

Configurer l'ID REST ISE 3.0 avec Azure Active Directory

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Présentation des flux de haut niveau](#)

[Configurer Azure AD pour l'intégration](#)

[Configurer ISE pour l'intégration](#)

[Exemples de politiques ISE pour différents cas d'utilisation](#)

[Vérifier](#)

[Dépannage](#)

[Problèmes avec le service d'authentification REST](#)

[Problèmes d'authentification REST ID](#)

[Utiliser les fichiers journaux](#)

Introduction

Ce document décrit l'intégration de Cisco ISE 3.0 avec Azure AD implémentée via le service d'identité REST avec les informations d'identification du mot de passe du propriétaire de la ressource.

Informations générales

Ce document décrit comment configurer et dépanner l'intégration d'Identity Services Engine (ISE) 3.0 avec Microsoft (MS) Azure Active Directory (AD) implémentée via le service d'identité (ID) de transfert d'état de représentation (REST) à l'aide des informations d'identification de mot de passe de propriétaire de ressource (ROPC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE

- MS Azure AD
- Compréhension de la mise en oeuvre et des limites du protocole ROPC ; [lien](#)

Composants utilisés

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

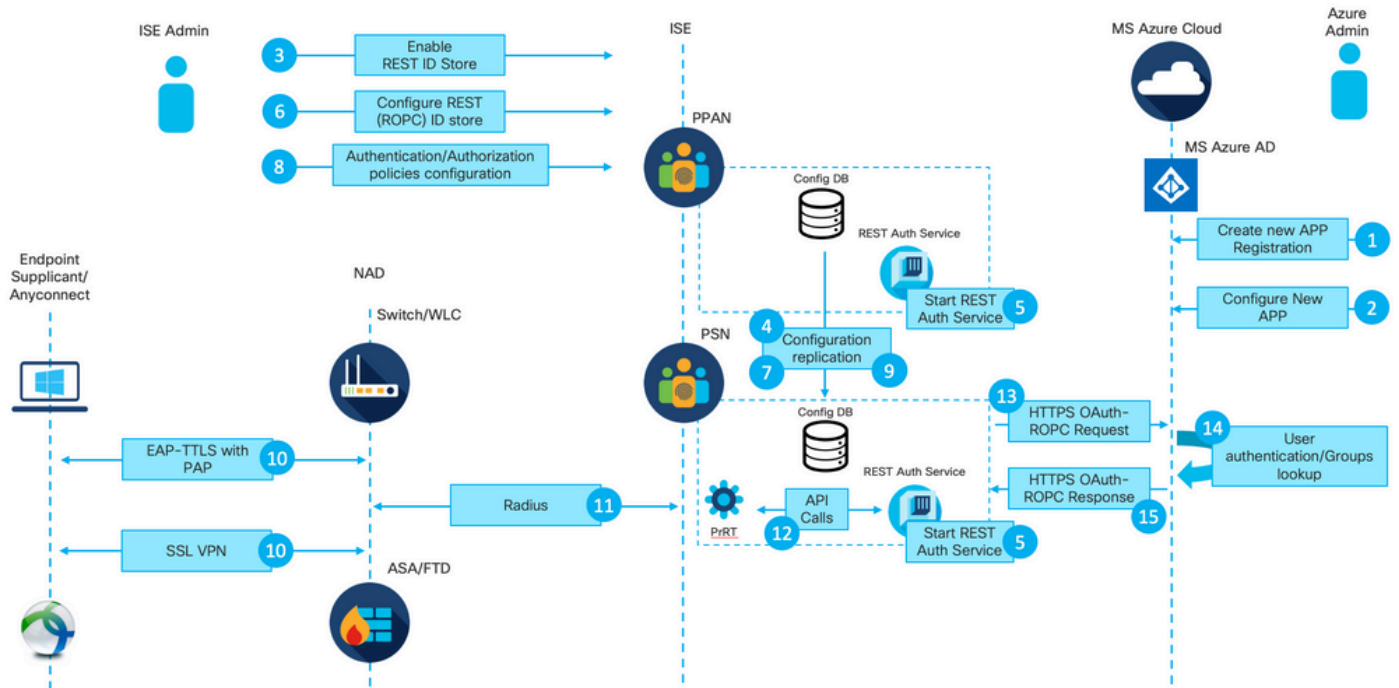
- Cisco ISE version 3.0
- MS Azure AD
- WS-C3850-24P avec logiciel 16.9.2
- ASAv avec 9.10 (1)
- Windows 10.0.18363

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.

Configurer

La fonctionnalité ISE REST ID est basée sur le nouveau service introduit dans ISE 3.0 - Service d'authentification REST. Ce service est responsable de la communication avec Azure AD sur les échanges ROPC OAuth (Open Authorization) afin d'effectuer l'authentification des utilisateurs et la récupération des groupes. Le service d'authentification REST est désactivé par défaut et, une fois que l'administrateur l'a activé, il s'exécute sur tous les noeuds ISE du déploiement. Puisque la communication du service d'authentification REST avec le cloud se produit au moment de l'authentification de l'utilisateur, tout retard sur le chemin apporte une latence supplémentaire dans le flux d'authentification/autorisation. Cette latence échappe au contrôle d'ISE et toute implémentation de l'authentification REST doit être soigneusement planifiée et testée afin d'éviter tout impact sur les autres services ISE.

Présentation des flux de haut niveau



1. L'administrateur du cloud Azure crée une nouvelle inscription d'application (App). Les détails de cette application sont utilisés ultérieurement sur ISE afin d'établir une connexion avec Azure AD.

2. L'administrateur du cloud Azure doit configurer l'application avec :

- Créer une clé secrète client
- Activer ROPC
- Ajouter des revendications de groupe
- Définir les autorisations API (Application Programming Interface)

3. L'administrateur ISE active le service d'authentification REST. Il doit être effectué avant que toute autre action puisse être exécutée.

4. Les modifications sont écrites dans la base de données de configuration et répliquées sur

l'ensemble du déploiement ISE.

5. Le service d'authentification REST démarre sur tous les noeuds.

6. L'administrateur ISE configure le magasin d'ID REST avec les détails de l'étape 2.

7. Les modifications sont écrites dans la base de données de configuration et répliquées sur l'ensemble du déploiement ISE.

8. L'administrateur ISE crée une nouvelle séquence de magasin d'identités ou modifie celle qui existe déjà et configure les stratégies d'authentification/d'autorisation.

9. Les modifications sont écrites dans la base de données de configuration et répliquées sur l'ensemble du déploiement ISE.

10. Le terminal initie l'authentification. Conformément à la spécification du protocole ROPC, le mot de passe utilisateur doit être fourni à la plate-forme d'identité Microsoft en texte clair sur une connexion HTTP chiffrée. Pour cette raison, les seules options d'authentification disponibles prises en charge par ISE à ce jour sont les suivantes :

- EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) avec PAP (Password Authentication Protocol) comme méthode interne
- Authentification VPN SSL AnyConnect avec PAP

11. Échange avec le noeud de service de stratégie ISE (PSN) sur Radius.

12. Process Runtime (PrRT) envoie une demande au service REST ID avec les détails de l'utilisateur (nom d'utilisateur/mot de passe) via l'API interne.

13. Le service d'ID REST envoie une requête ROPC OAuth à Azure AD via HyperText Transfer Protocol Secure (HTTPS).

14. Azure AD effectue l'authentification des utilisateurs et récupère les groupes d'utilisateurs.

15. Résultat d'authentification/autorisation renvoyé à ISE.

Après le point 15, le résultat de l'authentification et les groupes récupérés sont retournés à PrRT, ce qui implique un flux d'évaluation de stratégie et l'attribution du résultat final de l'authentification/autorisation. Access-Accept avec les attributs du profil d'autorisation ou Access-Reject renvoyé au périphérique d'accès réseau (NAD).

Configurer Azure AD pour l'intégration

1. Localisez AppRegistration Service comme indiqué dans l'image.

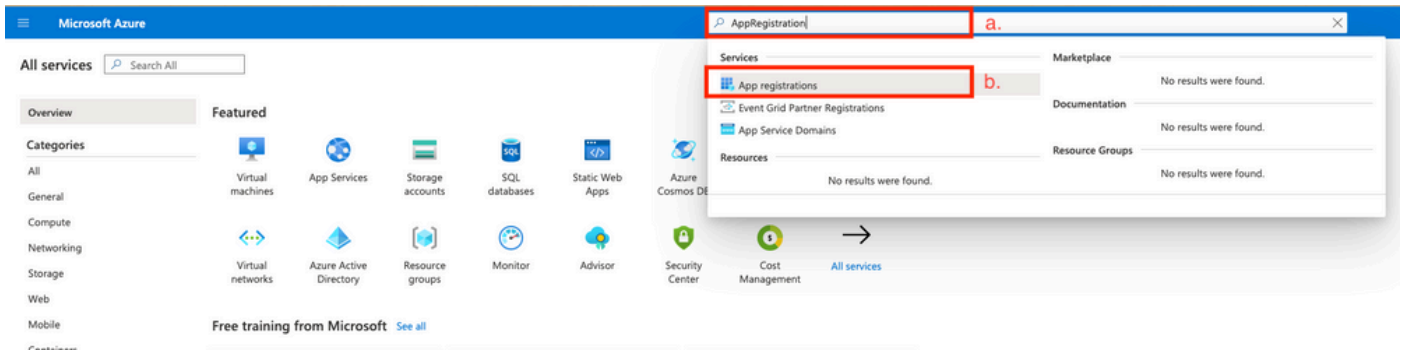


Figure 2.

a. Tapez AppRegistration dans la barre de recherche globale.

b. Cliquez sur le service d'enregistrement des applications.

2. Créez un enregistrement d'application.

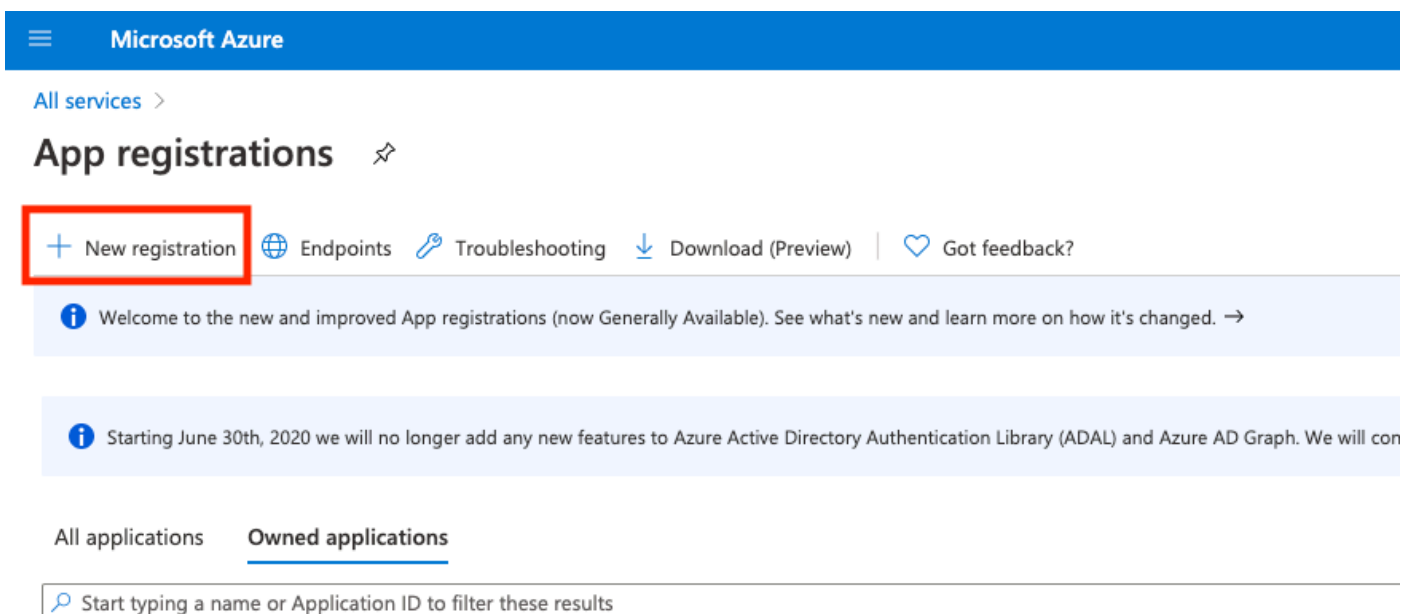


Figure 3.

3. Enregistrez une nouvelle application.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

✓

a.

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (DEMO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

b.

[Help me choose...](#)


Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

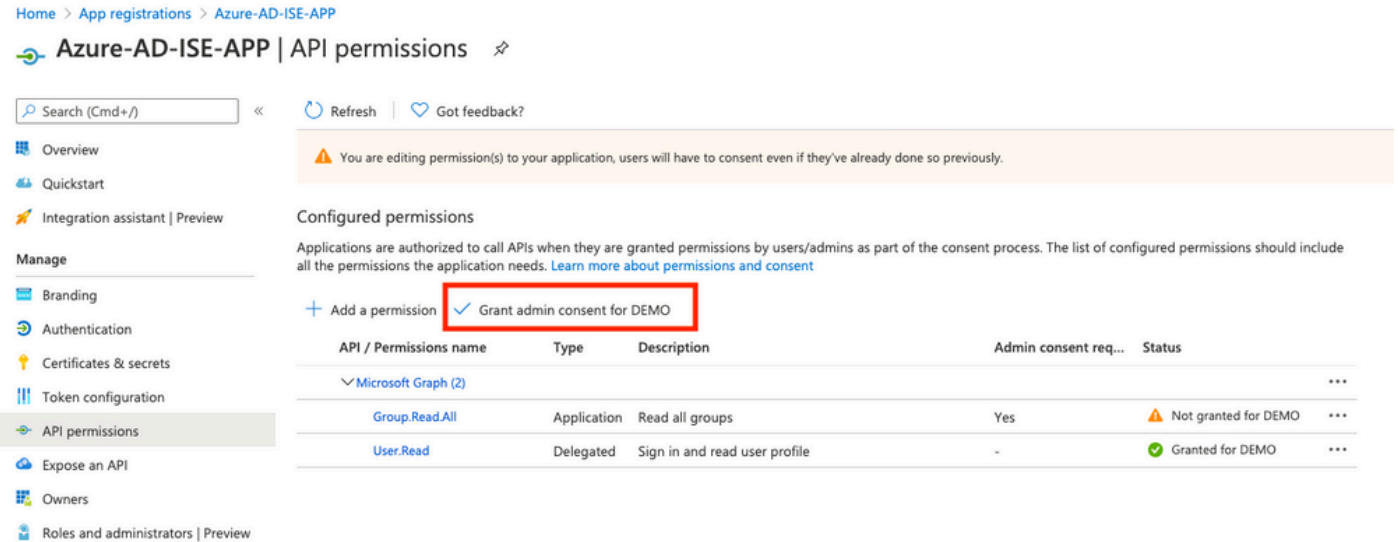
By proceeding, you agree to the [Microsoft Platform Policies](#)

c.

Figure 4.

 : les données de groupe d'utilisateurs peuvent être extraites d'Azure AD de plusieurs manières à l'aide d'une autorisation API différente. La méthode décrite dans cet exemple s'est révélée efficace dans le laboratoire du centre d'assistance technique Cisco. Utilisez d'autres autorisations API au cas où votre administrateur Azure AD le recommande.

16. Grant admin consent pour les autorisations API.



Home > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

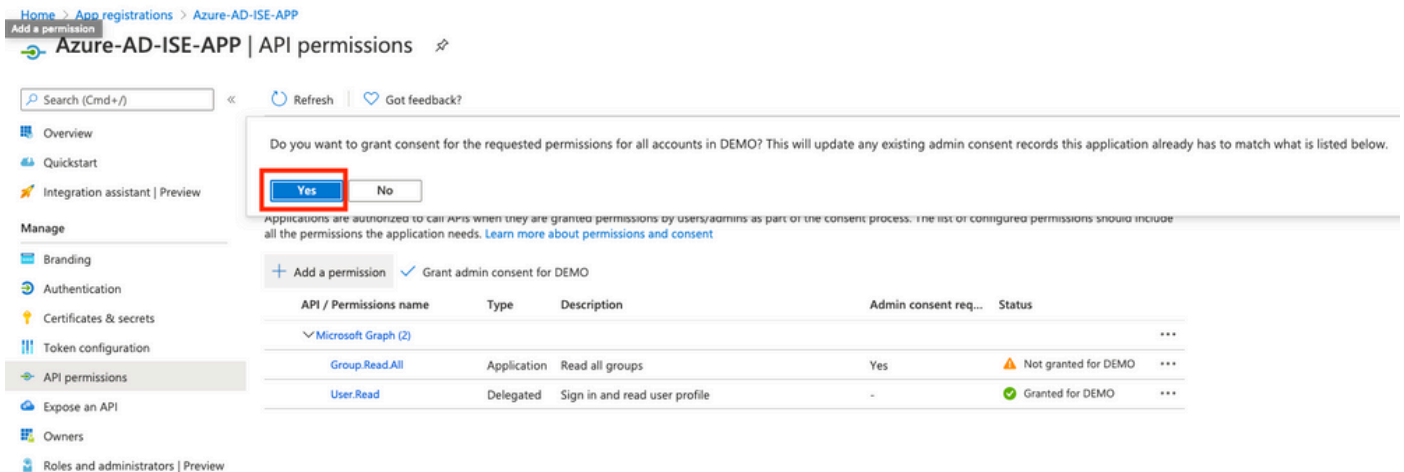
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	Not granted for DEMO
User.Read	Delegated	Sign in and read user profile	-	Granted for DEMO

Figure 17.

17. Confirmer l'autorisation de l'administrateur



Home > App registrations > Azure-AD-ISE-APP

Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview
Quickstart
Integration assistant | Preview

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators | Preview

Do you want to grant consent for the requested permissions for all accounts in DEMO? This will update any existing admin consent records this application already has to match what is listed below.

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	Not granted for DEMO
User.Read	Delegated	Sign in and read user profile	-	Granted for DEMO

Figure 18.

À ce stade, vous pouvez envisager une intégration entièrement configurée du côté d'Azure AD.

Configurer ISE pour l'intégration

1. Accédez aux paramètres de gestion des identités.

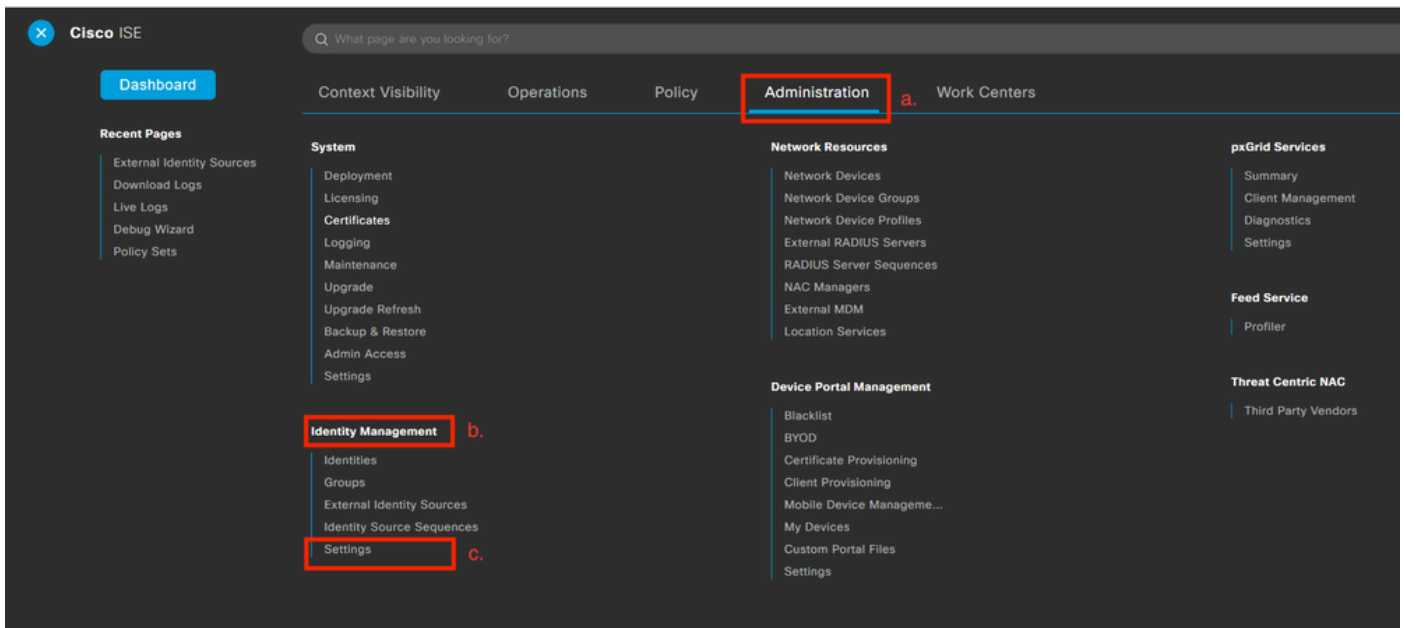


Figure 19.

Naviguez jusqu'à Administration > Identity Management > Settings .

2. Activez le service REST ID (désactivé par défaut).

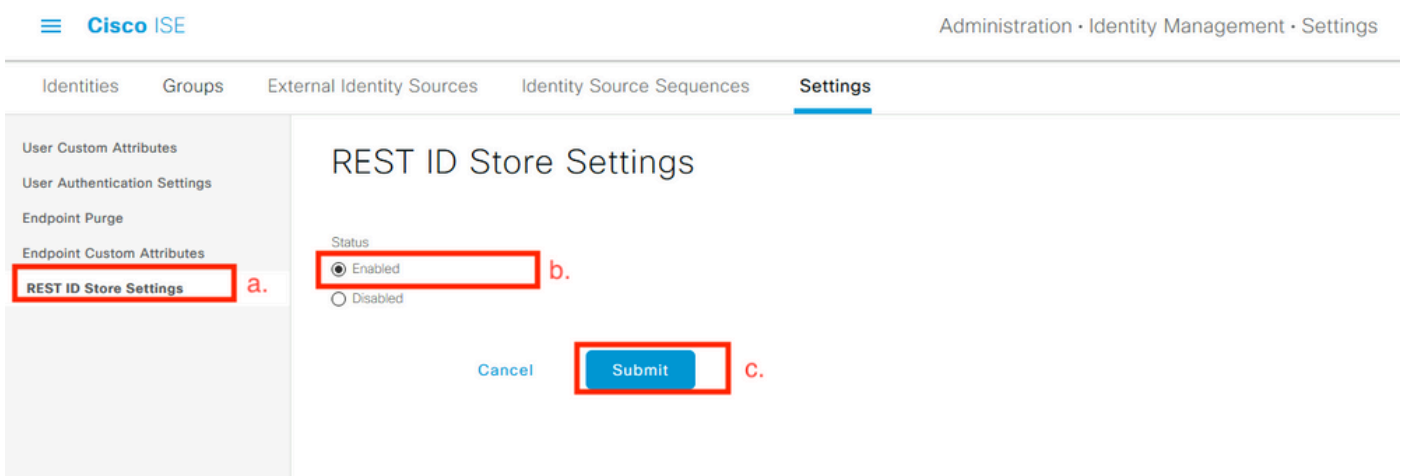


Figure 20.

Naviguez jusqu'à REST ID Store Settings et de modifier l'état des paramètres de stockage d'ID REST afin de Enable, puis Submit vos modifications.

3. Créez un magasin REST ID.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- > Certificate Authentication F
- ▼ Active Directory
 - EXAMPLE
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
- > SAML Id Providers
- Social Login
- REST (ROPC)** **b.**

REST (ROPC) **a.**

Refresh **+ Add** **c.** Duplicate Trash Edit

<input type="checkbox"/>	Name	Description	Type
No data found.			

Figure 21.

Basculez vers le External Identity Sources , cliquez sur REST (ROPC) , puis cliquez sur Ajouter.

4. Configurez le magasin REST ID.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- < [Icon] [Icon]
- > [Icon] Certificate Authentication F
- ▼ [Icon] Active Directory
- [Icon] EXAMPLE
- [Icon] LDAP
- [Icon] ODBC
- [Icon] RADIUS Token
- [Icon] RSA SecurID
- > [Icon] SAML Id Providers
- [Icon] Social Login
- [Icon] REST (ROPC)

REST (ROPC) > New

Name *
Azure_AD a.

Description
[Text Field]

REST Identity Provider *
Azure

Client ID *
[Yellow Field] b.

Client Secret *
[Redacted Field] c.

Tenant ID *
[Yellow Field] d.

[Test connection] f.

Groups
[Dropdown] [Load Groups] g.

Username Suffix
@skuchere.onmicrosoft.com e.

[Cancel] [Submit] h.

Figure 22.


a. Définissez le nom du magasin d'ID. Plus tard, ce nom se trouve dans la liste des dictionnaires ISE lorsque vous configurez les stratégies d'autorisation. En outre, ce nom est affiché dans la liste des magasins d'ID disponibles dans les paramètres de stratégie d'authentification et dans la liste des magasins d'ID disponibles dans la configuration de séquence de magasin d'identités.

b. Fournissez l'ID client (extrait d'Azure AD à l'étape 8. de la section de configuration de l'intégration Azure AD).

c. Fournissez le secret client (extrait d'Azure AD à l'étape 7. de la section de configuration de l'intégration Azure AD).


d. Fournissez l'ID de locataire (extrait d'Azure AD à l'étape 8. de la section de configuration de l'intégration Azure AD).

e. Configurer le suffixe du nom d'utilisateur - par défaut, ISE PSN utilise un nom d'utilisateur fourni par l'utilisateur final, qui est fourni au format sAMAccountName (nom d'utilisateur court, par exemple, bob) ; dans ce cas, Azure AD ne peut pas localiser l'utilisateur. Le suffixe du nom d'utilisateur est la valeur ajoutée au nom d'utilisateur fourni par l'utilisateur afin d'amener le nom d'utilisateur au format UPN.

 Remarque : le protocole ROPC est limité à l'authentification utilisateur, car il repose sur l'attribut Nom d'utilisateur lors de l'authentification. Les objets de périphérique dans Azure AD n'ont pas d'attributs de nom d'utilisateur.

f. Appuyez sur Tester la connexion afin de confirmer qu'ISE peut utiliser les détails d'application fournis afin d'établir une connexion avec Azure AD.

g. Appuyez sur Load Groups afin d'ajouter des groupes disponibles dans le magasin d'ID REST d'Azure AD. L'exemple ci-dessous montre à quoi ressemble l'expérience administrateur.

 Remarque : veuillez noter l'ID de bogue Cisco [CSCvx00345](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvx00345) défectueux, car il empêche le chargement des groupes. Le défaut est corrigé dans le correctif 2 d'ISE 3.0.

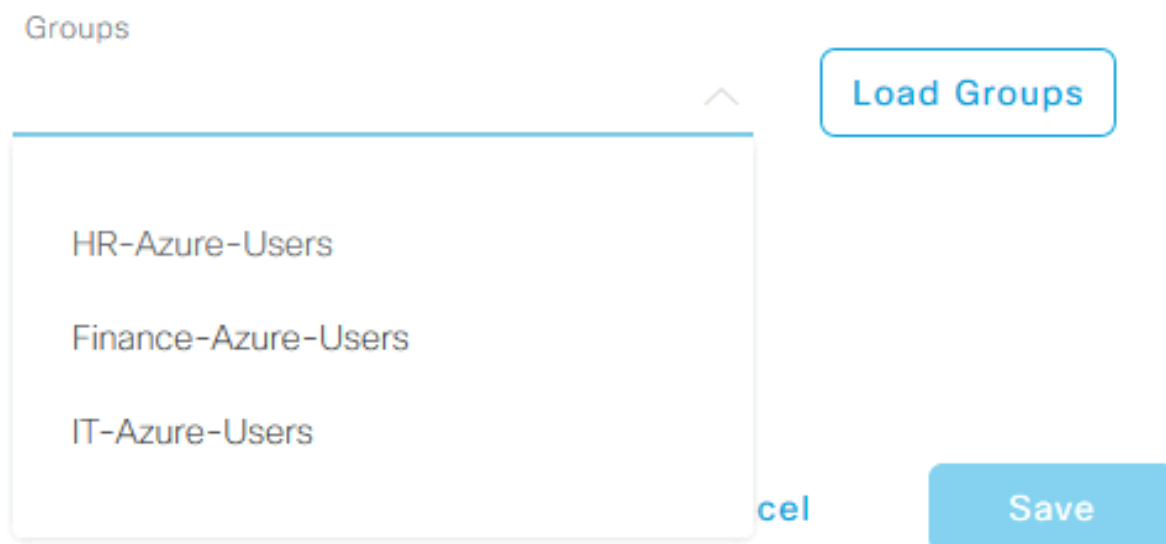


Figure 23.

h. Soumettez vos modifications.

5. À cette étape, envisagez la création d'une nouvelle séquence de magasin d'identités, qui inclut un magasin d'ID REST nouvellement créé.

6. Au moment où le magasin d'ID REST ou la séquence de magasin d'identités qui le contient est affecté à la stratégie d'authentification, remplacez une action par défaut pour Échec du processus

de DROP par REJECT, comme indiqué dans l'image.

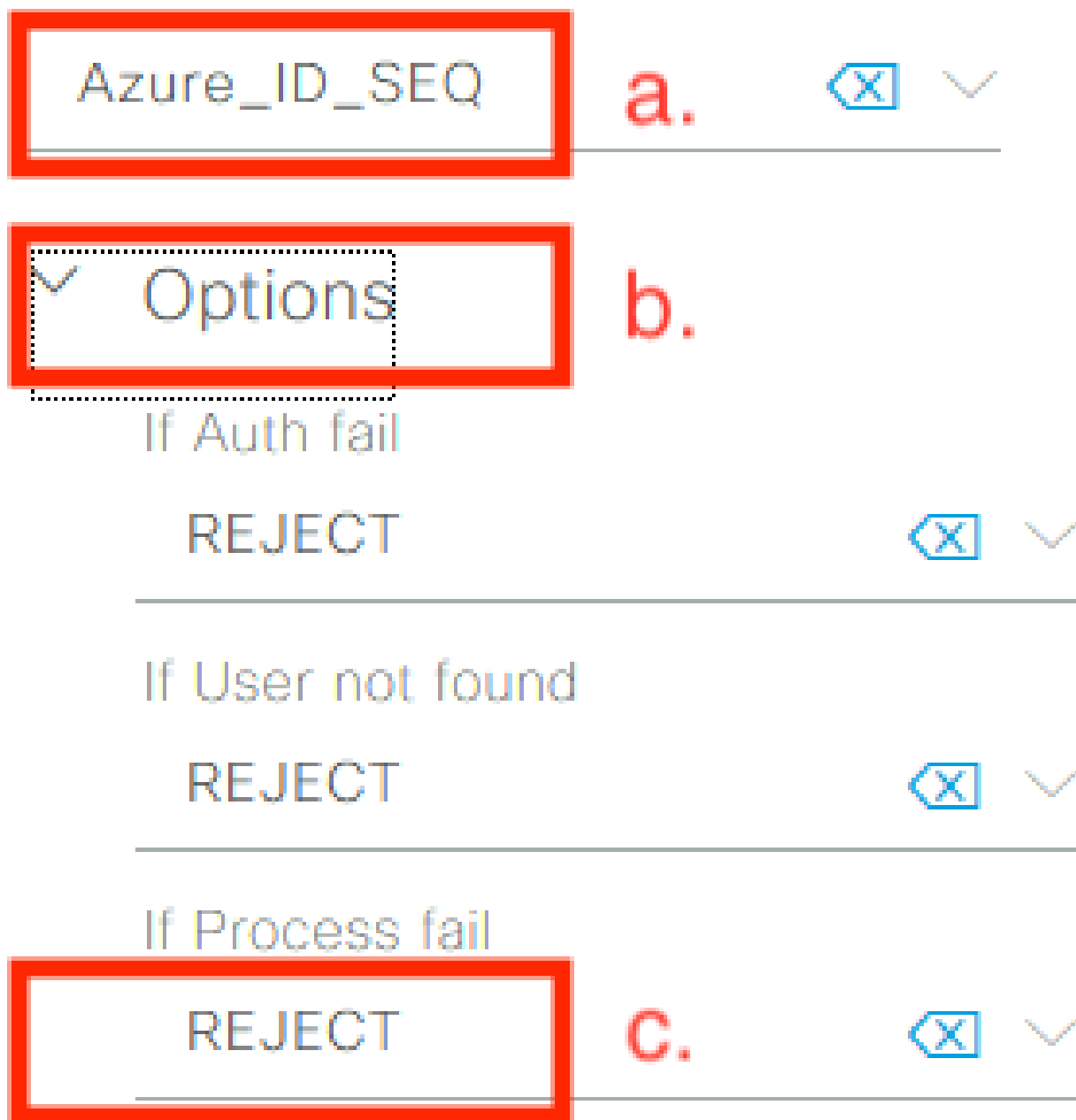


Figure 24.

- a. Localisez la stratégie d'authentification qui utilise le magasin d'ID REST.
- b. Ouvrez la liste déroulante Options.
- c. L'action de modification par défaut pour le processus a échoué de DROP à REJECT.

Ceci est nécessaire afin d'éviter que PSN soit marqué comme mort du côté des NAD à un moment où des défaillances spécifiques se produisent dans le magasin d'ID REST comme :

- L'utilisateur n'est membre d'aucun groupe dans Azure AD.

- Le mot de passe utilisateur doit être modifié.

7. Ajoutez le dictionnaire du magasin d'ID REST à la stratégie d'autorisation.

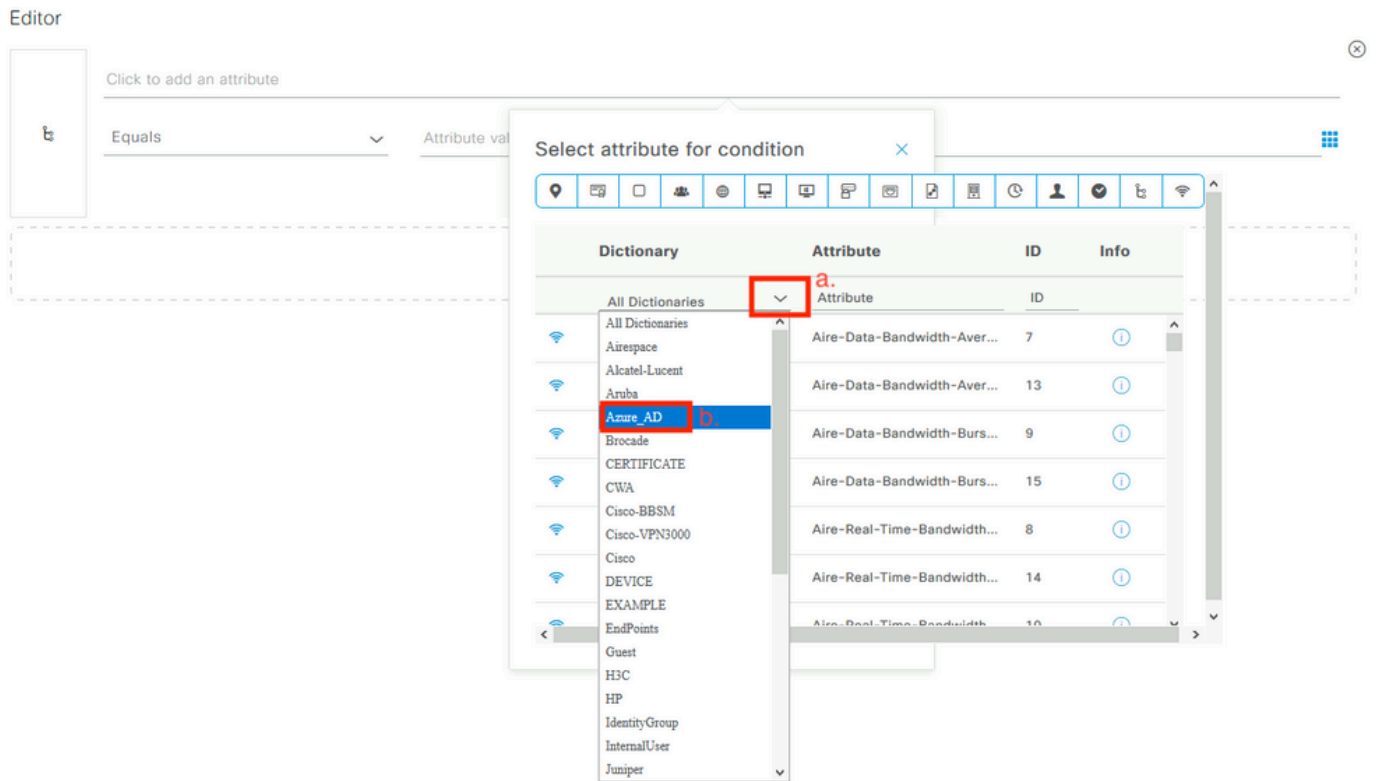


Figure 25.

a. Ouvrez la liste déroulante Tous les dictionnaires.

b. Localisez le dictionnaire nommé de la même manière que votre magasin REST ID.

8. Ajoutez des groupes d'identités externes (depuis ISE 3.0, le seul attribut disponible dans le dictionnaire du magasin d'ID REST est un groupe externe).

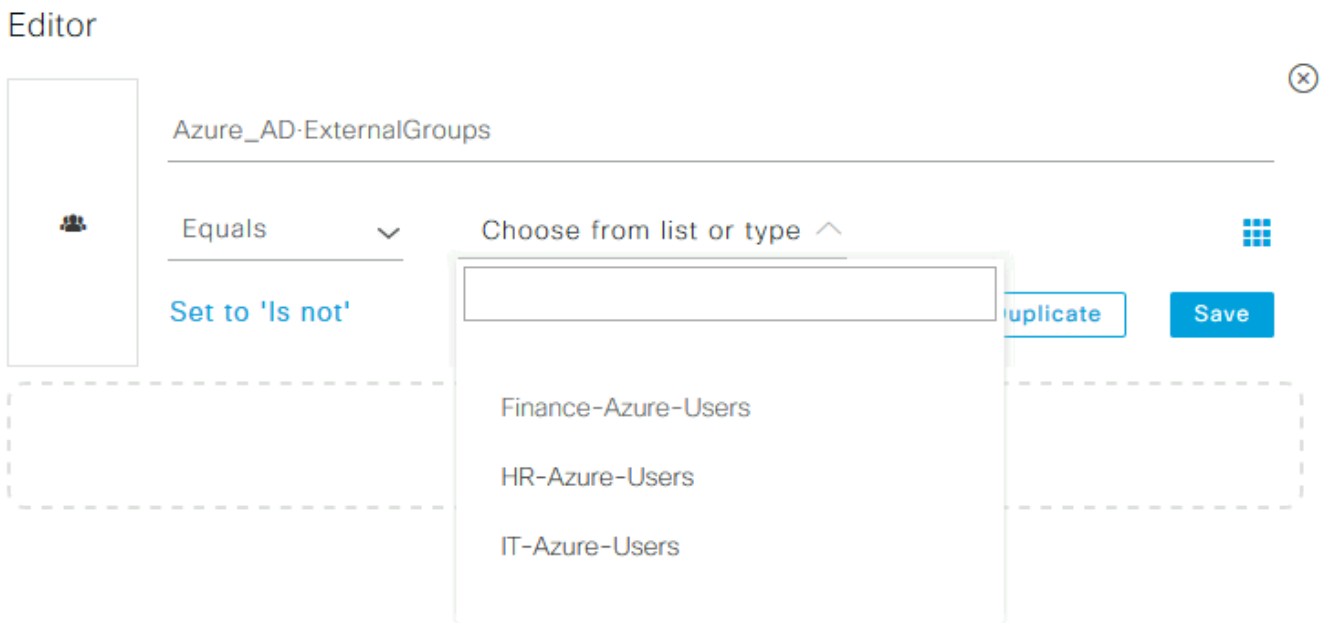


Figure 26.

Exemples de politiques ISE pour différents cas d'utilisation

Dans le cas de l'authentification Dot1x, la condition de tunnel EAP du dictionnaire d'accès réseau peut être utilisée pour faire correspondre les tentatives EAP-TTLS comme illustré dans l'image.

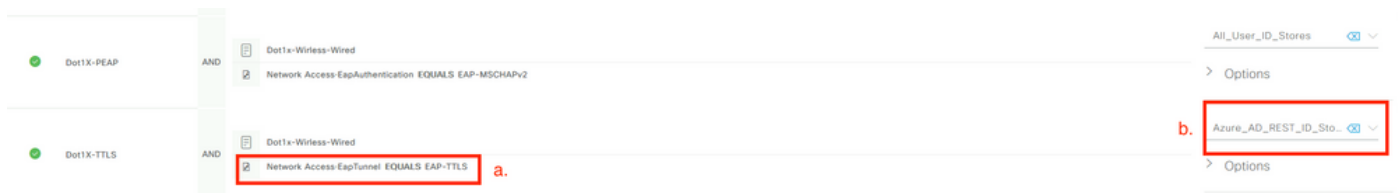


Figure 27.

a. Définissez EAP Tunnel EQUAL à EAP-TTLS pour faire correspondre les tentatives qui doivent être transmises au magasin d'ID REST.

b. Sélectionnez directement dans le magasin d'ID REST ou dans la séquence de magasin d'identités, qui le contient dans la colonne Utiliser.

Au sein des stratégies d'autorisation individuelles, les groupes externes d'Azure AD peuvent être utilisés avec le type de tunnel EAP :

✓	Dot1X-TTLS-Azure-Finance	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓	Dot1X-TTLS-Azure-HR	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓	Dot1X-TTLS-Azure-IT	AND	<ul style="list-style-type: none"> Dot1x-Wireless-Wired Network Access-EapTunnel EQUALS EAP-TTLS Azure_AD-ExternalGroups EQUALS IT-Azure-Users

Figure 28.

Pour un flux basé sur VPN, vous pouvez utiliser un nom de groupe de tunnels comme différenciateur :

Stratégie d'authentification :

Status	Rule Name	Conditions	Use
✓	Azure-AD	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere	Azure_AD_REST_ID_Sto... > Options

Stratégies d'autorisation :

✓	VPN-Azure-Finance	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS Finance-Azure-Users
✓	VPN-Azure-HR	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS HR-Azure-Users
✓	VPN-Azure-IT	AND	<ul style="list-style-type: none"> Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere Azure_AD-ExternalGroups EQUALS IT-Azure-Users

Figure 29.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Vérifiez que le service d'authentification REST s'exécute sur le noeud ISE.

Pour vérifier cela, vous devez exécuter la commande `show application status ise` dans l'interpréteur de commandes Secure Shell (SSH) d'un noeud ISE cible :

```
<#root>
```

```
skuchere-ise30-1/admin# show application status ise
```

```
ISE PROCESS NAME STATE PROCESS ID
```

```
-----  
Database Listener running 101790  
Database Server running 92 PROCESSES  
Application Server running 39355  
Profiler Database running 107909  
ISE Indexing Engine running 115132  
AD Connector running 116376  
M&T Session Database running 107694  
M&T Log Processor running 112553  
Certificate Authority Service running 116226  
EST Service running 119875  
SXP Engine Service disabled  
Docker Daemon running 104217  
TC-NAC Service disabled  
pxGrid Infrastructure Service disabled  
pxGrid Publisher Subscriber Service disabled  
pxGrid Connection Manager disabled  
pxGrid Controller disabled  
PassiveID WMI Service disabled  
PassiveID Syslog Service disabled  
PassiveID API Service disabled  
PassiveID Agent Service disabled  
PassiveID Endpoint Service disabled  
PassiveID SPAN Service disabled  
DHCP Server (dhcpd) disabled  
DNS Server (named) disabled  
ISE Messaging Service running 104876  
ISE API Gateway Database Service running 106853  
ISE API Gateway Service running 110426  
Segmentation Policy Service disabled
```

```
REST Auth Service running 63052
```

```
SSE Connector disabled
```

2. Vérifiez que le magasin d'ID REST est utilisé au moment de l'authentification (consultez la section Étapes. du rapport d'authentification détaillé).

15013 Selected Identity Source - Azure_AD

25103 Perform plain text password authentication in external REST ID store server - Azure_AD a.

25100 Connecting to external REST ID store server - Azure_AD b.

25101 Successfully connected to external REST ID store server - Azure_AD (🕒 Step latency=1660 ms) c.

25104 Plain text password authentication in external REST ID store server succeeded - Azure_AD d.

25107 REST ID store server respond with groups - Azure_AD e.

25110 User groups inserted to session cache - Azure_AD f.

22037 Authentication Passed

a. PSN démarre l'authentification en texte brut avec le magasin d'ID REST sélectionné.

b. Connexion établie avec le cloud Azure.

c. Étape d'authentification réelle - tenez compte de la valeur de latence présentée ici. Dans le cas où toutes vos authentifications avec le cloud Azure rencontreraient des problèmes de latence significative, cela affecterait l'autre flux ISE et, par conséquent, l'ensemble du déploiement ISE deviendrait instable.

d. Confirmation de l'authentification réussie.

e. Confirmation des données de groupe présentées en réponse.

f. Contexte de session renseigné avec les données du groupe d'utilisateurs. Pour plus d'informations sur le processus de gestion des sessions ISE, consultez cet article ([lien](#)).

3. Confirmez que les stratégies d'authentification/autorisation attendues sont sélectionnées (pour ce sujet, examinez la section Vue d'ensemble du rapport d'authentification détaillé).

Overview

Event 5200 Authentication succeeded

Username bob

Endpoint Id ED:37:E1:08:57:15 ⊕

Endpoint Profile

Authentication Policy SPRT-Policy-Set >> Azure-AD

Authorization Policy SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

Figure 30.

Dépannage

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

Problèmes avec le service d'authentification REST

Afin de dépanner tout problème avec le service d'authentification REST, vous devez commencer par la révision du fichier ADE.log. Emplacement du bundle de support - /support/adeos/ade

Un mot clé de recherche pour le service d'authentification REST est - ROPC-control.

Cet exemple montre comment le service d'authentification REST démarre :

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

Dans les cas où le service ne démarre pas ou s'arrête de façon inattendue, il est toujours logique de commencer par consulter le fichier ADE.log autour d'une période problématique.

Problèmes d'authentification REST ID

Dans le cas d'échecs d'authentification lorsque le magasin d'ID REST est utilisé, vous devez toujours commencer à partir d'un rapport d'authentification détaillé. Dans la zone Autres attributs, vous pouvez voir une section - RestAuthErrorMsg qui contient une erreur renvoyée par le cloud Azure :

```
RestAuthErrorMsg      Error Key - invalid_client | Error Description -
AADSTS7000218: The request body must contain the
following parameter: 'client_assertion' or 'client_secret'. Trace
ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID:
519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp:
2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI
- https://login.microsoftonline.com/error?code=7000218
```

Figure 31.

Utiliser les fichiers journaux

Dans ISE 3.0, en raison de la fonctionnalité Controlled Introduction of REST ID, les débogages pour cette fonctionnalité sont activés par défaut. Tous les journaux associés à l'ID REST sont stockés dans des fichiers ROPC qui peuvent être consultés via l'interface de ligne de commande :

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

Sur ISE 3.0 avec le correctif installé, notez que le nom du fichier est rest-id-store.log et non ropc.log. L'exemple de recherche précédent fourni fonctionne car le nom du dossier n'a pas changé.

Ces fichiers peuvent également être extraits du bundle de support ISE.

Voici quelques exemples de journaux qui montrent différents scénarios de travail et de non-travail :

1. Erreur de certificat lorsque Azure Graph n'est pas approuvé par le noeud ISE. Cette erreur est visible lorsque les groupes ne se chargent pas dans le paramètre du magasin d'ID REST.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appl
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

Ce problème indique que le certificat de l'API graphique Microsoft n'est pas approuvé par ISE. ISE 3.0.0.458 n'a pas d'autorité de certification DigiCert Global Root G2 installée dans le magasin de confiance. Ceci est documenté dans le défaut

- ID de bogue Cisco [CSCv80297](#) Pour résoudre ce problème, vous devez installer DigiCert Global Root G2 CA dans le magasin de confiance ISE et le marquer comme approuvé pour les services Cisco.

Le certificat peut être téléchargé à l'adresse suivante : <https://www.digicert.com/kb/digicert-root-certificates.htm>

2. Code secret d'application incorrect.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client s
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentity
```

3. ID d'application incorrect.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4. Utilisateur introuvable.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
```

```
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. Le mot de passe utilisateur a expiré. En général, cela peut se produire pour l'utilisateur nouvellement créé, car le mot de passe défini par l'administrateur Azure doit être modifié au moment de la connexion à Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. Impossible de charger les groupes en raison d'autorisations API incorrectes.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Stat
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. L'authentification échoue lorsque le ROPC n'est pas autorisé côté Azure.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_des
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
```

```
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8. L'authentification échoue car l'utilisateur n'appartient à aucun groupe du côté Azure.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9. Authentification des utilisateurs et récupération des groupes réussies.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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.

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.

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.