

Configuration du flux de connexion administrateur de l'interface utilisateur graphique ISE 3.1 via l'intégration SSO SAML avec Azure AD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Fournisseur d'identité \(IdP\)](#)

[Fournisseur de services \(SP\)](#)

[SAML](#)

[Assertion SAML](#)

[Diagramme D'Écoulement De Haut Niveau](#)

[Configurer l'intégration SSO SAML avec Azure AD](#)

[Étape 1. Configurer le fournisseur d'identité SAML sur ISE](#)

[1. Configurer Azure AD en tant que source d'identité SAML externe](#)

[2. Configurer la méthode d'authentification ISE](#)

[3. Exporter les informations du fournisseur de services](#)

[Étape 2. Configurer les paramètres Azure AD IdP](#)

[1. Créer un utilisateur Azure AD](#)

[2. Créer un groupe Azure AD](#)

[3. Affecter un utilisateur Azure AD au groupe](#)

[4. Créer une application Azure AD Enterprise](#)

[5. Ajouter un groupe à l'application](#)

[6. Configurer une application Azure AD Enterprise](#)

[7. Configurer l'attribut Groupe Active Directory](#)

[8. Télécharger le fichier XML de métadonnées de fédération Azure](#)

[Étape 3. Télécharger des métadonnées d'Azure Active Directory vers ISE](#)

[Étape 4. Configurer des groupes SAML sur ISE](#)

[\(Facultatif\) Étape 5. Configurer les 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

Fournisseur d'identité (IdP)

Dans ce cas, c'est l'autorité Azure AD qui vérifie et affirme l'identité d'un utilisateur et les privilèges d'accès à une ressource demandée (le « fournisseur de services »).

Fournisseur de services (SP)

La ressource ou le service hébergé auquel l'utilisateur a l'intention d'accéder, le serveur d'applications ISE dans ce cas.

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)

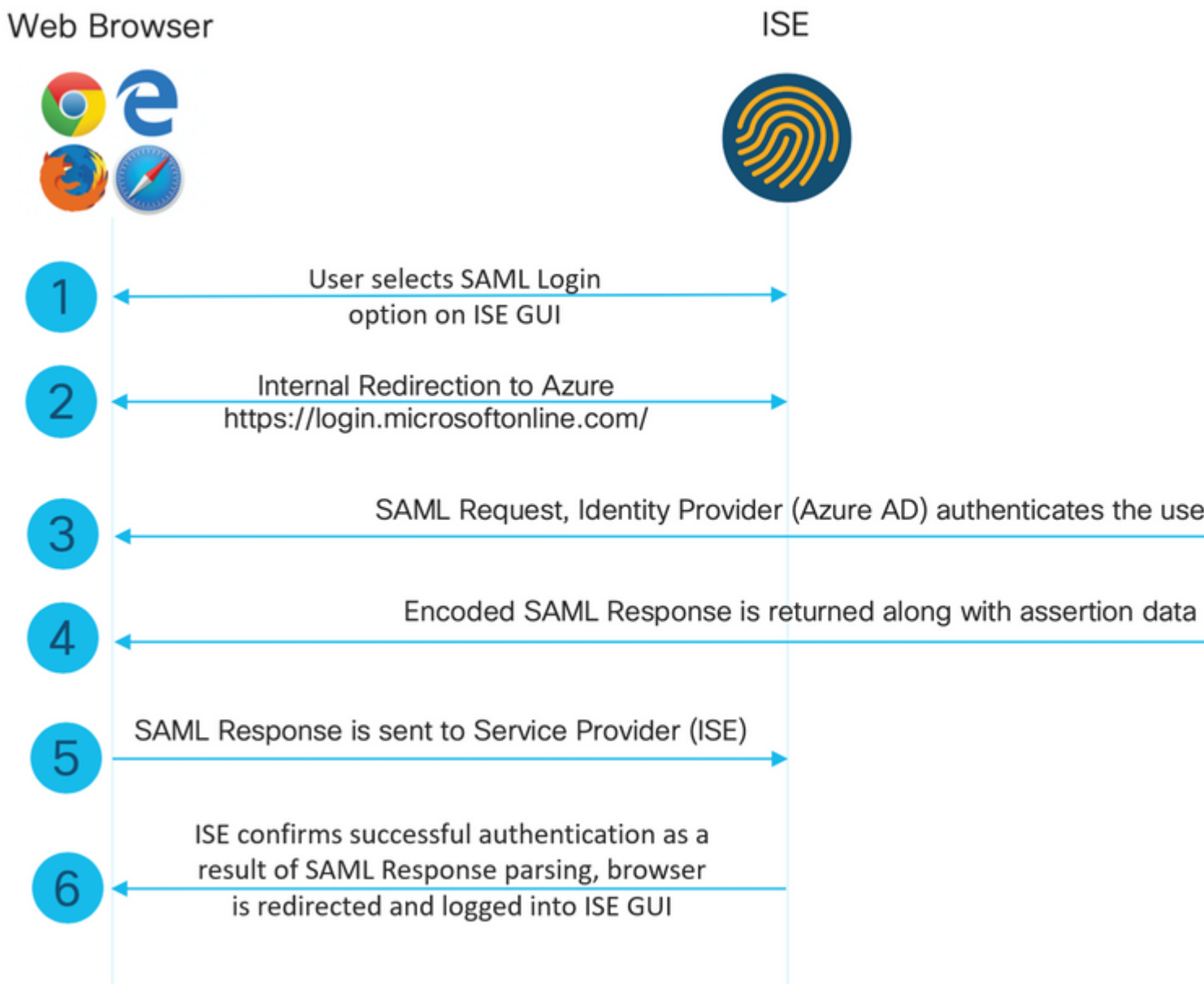
- L'assertion d'attribution transmet les attributs SAML, des données spécifiques qui fournissent des informations sur l'utilisateur, au fournisseur de services.
- Une assertion de décision d'autorisation déclare si l'utilisateur est autorisé à utiliser le service ou si le fournisseur d'identification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

Diagramme D'Écoulement De Haut Niveau

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 Azure AD, comme indiqué dans l'image.



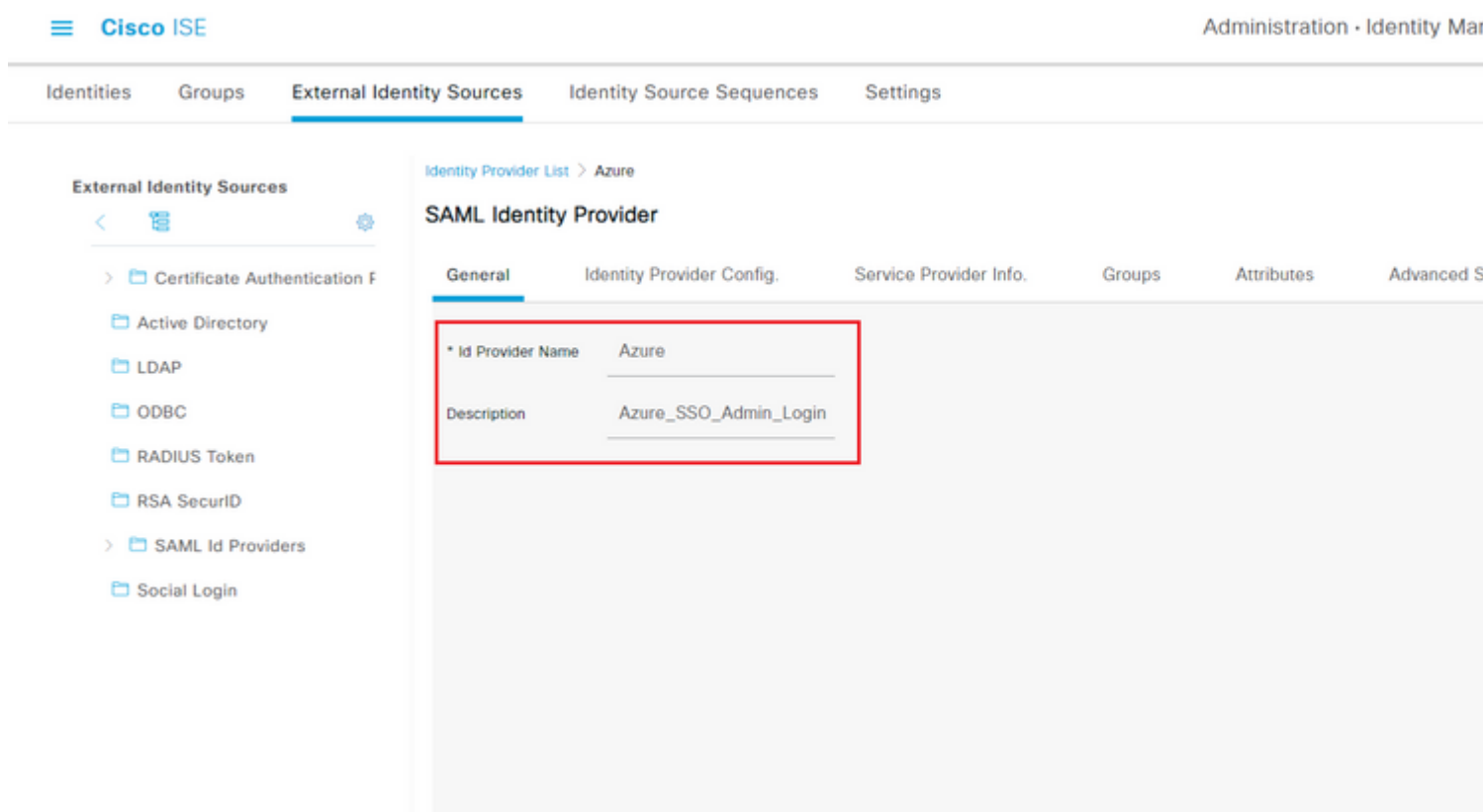
Configurer l'intégration SSO SAML avec Azure AD

Étape 1. Configurer le fournisseur d'identité SAML sur ISE

1. Configurer 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. Configurer 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.

- Authentication
- Authorization >
- Administrators >
- Settings >

Authentication Type ⓘ

Password Based

Client Certificate Based

* Identity Source

SAML:Azure



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 **Export** comme illustré dans l'image.

SAML Identity Provider

General Identity Provider Config. **Service Provider Info.** Groups Attribute

Service Provider Information

Load balancer (i)

Export Service Provider Info. Export (i)

Includes the following portals:

Sponsor Portal (default)

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:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" >
    <md:KeyDescriptor use="signing" >
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
        <ds:X509Data >
          <ds:X509Certificate >
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
QU1MX21zZTMtMS0xOjU5a3VtYXN1bWVtAEFw0yMTA3MTkwMzI4MDEBaFw0yMTA3MTkwMzI4MDEBa
MCUxIzAhBgNVBAMTG1NBTUxfaXN1My0xLW50aWw0LW50aWw0LW50aWw0LW50aWw0LW50aWw0LW50aWw0
AAOCAG8AMIICCGKCAgEAvila4+S0uP3j037yCOXnHAZADupfqcwcp1JQnFxfhVfnDd0ixGRT8iaQ
1zdKhpwF/BsJeSznXyaPVxFcmMFHbmyt46gQ/jjQEyt7YhyohG0t1op01qDGwt0nWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyJGKDDPf+1VM5JHCo6UNLFIIfyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqvrrYzuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g4L4WJWmizETO6Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0ssshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwnGo7pQI8CAwEAAAN9MHswIAAYDVR0RBbkwF4IVaXN1My0xLW50aWw0LW50aWw0LW50aWw0
MAwGA1UdEQUEFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwXqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHg0T2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GwlvccgreC7R46qenaonXVr1tRw11vVIdcf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUtEi6f0bqr0wCyd9Tj7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gFH0bE5luT4EYVuuHwMNGbZqqqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cXzoUxDm+HReSe+0JhRCyIJC0vUpdNmYC8cfAZuiV/e3wk0BLZM
lgV8FTVQSNra9LwHP/PgeNAPUCRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTET9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1P0KXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKWER/q1GgaVwh3X/G+z1shUQDrJcBdLcZI1WKUMA6XVDj18byhBM7pFGwg4z9YJZGF
```

```
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/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.action" />
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action" />

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

Attributs intéressants du fichier XML :

entityID=["http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2"](http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2)

AssertionConsumerService Location=["https://10.201.232.19:8443/portal/SSOLoginResponse.action"](https://10.201.232.19:8443/portal/SSOLoginResponse.action)

AssertionConsumerService Location=["https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action"](https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action)

Étape 2. Configurer les paramètres Azure AD IdP

1. Créer 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.

Azure Active Directory admin center

Dashboard > Default Directory

Default Directory | Overview

Azure Active Directory

Switch tenant Delete tenant Create a tenant What's new

Azure Active Directory can help you enable remote work for your employees and partners.

Default Directory

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Premium P2

Tenant ID
64ace648-115d-4ad9-a3bf-7660... [Copy](#)

Primary domain
ekorneyccisco.onmicrosoft.com

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

3
2.8
2.6
2.4
2.2
2

Aug 23

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.

Identity

User name * ⓘ

mck ✓

@ gdplab2021.onmicrosoft... ▾



The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

.....

Show Password

Create

2. Créer un groupe Azure AD

Sélectionnez **Groupes**. Cliquez sur **Nouveau groupe**.

[Dashboard](#) > [Default Directory](#) > [Groups](#)



Groups | All groups

Default Directory - Azure Active Directory



+ New group



Download groups



Delete



All groups



Deleted groups



Diagnose and solve problems



This page includes previews available for your evaluation



Search groups

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

Navigation sidebar with items: Dashboard, All services, FAVORITES, Azure Active Directory, Users, Enterprise applications.

Dashboard > TAC > Groups >

New Group ...

Group type * ⓘ

Security

Group name * ⓘ

ISE Admin Group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group ⓘ

Yes

No

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

No members selected

3. Affecter 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.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

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.

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems

Settings

- General
- Expiration
- Naming policy

+ New group | Download groups | Delete | Refresh | Columns | Pre

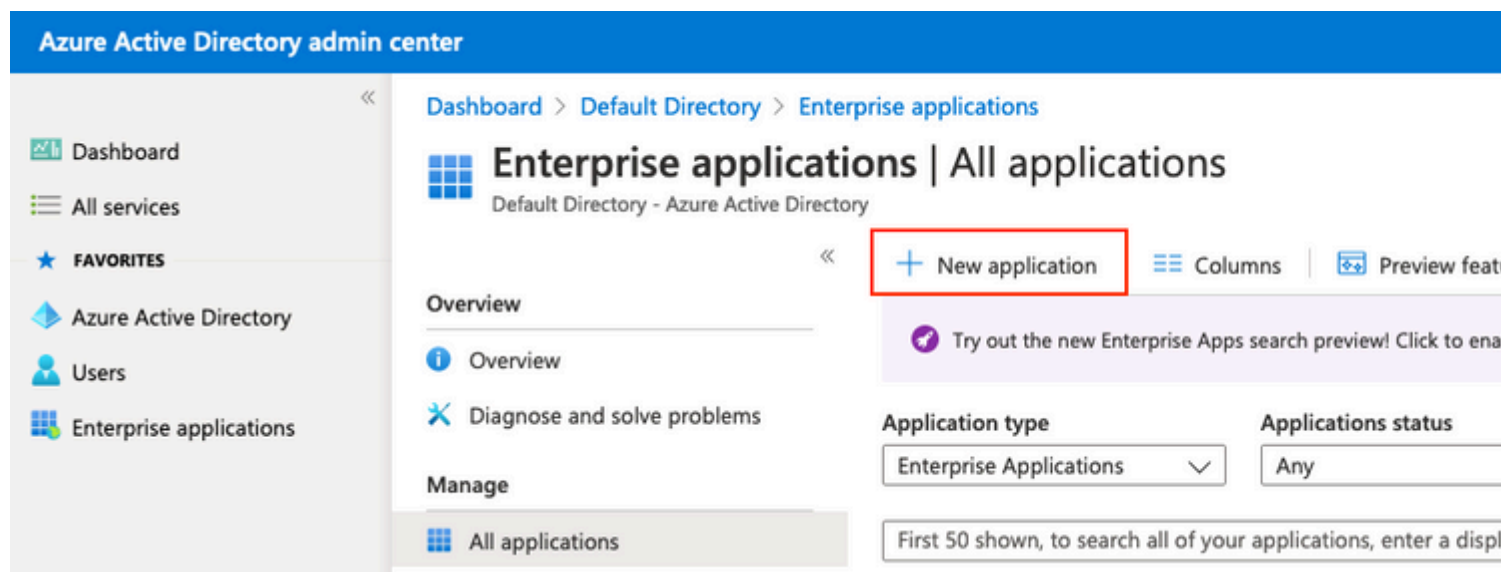
This page includes previews available for your evaluation. View previews →

Search groups | Add filters

	Name	Object Id	Group Type
<input type="checkbox"/>	ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security

4. Créer une application Azure AD Enterprise

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



The screenshot shows the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb path is "Dashboard > Default Directory > Enterprise applications". The main heading is "Enterprise applications | All applications" with the subtitle "Default Directory - Azure Active Directory". On the left side, there is a navigation pane with "Enterprise applications" selected. In the main content area, the "Overview" section is active, and the "+ New application" button is highlighted with a red rectangular box. Other visible elements include a "Columns" button, a "Preview feat" button, a notification banner about the new search preview, and filter dropdowns for "Application type" (set to "Enterprise Applications") and "Applications status" (set to "Any").

Sélectionnez l'option **Créer votre propre application**.

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Browse Azure AD Gallery

[+ Create your own application](#) | [Request new gallery app](#) | [Got feedback?](#)

[You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience.](#)

Search application

Single Sign-on : All

User Account Management : All

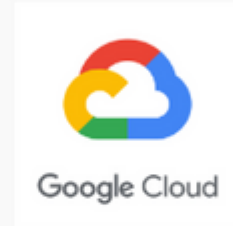
Category

Cloud platforms

Amazon Web Services (AWS)



Google Cloud Platform



On-premises applications

Add an on-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy

Learn how to use Application Proxy to provide secure access to your on-premises applications.

[Federated SSO](#) | [Provisioning](#)

Featured applications

 **Adobe Creative Cloud**
Microsoft Corporation

 **Adobe Identity Management**
Adobe Inc.

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.

Create your own application



What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

5. Ajouter un groupe à l'application

Sélectionnez **Affecter des utilisateurs et des groupes**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

ISE_3_1_Admin_SSO | Overview

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Properties

Name: ISE_3_1_Admin_SSO

Application ID: 76b82bcb-a918-4016-aad7-...

Object ID: 22aedf32-82c7-47f2-ab34-1...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

Cliquez sur **Ajouter un utilisateur/groupe**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO

ISE_3_1_Admin_SSO | Users and groups

Enterprise Application

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
--------------	-------------

Cliquez sur **Utilisateurs et groupes**.

Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

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.

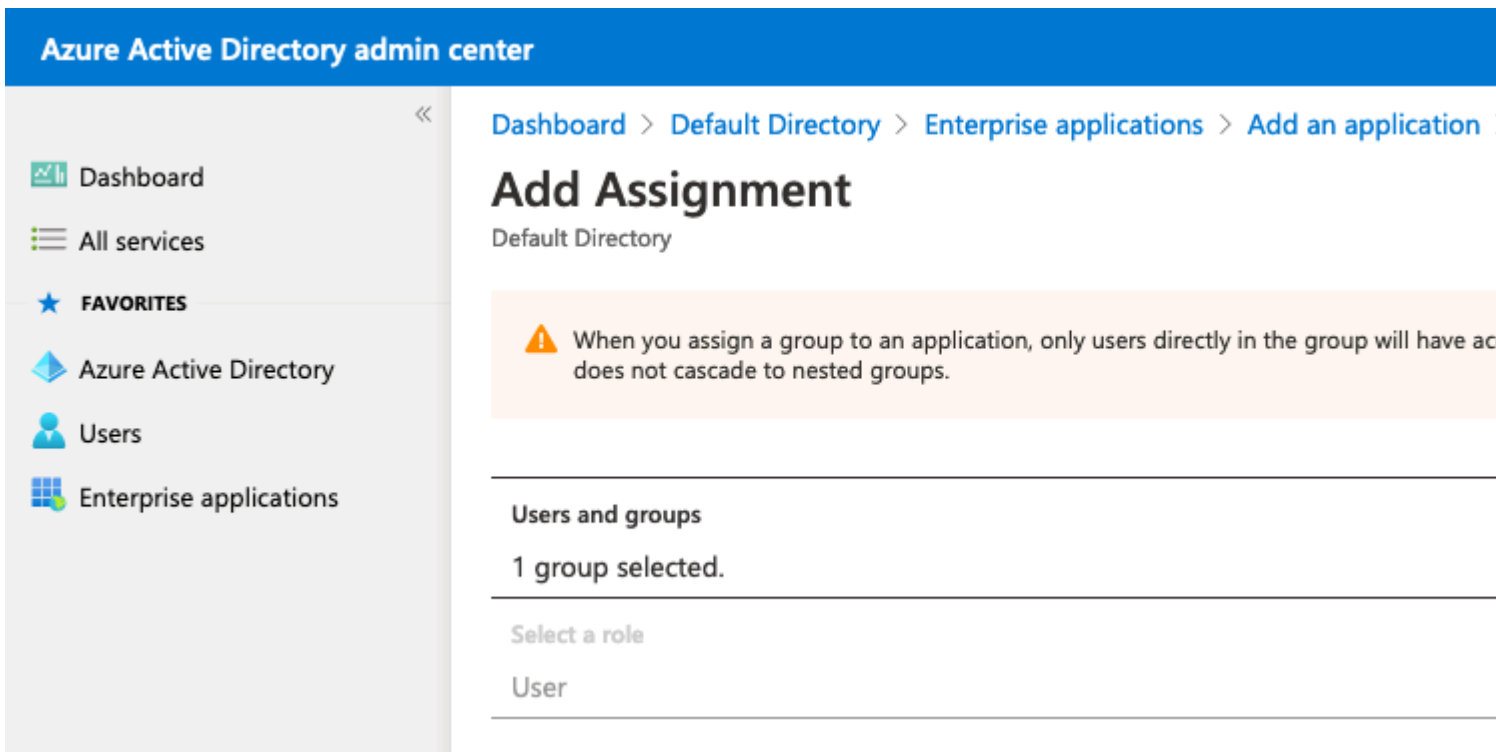
Users and groups

Search

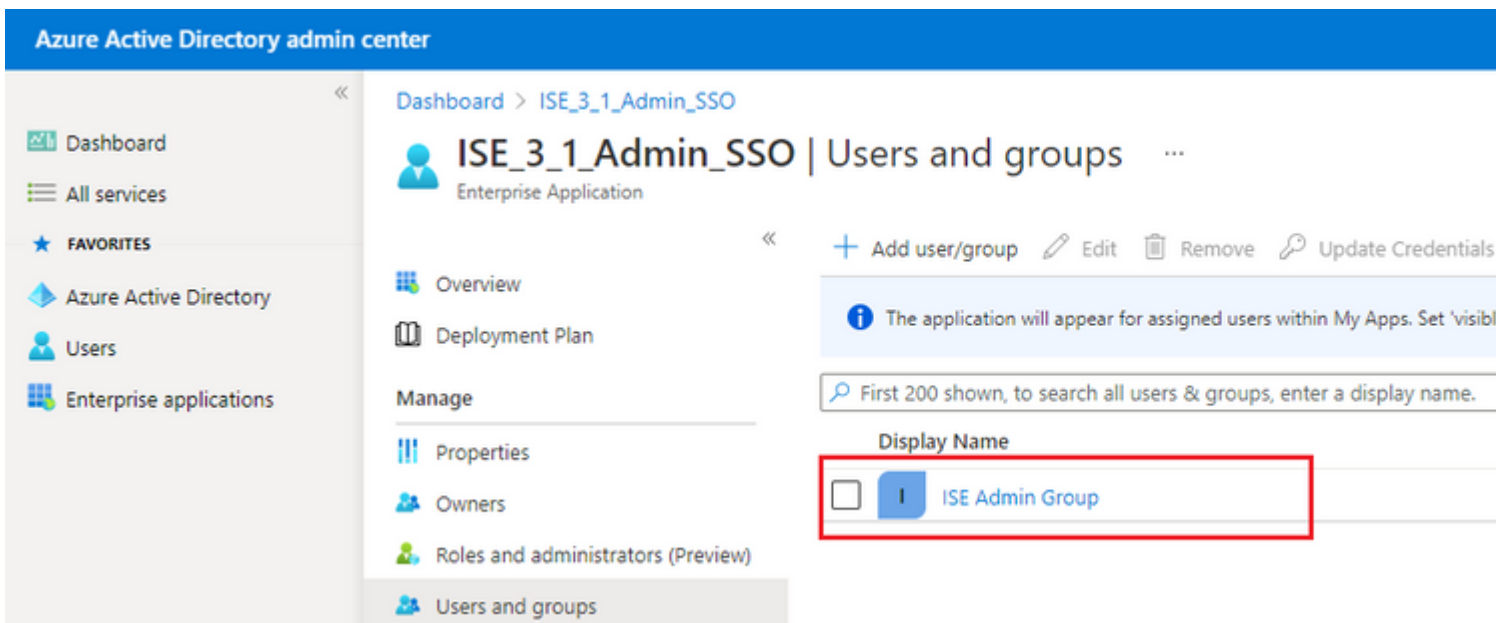
I ISE Admin Group

MC mck
mck@gdplab2021.onmicrosoft.com

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. Configurer une application Azure AD Enterprise

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

The screenshot displays the Azure Active Directory admin center interface. The top navigation bar is blue with the text 'Azure Active Directory admin center'. Below it, the breadcrumb path is 'Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview'. The main content area is divided into three sections: a left-hand navigation pane, a central 'Overview' section, and a right-hand 'Properties' section. The left pane includes 'Dashboard', 'All services', 'FAVORITES', 'Azure Active Directory', 'Users', and 'Enterprise applications'. The central pane shows 'Overview' selected, with sub-sections for 'Deployment Plan', 'Manage', and 'Security'. The 'Properties' section lists 'Name', 'Application ID', and 'Object ID' with their respective values and copy icons. Below the properties is a 'Getting Started' section with a task card for '1. Assign users and groups'.

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview ...

ISE_3_1_Admin_SSO
Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Properties

Name ⓘ
ISE_3_1_Admin_SSO

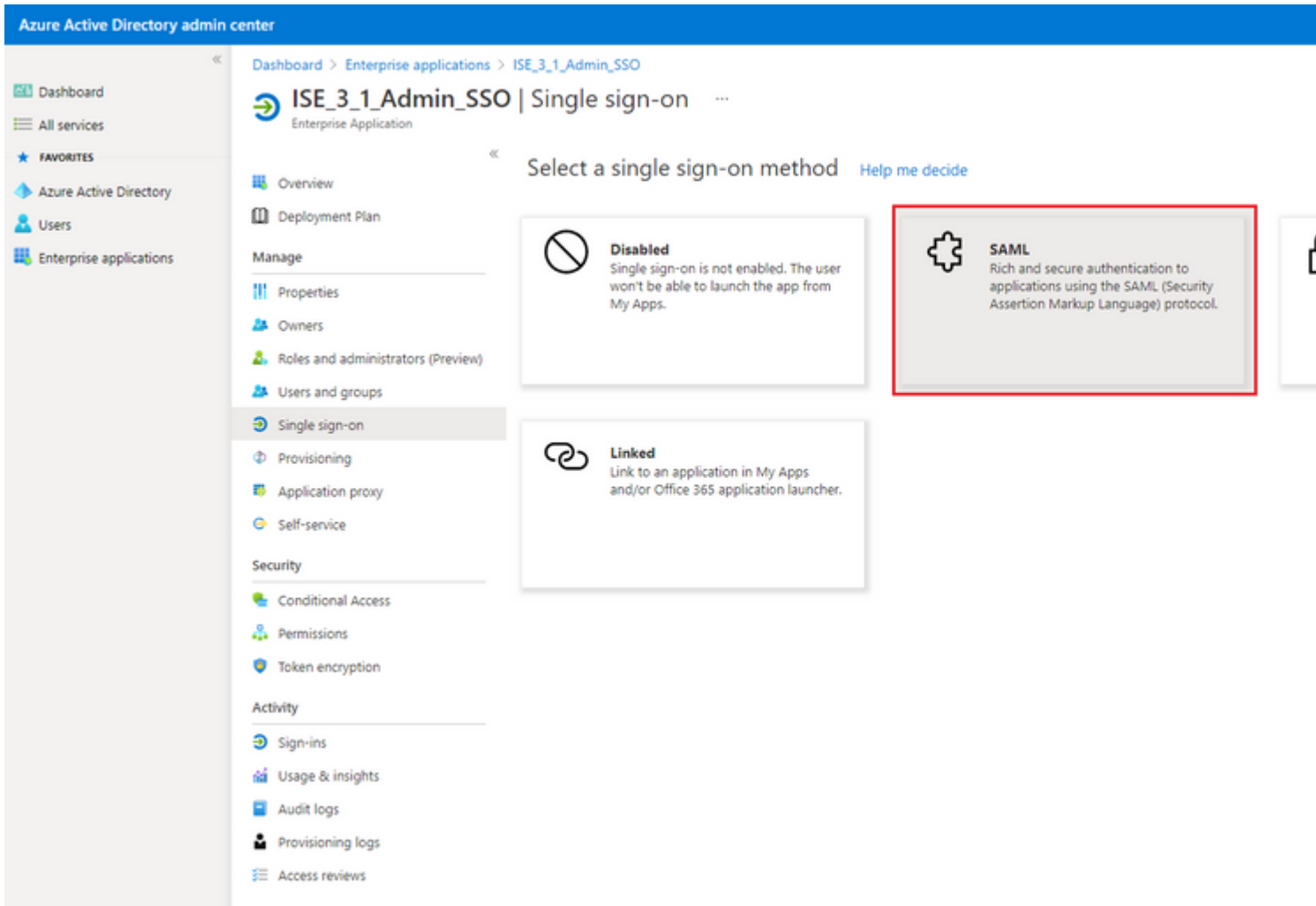
Application ID ⓘ
76b82bcb-a918-4016-aad7-...

Object ID ⓘ
22aedf32-82c7-47f2-ab34-1...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

Sélectionnez **SAML** sur l'écran suivant.



Cliquez sur **Edit** en regard de **Basic SAML Configuration**.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating ISE30.

- Basic SAML Configuration** Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>
- User Attributes & Claims** Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Renseignez Identifieur (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 client)**

d'assertion) avec la valeur **Emplacements de AssertionConsumerService**. Cliquez sur Save.

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.

Basic SAML Configuration



 Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default


  <http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd>

  <http://adapplicationregistry.onmicrosoft.com/customappsso/primary>

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

  <https://10.201.232.19:8443/portal/SSOLoginResponse.action>

Sign on URL

Relay State

Logout Url

7. Configurer l'attribut Groupe Active Directory

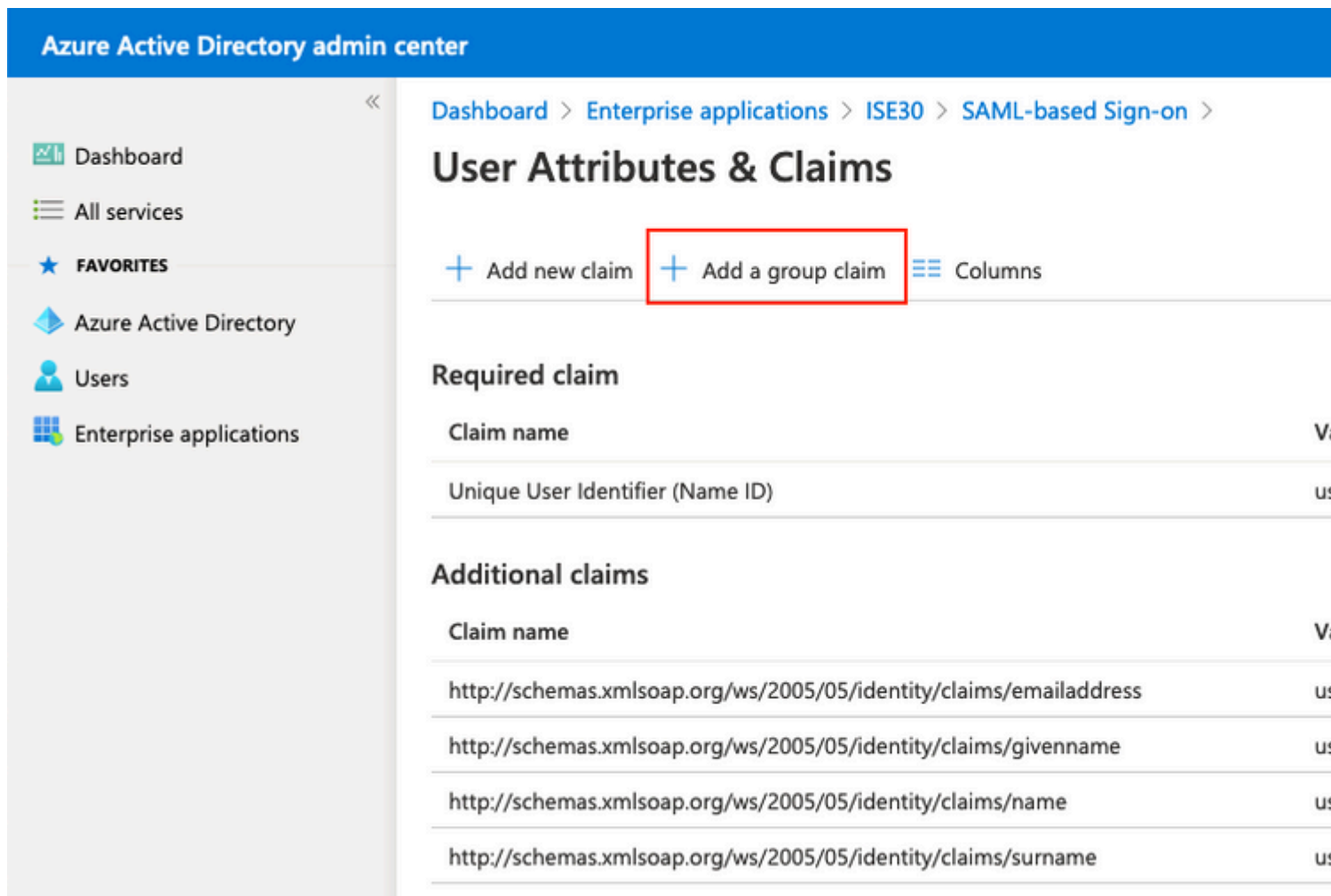
Afin de retourner la valeur d'attribut de groupe configurée précédemment, cliquez sur **Edit** à côté de **User Attributes & Claims**.

User Attributes & Claims



givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Cliquez sur **Ajouter une revendication de groupe**.

A screenshot of the Azure Active Directory admin center interface. The top navigation bar is blue with the text "Azure Active Directory admin center". The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area shows the breadcrumb "Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims". Below the breadcrumb, there are two buttons: "+ Add new claim" and "+ Add a group claim" (highlighted with a red box), followed by a "Columns" button. The page is divided into two sections: "Required claim" and "Additional claims". The "Required claim" section has a table with one row: "Unique User Identifier (Name ID)". The "Additional claims" section has a table with four rows, each with a "Claim name" and a value: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name", and "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname".

Sélectionnez **Security groups** et cliquez sur **Save**. Sélectionnez **ID de groupe** dans le menu déroulant **Attribut** source. Cochez la case pour personnaliser le nom de la revendication de groupe et entrez le nom **Groupes**.

Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID

Advanced options

- Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

- Emit groups as role claims ⓘ

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

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.o

Additional claims

Claim name	Value
Groups	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.m
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.g
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.r
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.s

8. Télécharger le fichier XML de métadonnées de fédération Azure

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

SAML Signing Certificate Edit

Status	Active
Thumbprint	B24F4BB47B350C93DE3D59EC87EE4C815C884462
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e960...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

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**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · Identity Management'. Below this, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' tab is selected. On the left, there is a sidebar with 'External Identity Sources' and a list of categories: 'Certificate Authentication F', 'Active Directory', 'LDAP', 'ODBC', 'RADIUS Token', 'RSA SecurID', 'SAML Id Providers', and 'Social Login'. The main content area is titled 'SAML Identity Provider' and has a breadcrumb 'Identity Provider List > Azure'. Below this, there are tabs for 'General', 'Identity Provider Config.', 'Service Provider Info.', and 'Groups'. The 'Identity Provider Config.' tab is active. The 'Identity Provider Configuration' section includes an 'Import Identity Provider Config File' button with a 'Choose File' button next to it. Below this, there are fields for 'Single Sign On URL' and 'Single Sign Out URL (Redirect)', both containing the URL 'https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197...'. The 'Sianina Certificates' section contains a table with columns for Subject, Issuer, Valid From, and Valid To (Ex). One certificate is listed with Subject 'CN=Microsoft Azure Federated SSO Certificate' and Issuer 'CN=Microsoft Azur...'. The table is partially obscured by a red border.

Étape 4. Configurer 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**.

External Identity Sources

- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. **Groups**

Groups

Group Membership Attribute groups

+ Add Edit Delete Name in Assertion ^ Name in

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**. Cliquez sur **OK**. Cliquez sur **Save**.

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

Add Group

*Name in Assertion 576c60ec-c0b6-4044-a8ec-d3

*Name in ISE Customization Admin

- Customization Admin
- ERS Admin
- ERS Operator
- Elevated System Admin
- Helpdesk Admin
- Identity Admin
- MnT Admin
- Network Device Admin
- Policy Admin
- RBAC Admin
- SPOG Admin
- Super Admin
- System Admin
- TACACS+ Admin

(Facultatif) Étape 5. Configurer les 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.

▼ RBAC Policies

	Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> ▼	<u>Customization Admin Policy</u>	If <u>Customization Admin</u> +	then <u>Customization Admin M</u>
<input checked="" type="checkbox"/> ▼	<u>Elevated System Admin Poli</u>	If <u>Elevated System Admin</u> +	then <u>System Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Admin Policy</u>	If <u>ERS Admin</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Operator Policy</u>	If <u>ERS Operator</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>ERS Trustsec Policy</u>	If <u>ERS Trustsec</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Helpdesk Admin Policy</u>	If <u>Helpdesk Admin</u> +	then <u>Helpdesk Admin Menu A</u>
<input checked="" type="checkbox"/> ▼	<u>Identity Admin Policy</u>	If <u>Identity Admin</u> +	then <u>Identity Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>MnT Admin Policy</u>	If <u>MnT Admin</u> +	then <u>MnT Admin Menu Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Network Device Policy</u>	If <u>Network Device Admin</u> +	then <u>Network Device Menu A</u>
<input checked="" type="checkbox"/> ▼	<u>Policy Admin Policy</u>	If <u>Policy Admin</u> +	then <u>Policy Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>RBAC Admin Policy</u>	If <u>RBAC Admin</u> +	then <u>RBAC Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>Read Only Admin Policy</u>	If <u>Read Only Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>SPOG Admin Policy</u>	If <u>SPOG Admin</u> +	then <u>Super Admin Data Acce</u>
<input checked="" type="checkbox"/> ▼	<u>Super Admin Policy</u>	If <u>Super Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>Super Admin_Azure</u>	If <u>Super Admin</u> +	then <u>Super Admin Menu Acc</u>
<input checked="" type="checkbox"/> ▼	<u>System Admin Policy</u>	If <u>System Admin</u> +	then <u>System Admin Menu Ac</u>
<input checked="" type="checkbox"/> ▼	<u>TACACS+ Admin Policy</u>	If <u>TACACS+ Admin</u> +	then <u>TACACS+ Admin Menu</u>

Vérifier

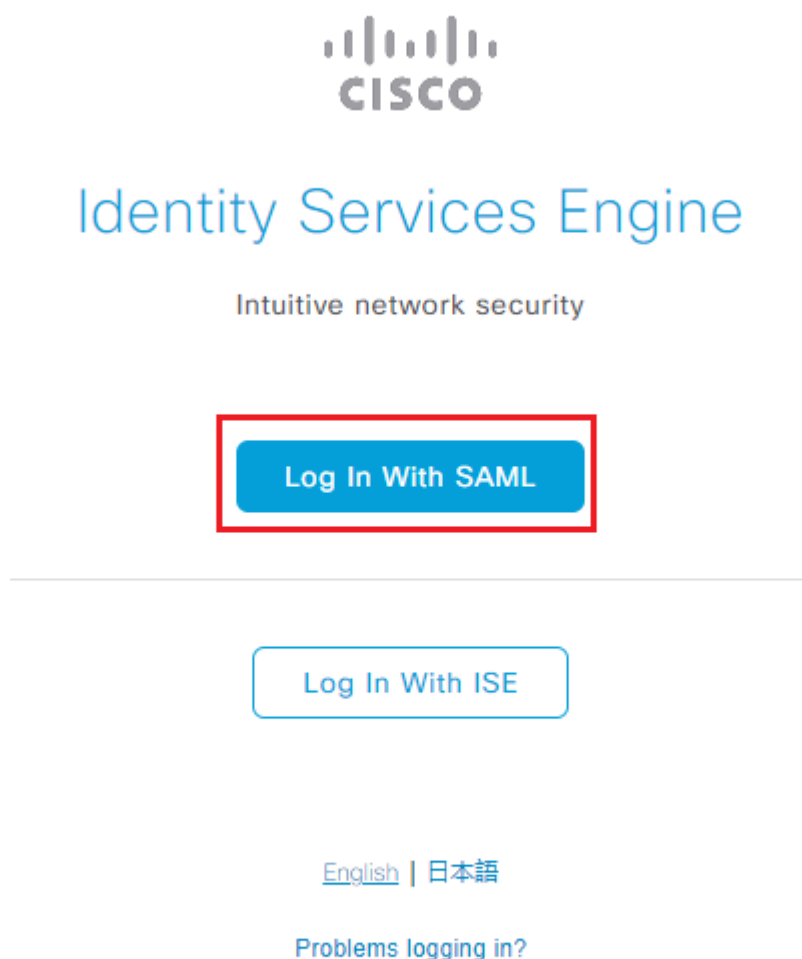
Vérifiez que votre configuration fonctionne correctement.

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.



Sign in

mck@gdplab2021.onmicrosoft.com

[Can't access your account?](#)

Next

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



← mck@gdplab2021.onmicrosoft.com

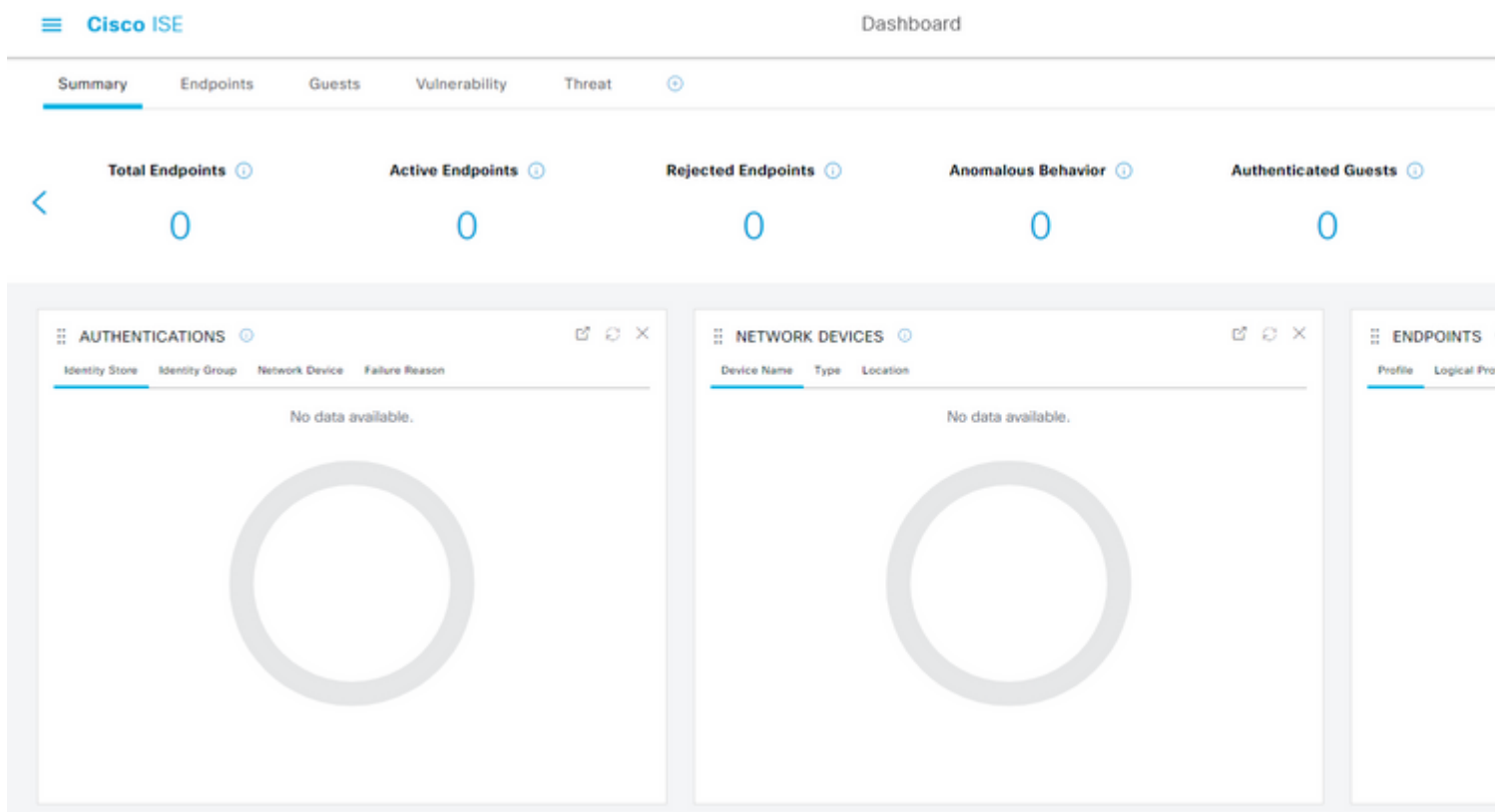
Enter password

.....

[Forgot my password](#)

Sign in

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 corriger : réinitialisez le mot de passe ou fournissez le mot de passe correct pour ce compte comme indiqué dans l'image.



← mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, [reset it now](#).

Password

[Forgot my password](#)

Sign in

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).

Afin de corriger ceci : vérifiez que le **groupe Add à l'étape de configuration Application** est correctement exécuté comme montré dans l'image.



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ✕

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

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.



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Upload metadata file | Change single sign-on mode | Test this application

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Groups	user.groups
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	824F4BB47B350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/182
Azure AD Identifier	https://sts.windows.net/182900ec-e96
Logout URL	https://login.microsoftonline.com/182

View step-by-step instructions

5 Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension to allow third-party cookies if you have installed it but this message

Please make sure you have configured ISE_3_1_Admin_SSO before

Sign in as current user
Sign in as someone else (requires browser)

Resolving errors

If you encounter an error in the sign-in page, please paste it below and retry.

What does the error look like?

Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: Saa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX

Get resolution guidance

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.

Pour résoudre ce problème : 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.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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

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

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

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

-:::- Decoded SAML relay state of: `_0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2`

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

-:::- Decoded SAML message

```
2021-07-29 13:48:27,182 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
opensaml.common.binding.decoder.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: https://10.201.232.19:8443/identity-provider/identity-provider
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
```

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

[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.SAMLMessageDecoder
```

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.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAMLMessageDecoder
```

```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
    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-8907-5a05a94ff5fd
    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.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
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.validato
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.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,358 INFO [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl

```

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 cache
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 save
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.