Intune MDM integreren met Identity Services Engine

Inhoud

Inleiding

Dit document beschrijft hoe u Intune Mobile Device Management (MDM) kunt integreren met Cisco Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van MDM-services in Cisco ISE
- Kennis van Microsoft Azure Intune Services

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine 3.0
- Microsoft Azure Intune-toepassing

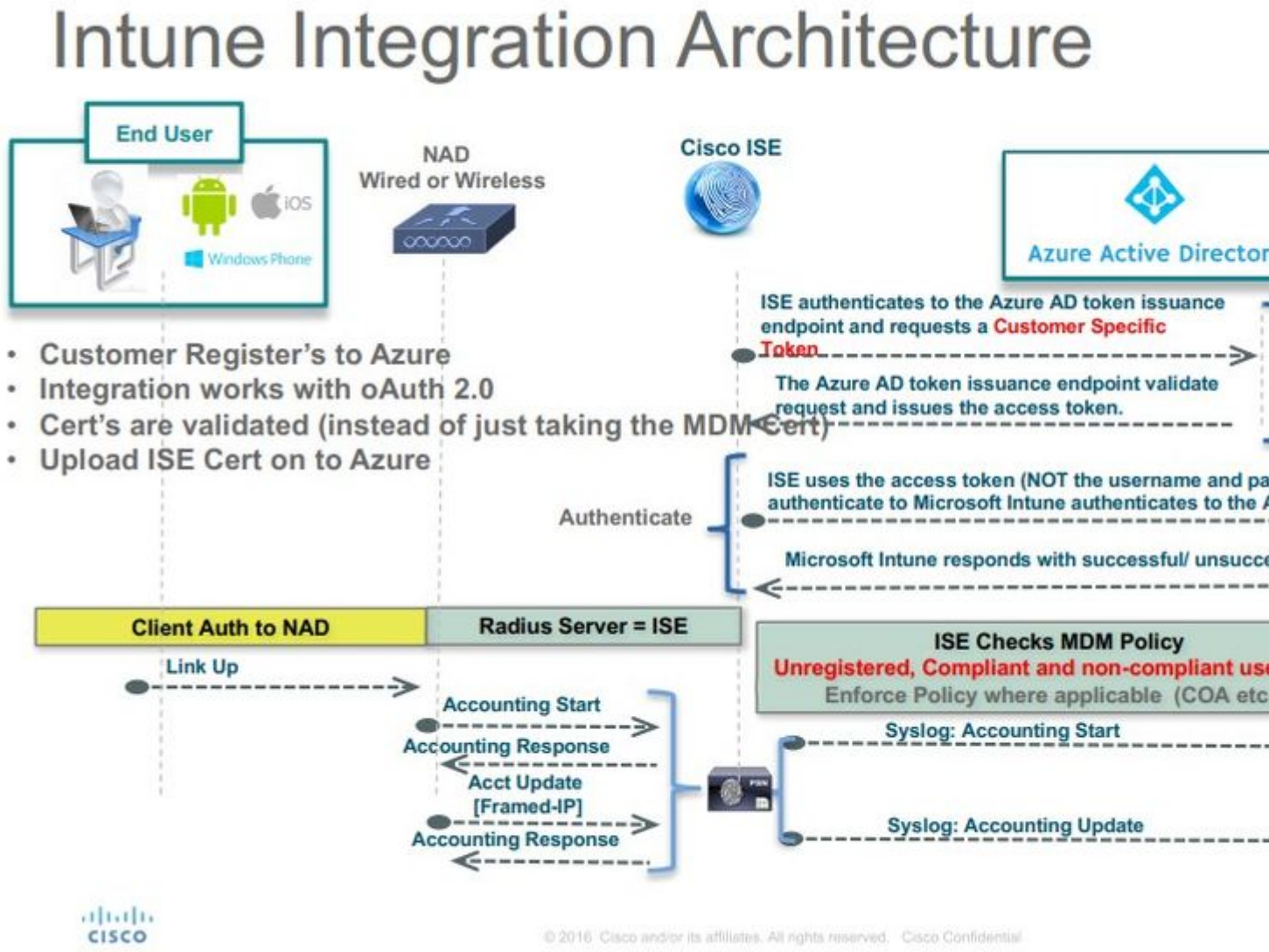
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

MDM-servers beveiligen, monitoren, beheren en ondersteunen mobiele apparaten die worden ingezet bij mobiele operatoren, serviceproviders en bedrijven. Deze servers fungeren als de beleidsserver die het gebruik van bepaalde toepassingen op een mobiel apparaat (bijvoorbeeld een e-mailtoepassing) in de geïmplementeerde omgeving regelt. Het netwerk is echter de enige entiteit die granulaire toegang tot endpoints kan bieden op basis van toegangscontrolelijsten (ACLâ€™s). ISE vraagt de MDM-servers om de benodigde apparaatkenmerken om ACLâ€™s te maken die netwerktoegangscontrole voor die apparaten bieden. Cisco ISE wordt geïntegreerd met Microsoft Intune MDM Server om organisaties te helpen bedrijfsgegevens te beveiligen wanneer apparaten proberen toegang te krijgen tot resources op locatie.

Configureren

Netwerkdiagram



Microsoft Intune configureren

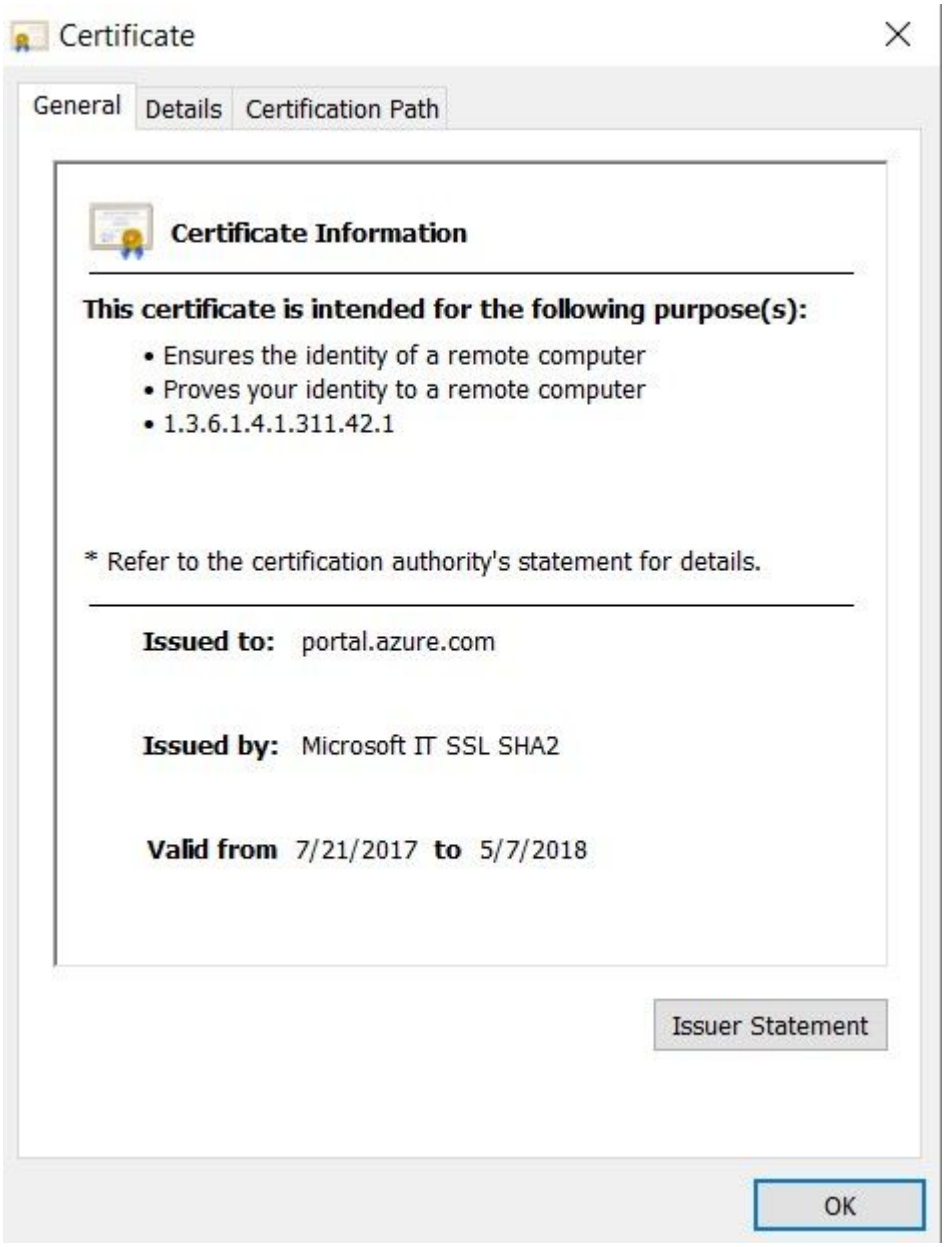
Importeer de certificaten van de Intune-portal naar de ISE Trusted Store

Meld u aan bij de Intune Admin-console of Azure Admin-console, afhankelijk van welke site uw huurder heeft. Gebruik de browser om de certificaatgegevens te verkrijgen:

Stap 1. Open de Microsoft Azure portal van een webbrowser.

Stap 2. Klik op het vergrendelingssymbool in de browserwerkbalk en klik vervolgens op View Certificates.

Stap 3. Klik in het venster Certificaat op het Certification Path tabblad. Hier is een voorbeeld te zien:

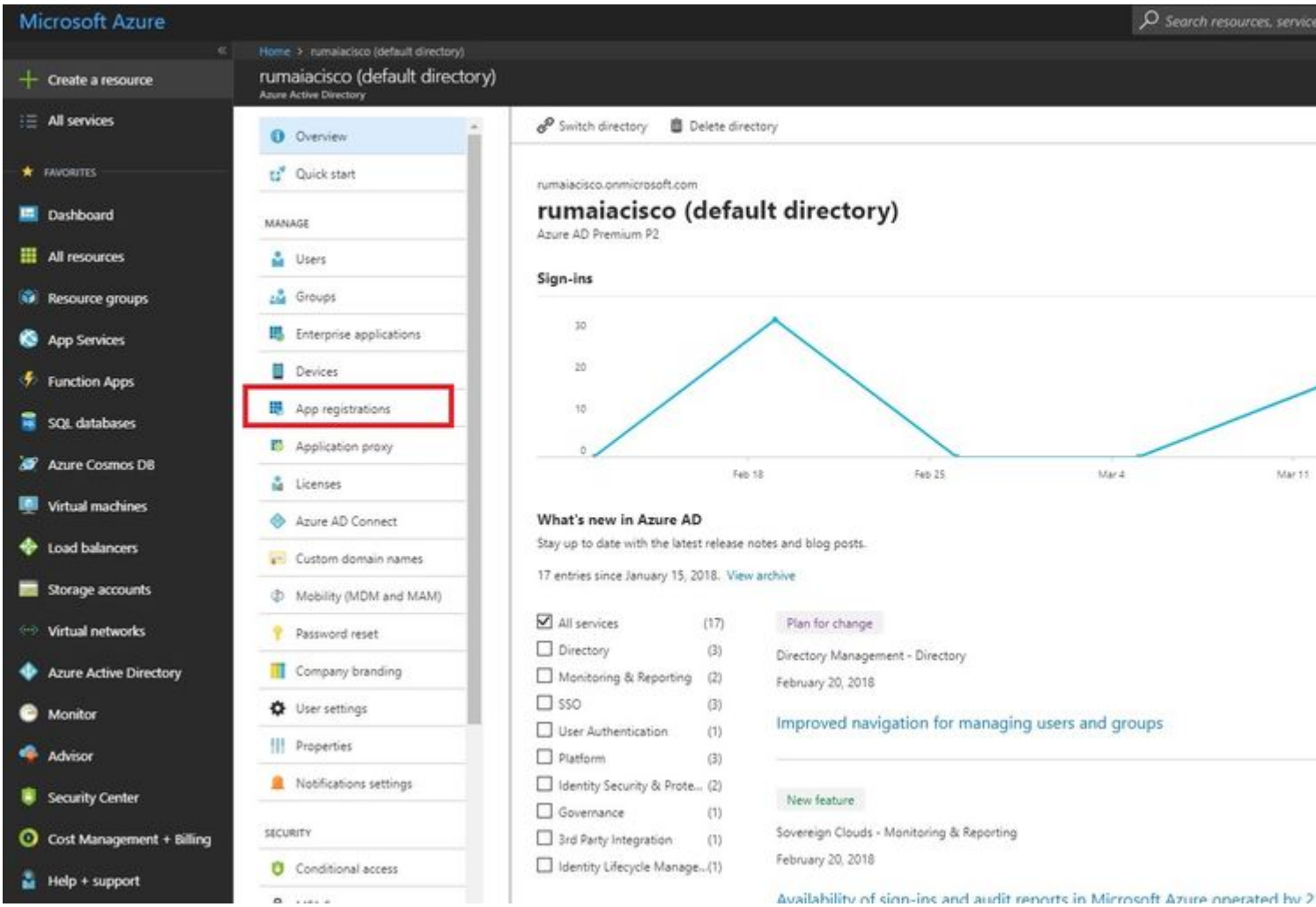


Stap 4. Zoeken Baltimore Cyber Trust root, wat de gebruikelijke root-CA is. Als er echter een andere Root CA is, klik dan op dat Root CA certificaat. Op het tabblad Details van dat Root CA-certificaat, kunt u het kopiëren naar het bestand en opslaan als BASE64 cert.

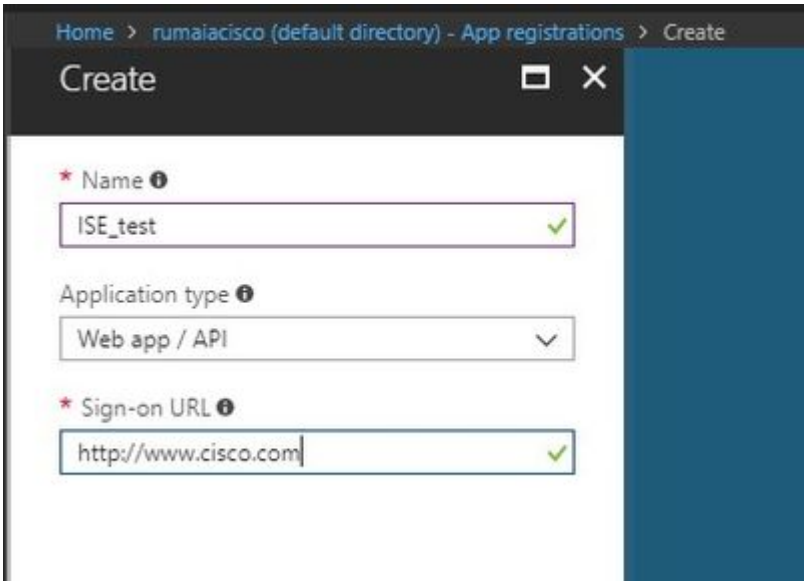
Stap 5. In ISE navigeer je naar Administration > System > Certificates > Trusted Certificates, en importeer het basiscertificaat dat zojuist is opgeslagen. Geef het certificaat een zinvolle naam, zoals Azure MDM. Herhaal ook de procedure voor de tussenliggende CA-certificaten.

ISE als een toepassing implementeren in de Azure-portal

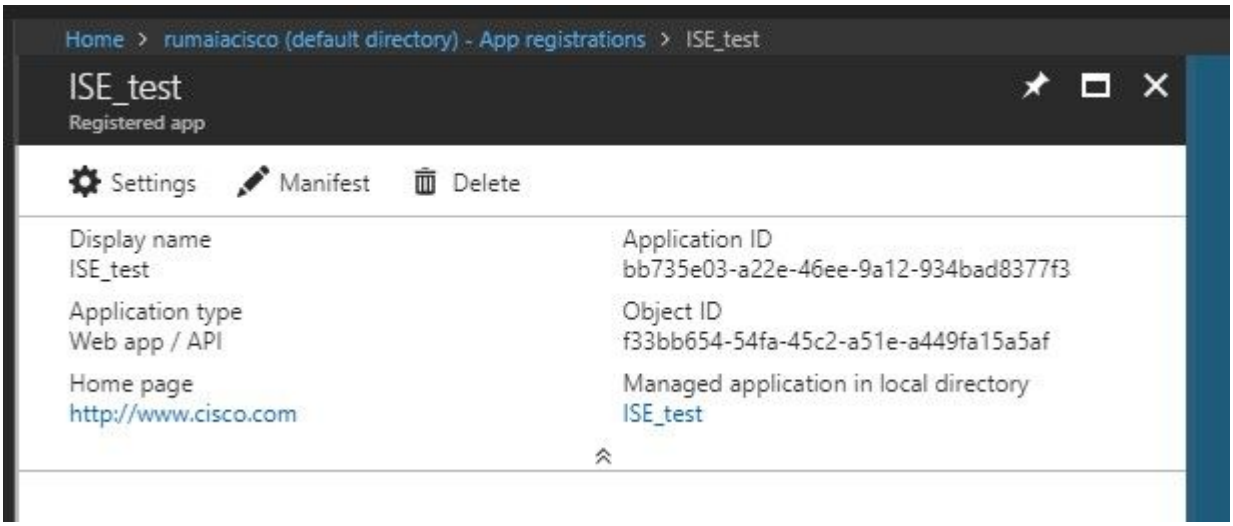
Stap 1. Naar het Azure Active Directory en kiezen App registrations.



Stap 2. In het App registrations, een nieuwe inschrijving met de ISE-naam aan te maken. Klik op de knop Create zoals in deze afbeelding.



Stap 3. Kiezen Settings om de toepassing te bewerken en de vereiste onderdelen toe te voegen.



Stap 4. Onder Settings, kies de vereiste rechten en pas deze opties toe:

1. Microsoft Graph
    - Toepassingsrechten
        - Lezen van directorygegevens
    - Gedelegeerde rechten
        - Microsoft Intune-apparaatconfiguratie en -beleid lezen
        - Microsoft Intune-configuratie lezen
        - Gebruikers inloggen
        - Toegang tot de gegevens van de gebruiker altijd

2. Microsoft Intune API
    - Toepassingsrechten
        - Ontvang informatie over apparaatstatus en naleving van Microsoft Intune

3. Windows Azure Active Directory
    - Toepassingsrechten
        - Lezen van directorygegevens

    - Gedelegeerde rechten
        - Lezen van directorygegevens
        - Aanmelden en het gebruikersprofiel lezen

Het resultaat van de configuratie lijkt op wat hier wordt getoond:

+ 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	Gra
Directory.Read.All	Application	Read directory data	Yes	Gra
User.Read.All	Delegated	Read all users' full profiles	Yes	Gra
Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	Gra
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Gra
Directory.Read.All	Application	Read directory data	Yes	Gra
offline_access	Delegated	Maintain access to data you have given it access to	No	Gra
openid	Delegated	Sign users in	No	Gra
User.Read	Delegated	Sign in and read user profile	No	Gra
User.Read.All	Delegated	Read all users' full profiles	Yes	Gra
User.Read.All	Application	Read all users' full profiles	Yes	Gra

Settings

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Required permissions

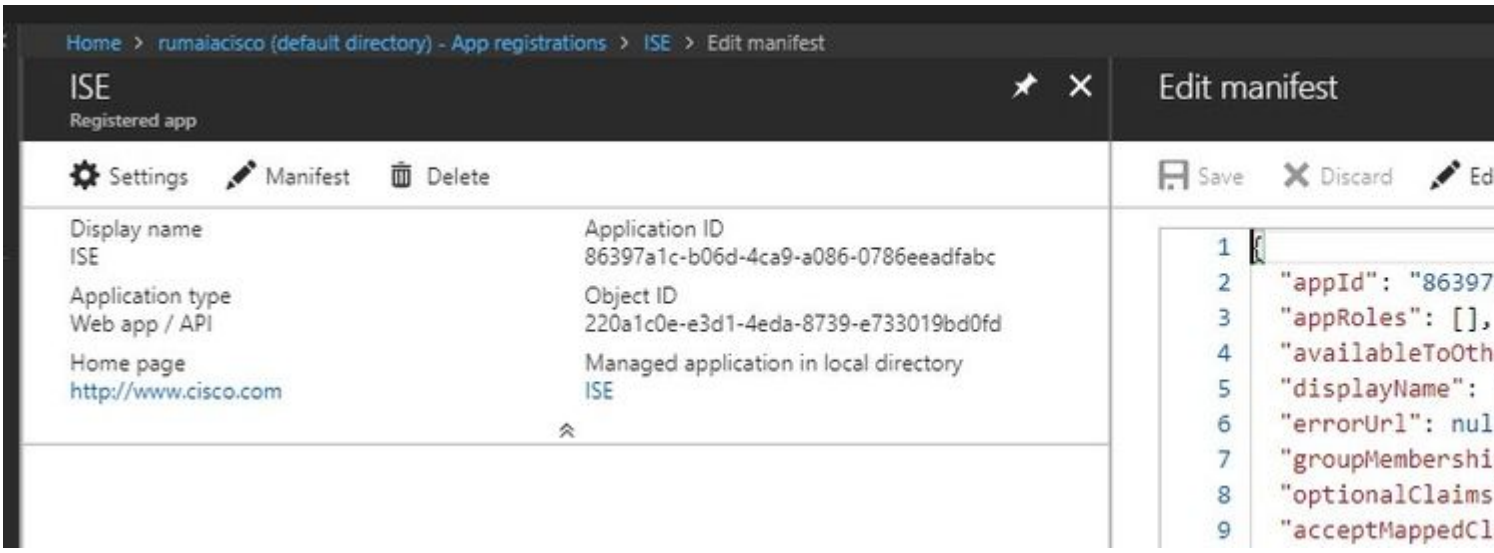
+ Add Grant Permissions

API	APPLICATION PERMI
Microsoft Graph	1
Microsoft Intune API	1
Windows Azure Active Directory	1

Stap 5. Klik op de knop Grant Permissions om alle toepassingstoestemmingen te bevestigen. Dit proces duurt 5-10 minuten. Het bestand bewerken Azure Manifest bestand voor de toepassing gemaakt om interne ISE CA-certificaten te importeren.

ISE-certificaten importeren in de toepassing in Azure

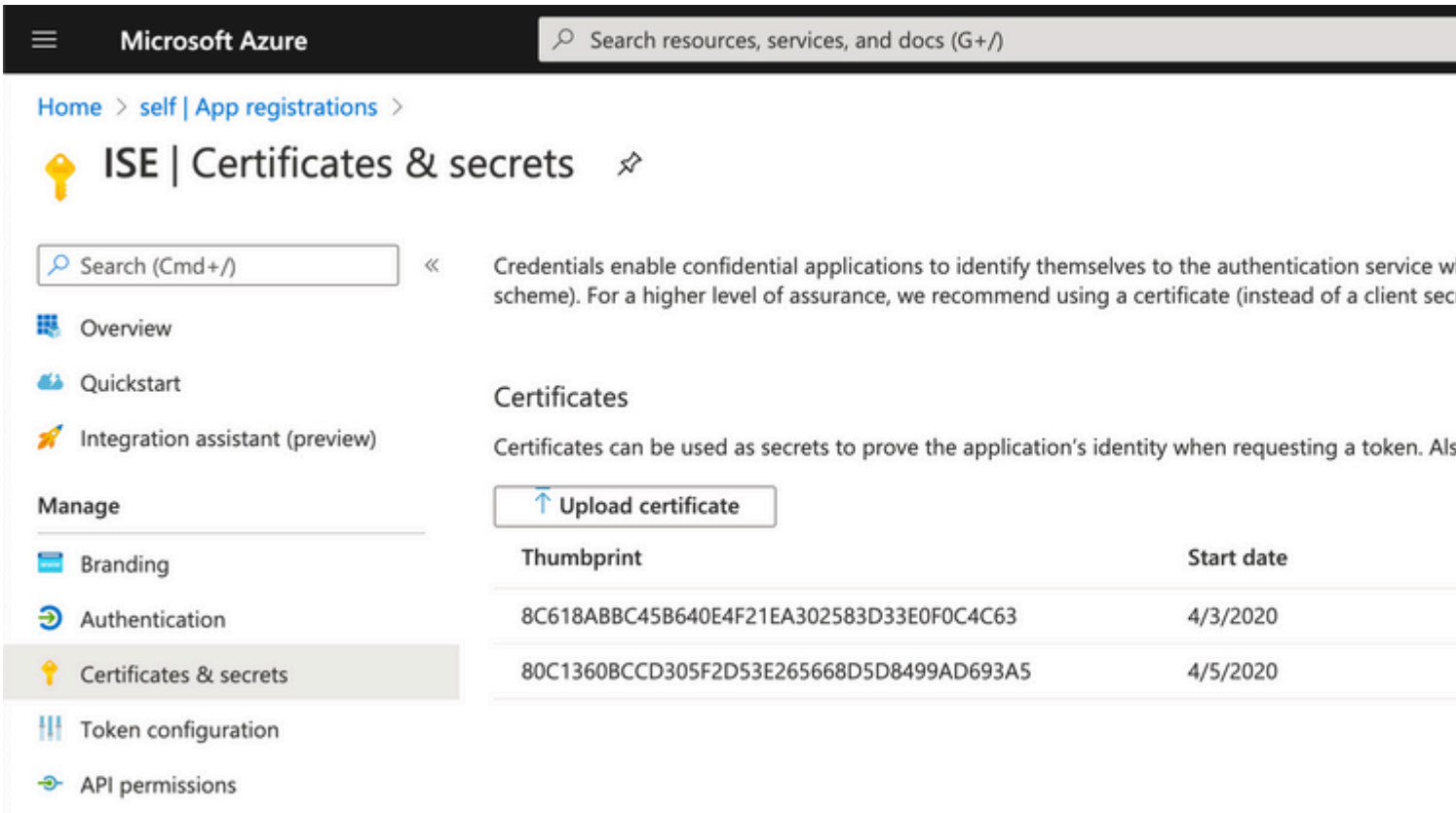
Stap 1. Download het manifest bestand voor de toepassing.



> **Opmerking**: Het is een bestand met de extensie JSON. Wijzig de bestandsnaam of de extensie niet, anders mislukt het.

Stap 2. Exporteer het ISE-systeemcertificaat vanuit alle knooppunten. Blader in het PAN naar Administration > System > Certificates > System Certificates, kiest u het standaard zelf ondertekende servercertificaat en klikt u op Export. Kiezen Export Certificate Only (standaard), en kies een plaats om het op te slaan. Verwijdert de begin- en eindtags van het certificaat en kopieert de rest van de tekst als één regel. Dit is van toepassing op versies vóór juni 2020 die in het gedeelte Verouderde opties zijn beschreven.

Vanaf juni 2020 kunt u via de portal rechtstreeks certificaten uploaden.



Verouderde optie:

Stap 1. Voer een PowerShell-procedure uit om het certificaat naar BASE64 te draaien en het correct te importeren naar het Azure JSON-manifest. Gebruik de Windows PowerShell of Windows PowerShell ISE-toepassing vanuit Windows. Gebruik deze opdrachten:

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

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

Stap 2. De waarden behouden voor $base64Thumbprint, $base64Value, en $keyid, die bij de volgende stap worden gebruikt. Al deze waarden worden toegevoegd aan het JSON-veld keyCredentials aangezien het door gebrek, kijkt het als dit:

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

Zorg ervoor dat u de waarden in deze volgorde gebruikt:

```
"keyCredentials": [

  {

  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_PPANâ€,

  â€œkeyIdâ€œ: â€œ$keyid_from_above_PPANâ€œ,

  "type": "AsymmetricX509Cert",

  "usage": "Verify",

  "value": "Base64 Encoded String of ISE PPAN cert"

  },

  {

  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_SPANâ€,

  â€œkeyIdâ€œ: â€œ$keyid_from_above_SPANâ€œ,

  "type": "AsymmetricX509Cert",

  "usage": "Verify",
```

```
  "value": "Base64 Encoded String of ISE SPAN cert"

  }
],
```

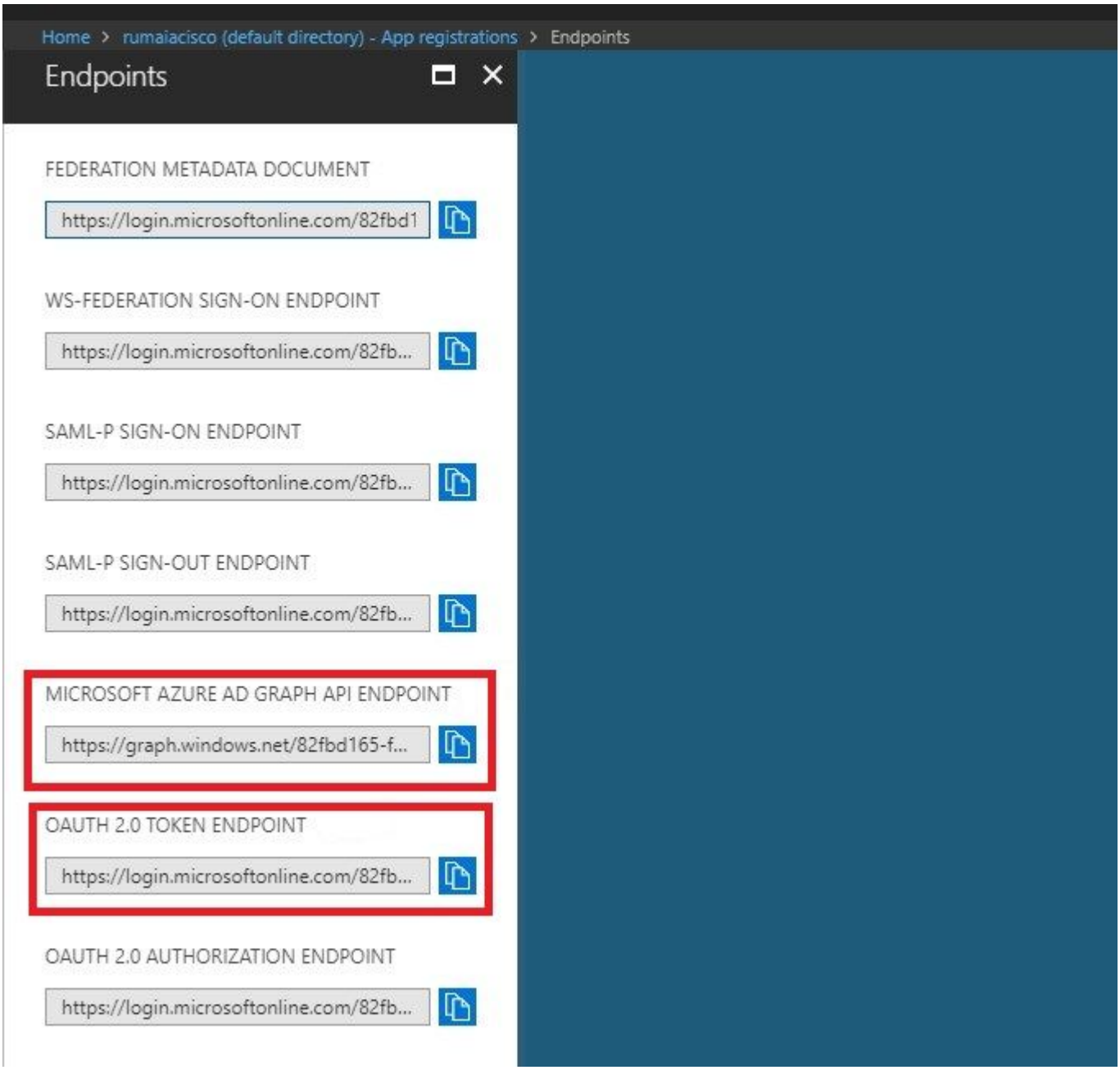
Stap 3. Upload de bewerkte tekst JSON bestand naar Azure Portal om de keyCredentials van de op ISE gebruikte certificaten.

Het moet er ongeveer als volgt uitzien:


```
"keyCredentials": [
  {
    "customKeyIdentifier": "wteOPVePuM0wUeFNB9s22fkDYZE=",
    "endDate": "2019-01-22T11:41:01Z",
    "keyId": "eb7b1833-3240-4203-98a6-c3ccc6790d9d",
    "startDate": "2018-01-22T11:41:01Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
  {
    "customKeyIdentifier": "B5Zz60fZKHGN6qAMvt43swIZQko=",
    "endDate": "2019-01-05T14:32:30Z",
    "keyId": "86462728-544b-423d-8e5e-22adf3521d23",
    "startDate": "2018-01-05T14:32:30Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
  {
    "customKeyIdentifier": "GMlDp/1DYiNknFIJkgjnTbjo9nk=",
    "endDate": "2018-12-06T10:46:32Z",
    "keyId": "2ed5b262-ced6-4c1a-8a1a-c0abb82ae3c1",
    "startDate": "2017-12-06T10:46:32Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
```

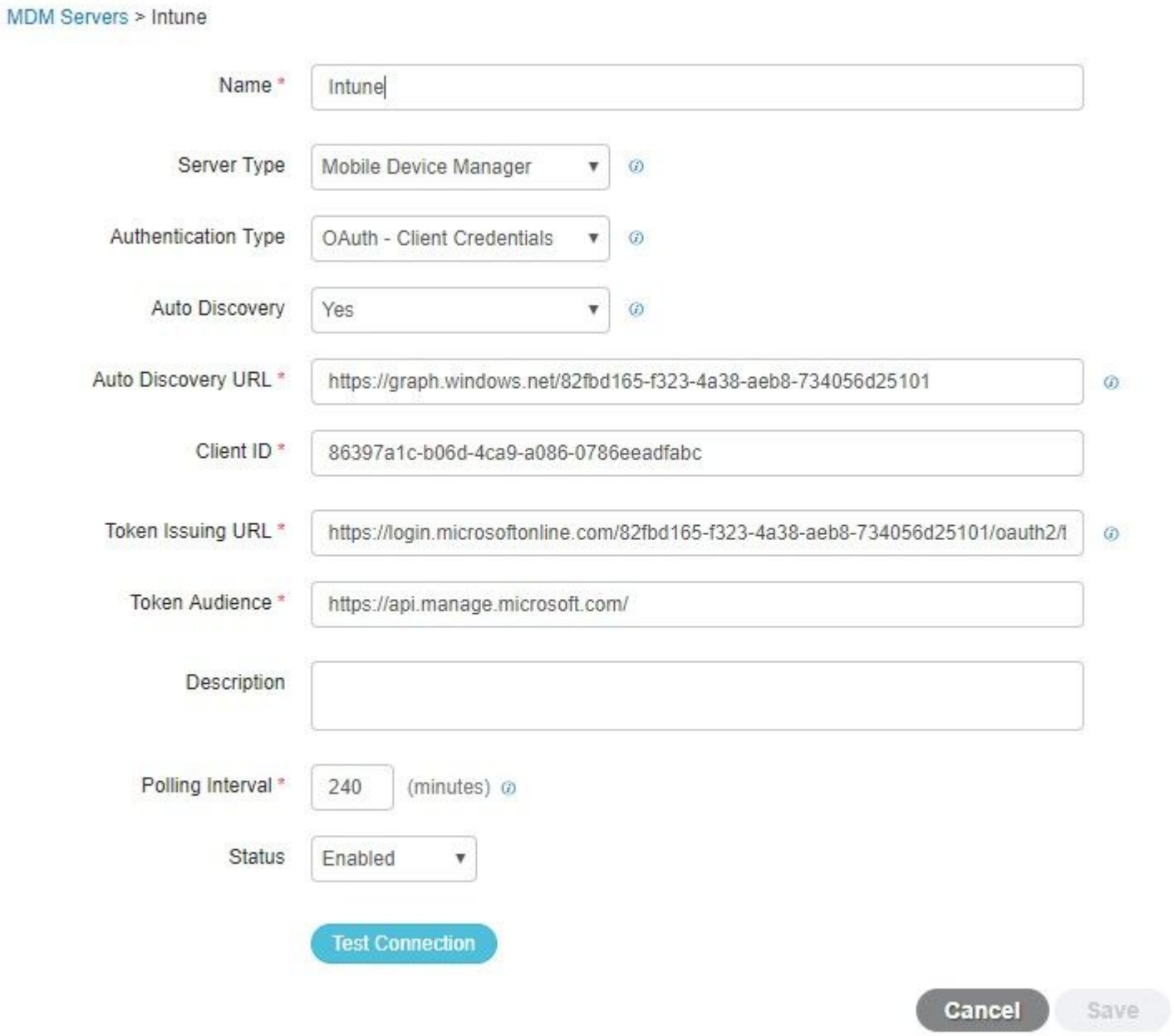

Stap 4. Houd er rekening mee dat na het uploaden de value veld onder keyCredentials voorstelling null aangezien dit door Microsoft wordt afgedwongen om deze waarden niet toe te staan om na de eerste Upload te worden gezien.

De waarden die vereist zijn om de MDM-server in ISE toe te voegen, kunnen worden gekopieerd van Microsoft Azure AD Graph API Endpoint en OAUTH 2.0 Token Endpoint.

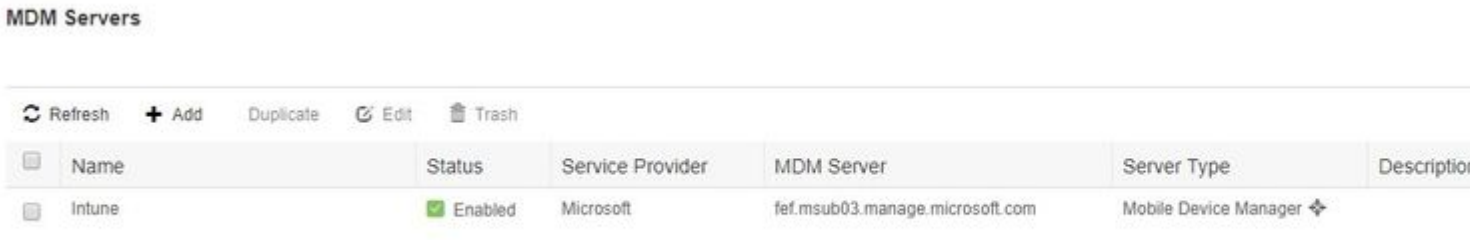


Deze waarden moeten in de ISE GUI worden ingevoerd. Naar navigeren Administration > Network Resources > External MDM en voeg een nieuwe server toe:

ISE	Intune
URL voor automatische detectie	Endpoints > Microsoft Azure AD Graph API-endpoint
Klant-ID	{Registered-App-Name} > Applicatie-ID
Token Issuing URL	Eindpunten > Anyuth 2.0 Token Endpoint

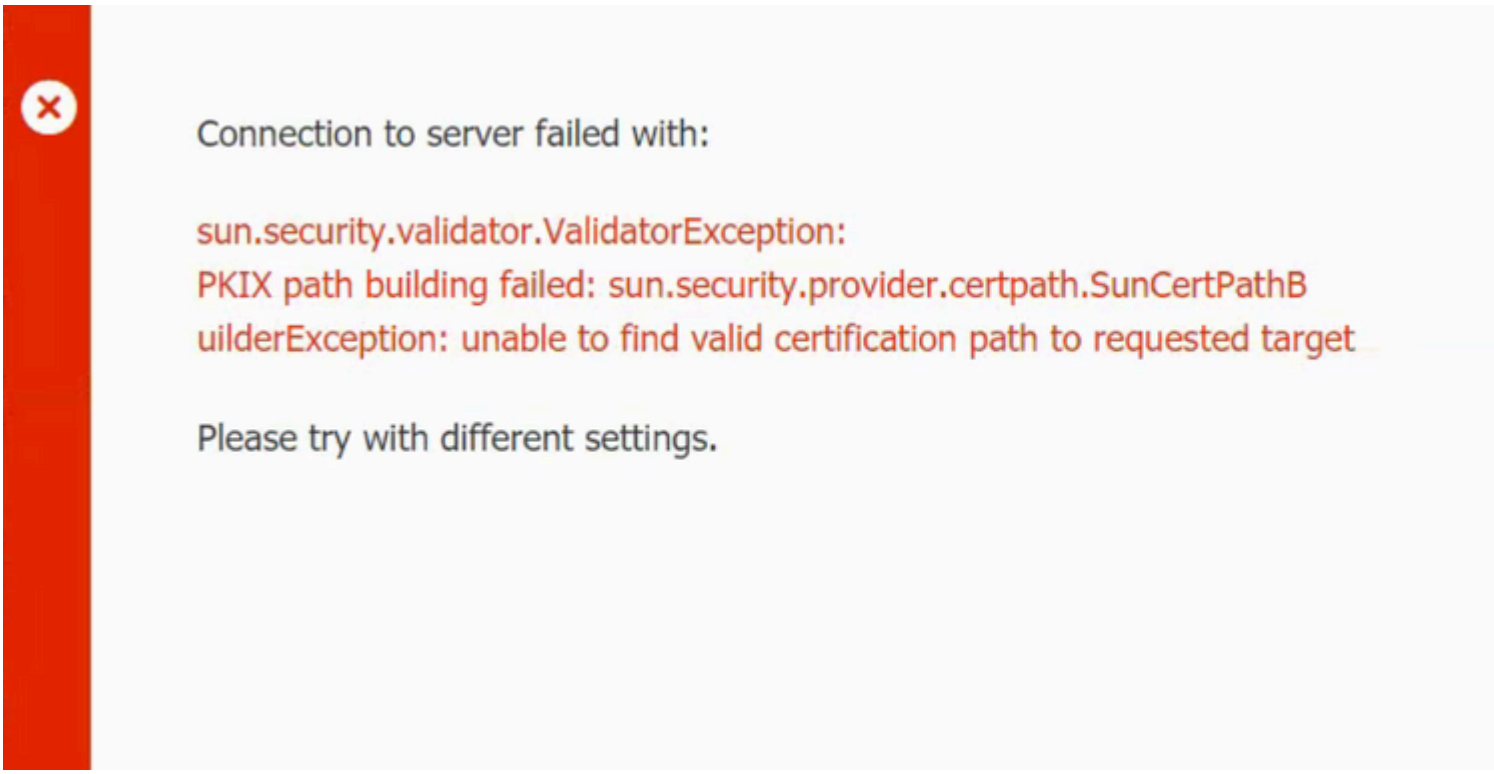


Nadat de configuratie is voltooid, wordt de status ingeschakeld.



Verifiëren en probleemoplossing

"Verbinding met de server is mislukt", gebaseerd op sun.security.validatorException



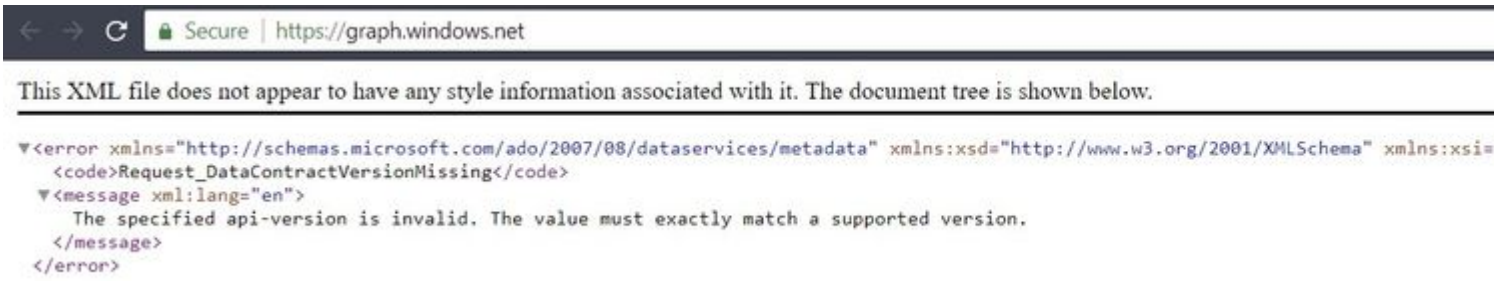
Stap 1. Verzamel de ondersteuningsbundel met deze logs op TRACE-niveau:

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

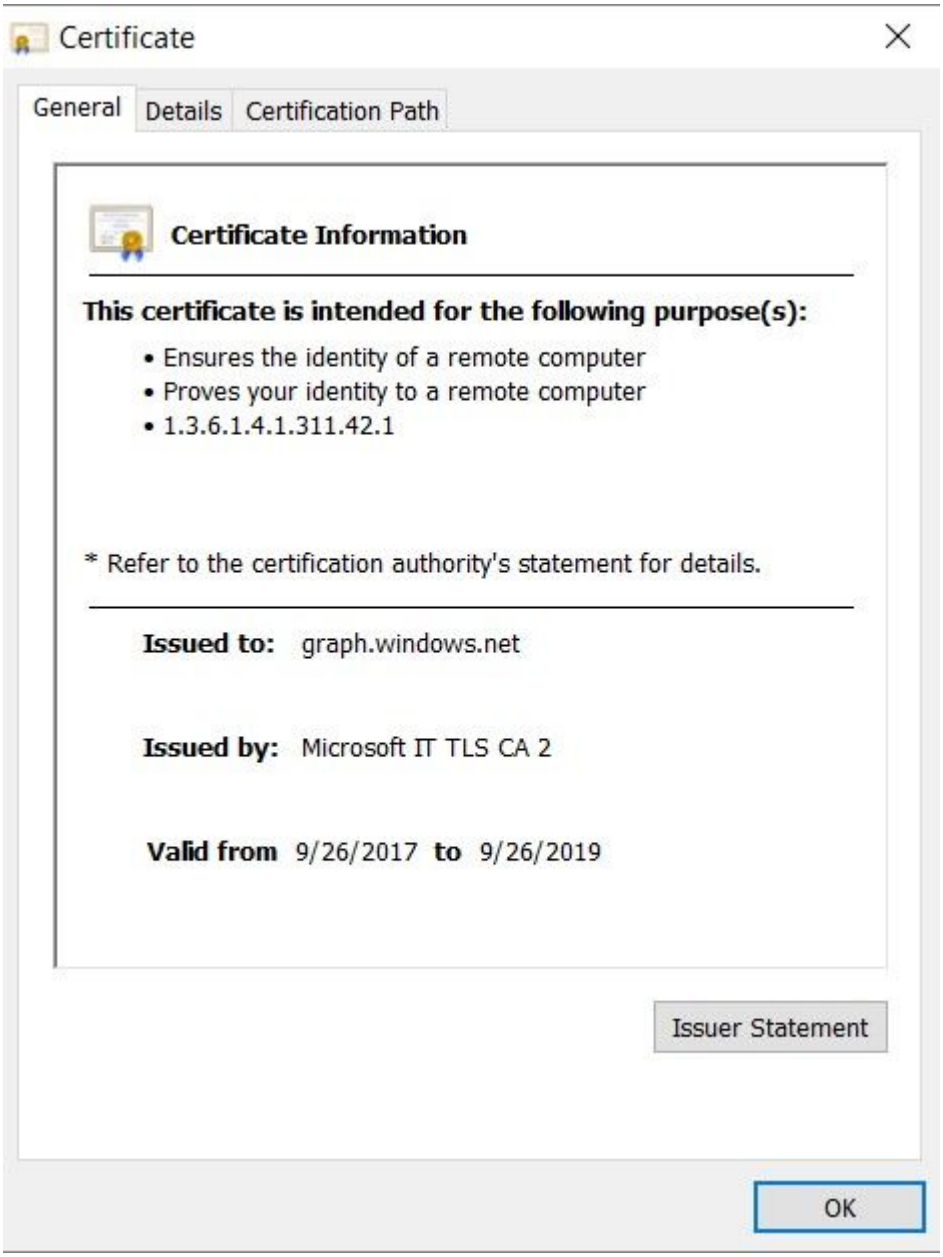
Stap 2. controleren ise-psc.log voor deze logbestanden:

- 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 -::::- Successfuly 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

Dit geeft aan dat het noodzakelijk is om de graph.microsoft.com certificaat, op deze pagina aanwezig.

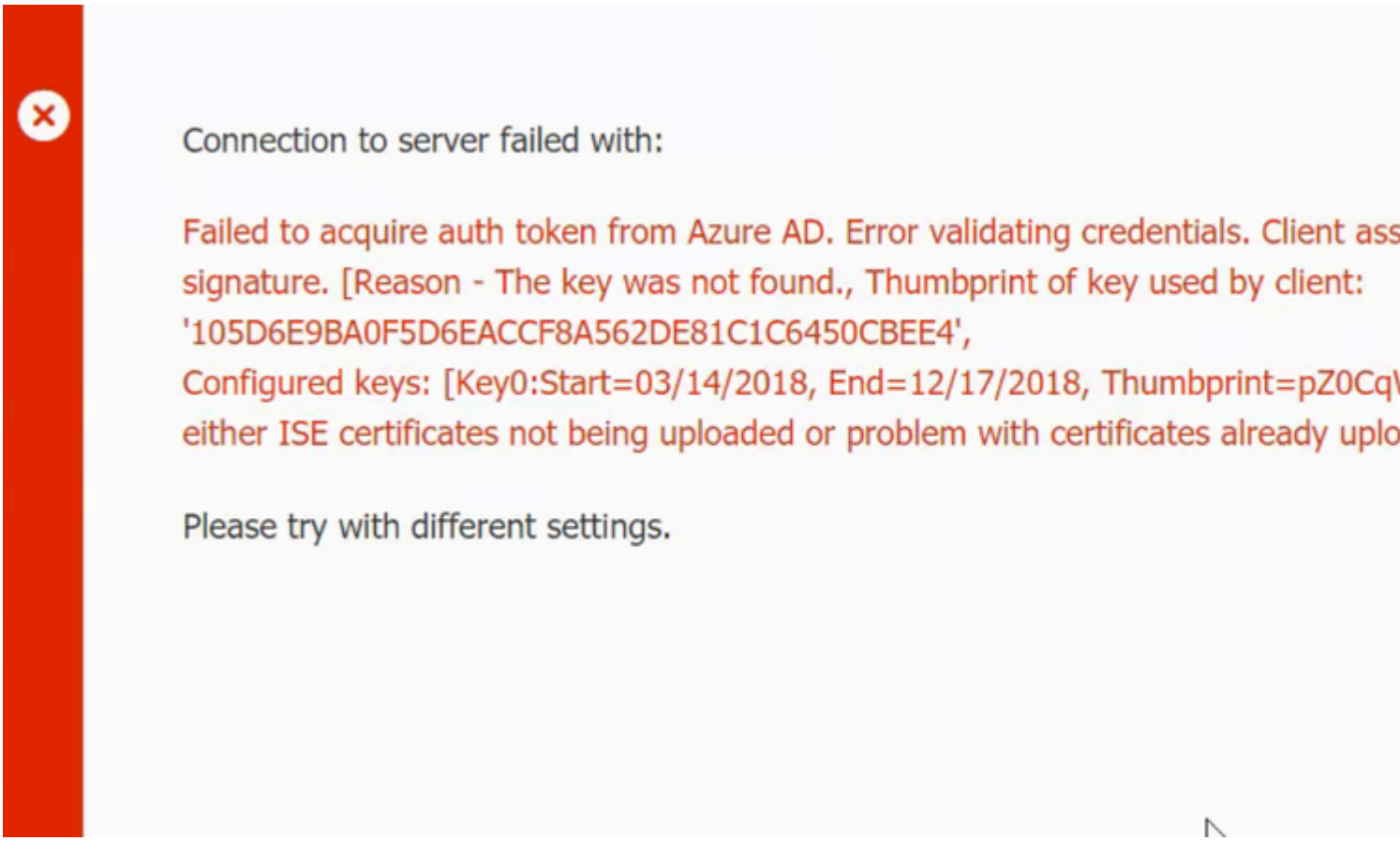


Stap 3. Klik op de locker pictogram en controleer de certificaatgegevens.



Stap 4. Sla het op in een bestand in BASE64-indeling en importeer het in ISE Trusted Store. Zorg ervoor dat u de volledige certificaatketen importeert. Na dit, test opnieuw de verbinding aan de MDM server.

Aankopen van autorisatieteken van Azure AD mislukt



Deze fout doet zich gewoonlijk voor wanneer het manifest JSON bestand bevat de verkeerde ISE-certificaatketen. Alvorens u het duidelijke bestand naar Azure uploadt, moet u controleren of ten minste deze configuratie aanwezig is:

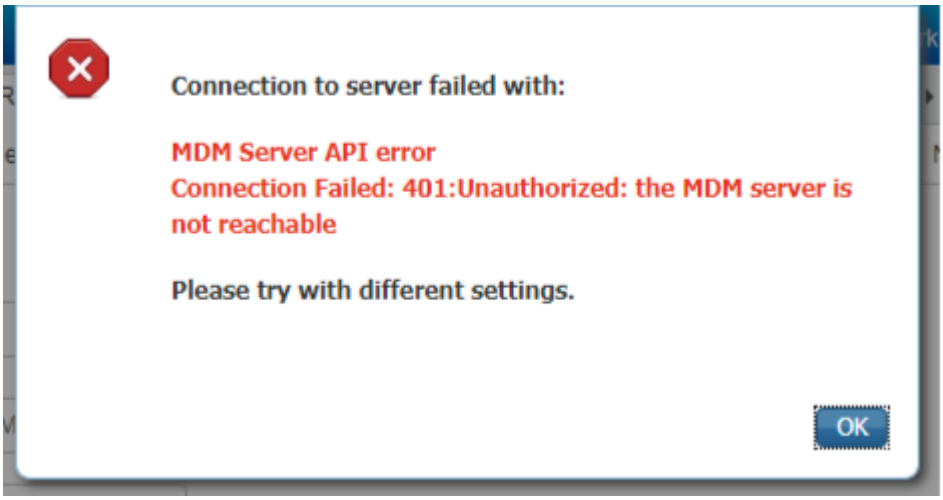
```
"keyCredentials": [
  {
  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_PPANâ€ï¿½,
  â€œkeyIdâ€œ: â€œ$keyid_from_above_PPANâ€œ,
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "Base64 Encoded String of ISE PPAN cert"
  },
  {
  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_SPANâ€ï¿½,
  â€œkeyIdâ€œ: â€œ$keyid_from_above_SPANâ€œ,
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "Base64 Encoded String of ISE SPAN cert"
  }
}
],
```

Het vorige voorbeeld is gebaseerd op een scenario waarin een PAN en een SAN worden gebruikt. Start de scripts vanuit PowerShell opnieuw en importeer de juiste BASE64-waarden. Probeer het duidelijke bestand te uploaden en je mag geen fouten tegenkomen.

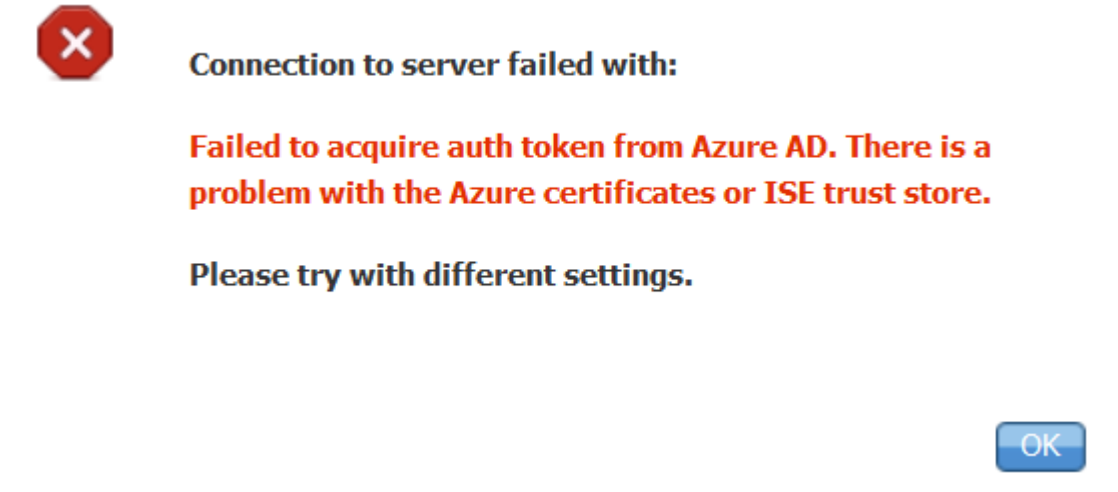
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(â€œmycer.crtâ€)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

Vergeet niet de waarden toe te passen voor $base64Thumbprint, $base64Value en $keyid zoals aangegeven in de stappen in het vak Configureren.

Aankopen van autorisatieteken van Azure AD mislukt



Deze fout treedt vaak op wanneer de juiste rechten niet worden gegeven aan de Azure-app in portal.azure.com. Controleer of uw app de juiste kenmerken heeft en zorg ervoor dat u klikt Grant Permissions na elke verandering.



Dit bericht wordt weergegeven wanneer ISE toegang probeert te krijgen tot de URL voor Token Issuing en het geeft een certificaat terug dat de ISE niet heeft. Zorg ervoor dat de volledige CA-keten zich in de ISE-trustwinkel bevindt. Als de kwestie nog steeds voortduurt nadat het juiste certificaat is geïnstalleerd in de vertrouwde winkel van ISE, voert u pakketopnamen uit en test u de connectiviteit om te zien wat er wordt

verzonden.

Gerelateerde informatie

- Service-to-serviceoproepen met clientreferenties
- Azure - Verificatie vs. autorisatie
- Azure - Quickstart: registreer een toepassing bij het Microsoft Identity Platform
- Azure Active Directory-app-manifest
- Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.