

# Intégrer Intune MDM à Identity Services Engine

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer Microsoft Intune](#)

[Importer les certificats du portail Intune vers le magasin de confiance ISE](#)

[Déployer ISE en tant qu'application sur le portail Azure](#)

[Importer des certificats ISE dans l'application dans Azure](#)

[Vérifiez et dépannez](#)

["Échec de la connexion au serveur" basé sur sun.security.validator.ValidatorException](#)

[Impossible d'acquérir le jeton d'authentification d'Azure AD](#)

[Impossible d'acquérir le jeton d'authentification d'Azure AD](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment intégrer Intune Mobile Device Management (MDM) avec Cisco Identity Services Engine (ISE).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance des services MDM dans Cisco ISE
- Connaissance de Microsoft Azure Intune Services

### Composants utilisés

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

- Cisco Identity Services Engine 3.0
- Application Microsoft Azure Intune

The information in this document was created from the devices in a specific lab environment. All of

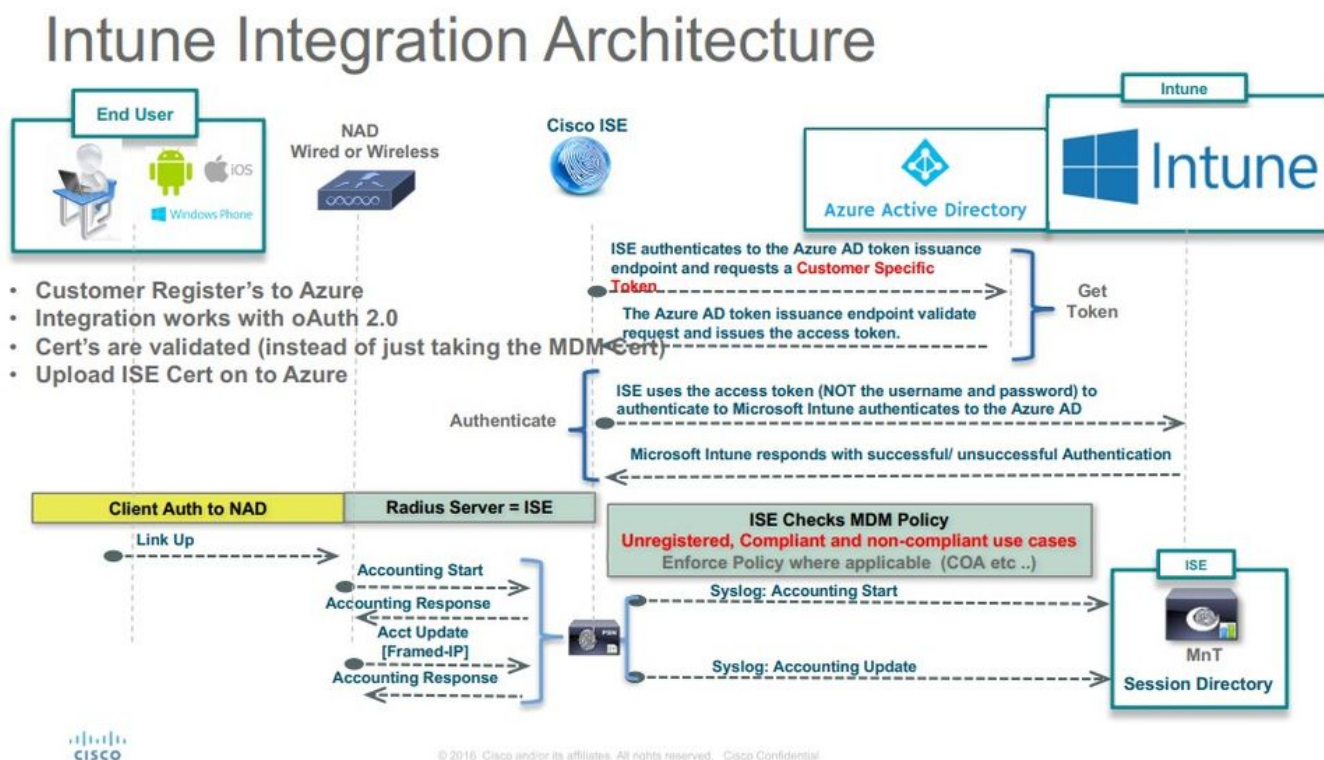
the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les serveurs MDM sécurisent, surveillent, gèrent et prennent en charge les appareils mobiles déployés par les opérateurs mobiles, les fournisseurs de services et les entreprises. Ces serveurs agissent en tant que serveur de stratégie qui contrôle l'utilisation de certaines applications sur un périphérique mobile (par exemple, une application de messagerie) dans l'environnement déployé. Cependant, le réseau est la seule entité qui peut fournir un accès granulaire aux points d'extrémité en fonction des listes de contrôle d'accès (ACL). ISE demande aux serveurs MDM les attributs de périphérique nécessaires afin de créer des listes de contrôle d'accès qui fournissent un contrôle d'accès au réseau pour ces périphériques. Cisco ISE s'intègre à Microsoft Intune MDM Server afin d'aider les entreprises à sécuriser leurs données lorsque des périphériques tentent d'accéder à des ressources sur site.

## Configurer

### Diagramme du réseau



### Configurer Microsoft Intune

Importer les certificats du portail Intune vers le magasin de confiance ISE

Connectez-vous à la console d'administration Intune ou à la console d'administration Azure, quel

que soit le site de votre locataire. Utilisez le navigateur afin d'obtenir les détails du certificat :

Étape 1. Ouvrez le Microsoft Azure portal à partir d'un navigateur Web.

Étape 2. Cliquez sur le **symbole de verrouillage** dans la barre d'outils du navigateur, puis cliquez sur View Certificates.

Étape 3. Dans la fenêtre Certificat, cliquez sur l'Certification Path onglet. Un exemple est montré ici :

General Details Certification Path



### Certificate Information

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.311.42.1

\* Refer to the certification authority's statement for details.

**Issued to:** portal.azure.com

**Issued by:** Microsoft IT SSL SHA2

**Valid from** 7/21/2017 **to** 5/7/2018

Issuer Statement

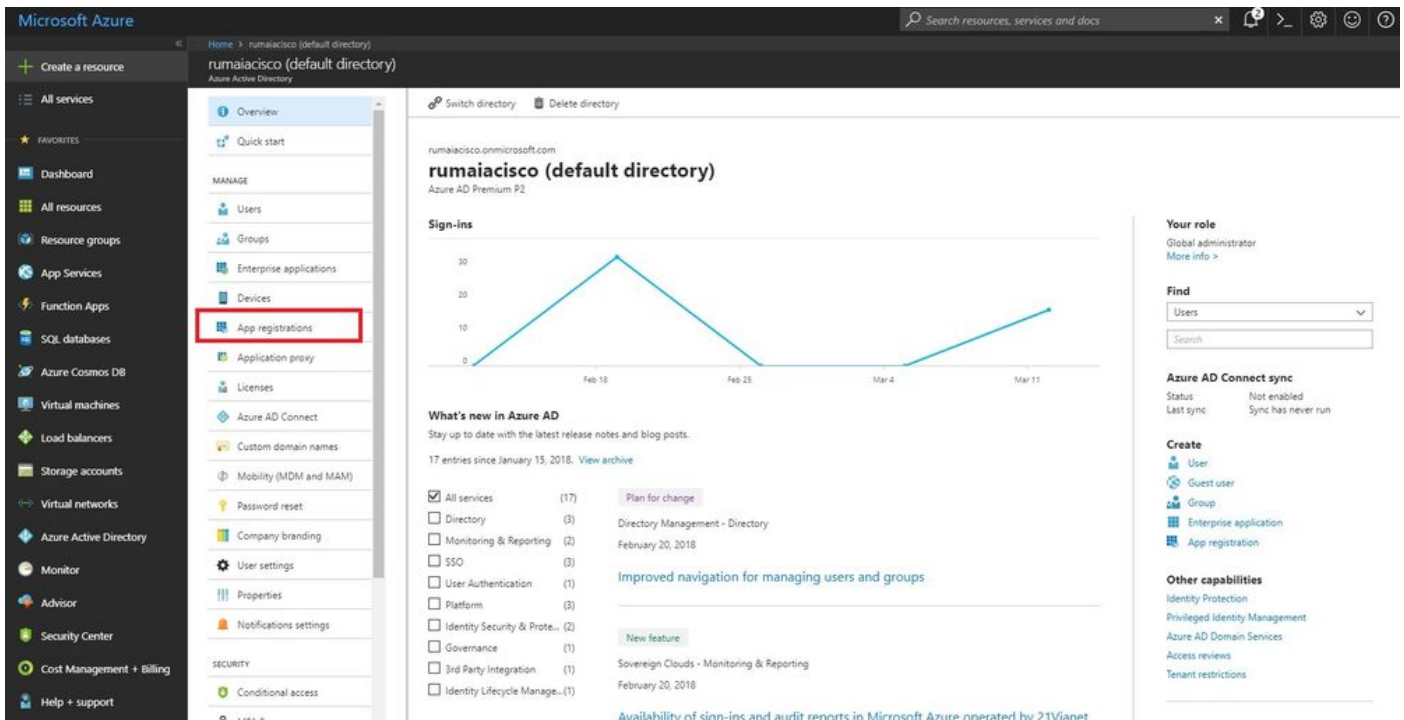
OK

racine, vous pouvez le **copier** dans le fichier et l'**enregistrer** en tant que certificat BASE64.

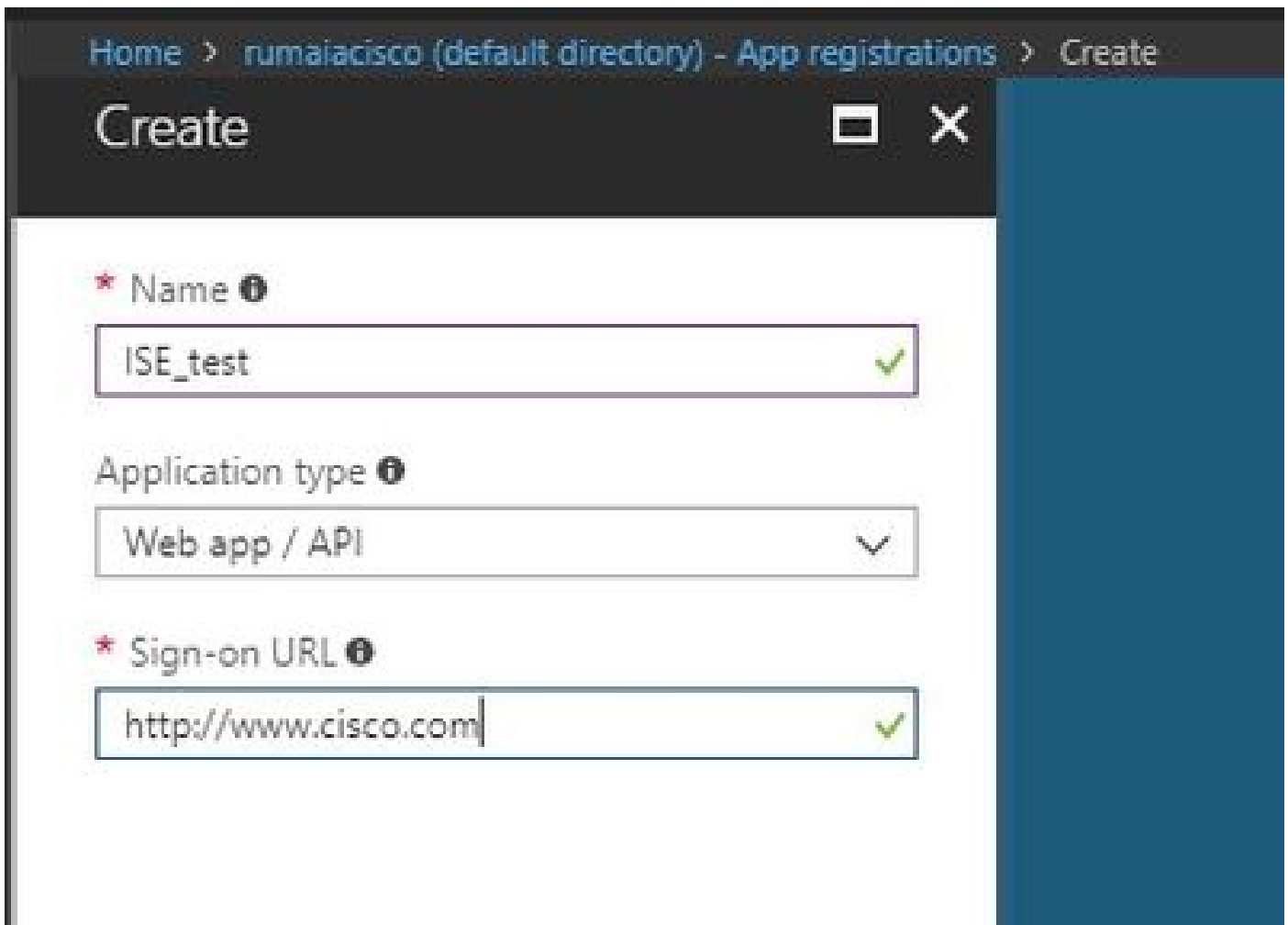
Étape 5. Dans ISE, accédez au certificat racine qui vient d'être enregistré Administration > System > Certificates > Trusted Certificates, et importez-le. Attribuez un nom significatif au certificat, par exemple Azure MDM. Répétez également la procédure pour les certificats CA intermédiaires.

Déployer ISE en tant qu'application sur le portail Azure

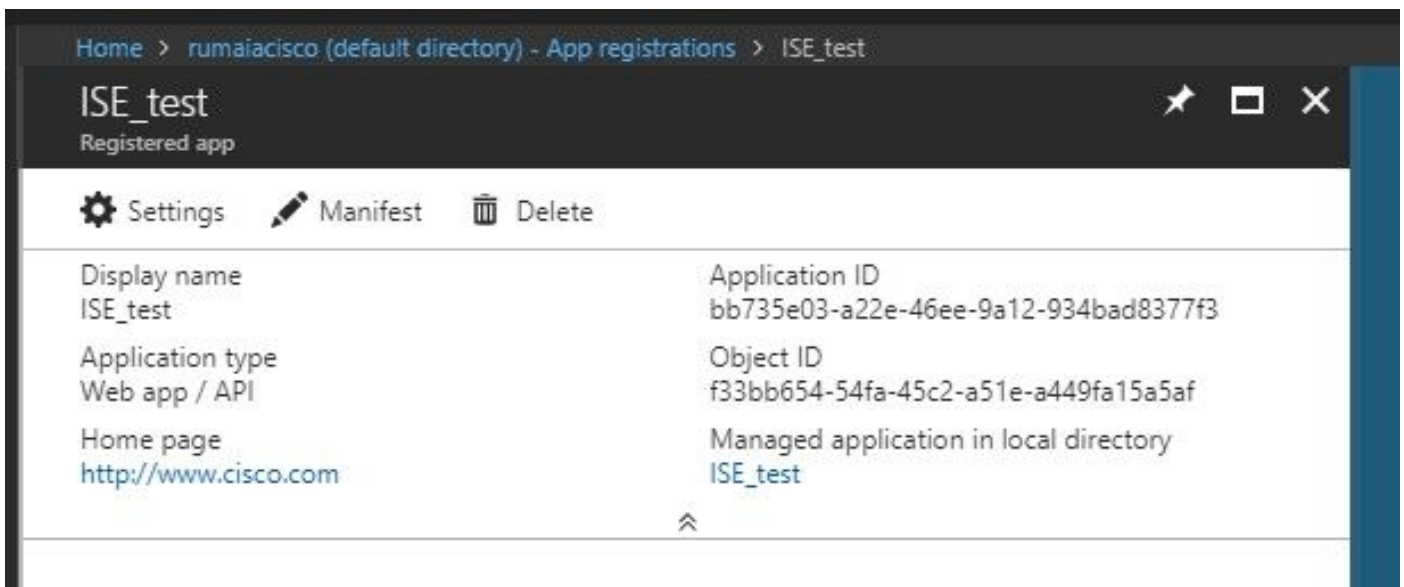
Étape 1. Accédez à la Azure Active Directory et sélectionnez App registrations.



Étape 2. Dans App registrations, créez une nouvelle inscription d'application avec le nom ISE. Cliquez sur Create comme illustré dans cette image.



Étape 3. Choisissez Settings afin de modifier l'application et ajouter les composants requis.



Étape 4. Sous Settings, choisissez les autorisations requises et **appliquez** les options suivantes :

- Microsoft Graph

- Autorisations des applications

- Lire les données du répertoire

- Autorisations déléguées

- Lire la configuration et les stratégies de Microsoft Intune Device

- Lire la configuration de Microsoft Intune

- Connecter les utilisateurs

- Accéder aux données de l'utilisateur à tout moment

- API Microsoft Intune

- Autorisations des applications

- Obtenir des informations sur l'état et la conformité des périphériques de Microsoft Intune

- Windows Azure Active Directory
  - Autorisations des applications
    - Lire les données du répertoire
  - Autorisations déléguées
    - Lire les données du répertoire
    - Se connecter et lire le profil utilisateur

Le résultat de la configuration ressemble à ce qui est affiché ici :



+ Add a permission ✓ Grant admin consent for pavagupt-tme

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Azure Active Directory Graph (3) ...				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for pavagupt-t... ...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for pavagupt-t... ...
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for pavagupt-t... ...
▼ Intune (1) ...				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	✓ Granted for pavagupt-t... ...
▼ Microsoft Graph (7) ...				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for pavagupt-t... ...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for pavagupt-t... ...
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for pavagupt-t... ...
openid	Delegated	Sign users in	No	✓ Granted for pavagupt-t... ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for pavagupt-t... ...
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for pavagupt-t... ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for pavagupt-t... ...

Settings

Filter settings

GENERAL

- Properties >
- Reply URLs >
- Owners >

API ACCESS

- Required permissions >**
- Keys >

TROUBLESHOOTING + SUPPORT

- Troubleshoot >
- New support request >

Required permissions

+ Add Grant Permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	1	4
Microsoft Intune API	1	0
Windows Azure Active Directory	1	2

Étape 5. Cliquez sur Grant Permissions afin de confirmer toutes les autorisations d'application. La mise en oeuvre de ce processus prend entre 5 et 10 minutes. Modifiez le fichier Azure Manifest de l'application créée afin d'importer des certificats d'autorité de certification ISE internes.

Importer des certificats ISE dans l'application dans Azure

Étape 1. **Téléchargez** le fichier manifeste de l'application.

Home > rumaiacisco (default directory) - App registrations > ISE > Edit manifest

ISE  
Registered app

Settings Manifest Delete

Display name: ISE  
Application ID: 86397a1c-b06d-4ca9-a086-0786eeadfabc  
Application type: Object ID  
Web app / API: 220a1c0e-e3d1-4eda-8739-e733019bd0fd  
Home page: http://www.cisco.com  
Managed application in local directory: ISE

Edit manifest

Save Discard Edit Upload Download

```

1 [
2   "appId": "86397a1c-b06d-4ca9-a086-0786eeadfabc",
3   "appRoles": [],
4   "availableToOtherTenants": false,
5   "displayName": "ISE",
6   "errorUrl": null,
7   "groupMembershipClaims": null,
8   "optionalClaims": null,
9   "acceptMappedClaims": null,

```

**Remarque :** il s'agit d'un fichier portant l'extension JSON. Ne modifiez pas le nom de fichier ou l'extension, sinon, il échoue.

Étape 2. Exportez le certificat système ISE à partir de tous les noeuds. Dans le PAN, naviguez jusqu'à Administration > System > Certificates > System Certificates, sélectionner le **certificat de serveur auto-signé par défaut**, puis cliquez sur Export.. Choisissez (Export Certificate Only par défaut) et choisissez un emplacement pour l'enregistrer. **Supprimez** les balises BEGIN et END du certificat et **copiez** le reste du texte sur une seule ligne. Cette option s'applique aux versions antérieures à juin 2020 décrites dans la section Options héritées.

Administration > Certificates > System Certificates

**Client Machine**

```

-----BEGIN CERTIFICATE-----
MIIE9jCCAT6gAwIBAgIQPzfz/HZnjsVkr1AgAYF/scjANBgkqhkiG9w00
aXN0aW50eS8zLj00YnAn2op3k8EYwWHQYVFR0OBBVFEFH3VvYTD0gukicbng1N
0pm3w08BMA4GA1UdDwES/wgEwIF4dBgNVHSMFAiSEZjKUBggrBGFQcDAZYI
KwYBBQUHAIwDAYVR0TAQH/BAlwADANBgkqhkiG9w0BAQwFAAOCQgEAnmaImaDl
341hLMDjtrh9OrjQwOSPk+EqIvYI2Au5ACLkEQgDedrCbLP4MeP1gmXkEg+Xewt
HtuJ+AQX063KD2UhlLR7RAM5Pa6UZY5oqa8a37HJGP75Wa814aT3atnd7peQ2ML
jDeFb+6RVYjzBEMAnms+rWgJV0NBjqlEJggjWv7h00Cq+oQmzLHsLlawqu5szv
ukkyJfslLkZEBBkNri87jgt00jYQLiUe2peJprvkQm2+/JwcuUa0RQeJGtabFR
DYoRqteVqanJaNgS1fBC2ta5yVrctDaujkbD1LzJG3sVWmt6N1o0CqQzWz2D
TnD7w+8EfeTnuhQWQy82a88/UKRhw/9c1PrcPp2+LshFFvKXJgmyMPW0e
dq+6qCAMJF3oYus3JD+xEzr3pgkvwDB14iNORtFEY7rSpIDe1FG0R11uIatI
q/y+hUQTvKvYq2QdMhNC1civEapp3B8e+8vFKSE2PMSTAc24wDMDpN4W2Nj
gL254hNTJ0F04ezQyYaaF1J1N9UaSYObQy22pPdZUxzC33xrvpjcp1T3w0AJK
WgMg18NGR1Lr6taZqf1OU690nk529BYtFenJ+UT/goFUE8oJHPy18QI+XHW+yft
DJqgtR8gV6xuvYoZGktTfoMD2e-
-----END CERTIFICATE-----

```

Delete this line

Delete this line

**System Certificates** ⚠ For disaster recovery it is recommended to export certificate and private key pa

Cisco ISE Edit Generate Self Signed Certificate Import Exp Delete View

Friendly Name	Used By	Portal group tag	Issued To
ise-1			
<input checked="" type="checkbox"/> ise-1.demo.local#Certificate Services Endpoint Sub CA - ise-1#00001	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise-1.demo.local

**Things to do with the ISE System Cert**

- Delete the -----BEGIN CERTIFICATE-----
- Delete the -----END CERTIFICATE-----
- All the text should be in single line ...

```
MIIE9jCCAT6gAwIBAgIQPzfz/HZnjsVkr1AgAYF/scjANBgkqhkiG9w00
```

Depuis juin 2020, le portail vous permet de télécharger des certificats directement.

Microsoft Azure Search resources, services, and docs (G+)

Home > self | App registrations >

## ISE | Certificates & secrets

Search (Cmd+/) << Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Overview  
Quickstart  
Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions

### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

Thumbprint	Start date	Expires
8C618ABBC45B640E4F21EA302583D33E0F0C4C63	4/3/2020	4/2/2025
80C1360BCCD305F2D53E265668D5D8499AD693A5	4/5/2020	4/4/2025

Option héritée :

Étape 1. Exécutez une procédure PowerShell afin de transformer le certificat en BASE64 et de l'importer correctement dans le fichier manifeste Azure JSON. Utilisez l'application Windows PowerShell ou Windows PowerShell ISE à partir de Windows. Utilisez les commandes suivantes :

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import("mycer.cer") $bin = $cer.GetRawCertData() $base64Value = [Convert]::ToBase64String($bin)
```

Étape 2. Conservez les valeurs de \$base64Thumbprint, \$base64Value, et \$keyid, qui sont utilisées à l'étape suivante. Toutes ces valeurs sont ajoutées au champ JSON keyCredentials, par défaut, il ressemble à ceci :

```
15 | "identifiantUris": [
16 |   "https://rumaiacisco.onmicrosoft.com/239c7d6d-12d6-453c-8d3e-acfa701dc063"
17 | ],
18 | "keyCredentials": [],
19 | "knownClientApplications": [],
```

Pour ce faire, assurez-vous d'utiliser les valeurs dans cet ordre :

```
"keyCredentials": [ { "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN", "keyId": "$keyid_from_above_PPAN", "type": "AsymmetricX509Cert"
```

Étape 3. **Téléchargez** le fichier modifié JSON sur Azure Portal afin de valider le keyCredentials à partir des certificats utilisés sur ISE.

Il doit ressembler à ceci :

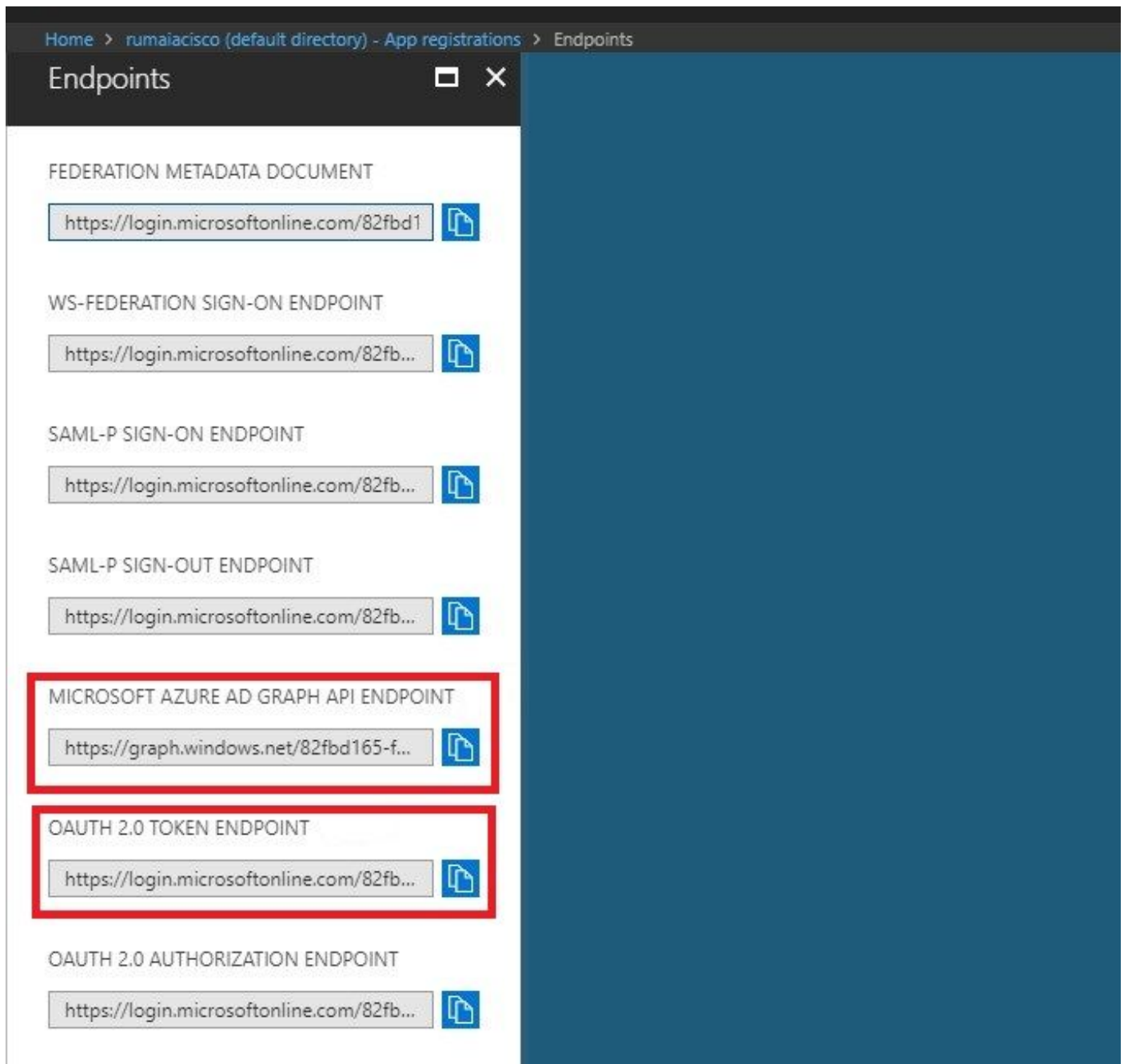
```

18 "keyCredentials": [
19   {
20     "customKeyIdentifier": "wteOPVePuM0wUeFNB9s22fkDYZE=",
21     "endDate": "2019-01-22T11:41:01Z",
22     "keyId": "eb7b1833-3240-4203-98a6-c3ccc6790d9d",
23     "startDate": "2018-01-22T11:41:01Z",
24     "type": "AsymmetricX509Cert",
25     "usage": "Verify",
26     "value": null
27   },
28   {
29     "customKeyIdentifier": "B5Zz60fZKHGN6qAMvt43swIZQko=",
30     "endDate": "2019-01-05T14:32:30Z",
31     "keyId": "86462728-544b-423d-8e5e-22adf3521d23",
32     "startDate": "2018-01-05T14:32:30Z",
33     "type": "AsymmetricX509Cert",
34     "usage": "Verify",
35     "value": null
36   },
37   {
38     "customKeyIdentifier": "GMlDp/1DYiNknFIJkgjnTbjo9nk=",
39     "endDate": "2018-12-06T10:46:32Z",
40     "keyId": "2ed5b262-ced6-4c1a-8a1a-c0abb82ae3c1",
41     "startDate": "2017-12-06T10:46:32Z",
42     "type": "AsymmetricX509Cert",
43     "usage": "Verify",
44     "value": null
45   },

```

Étape 4. Sachez qu'après le téléchargement, le value champ en dessous keyCredentials s'affiche null puisque ceci est imposé par le côté Microsoft pour ne pas permettre à ces valeurs d'être vues après le premier téléchargement.

Les valeurs requises pour ajouter le serveur MDM dans ISE peuvent être copiées depuis Microsoft Azure AD Graph API Endpoint et OAUTH 2.0 Token Endpoint.



Ces valeurs doivent être entrées dans l'interface utilisateur graphique ISE. Accédez à Administration > Network Resources > External MDM et ajoutez un nouveau serveur :

ISE	Intune
URL de détection automatique	Terminaux > Point de terminaison de l'API Microsoft Azure AD Graph
ID client	{Registered-App-Name} > ID d'application
URL d'émission de jeton	Terminaux > Terminaux Token OAuth 2.0



MDM Servers > Intune

Name \*

Server Type  ⓘ

Authentication Type  ⓘ

Auto Discovery  ⓘ

Auto Discovery URL \*  ⓘ

Client ID \*

Token Issuing URL \*  ⓘ

Token Audience \*

Description

Polling Interval \*  (minutes) ⓘ

Status

Une fois la configuration terminée, l'état affiche enabled (activé).

MDM Servers

	Name	Status	Service Provider	MDM Server	Server Type	Description
<input type="checkbox"/>	Intune	<span style="color: green;">■</span> Enabled	Microsoft	fef.ms03.manage.microsoft.com	Mobile Device Manager ↕	

Vérifiez et dépannez

"Échec de la connexion au serveur" basé sur sun.security.validator.ValidatorException



Connection to server failed with:

**sun.security.validator.ValidatorException:**

**PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target**

Please try with different settings.

OK

Étape 1. Collectez l'offre groupée de support avec ces journaux au niveau TRACE :

- portal (guest.log)
- mdmportal (ise-psc.log)
- external-mdm (ise-psc.log)

Étape 2. Recherchez ise-psc.log les journaux suivants :

- 2016-10-17 12:45:52,158 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- ClientId - a46a6fd7-4a31-4471-9078-59cb2bb6a5ab, Token issuance endpoint - <https://login>
- microsoftonline.com/273106dc-2878-42eb-b7c8-069dcf334687/oauth2/token, ResourceId/App Id uri - <https://graph.windows.net>
- 2016-10-17 12:45:52,329 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Certificate Friendly Name -USMEM-AM01-ISE.Sncorp.smith-nephew.com#USMEM-AM01-ISE.Sncorp.smith-nephew.c
- om#00003
- 2016-10-17 12:45:52,354 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Result of command invocation
- 2016-10-17 12:45:52,363 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Result of command invocation
- 2016-10-17 12:45:52,364 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Successfully decrypted private key
- 2016-10-17 12:45:52,794 ERROR [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- There is a problem with the Azure certificates or ISE trust store. sun.security.validator
- .ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

- 2016-10-17 12:45:52,794 ERROR [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::- Unable to acquire access token from Azure
- java.util.concurrent.ExecutionException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException
- : unable to find valid certification path to requested target

Cela indique qu'il est nécessaire d'importer le graph.microsoft.com certificat présent sur cette page.



The screenshot shows a web browser window with the address bar displaying "Secure | https://graph.windows.net". Below the address bar, a message states: "This XML file does not appear to have any style information associated with it. The document tree is shown below." The XML content is as follows:

```
<error xmlns="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <code>Request_DataContractVersionMissing</code>
  <message xml:lang="en">
    The specified api-version is invalid. The value must exactly match a supported version.
  </message>
</error>
```

Étape 3. Cliquez sur l'locker icône et vérifiez les détails du certificat.



General Details Certification Path



### Certificate Information

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.311.42.1

\* Refer to the certification authority's statement for details.

**Issued to:** graph.windows.net

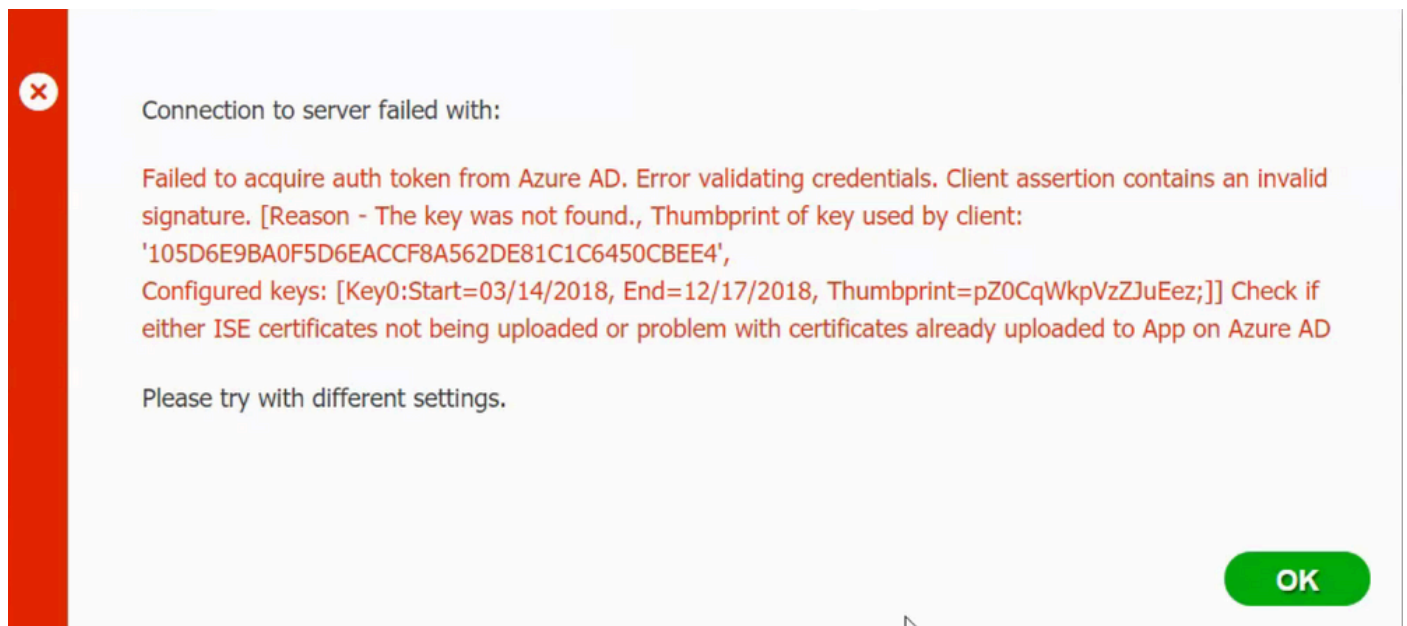
**Issued by:** Microsoft IT TLS CA 2

**Valid from** 9/26/2017 **to** 9/26/2019

Issuer Statement

OK

Impossible d'acquérir le jeton d'authentification d'Azure AD



Généralement, cette erreur se produit lorsque le JSON fichier manifeste contient la mauvaise chaîne de certificats ISE. Avant de télécharger le fichier manifeste sur Azure, vérifiez si au moins cette configuration est présente :

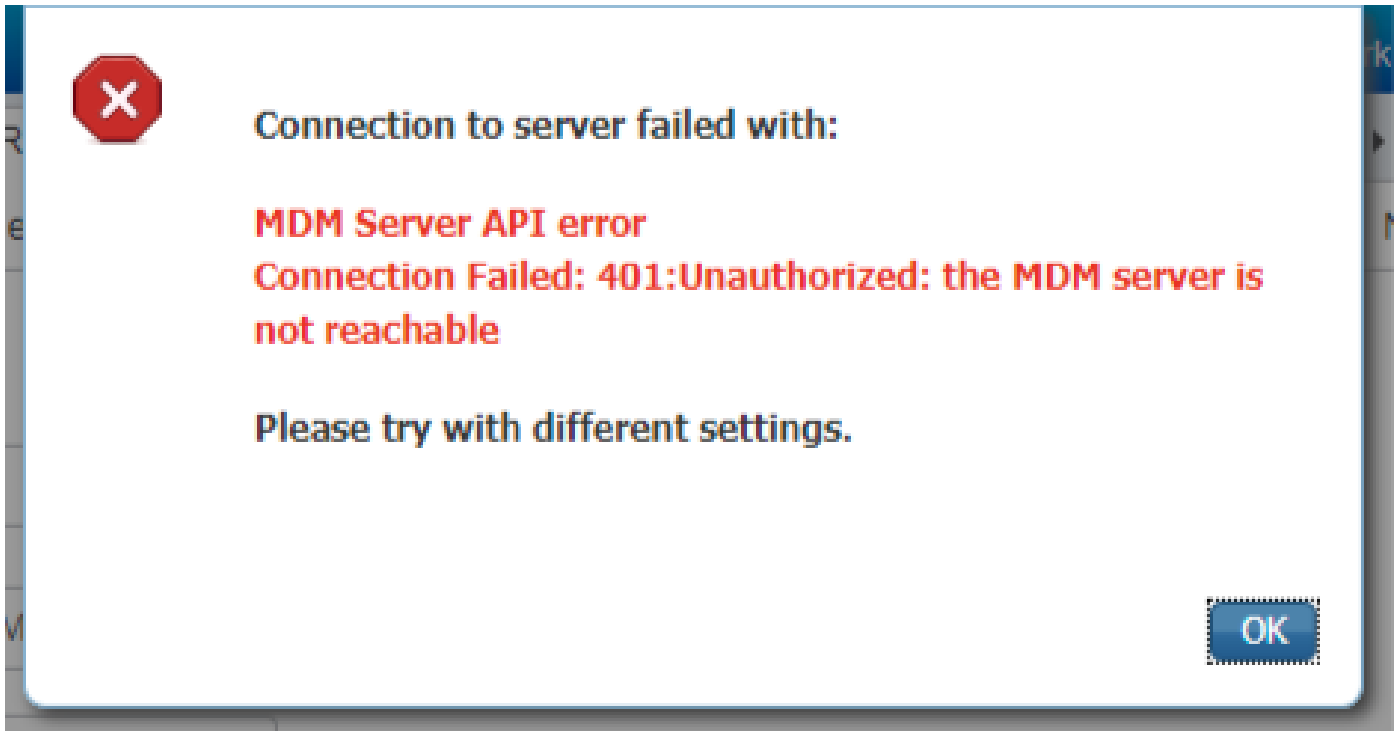
```
"keyCredentials": [ { "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN", "keyId": "$keyid_from_above_PPAN", "type": "Asym
```

L'exemple précédent est basé sur un scénario dans lequel il existe un réseau PAN et un réseau SAN. **Exécutez** à nouveau les scripts à partir de PowerShell et **importez** les valeurs BASE64 appropriées. Essayez de télécharger le fichier manifeste et vous ne devez faire face à aucune erreur.

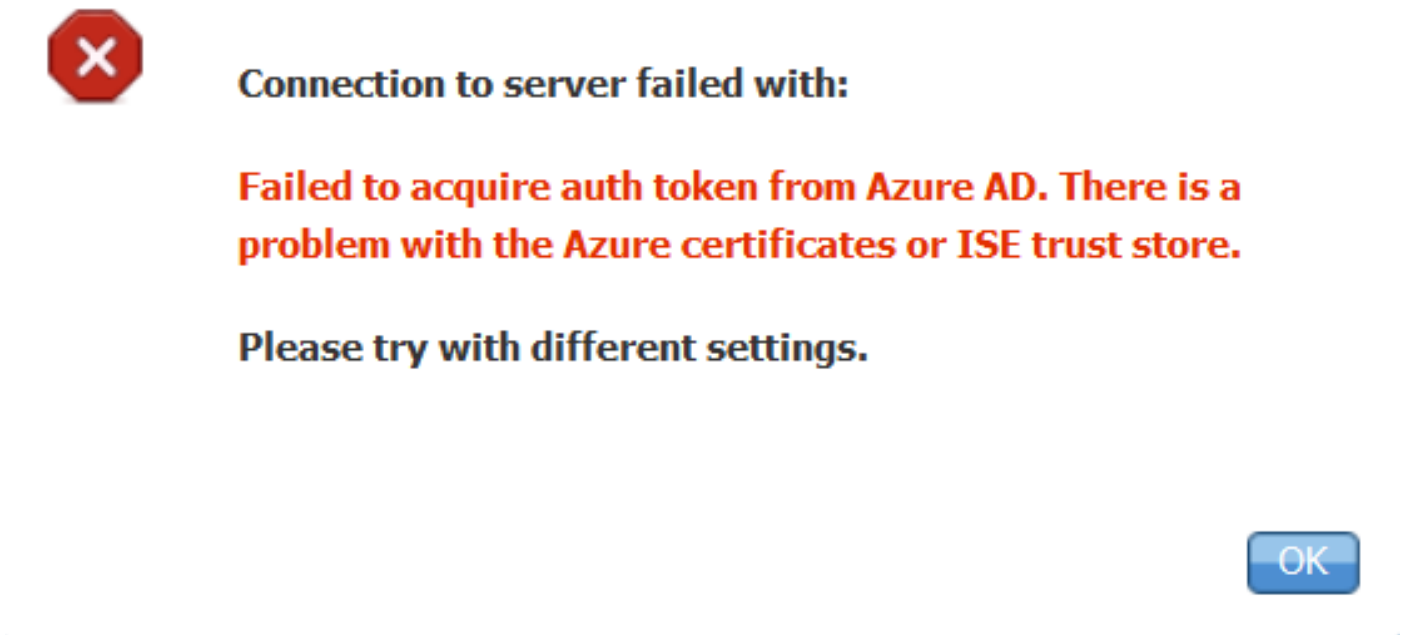
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import("mycer.cer") $bin = $cer.GetRawCertData() $base64V
```

N'oubliez pas d'appliquer les valeurs pour \$base64Thumbprint, \$base64Value et \$keyid comme indiqué dans les étapes de la section Configurer.

Impossible d'acquérir le jeton d'authentification d'Azure AD



Cette erreur se produit souvent lorsque les autorisations appropriées ne sont pas accordées à l'application Azure dans portal.azure.com. Vérifiez que les attributs de votre application sont corrects et assurez-vous que vous cliquez Grant Permissions après chaque modification.



Ce message se produit lorsque ISE tente d'accéder à l'URL d'émission de jeton et renvoie un certificat que l'ISE ne renvoie pas. Assurez-vous que toute la chaîne CA se trouve dans le magasin de confiance ISE. Si le problème persiste après l'installation du certificat correct dans le magasin de confiance d'ISE, effectuez des captures de paquets et testez la connectivité afin de voir ce qui est envoyé.

Informations connexes

- [Service pour traiter les appels en utilisant les identifiants du client](#)

- [Azure - Authentification et autorisation](#)
- [Azure - Démarrage rapide : enregistrement d'une application avec la plateforme d'identité Microsoft](#)
- [Manifeste d'application Azure Active Directory](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.