise
    - 4. Affectez le groupe (ou l'utilisateur) à l'application
  - Étape 3. Configuration de l'authentification unique SAML dans l'ID d'entrée
    - 2. Configurer l'attribut Groupe supplémentaire
    - 3. Téléchargez le fichier XML des métadonnées de fédération
  - Étape 4. Télécharger des métadonnées d'Entra vers ISE
    - Importer les métadonnées de fédération
    - Configurer des groupes SAML sur ISE
  - Étape 5 : configuration du mappage de groupe de sponsors sur ISE
- Vérifier
- Dépannage
  - Problème 2 — Utilisateur non affecté à l'application (AADSTS50105)
  - Problème 3 : échec de la déconnexion (« Échec de la déconnexion SSO »)
  - Problème 4 — Certificat de signature modifié (« L'authentification a échoué »)
  - Problème 5 : la session expire rapidement
  - Dépannage client
  - Dépannage ISE
  - Analyse de capture de paquets
    - Hello du client TLS : où le nom du portail est visible
    - La même connexion capturée sur le client

Introduction

Ce document décrit comment configurer Microsoft Entra ID en tant que fournisseur d'identité

SAML pour le portail des sponsors Cisco ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ID d'entrée Microsoft
- Cisco Identity Services Engine (ISE) 3.0
- Connaissances de base sur les déploiements SSO (Single Sign-On) SAML (Security Assertion Markup Language)

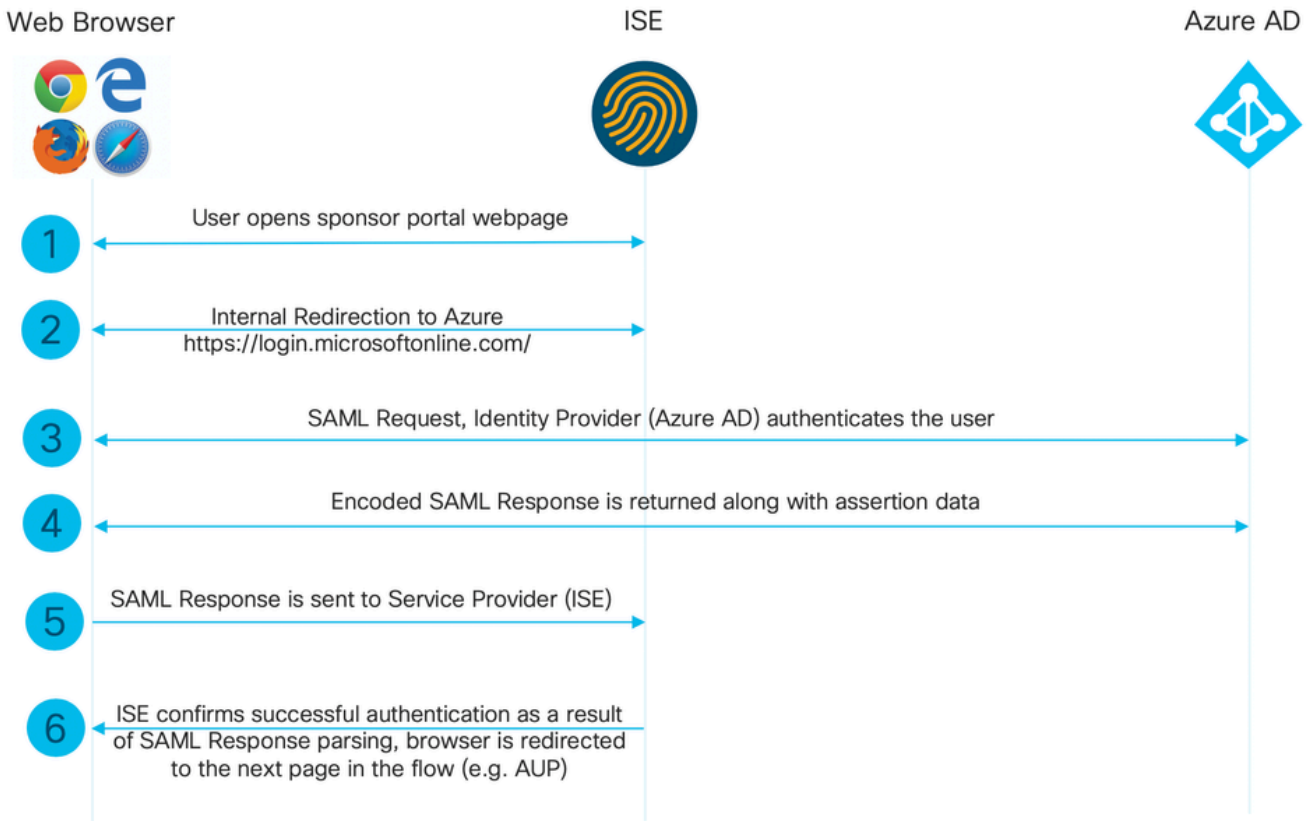
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions matérielles et logicielles suivantes :

- Cisco ISE 3.4 (la procédure s'applique à Cisco ISE 3.1 et versions ultérieures)
- ID d'entrée Microsoft

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.

Diagramme D'Écoulement De Haut Niveau



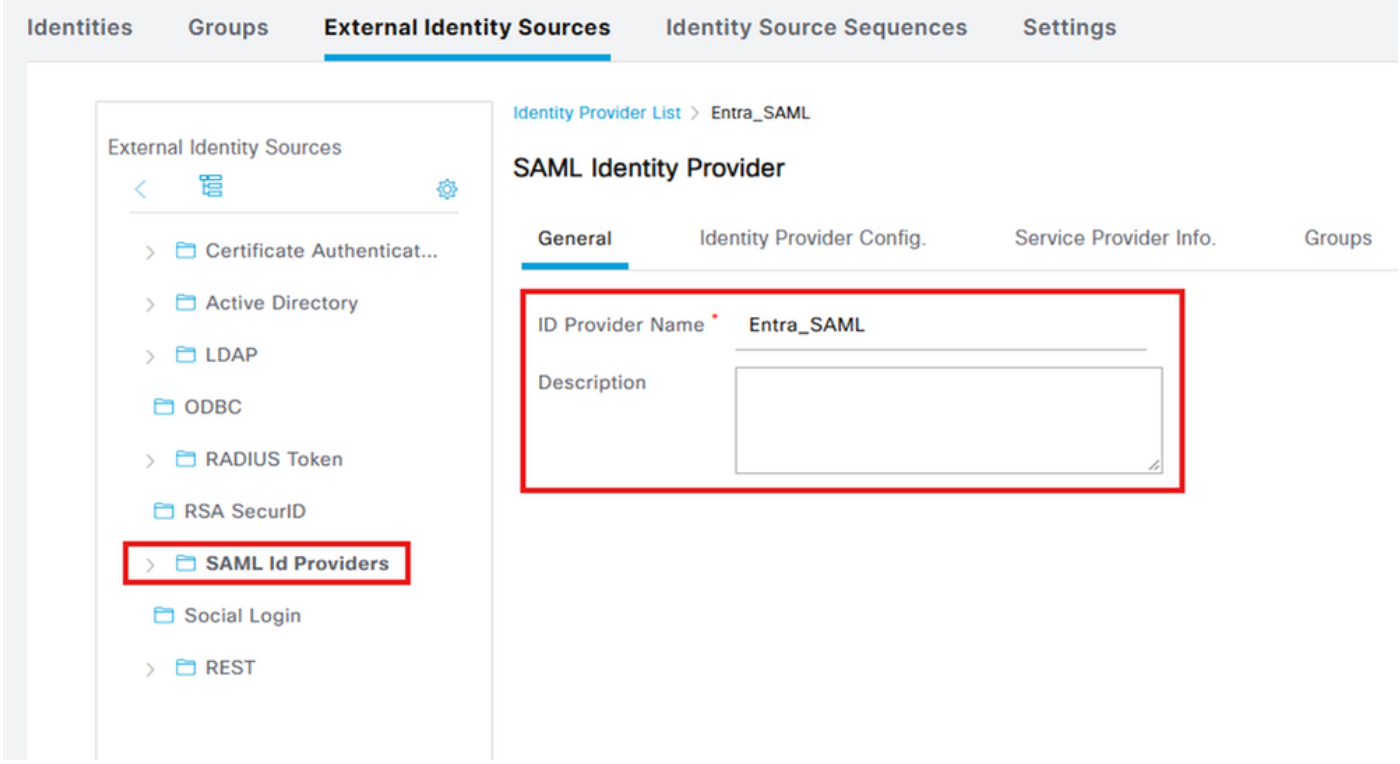
Configurer

Étape 1 : configuration du fournisseur d'identité SAML et du portail de sponsor sur ISE

Ajouter le fournisseur d'identité SAML

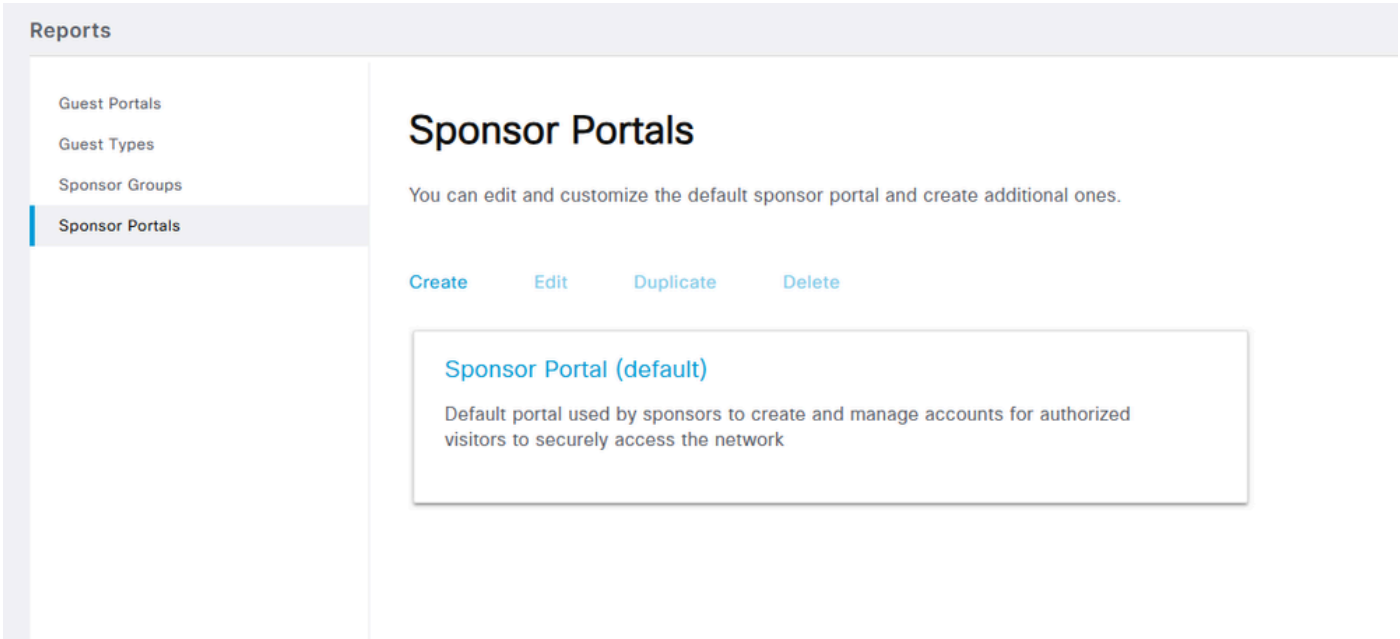
1. Sur ISE, accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers et cliquez sur le bouton Add.

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



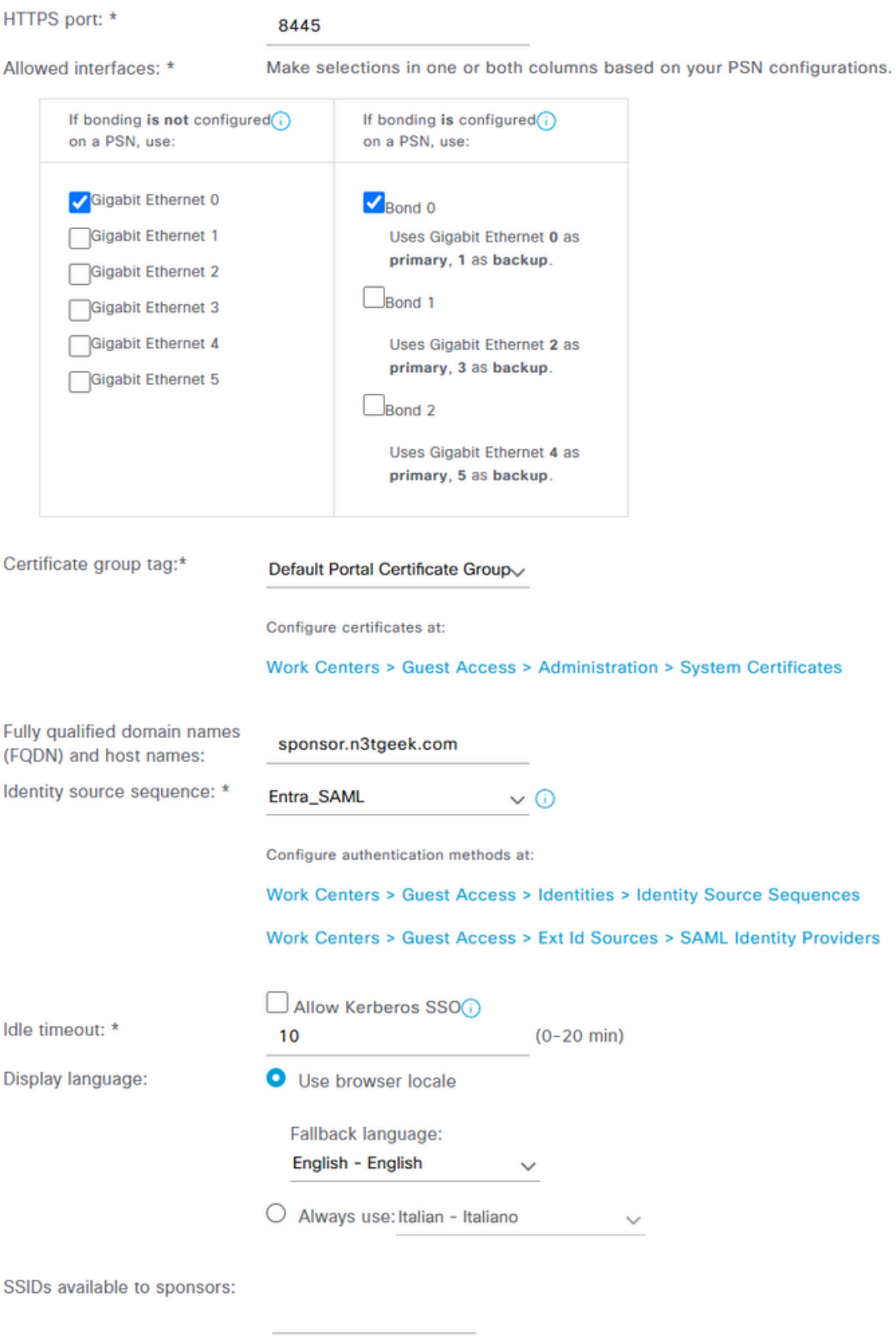
Configurer le portail de sponsor sur l'idP

1. Accédez à Work Centers > Guest Access > Portals & Components > Sponsor Portals et sélectionnez votre portail de sponsor. Dans cet exemple, le portail de sponsor (par défaut) est utilisé.



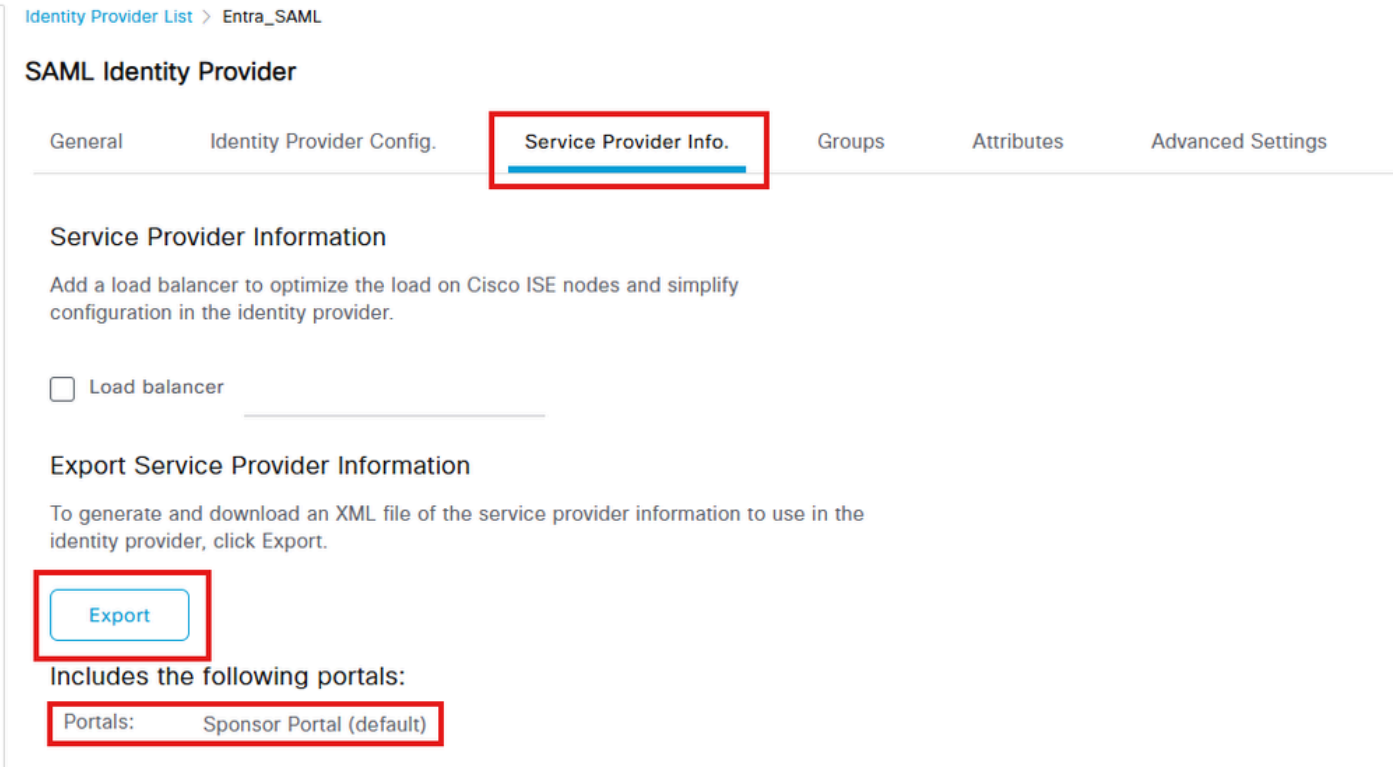
2. Développez Portal Settings et sélectionnez le nouveau fournisseur d'identité SAML dans Identity Source Sequence. Configurez le nom de domaine complet (FQDN) pour le portail sponsor

et notez le port HTTPS (8445 est le port par défaut du portail sponsor). Cliquez sur Save.



Exporter les informations du fournisseur de services

1. Revenez au fournisseur SAML et ouvrez l'onglet Infos fournisseur de services. Vérifiez que le portail du sponsor apparaît sous « Inclut les portails suivants » : le portail doit être lié à l'IdP avant l'exportation, sinon les métadonnées ne l'incluent pas. Cliquez sur Exporter.



2. À partir du fichier XML téléchargé, notez :

- entityID : Par exemple, http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2.
- Chaque emplacement AssertionConsumerService (un par nom de noeud/IP — un noeud autonome en produit trois ; les déploiements à plusieurs noeuds produisent davantage).
- SingleLogoutService ResponseLocation : Portail du sponsor - Réponse de déconnexion

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" ...>
    <md:KeyDescriptor use="signing">
      <ds:X509Certificate>MIIFUDCC...(ISE portal signing certificate)...</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutRequest.action?portal=1f789a0
        ResponseLocation="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    ...(additional NameIDFormat entries)...
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action" index="0"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action" index="1"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://prox-ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action" index="2"/
```

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



Mise en garde : Le fichier XML contient également un SSOLogoutRequest.action?portal=... URL dans l'attribut Emplacement. Ce n'est pas la valeur à utiliser comme URL de déconnexion dans Entra ID — son utilisation entraîne l'erreur « Échec de la déconnexion SSO » décrite dans la section Dépannage. La valeur correcte se termine par SSOLogoutResponse.action.



Remarque : Réexportez et réimportez ces métadonnées chaque fois que l'une des modifications suivantes est apportée : un nouveau noeud ISE est enregistré, un nom d'hôte de noeud ou des modifications IP, les modifications du nom de domaine complet du portail sponsor, les modifications des paramètres de port ou d'interface, ou un équilibreur de charge est associé. Si le fournisseur d'identité conserve des métadonnées périmées, il rejette les demandes d'authentification. Le fichier ZIP exporté inclut également un fichier Readme contenant des instructions de configuration par IDp.

D'après le fichier XML :

SingleLogoutService
ResponseLocation=https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action
entityID="http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2"
AssertionConsumerService
Location="https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action"
AssertionConsumerService
Location="https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action"
AssertionConsumerService Location="https://prox-
ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action"



Remarque : Dans ces travaux pratiques, un seul noeud ISE est utilisé. Le code XML exporté ne contient donc que trois entrées AssertionConsumerService : le nom de domaine complet du portail du sponsor, l’adresse IP du noeud et le nom de domaine complet du noeud. Dans un déploiement à plusieurs noeuds, le code XML répertorie les entrées de chaque noeud qui dessert le portail du sponsor (le nom de domaine complet du portail, plus une adresse IP et un nom de domaine complet pour chaque noeud). Ajoutez tous ces éléments en tant qu'URL de réponse dans Entra ID, et pas seulement ceux d'un noeud. Si l'URL d'un noeud est absente des URL de réponse, l'authentification

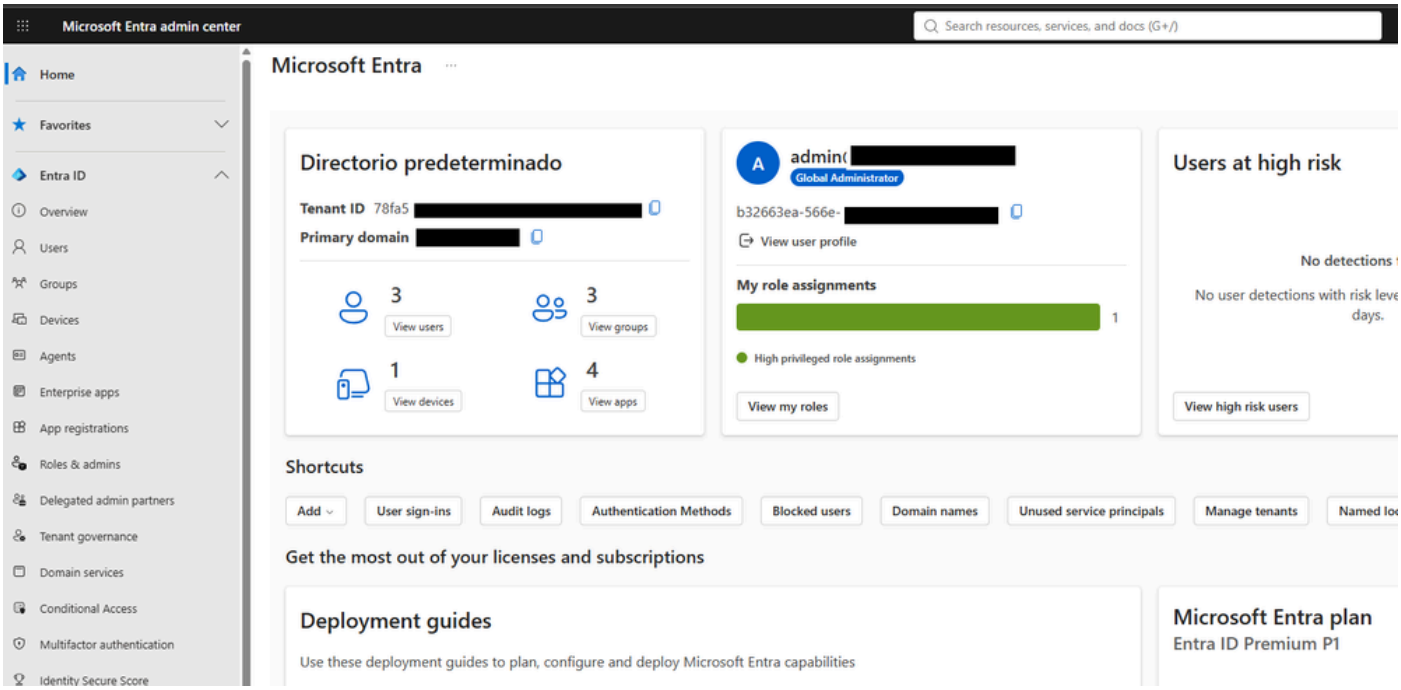
---

échoue lorsque l'utilisateur est redirigé vers ce noeud.

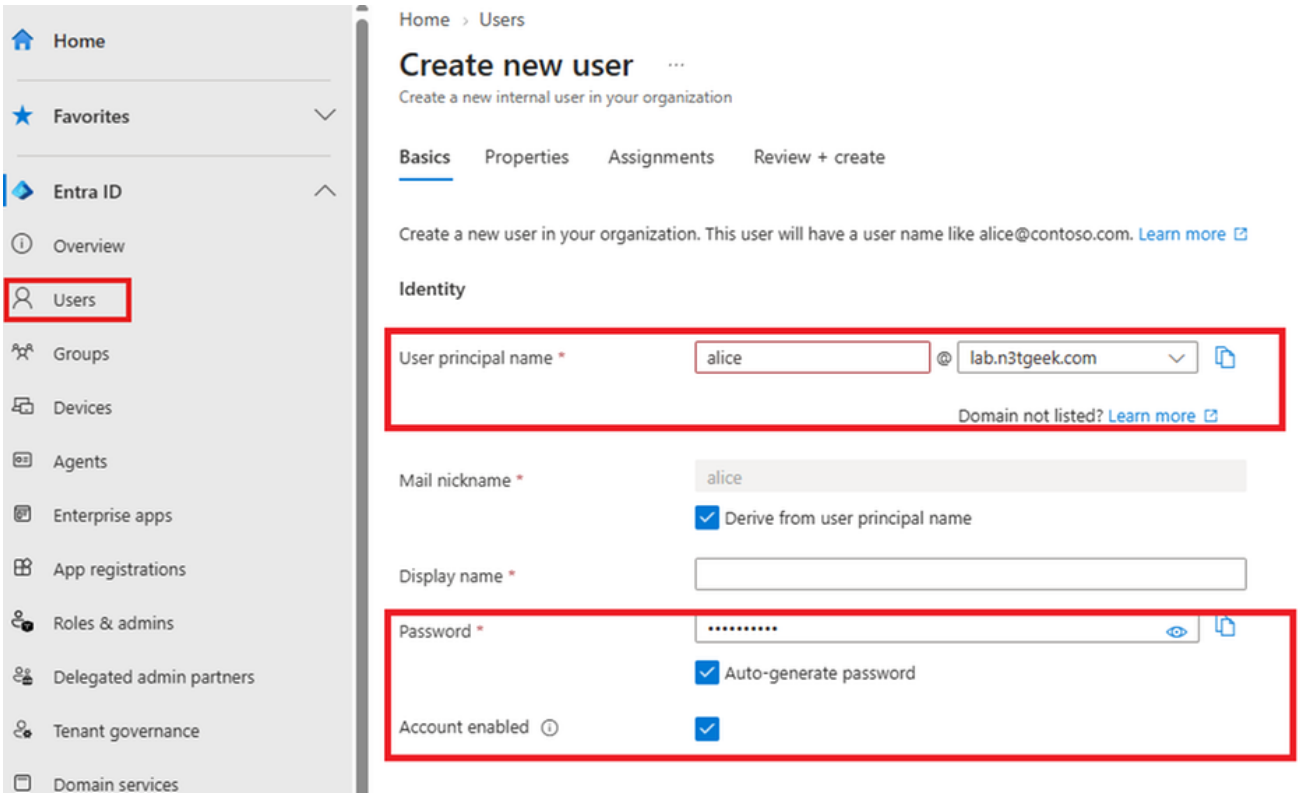
Étape 2 : configuration de l'identifiant Microsoft Entra ID

Créer un utilisateur Azure AD

1. Connectez-vous au Centre d'administration Microsoft Entra.



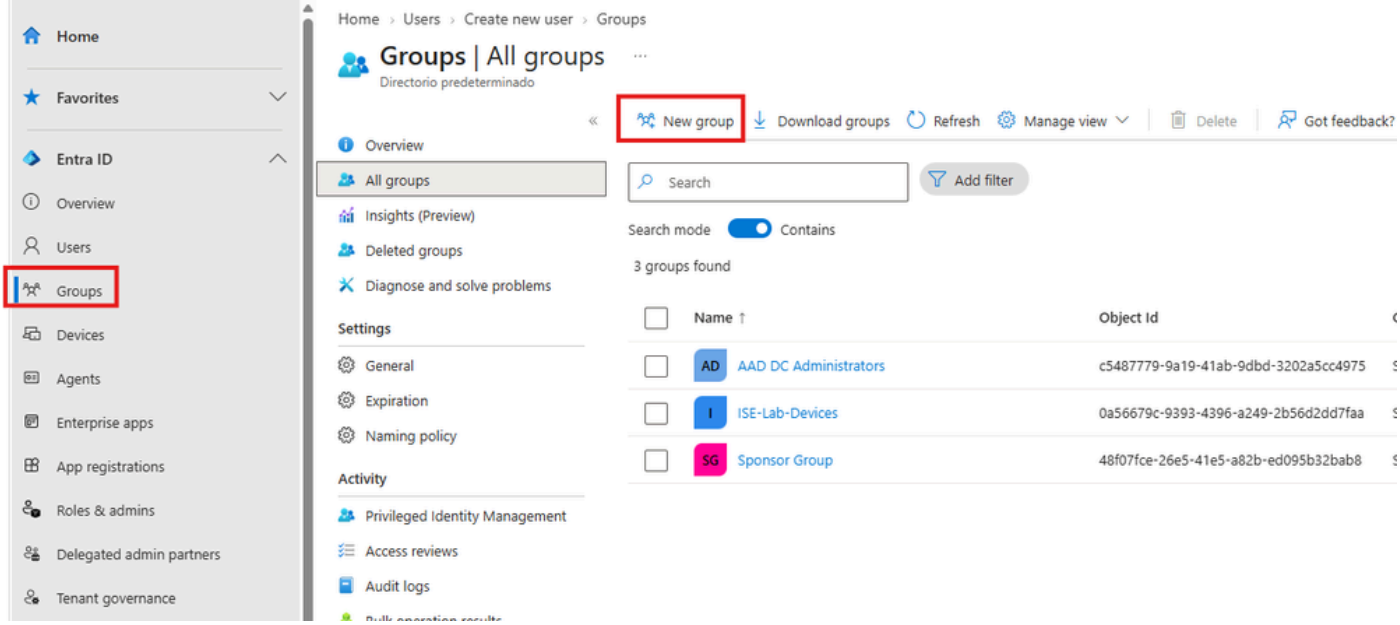
2. Accédez à Saisir un ID > Utilisateurs > Nouvel utilisateur > Créer un nouvel utilisateur et créez un utilisateur test dans le cloud uniquement.



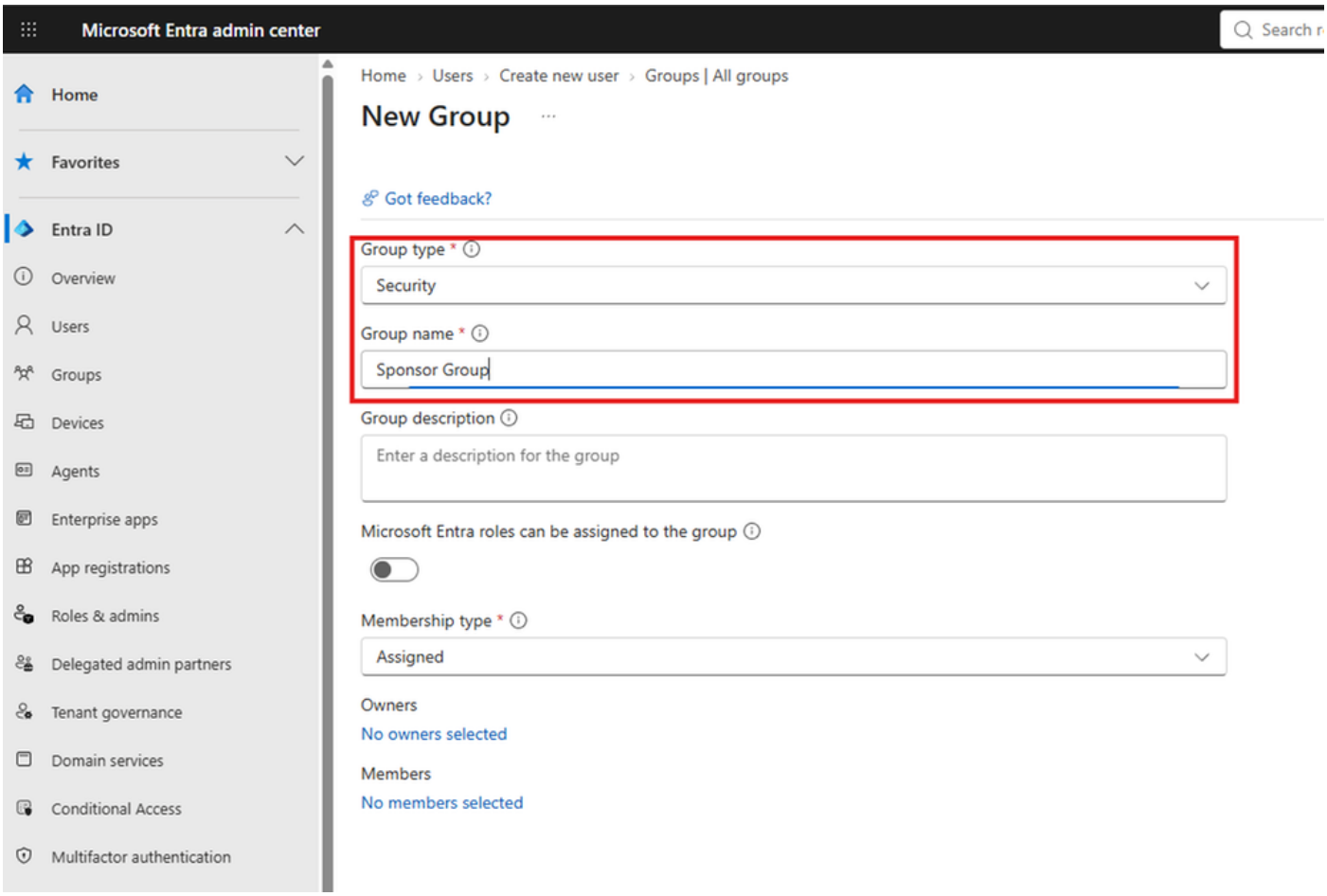
Remarque : Utilisez un utilisateur membre uniquement dans le cloud, et non un invité : les invités s'authentifient auprès de leur locataire à domicile et le format NameID résultant empêche ISE d'extraire le nom d'utilisateur. Un nouvel utilisateur doit changer le mot de passe lors de sa première connexion, et les locataires avec des paramètres de sécurité par défaut doivent également s'inscrire à l'AMF ; complétez les deux une fois avant la section Vérifier.

2. Créez un groupe et ajoutez l'utilisateur

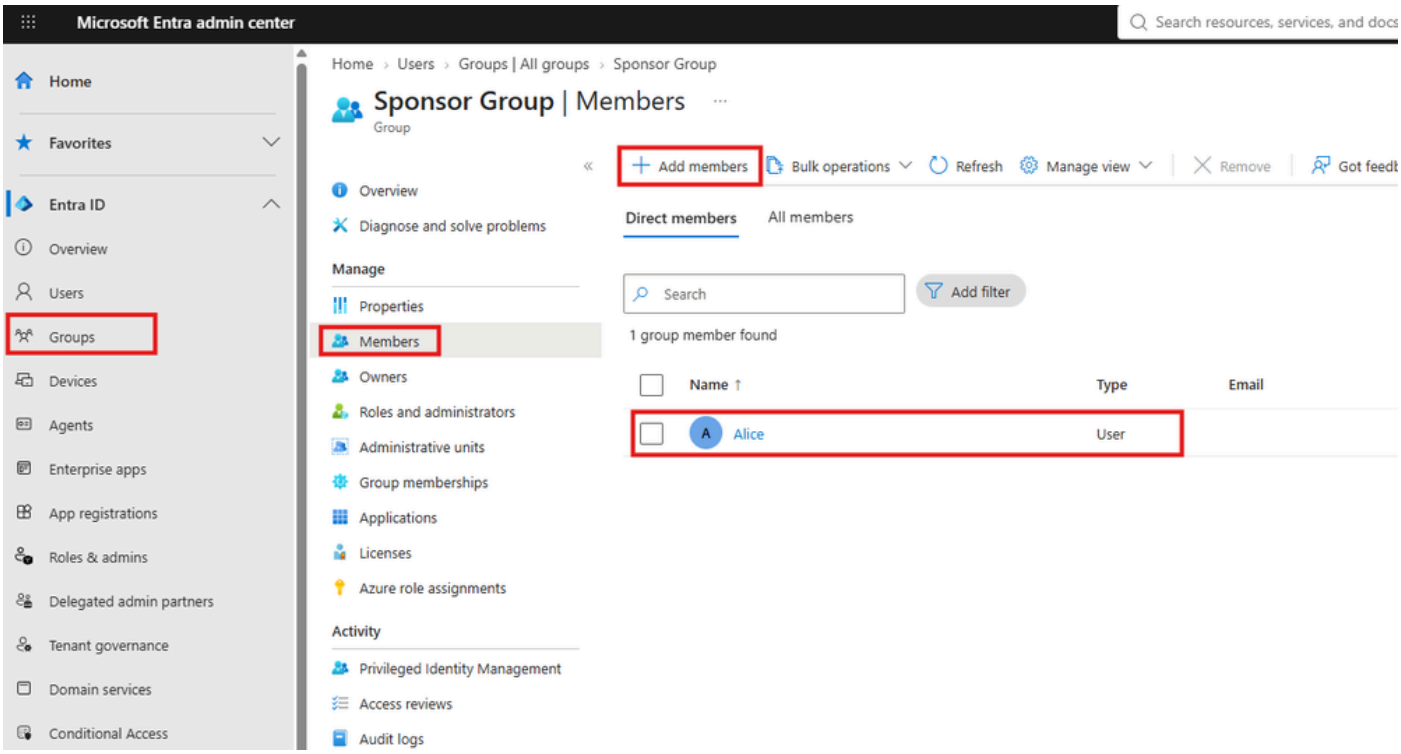
1. Accédez à Saisir un ID > Groupes > Nouveau groupe.



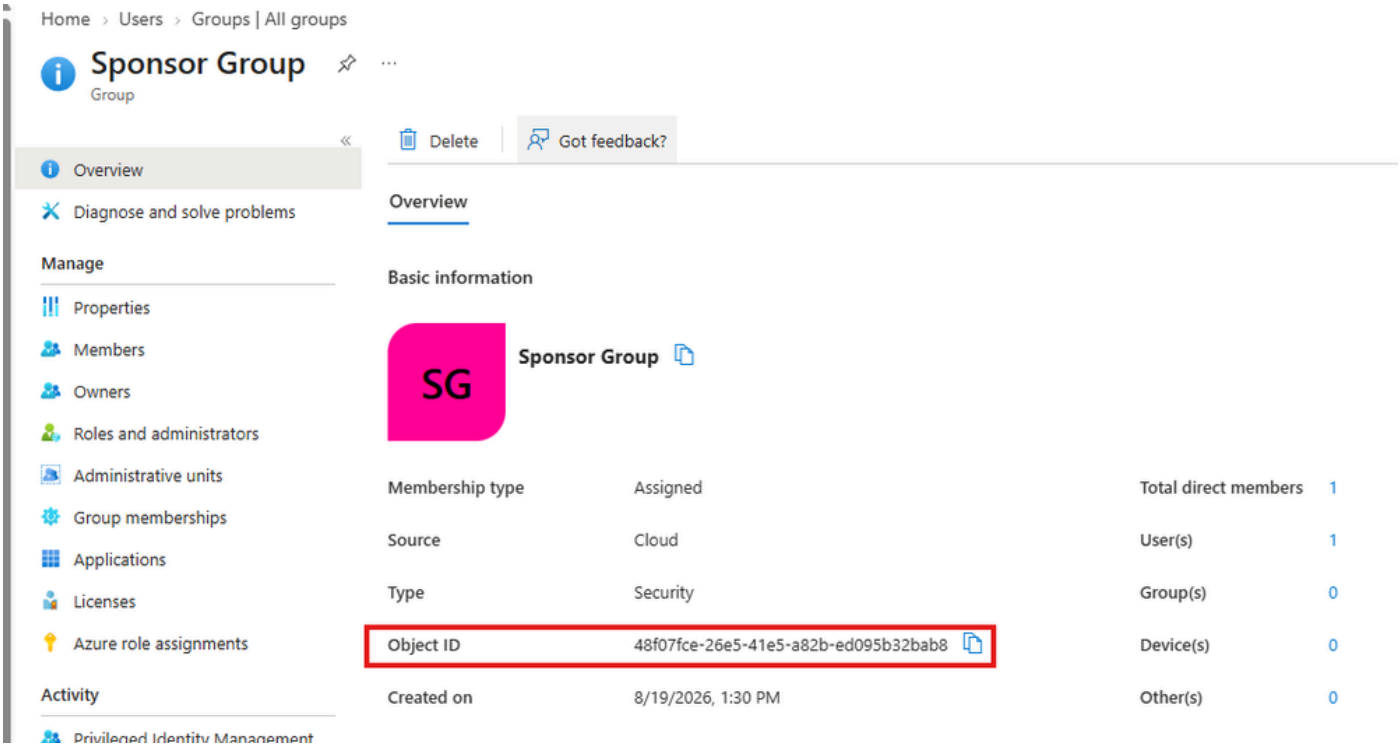
2. Conservez le type de groupe comme Sécurité. Configurez le nom du groupe comme indiqué dans l'image :



3. Ouvrez la page Membres du groupe, cliquez sur Ajouter des membres, recherchez l'utilisateur test, sélectionnez-le, puis cliquez sur Sélectionner.

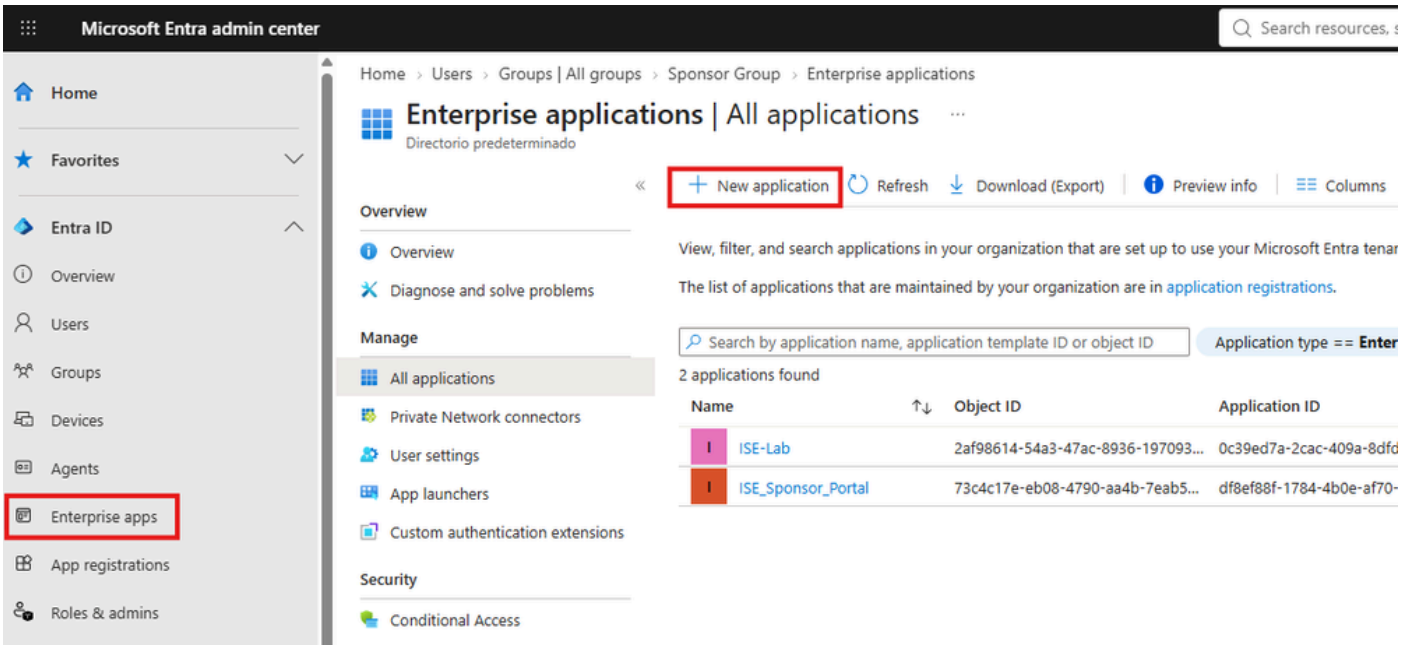


4. Notez l'ID d'objet de groupe, dans cet écran, il s'agit de 48f07fce-26e5-41e5-a82b-ed095b32bab8 pour le groupe sponsor.

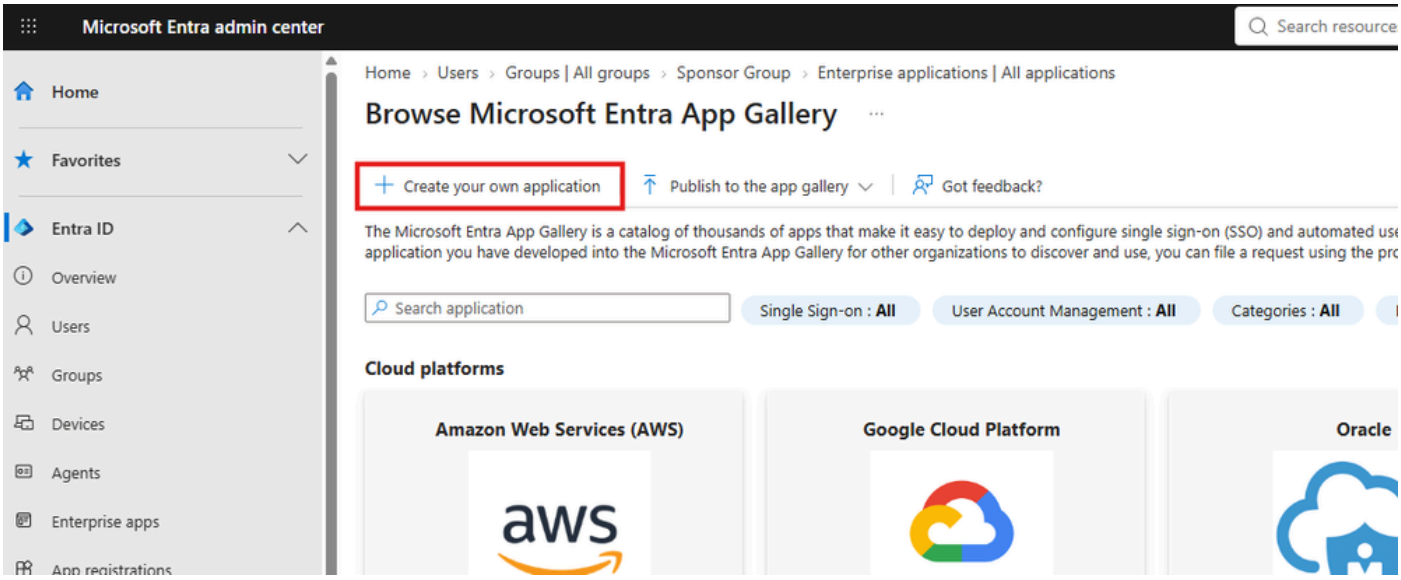


3. Créer une application Entreprise

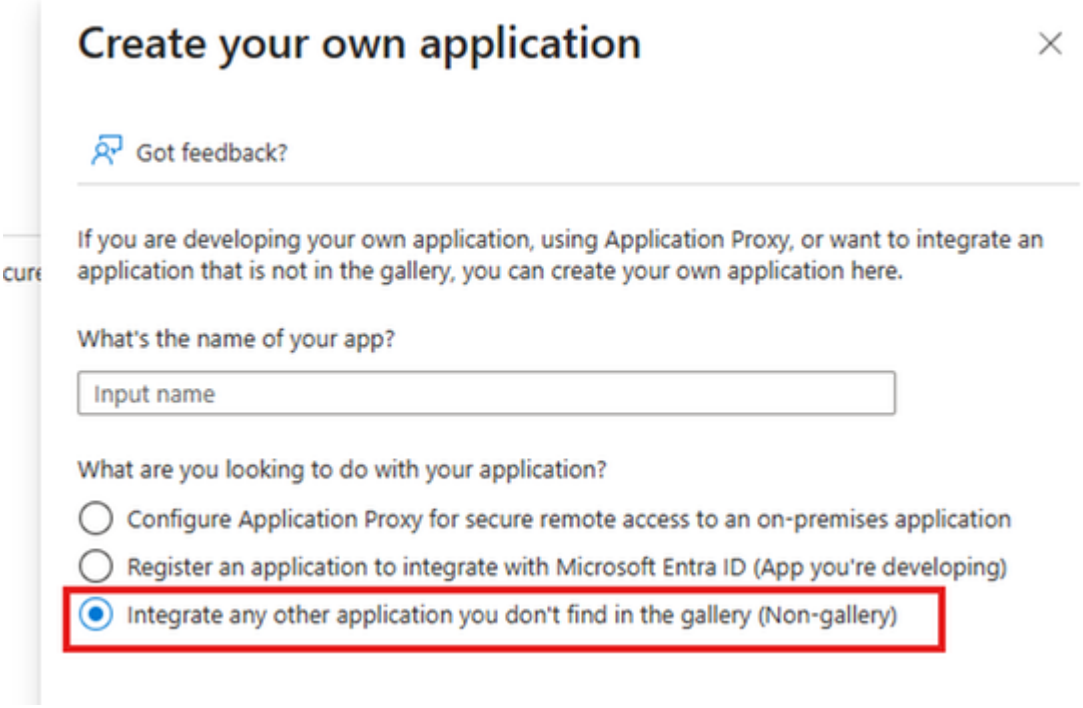
1. Accédez à Entra ID > Applications d'entreprise > Toutes les applications > Nouvelle application.



2. Sélectionnez Créer votre propre application.

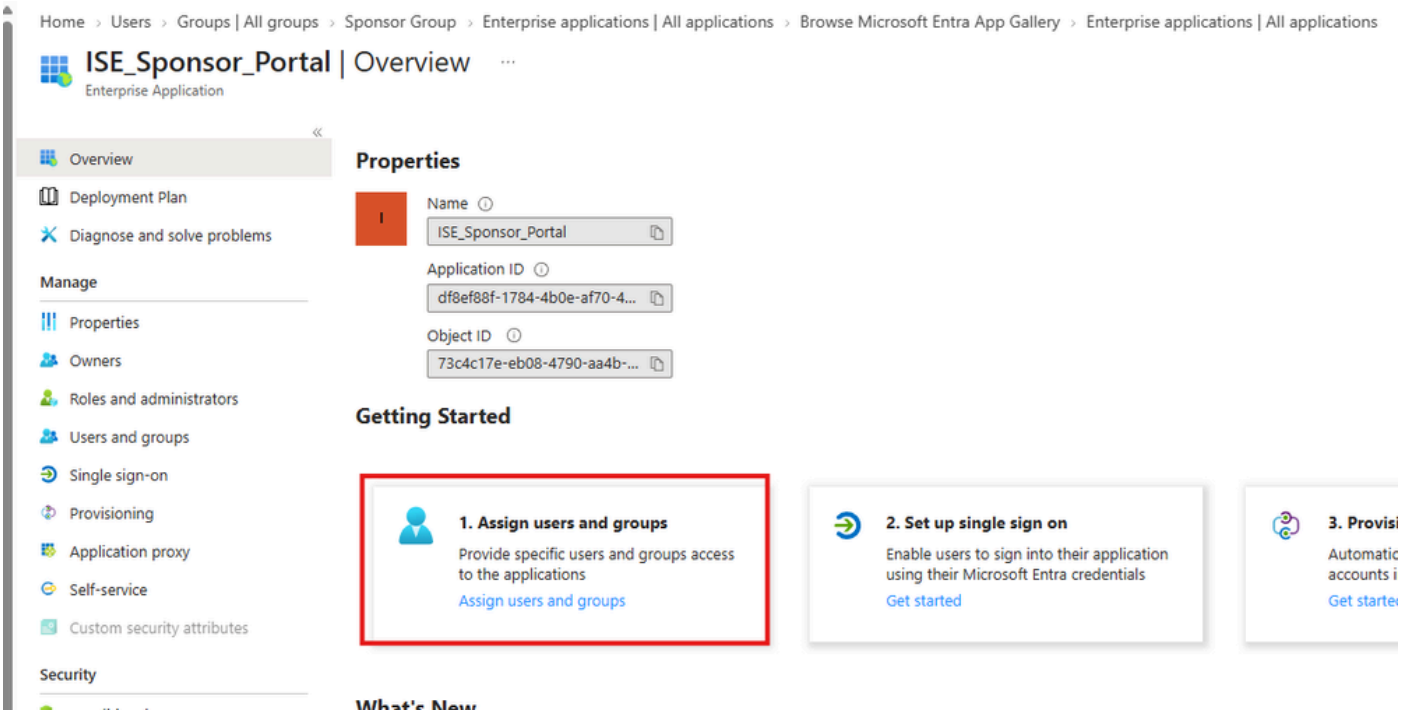


3. Entrez un nom, sélectionnez "Intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie)" et cliquez sur Créer.



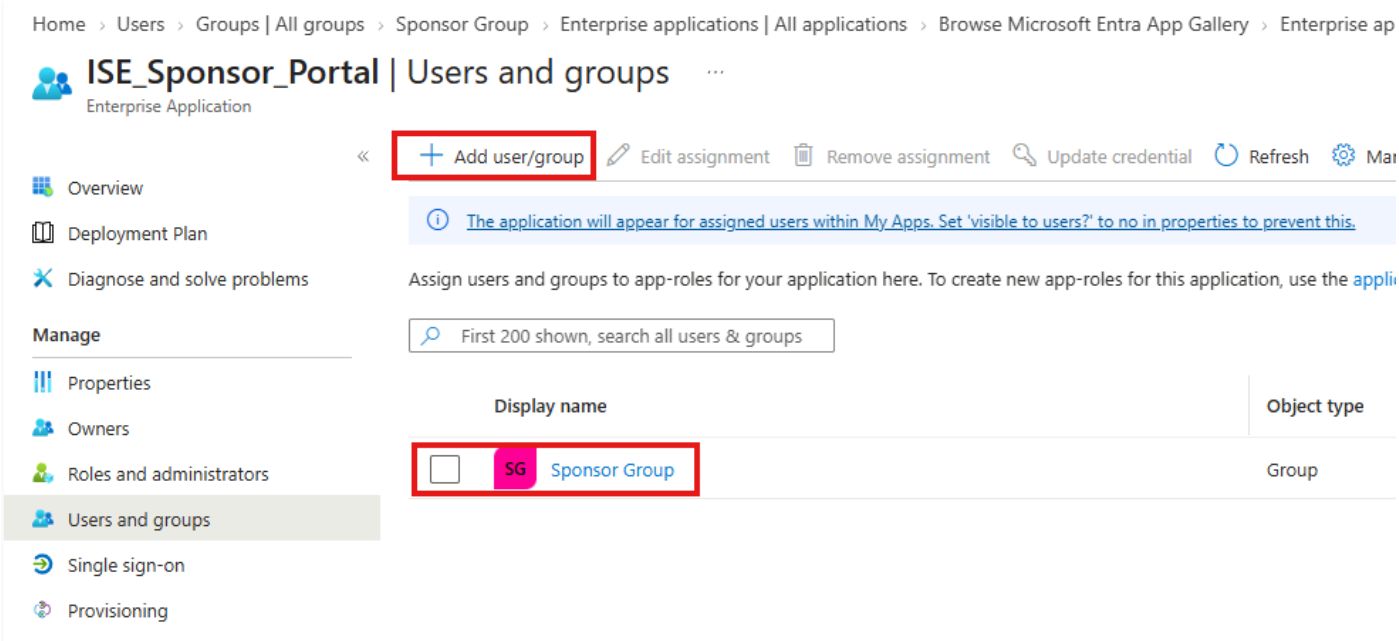
4. Affectez le groupe (ou l'utilisateur) à l'application

1. Dans l'application, accédez à Utilisateurs et groupes > Ajouter un utilisateur/groupe et affectez le groupe créé précédemment.



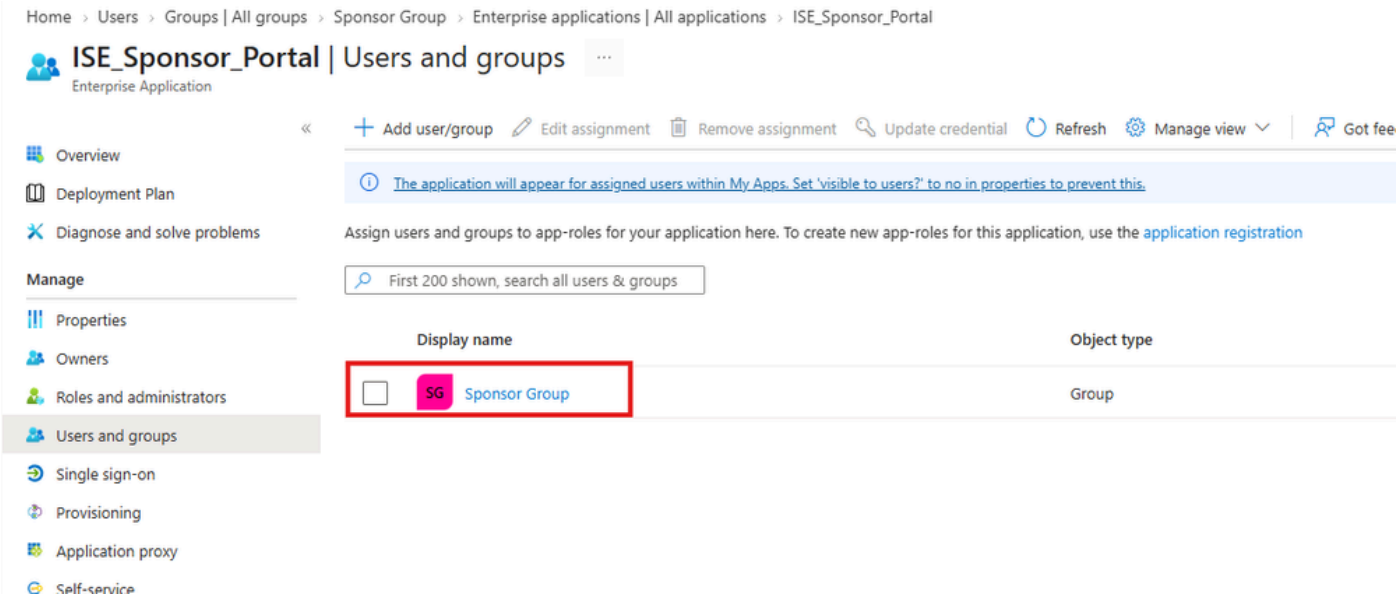
Ajouter un utilisateur/groupe :

Remarque : Si votre locataire est sur Microsoft Entra ID Free, l'affectation de groupe n'est pas disponible — affectez l'utilisateur test directement à la place ; toutes les autres étapes sont identiques.



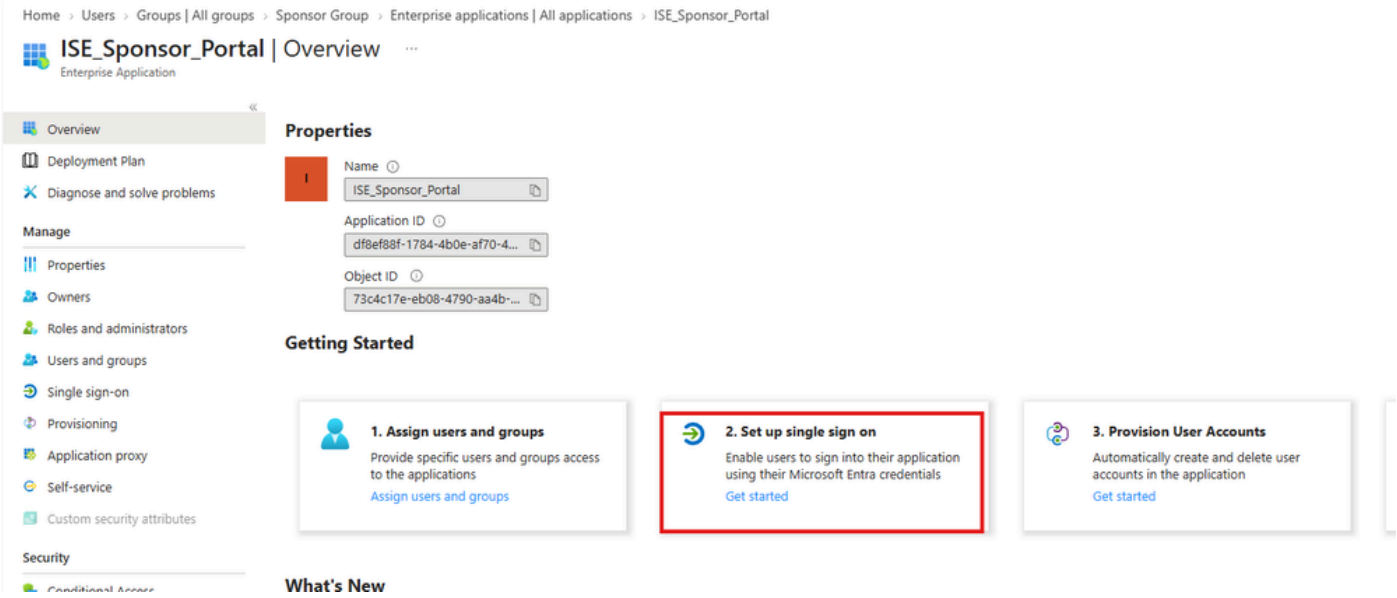
Remarque : C'est à vous de sélectionner le bon groupe d'utilisateurs ou de groupes pour appliquer l'accès.

1. Par conséquent, le menu Utilisateurs et groupes de votre application doit être renseigné avec le groupe sélectionné.

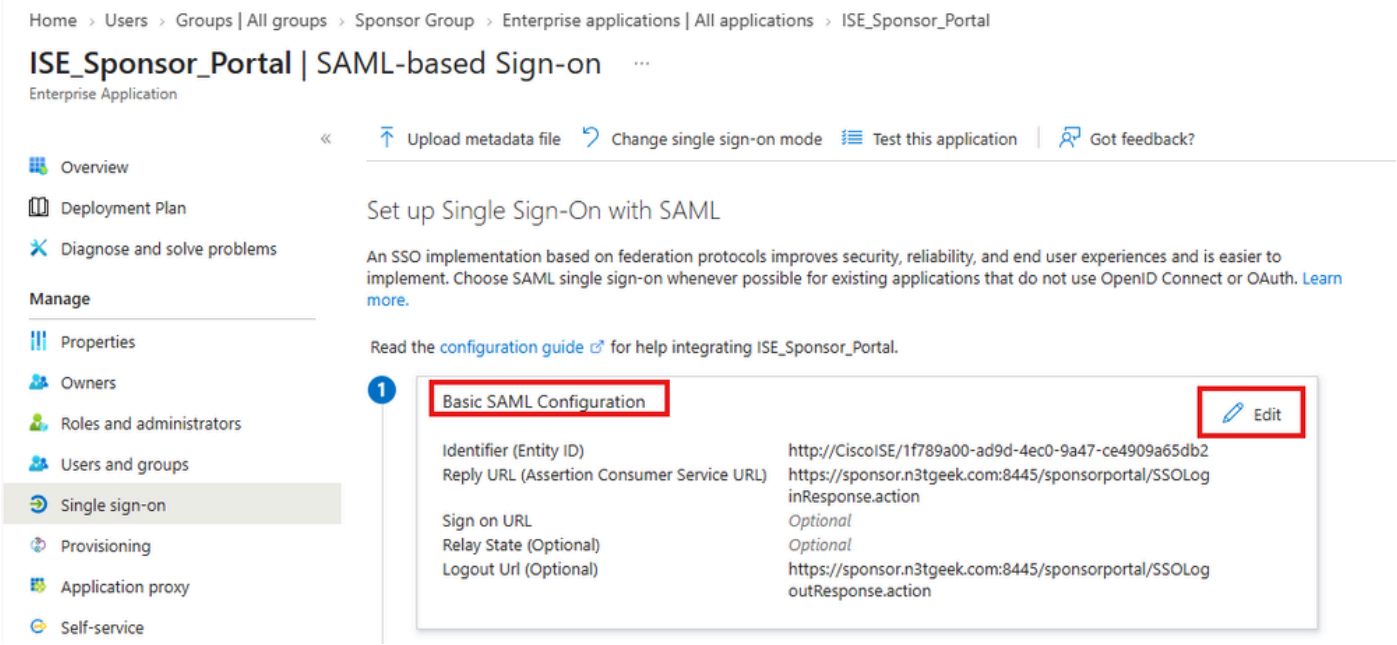


Étape 3. Configuration de l'authentification unique SAML dans l'ID d'entrée

1. Dans l'application, accédez à Configurer l'authentification unique.



2. Sélectionnez SAML et cliquez sur Modifier en regard de Configuration SAML de base.



3. Renseignez l'identificateur (ID d'entité) avec la valeur entityID du fichier XML de métadonnées du fournisseur de services ISE, et répondez à l'URL avec chaque emplacement de service d'assertionConsumer répertorié ici. Pour URL de déconnexion, utilisez la valeur SingleLogoutService ResponseLocation. Laissez les champs Sign-on URL et Relay State vides, puis cliquez sur Save.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2	☑

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://prox-ise04.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action		☐
https://192.168.1.204:8445/sponsorportal/SSOLoginResponse.action		☐
https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action		☑

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

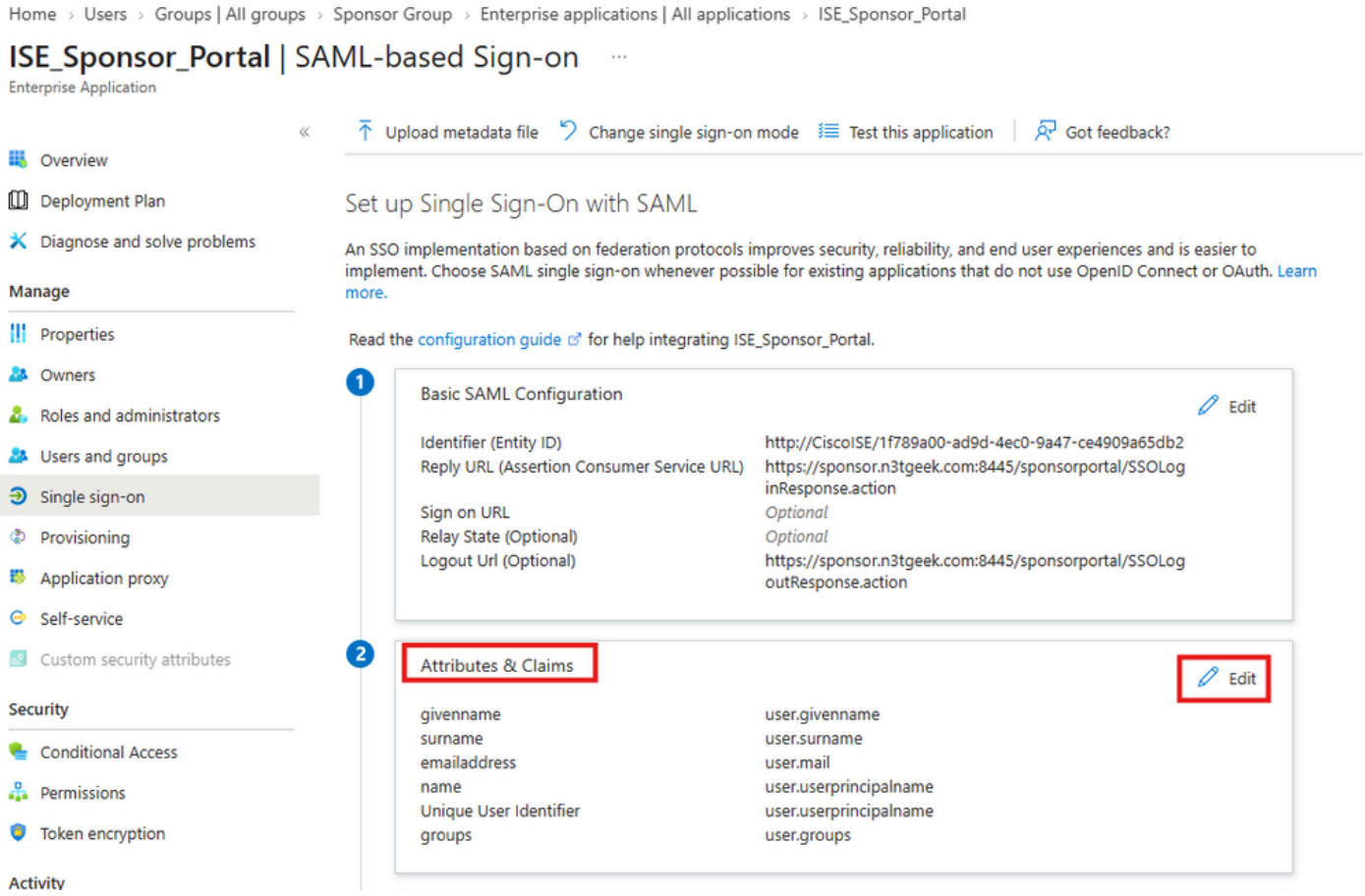
This URL is used to send the SAML logout response back to the application.

https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLogoutResponse.action

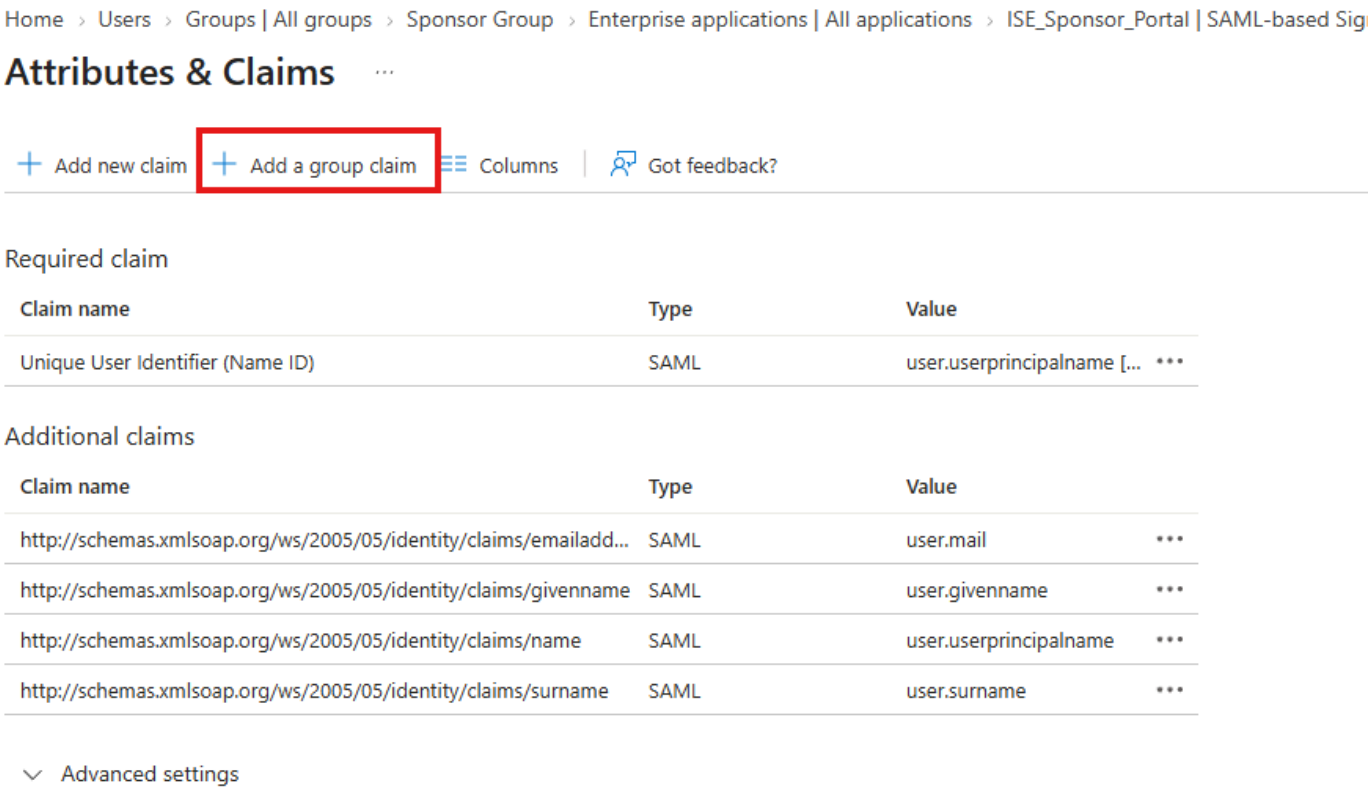
Remarque : L'URL de réponse agit comme une liste de passage, ce qui permet à certaines URL d'agir en tant que source lorsqu'elles sont redirigées vers la page du fournisseur d'identité.

2. Configurer l'attribut Groupe supplémentaire

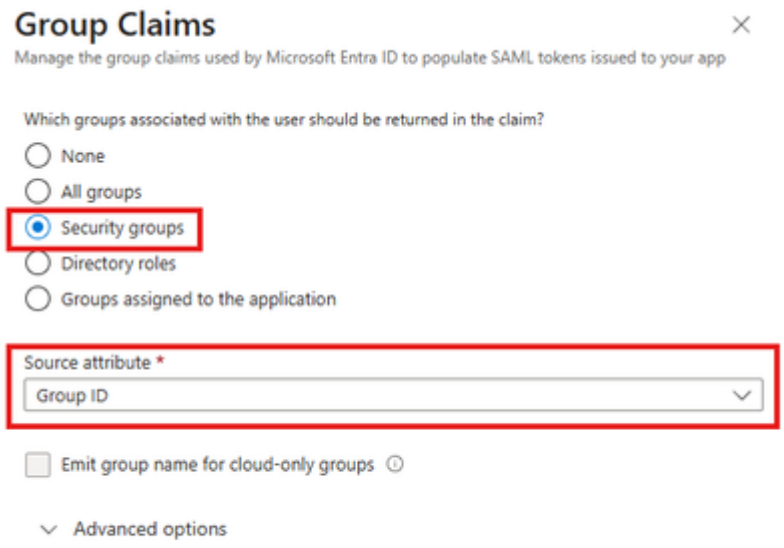
1. Cliquez sur Modifier en regard de Attributs et revendications.



2. Ajoutez ensuite une revendication de groupe.

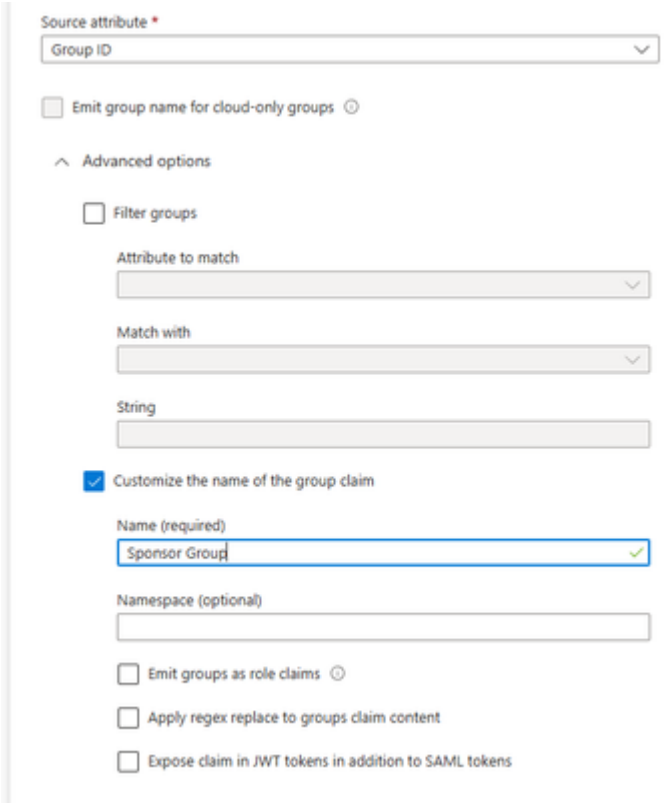


3. Sélectionnez Groupes de sécurité avec l'attribut source ID de groupe et cliquez sur Enregistrer. Laissez le reste à ses valeurs par défaut.

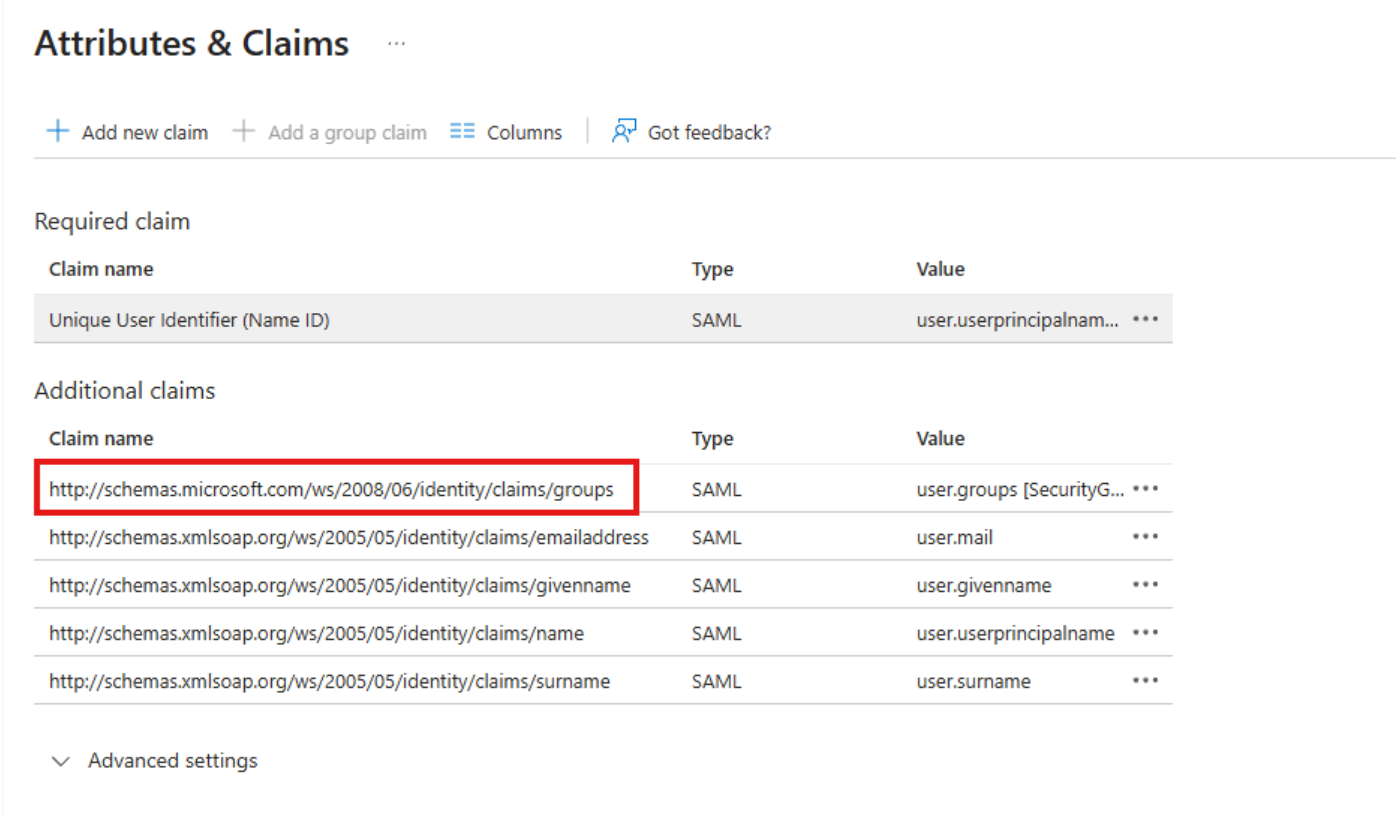


⚠ Mise en garde : Ne cochez pas "Personnaliser le nom de la revendication de groupe". Le changement de nom de la revendication nécessiterait le même nom personnalisé dans le champ d'attribut d'appartenance au groupe ISE, et le reste de ce document prend le nom de la revendication par défaut.

4. Si vous voulez le personnaliser quand même, vous pouvez, mais le même nom personnalisé doit être entré dans le champ Attribut d'appartenance au groupe dans ISE. Par exemple, si vous entrez Groupe de sponsor dans ID d'entrée, le champ ISE doit contenir exactement Groupe de sponsor. Dans Entra ID, le paramètre ressemble à ceci :

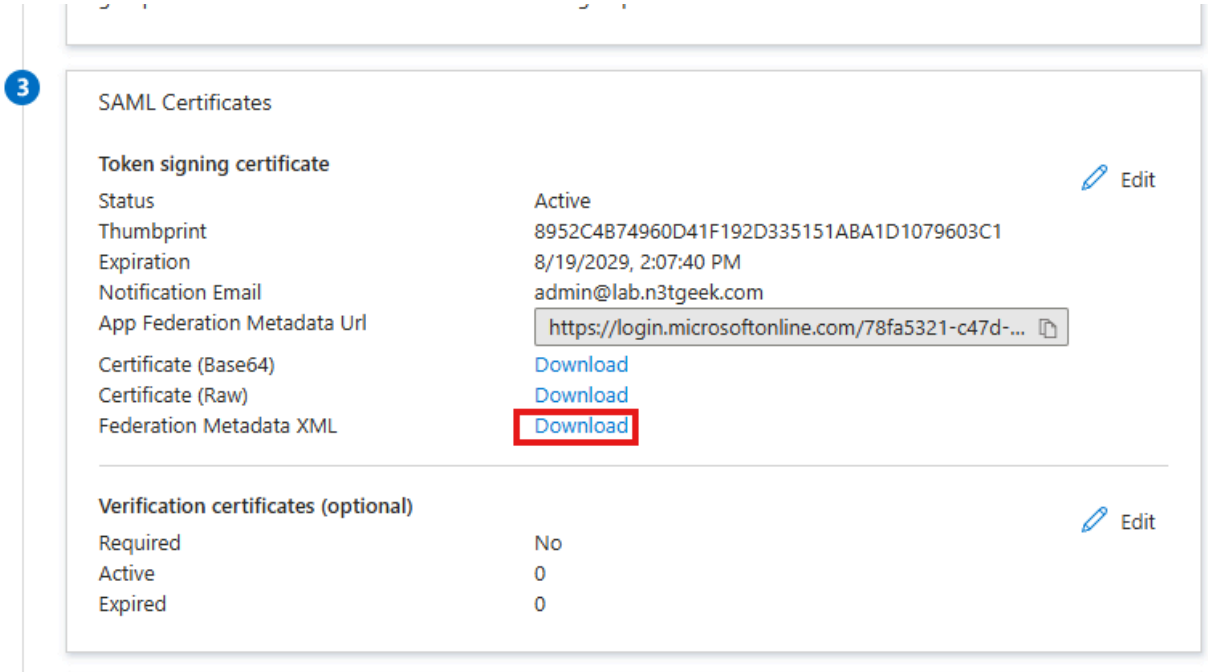


5. Notez le nom de la demande pour le groupe.



3. Téléchargez le fichier XML des métadonnées de fédération

1. Cliquez sur Download against Federation Metadata XML dans le certificat de signature SAML.



2. Les métadonnées de fédération téléchargées sont signées par Microsoft et contiennent tout ce dont ISE a besoin ; l'ID d'entité du fournisseur d'identité, les terminaux SSO/SLO et le certificat de

signature de jeton (abrégé ici) :

```
<EntityDescriptor entityID="https://sts.windows.net/<Tenant-ID>/">
  <Signature>...(signed by Microsoft)...</Signature>
  ...(WS-Fed RoleDescriptor sections – not used by ISE)...
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <X509Certificate>MIIC8DCC...(Entra ID token signing certificate)...</X509Certificate>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://login.microsoftonline.com/<Tenant-ID>/saml2"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://login.microsoftonline.com/<Tenant-ID>/saml2"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

3. Lors de l'importation (étape 4), ces champs deviennent les URL d'authentification unique/déconnexion et l'entrée Certificats de signature dans l'onglet Configuration du fournisseur d'identités.

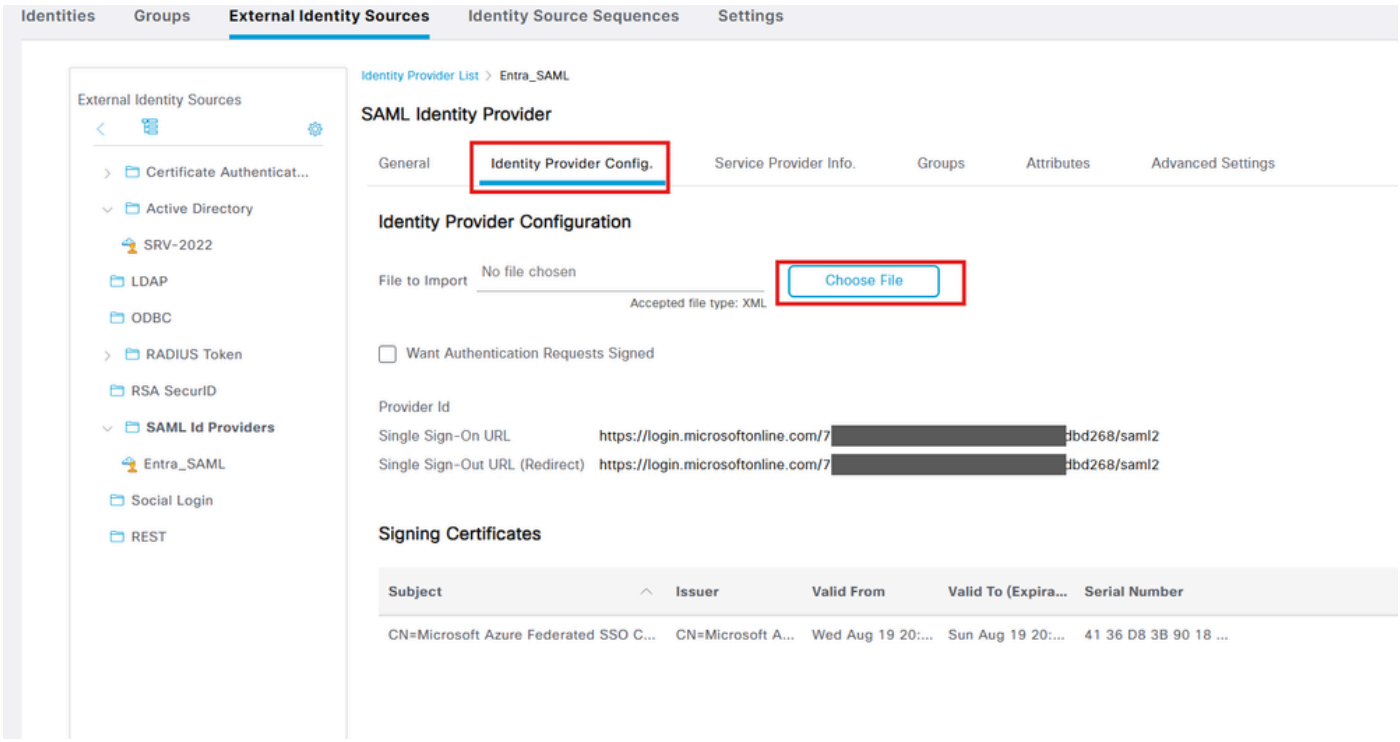
Remarque : Le certificat de signature de jeton Entra ID est valide pendant trois ans. Lorsqu'il pivote, téléchargez à nouveau le fichier XML de métadonnées de fédération et réimportez-le dans ISE, ou l'authentification unique cesse brusquement de fonctionner. Configurez l'e-mail de notification sur le certificat pour obtenir un avertissement d'expiration.

Étape 4. Télécharger des métadonnées d'Entra vers ISE

Importer les métadonnées de fédération

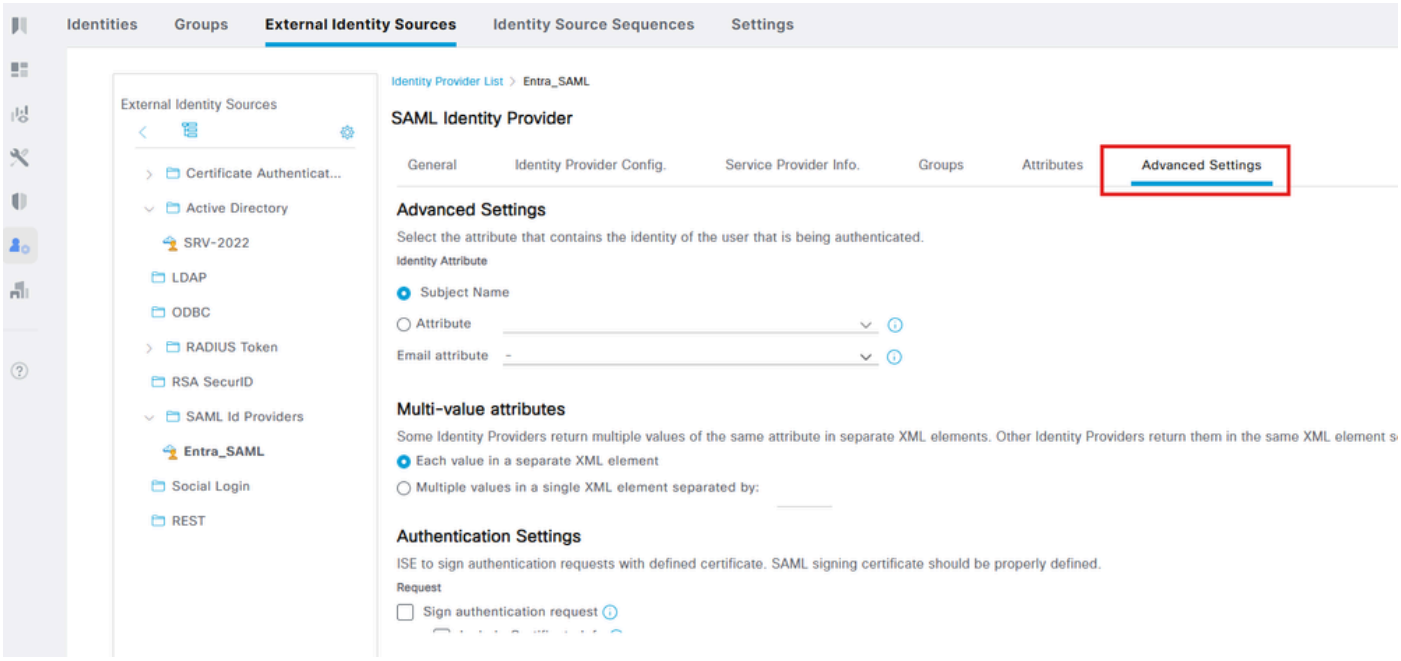
1. Accédez à Administration > Identity Management > External Identity Sources > SAML Id Providers > [votre fournisseur], ouvrez l'onglet Identity Provider Config, cliquez sur Choose File, sélectionnez Federation Metadata XML et cliquez sur Save. Les URL d'authentification unique/déconnexion et le certificat de signature sont renseignés.

Remarque : Le champ ID fournisseur reste vide dans cet onglet même après l'importation et l'enregistrement du fichier de métadonnées. Il s'agit d'un problème d'affichage uniquement suivi par l'ID de bogue Cisco CSCv74517. L'ID d'entité du fournisseur d'identité est stocké correctement et utilisé au moment de l'exécution, et peut être confirmé dans la sortie de débogage ise-psc.log comme strong>URI du fournisseur d'identité.



Remarque : Les métadonnées SP que les versions actuelles d'ISE exportent déclarent WantAssertionsSigned="false" (les versions plus anciennes ont été déclarées vraies) ; l'attribut suit désormais la case à cocher Exiger les assertions signées dans l'onglet Paramètres avancés, qui est désactivée par défaut. Cela ne signifie pas que les assertions non signées sont acceptées. ISE nécessite toujours au moins une signature sur la réponse SAML ou sur l'assertion, même si les deux cases sont décochées.

Onglet Paramètres avancés facultatifs : Attribut d'identité (par défaut : Subject Name) sélectionne l'origine du nom d'utilisateur ; l'attribut Email doit être configuré si les sponsors filtrent la liste des invités en attente d'approbation ; Sign Authentication Request contrôle la signature des demandes et est prioritaire sur la case à cocher « Want Authentication Requests Signed » en lecture seule de l'onglet précédent.

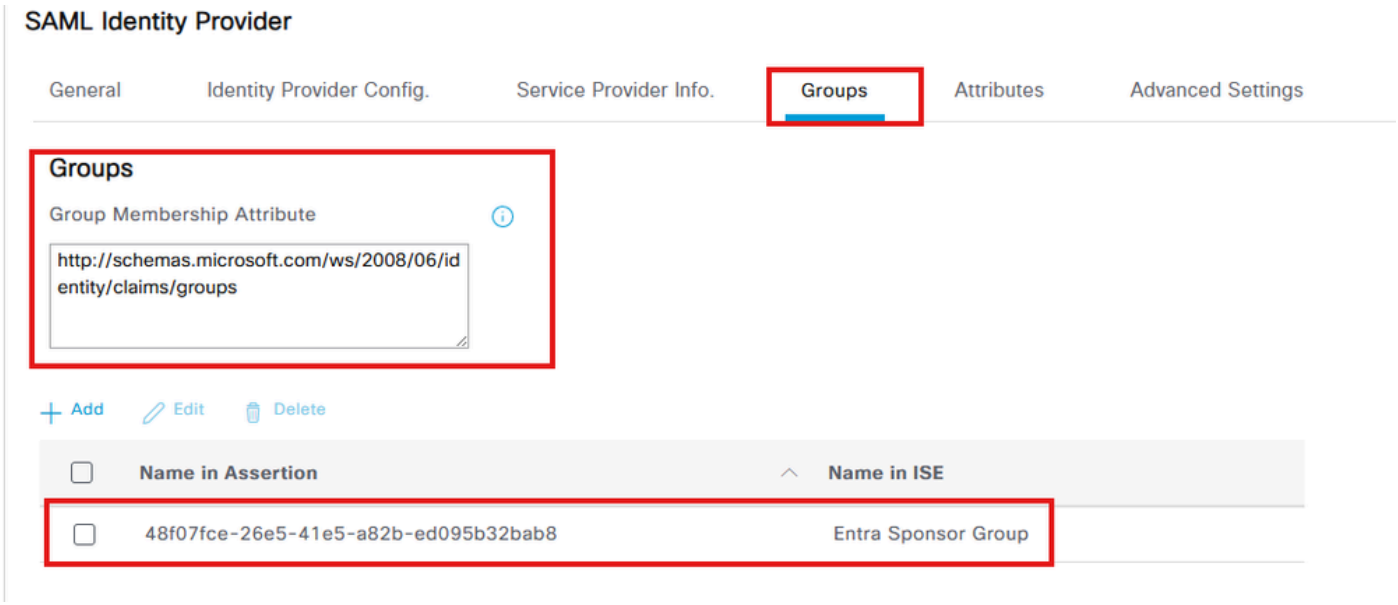


Configurer des groupes SAML sur ISE

1. Ouvrez l'onglet Groupes et, dans l'attribut Appartenance au groupe, collez le nom de la revendication de l'étape 3 :

```
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
```

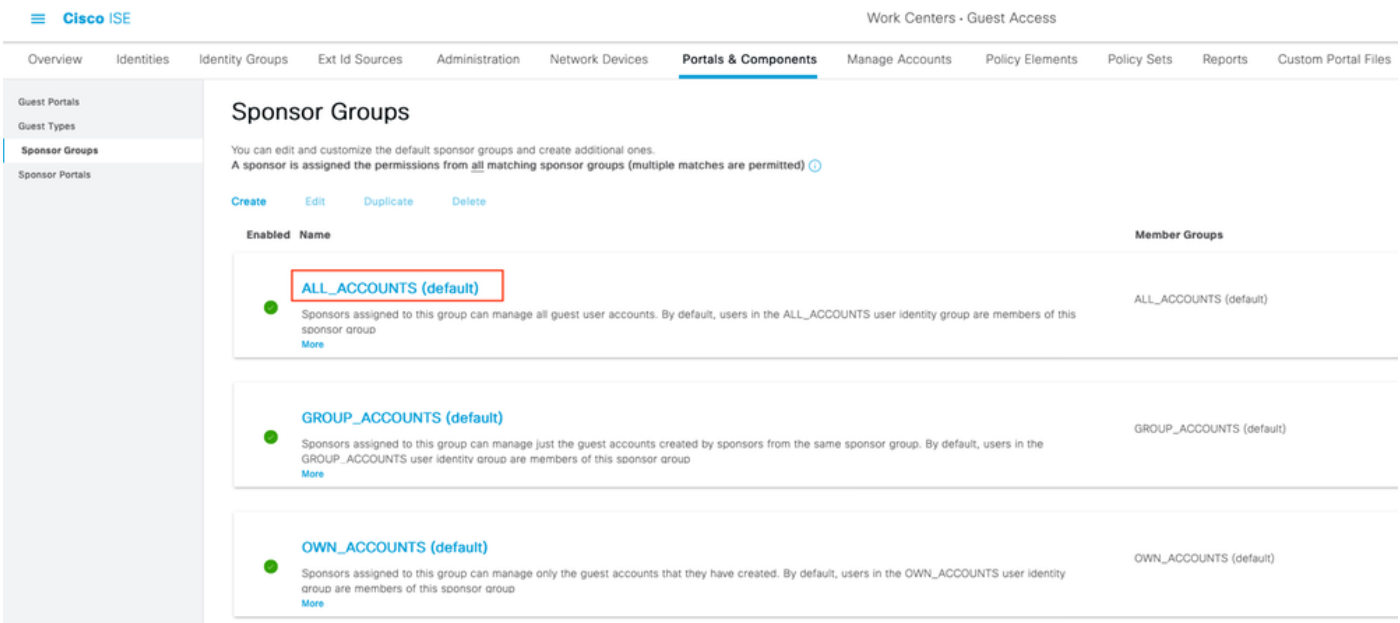
2. Cliquez sur Ajouter. Dans Nom dans Assertion, entrez l'ID d'objet du groupe capturé à l'étape 2 (cette valeur doit correspondre exactement). Dans Nom dans ISE, entrez n'importe quelle étiquette locale significative (un alias de forme libre utilisé uniquement dans les menus ISE). Cliquez sur OK, puis sur Save.



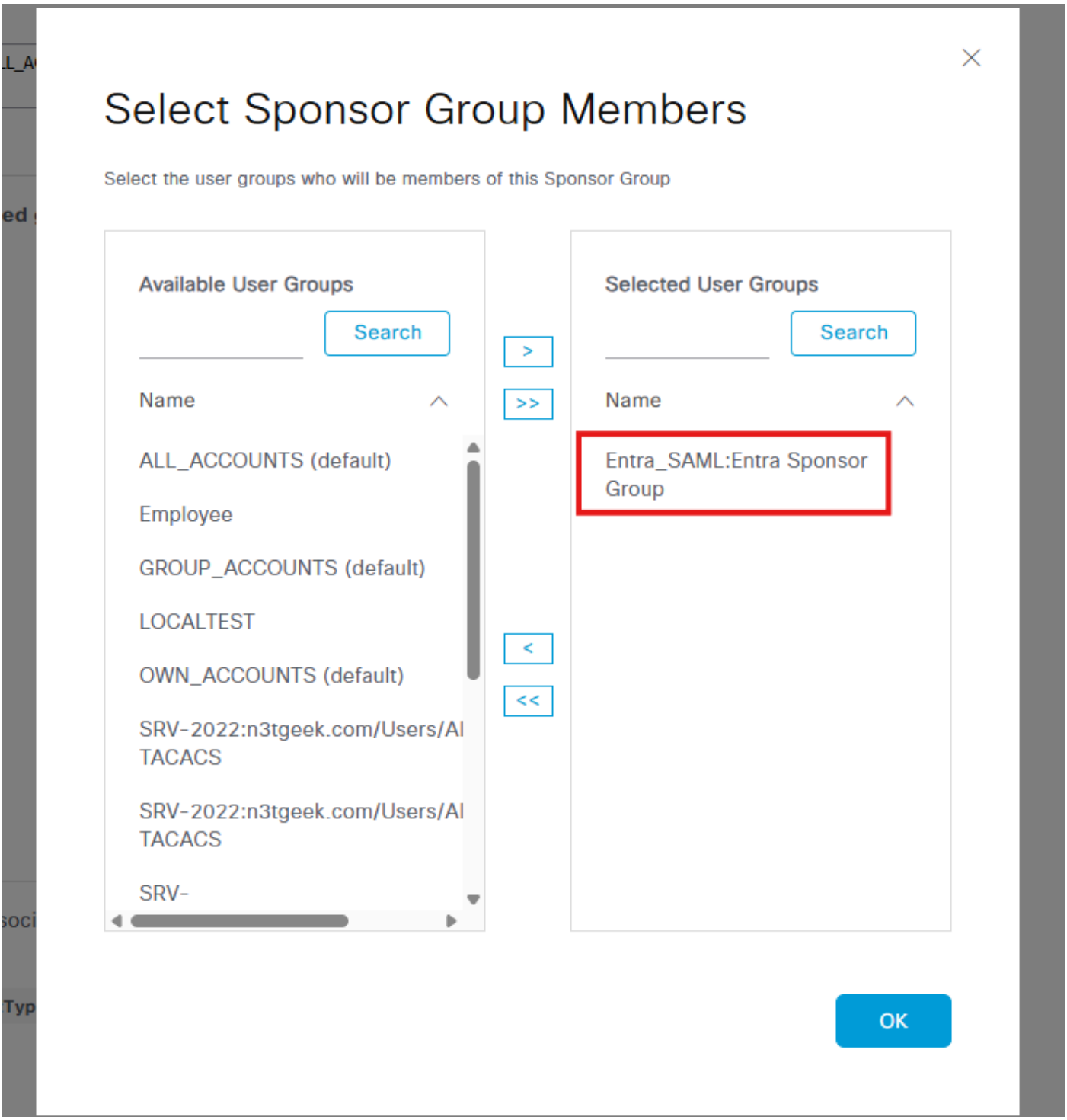
3. Ceci crée un mappage entre le groupe dans Entra et le nom du groupe qui peut être utilisé sur ISE.

Étape 5 : configuration du mappage de groupe de sponsors sur ISE

1. Accédez à Work Centers > Guest Access > Portals & Components > Sponsor Groups et sélectionnez le groupe de sponsors à mapper. Dans cet exemple, ALL_ACCOUNTS (valeur par défaut).



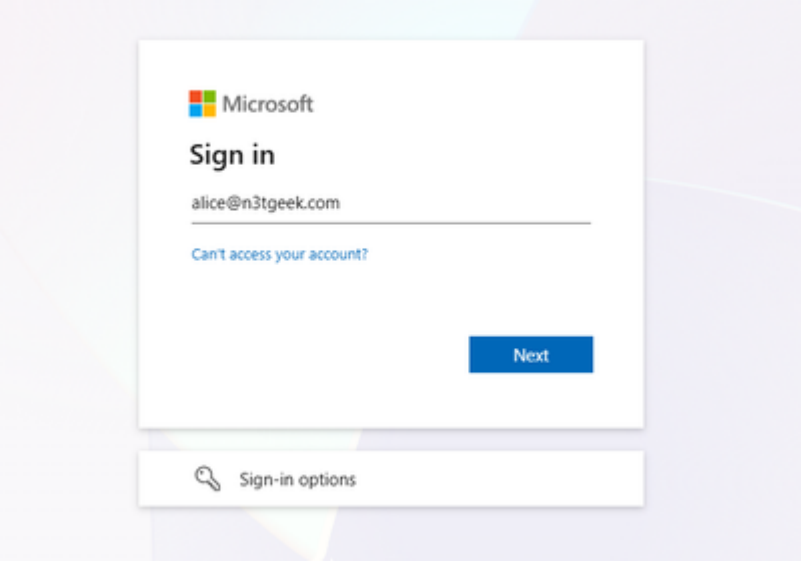
2. Cliquez sur Members..., déplacez l'entrée IdP : Name dans ISE vers Selected User Groups, cliquez sur OK, puis sur Save.



Remarque : Un sponsor se voit attribuer les autorisations de tous les groupes de sponsors correspondants. Mappez le groupe Entra ID à un seul groupe de sponsor, sauf si l'accumulation d'autorisations est prévue.

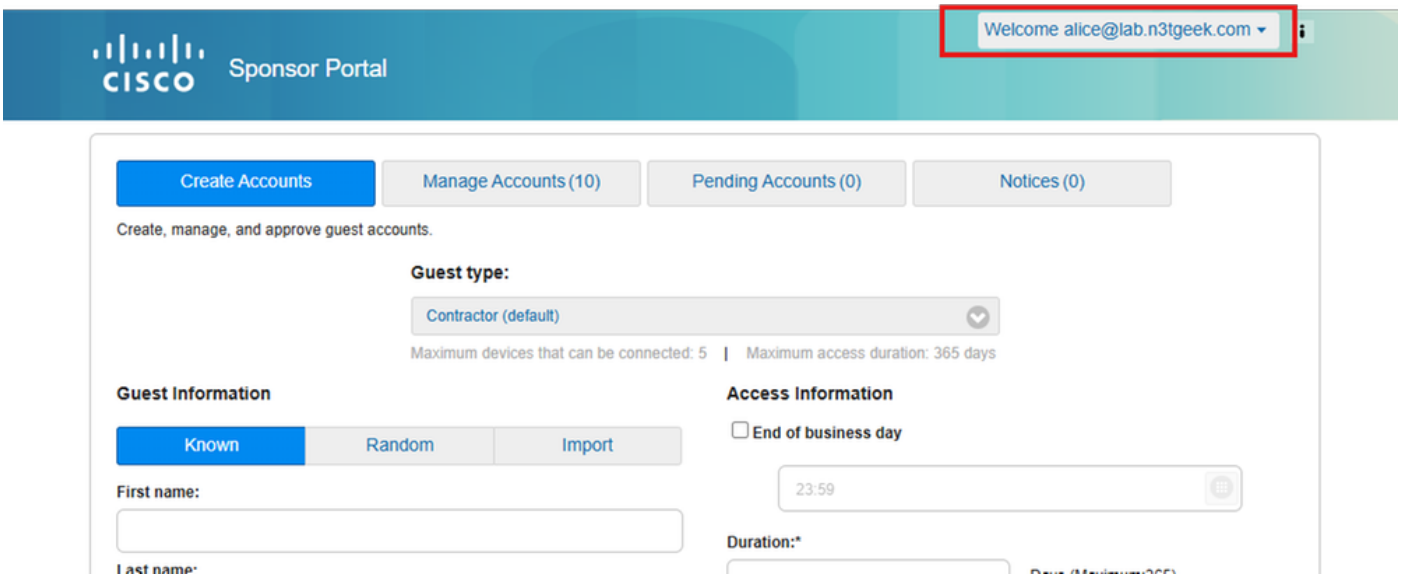
Vérifier

1. Lancez le portail de sponsor à partir du lien URL de test du portail. ISE redirige vers la page de connexion Microsoft ; authentifiez-vous avec les informations d'identification utilisateur test.

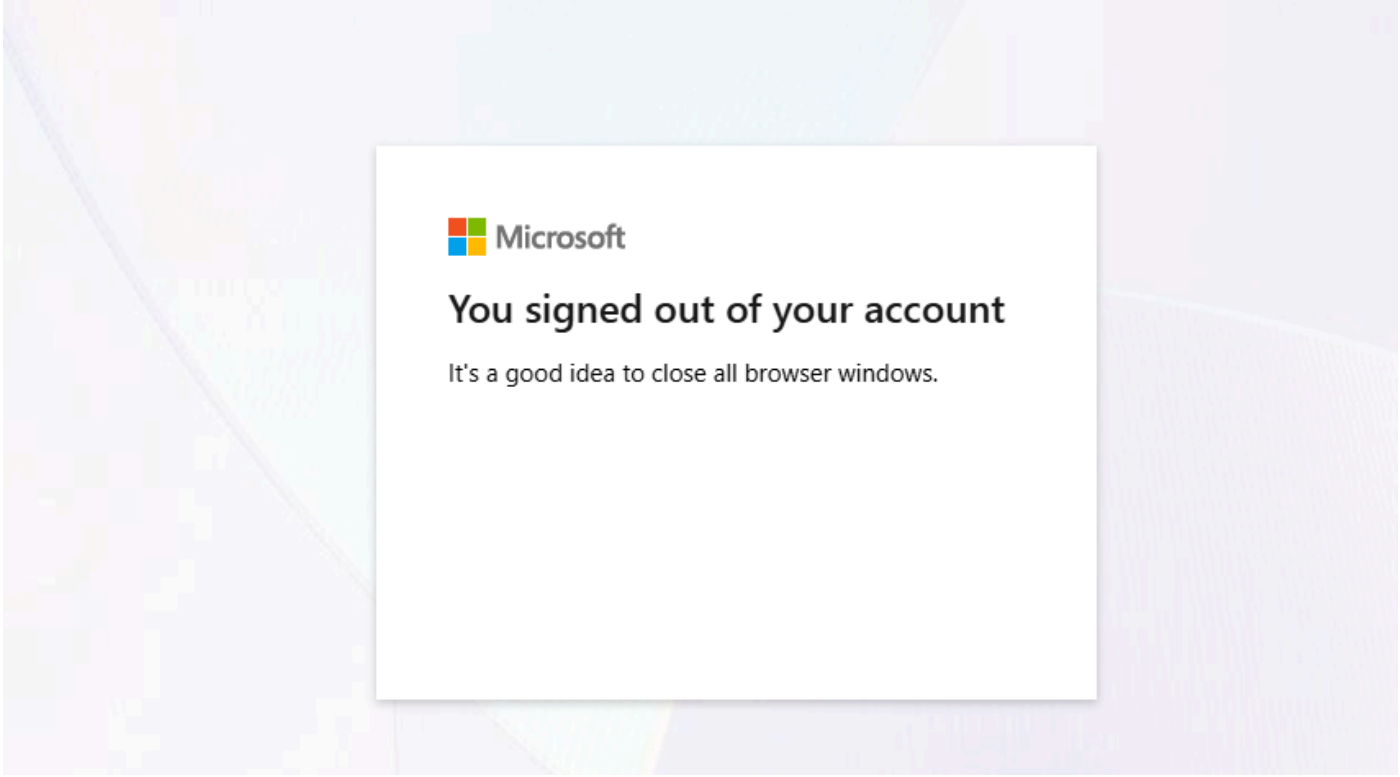


Remarque : Un nouvel utilisateur est forcé de modifier son mot de passe lors de sa première connexion. Et Accepter les étapes de vérification AUP ne le couvre pas. La vérification couvre le scénario où les utilisateurs se connectent après la première fois, et l'AUP a déjà été acceptée une fois par le sponsor (Alice).

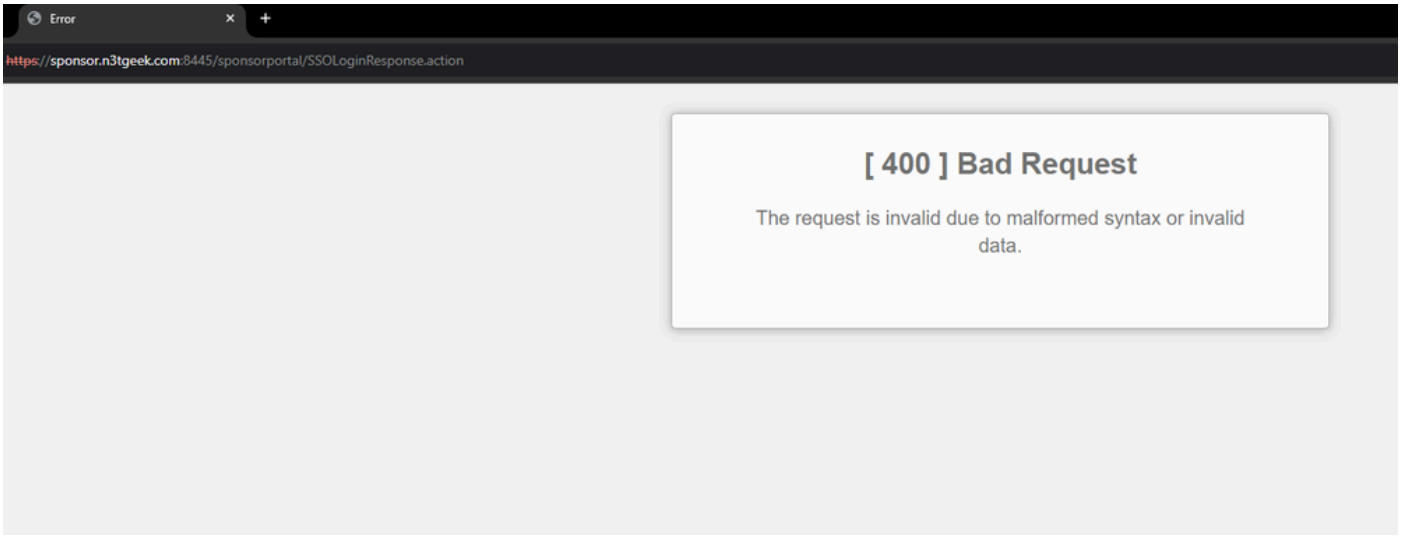
2. Après l'authentification, le navigateur retourne au portail et AUP s'affiche. Après acceptation, le sponsor dispose des autorisations de groupe de sponsors mappées.



3. La déconnexion à partir du menu de bienvenue met fin à la session du portail et à la session SSO proprement.



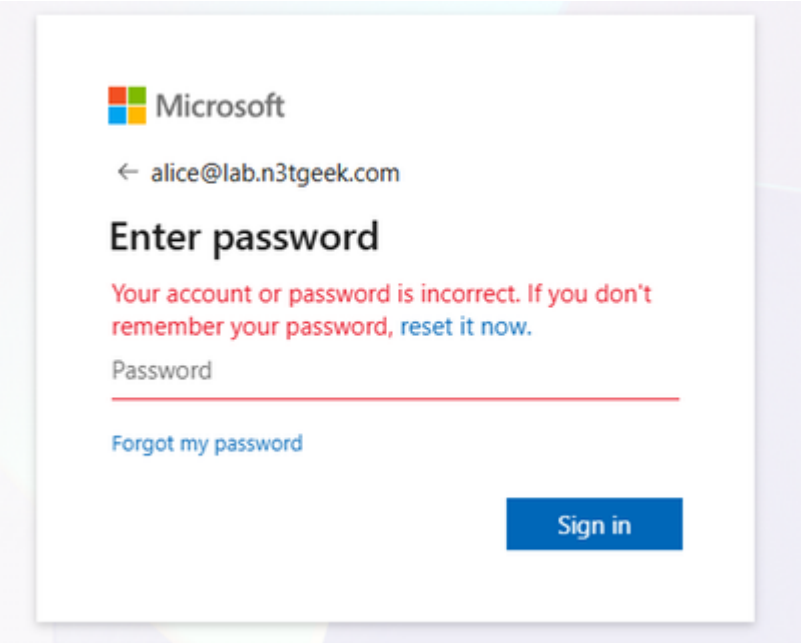
L'authentification SSO initiée par IdP n'est pas prise en charge : Cisco ISE ne prend pas en charge le SAML initié par IdP. Le bouton Test Single Sign-On (« Tester cette application ») dans Microsoft Entra ID échoue toujours pour cette intégration : le POST initié par IdP atteint SSOLoginResponse.action et le portail renvoie une requête HTTP [400] incorrecte (« La requête n'est pas valide en raison d'une syntaxe incorrecte ou de données non valides »). Il s'agit d'un comportement normal, et non d'une mauvaise configuration. Vérifiez toujours du côté du portail du sponsor.



Dépannage

L'authentification SAML s'effectue entre le navigateur et l'identifiant Microsoft Entra ; Les erreurs peuvent apparaître directement à partir du fournisseur d'identité avant même qu'ISE ne soit impliquée.

Problème 1 : Mot de passe incorrect



L'erreur apparaît sur la page de connexion Microsoft ; aucune donnée utilisateur n'a atteint ISE. Du côté ISE, les journaux affichent uniquement la branche sortante, puis rien. Dans le fichier guest.log, le flux du portail atteint SSO_LOGIN, crée la requête SAML, redirige le navigateur vers le fournisseur d'identité et la session ne revient jamais :

<#root>

```
01:20:46 DEBUG StepExecutor          -- StepTran for Step=INIT => tranEnum=PROCEED_SSO, toStep=SSO_LOGI
01:20:46 DEBUG SSOLoginConfigHandler -- Redirect to IDP:
    https://login.microsoftonline.com/<Tenant-ID>/saml2?SAMLRequest=jZNRc6IwFIX...
01:20:46 INFO  ISEPortalControllerUtils -- forwarding to: pages/ssoLoginRequest.jsp
(the portal session ends here --
```

no SSOLoginResponse is ever POSTed back

)

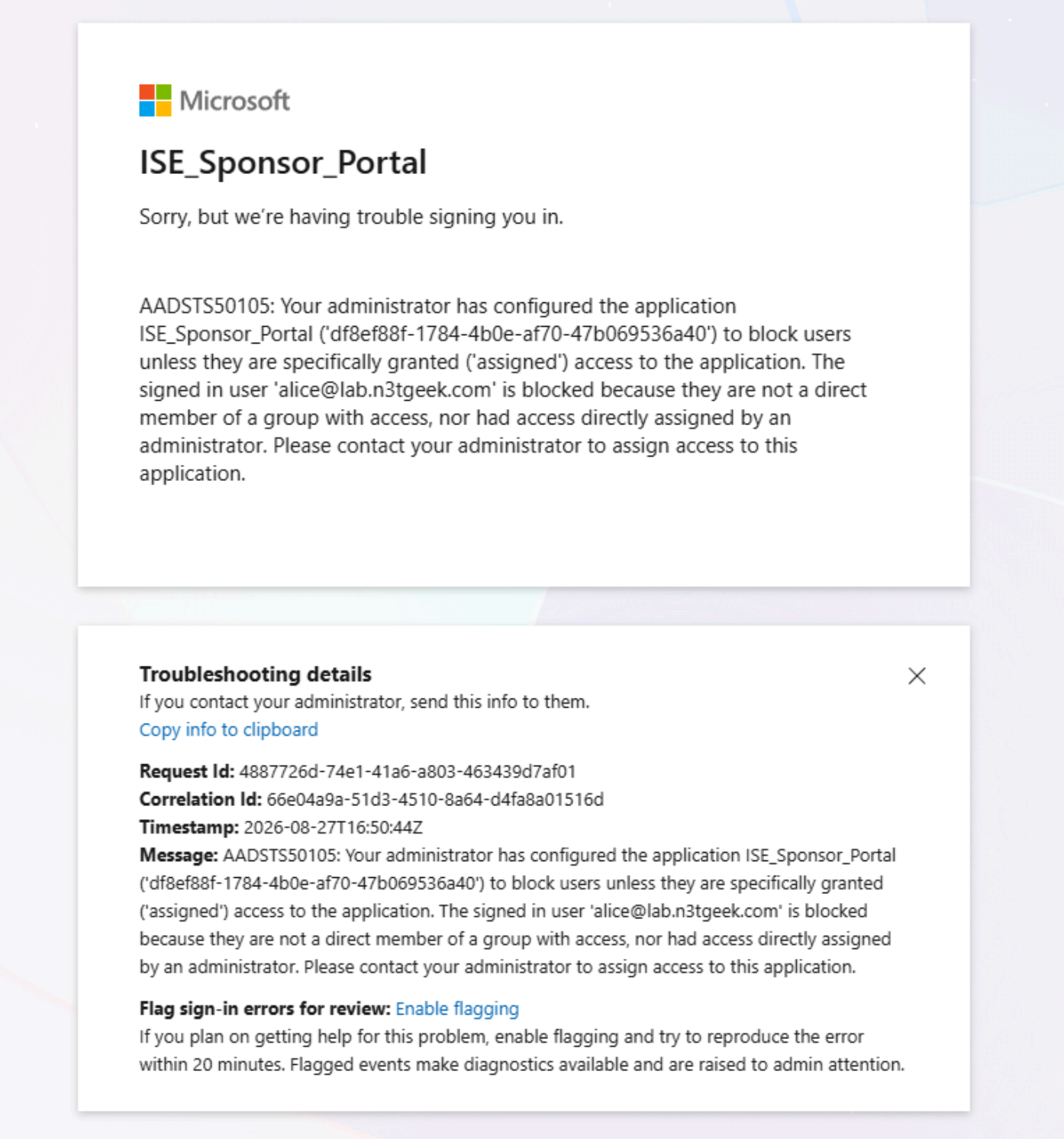
Le ise-psc.log raconte la même histoire du côté du framework SAML :

```
01:20:46 DEBUG SAMLFacadeImpl  -- SAML request - providerId (as should be found in IdP
    configuration): http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2
01:20:46 DEBUG SAMLFacadeImpl  -- SAML request - spUrlToReturnTo:
```

```
    https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action
01:20:46 DEBUG SAMLFacadeImpl  -- SignAuthenRequest configuration is - off
01:20:46 DEBUG MessageComposer -- local cert is null, request won't be signed
(capture ends here -- ISE never receives a SAML response)
```

Problème 2 — Utilisateur non affecté à l'application (AADSTS50105)

Entra ID bloque la connexion avant l'émission d'une réponse SAML.



Le fichier nguest.log affiche uniquement la redirection en cours de préparation, et ise-psc.log n'affiche aucune activité SAML. L'échec est du côté IdP :

<#root>

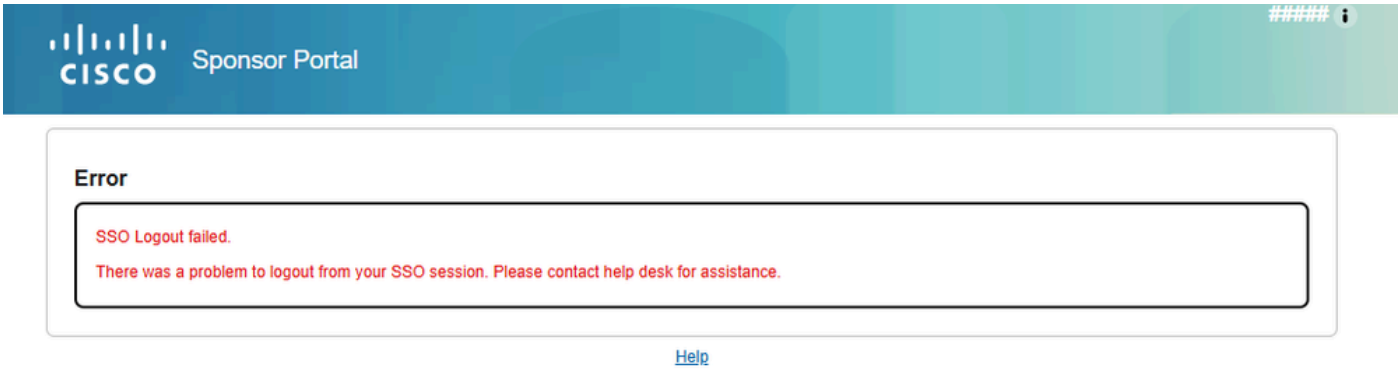
```
16:50:21 INFO  ISEPortalControllerUtils -- forwarding to: pages/ssoLoginRequest.jsp
(nothing follows --
```

the user never returns from the IdP

)

Régler: Attribuez l'utilisateur ou le groupe à l'application d'entreprise (étape 2.4).

Problème 3 : échec de la déconnexion (« Échec de la déconnexion SSO »)



Cela se produit lorsque l'URL de déconnexion dans l'ID d'entrée a été configurée avec SSOLogoutRequest.action?portal=... URL au lieu de SSOLogoutResponse.action. Dans guest.log, la déconnexion est lancée et la réponse renvoyée ne peut pas être traitée :

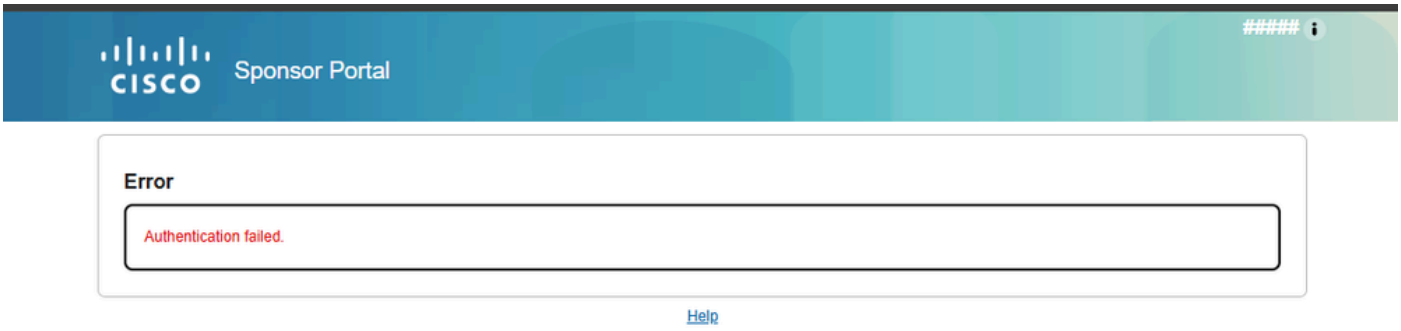
```
16:54:12 INFO  ISEPortalControllerUtils -- forwarding to: /pages/ssoLogoutRequest.jsp
16:54:13 ERROR SponsorSSOLogin -- SAML Response is invalid or subject is NULL!
16:54:13 INFO  ISEPortalControllerUtils -- forwarding to: pages/error.jsp
```

Régler: corrigez l'URL de déconnexion dans la configuration SAML de base.

Problème 4 — Certificat de signature modifié (« L'authentification a échoué »)

Lorsque le certificat de signature de jeton d'ID d'entrée pivote (durée de vie de trois ans), un

nouveau certificat est activé et le XML de métadonnées de fédération n'est pas réimporté dans ISE, CHAQUE connexion échoue avec un "Authentication failed" générique sur le portail, même si rien n'a visiblement changé de chaque côté.



Le fichier ise-psc.log indique explicitement la cause réelle :

```
16:58:30,429 WARN  apache.xml.security.signature.XMLSignature -- Signature verification failed.
16:58:30,430 ERROR cpm.saml.framework.impl.SAMLFacadeImpl -- SAML Response: processing failed:
com.cisco.cpm.saml.exceptions.SAMLException: Assertion signature did not validate
    against the IdP signature certificate
Caused by: org.opensaml.xml.validation.ValidationException: Signature did not validate
    against the credential's key
```

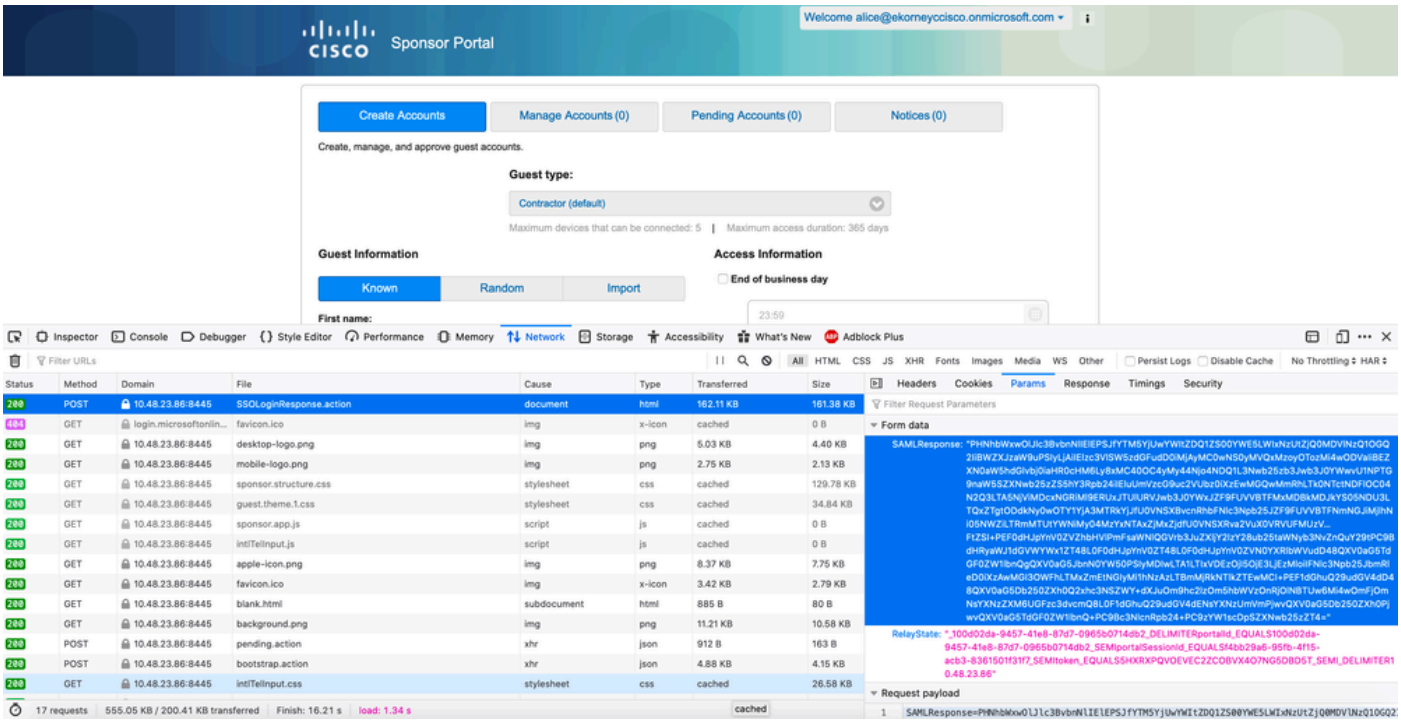
Régler: Téléchargez à nouveau le fichier XML des métadonnées de fédération à partir de l'ID d'entrée et réimportez-le dans ISE.

Problème 5 : la session expire rapidement

Le délai d'inactivité de la session SSO du portail est défini par défaut sur 5 minutes (configurable par portail et ce TP utilise 10). Un bouton "Se reconnecter" peut être ajouté à la page d'erreur du portail via le champ Contenu facultatif.

Dépannage client

Comme les messages SAML circulent dans le navigateur, les outils de développement du navigateur (F12 > Onglet Réseau) affichent l'intégralité de l'échange. Reproduisez la connexion avec l'onglet Réseau ouvert et recherchez le POST vers SSOLoginResponse.action. Au moment où le navigateur transmet l'assertion SAML à ISE :



Dépannage 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
accès invité	DÉBOGUER	guest.log
portal-web-action	DÉBOGUER	guest.log
ouvert	DÉBOGUER	ise-psc.log
petit	DÉBOGUER	ise-psc.log

Ensemble de travail des débogages au moment de l'exécution correcte du flux (ise-psc.log) :

1. L'utilisateur est redirigé vers l'URL IdP à partir du portail du sponsor.

```
2026-08-27 01:55:58,021 DEBUG  [admin-http-pool3][[]] guestaccess.apiservices.portal.view.PortalConfigC
 ::::- hostName =sponsor.n3tgeek.com will be applied to URL!
    reqUtl =https://sponsor.n3tgeek.com:8445/sponsorportal/PortalSetup.action
2026-08-27 01:55:58,036 DEBUG  [https-jsse-nio-192.168.1.204-8445-exec-2][[]]
cisco.ise.portalwebaction.utils.PortalSessionUtil -::::- Portal URL:
    https://sponsor.n3tgeek.com:8445/sponsorportal/PortalSetup.action
2026-08-27 01:55:58,037 DEBUG  cisco.ise.portalwebaction.actions.BasePortalAction -::::-
    Action com.cisco.ise.portalwebaction.actions.PortalSetupAction Complete for request /sponsorportal/
```

2. La réponse SAML est reçue du navigateur :

```
2026-08-27 01:56:19,384 DEBUG cpm.saml.framework.impl.SAMLFacadeImpl -::::-
    SAML Response: statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
IdP URI: https://sts.windows.net/<Tenant-ID>/
SP URI: http://CiscoISE/1f789a00-ad9d-4ec0-9a47-ce4909a65db2
Assertion Consumer URL: https://sponsor.n3tgeek.com:8445/sponsorportal/SSOLoginResponse.action
```

3. L'analyse d'attribut (assertion) démarre :

```
cpm.saml.framework.validators.SAMLSignatureValidator -::::- no signature in response
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Validating signature of assertion
org.opensaml.xml.signature.SignatureValidator -::::- Signature validated with key from supplied credent
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated succesfully
cpm.saml.framework.validators.AssertionValidator -::::- Conditions succesfully validated
```

4. Le nom d'utilisateur et l'attribut de groupe (48f07fce-26e5-41e5-a82b-ed095b32bab8) sont extraits de l'assertion et l'authentification passe :

```
SAMLUtils::getUserNameFromAssertion: username value from Subject is=[alice@lab.n3tgeek.com]
loginInfo: ... format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
[cacheGroupAttr] Adding to cache ExternalGroup values=<48f07fce-26e5-41e5-a82b-ed095b32bab8>
AuthenticatePortalUser - added user groups from SAML response to AuthenticationResult,
    all retrieved groups:[48f07fce-26e5-41e5-a82b-ed095b32bab8]
Authenticate SAML User - result:PASSED
```

5. Le groupe d'utilisateurs est ajouté aux résultats de l'authentification afin d'être utilisé par le portail et l'authentification SAML est transmise :

```
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
2020-09-16 10:44:11,320 DEBUG [https-jsse-nio-10.48.23.86-8445-exec-8][] cpm.saml.framework.impl.SAMLFa
```

Analyse de capture de paquets

Une capture effectuée sur l'interface ISE (Opérations > Dépannage > Outils de diagnostic > Dépôt TCP) lors d'une connexion de sponsor réussie n'affiche que deux types de trafic. Résolution DNS du client du FQDN du portail et sessions TLS du client au portail sur le port 8445, avec le FQDN du portail visible comme indication de nom de serveur TLS (SNI).

Conversation	Direction	Ce que c'est
client <-> ISE:8445 (TLS, SNI = FQDN du portail)	navigateur -> PSN	Pages du portail + SAML POST (ACS)
client -> DNS : FQDN du portail	navigateur -> résolveur	Résolution du nom du portail
aucun trafic vers login.microsoftonline.com	—	La branche IdP ne touche jamais ISE

Hello du client TLS : où le nom du portail est visible

Bien que tout soit chiffré, le TLS Client Hello se déplace en texte clair et transporte le FQDN du portail comme indication de nom de serveur (SNI). C'est le seul endroit de la capture où vous pouvez faire correspondre un flux TCP au portail du sponsor.

```
Frame 96: 1981 bytes on wire
Internet Protocol Version 4, Src: 192.168.1.162 (client), Dst: 192.168.1.204 (ISE PSN)
Transmission Control Protocol, Src Port: 43395, Dst Port: 8445
Transport Layer Security
    TLSv1 Record Layer: Handshake Protocol: Client Hello
        Handshake Protocol: Client Hello
            Extension: server_name (len=24)
                Server Name Indication extension
                    Server Name: sponsor.n3tgeek.com
            Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
```

La même connexion capturée sur le client

```
  8445  sponsor.n3tgeek.com         (x12 -- the portal leg, to ISE)
  443  login.microsoftonline.com   (the IdP leg -- never seen on ISE)
  443  aadcdn.msauth.net           (Microsoft sign-in page assets)
  443  login.live.com / login.microsoft.com
(unrelated background traffic omitted for clarity)
```



Remarque : ISE ne communique jamais avec Entra ID pendant l'authentification du sponsor. La requête et la réponse SAML parcourent le navigateur des utilisateurs (redirection et liaisons POST). Cela signifie que le noeud ISE n'a besoin d'aucune connectivité sortante vers Microsoft pour que l'authentification SSO du portail fonctionne, et lors du dépannage, la branche IdP doit être capturée sur le client, et non sur ISE.

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.