

# Integre o Intune MDM ao Identity Services Engine

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o Microsoft Intune](#)

[Importar os Certificados do Portal do Intune para o Repositório Confiável do ISE](#)

[Implantar o ISE como um Aplicativo no Portal do Azure](#)

[Importar Certificados ISE para o Aplicativo no Azure](#)

[Verificar e solucionar problemas](#)

["Falha na conexão com o servidor" com base em sun.security.validatorException](#)

[Falha ao Adquirir o Token de Autenticação do Azure AD](#)

[Falha ao Adquirir o Token de Autenticação do Azure AD](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como integrar o Intune Mobile Device Management (MDM) com o Cisco Identity Services Engine (ISE).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de serviços MDM no Cisco ISE
- Conhecimento dos Serviços do Microsoft Azure Intune

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine 3.0
- Aplicativo do Microsoft Azure Intune

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

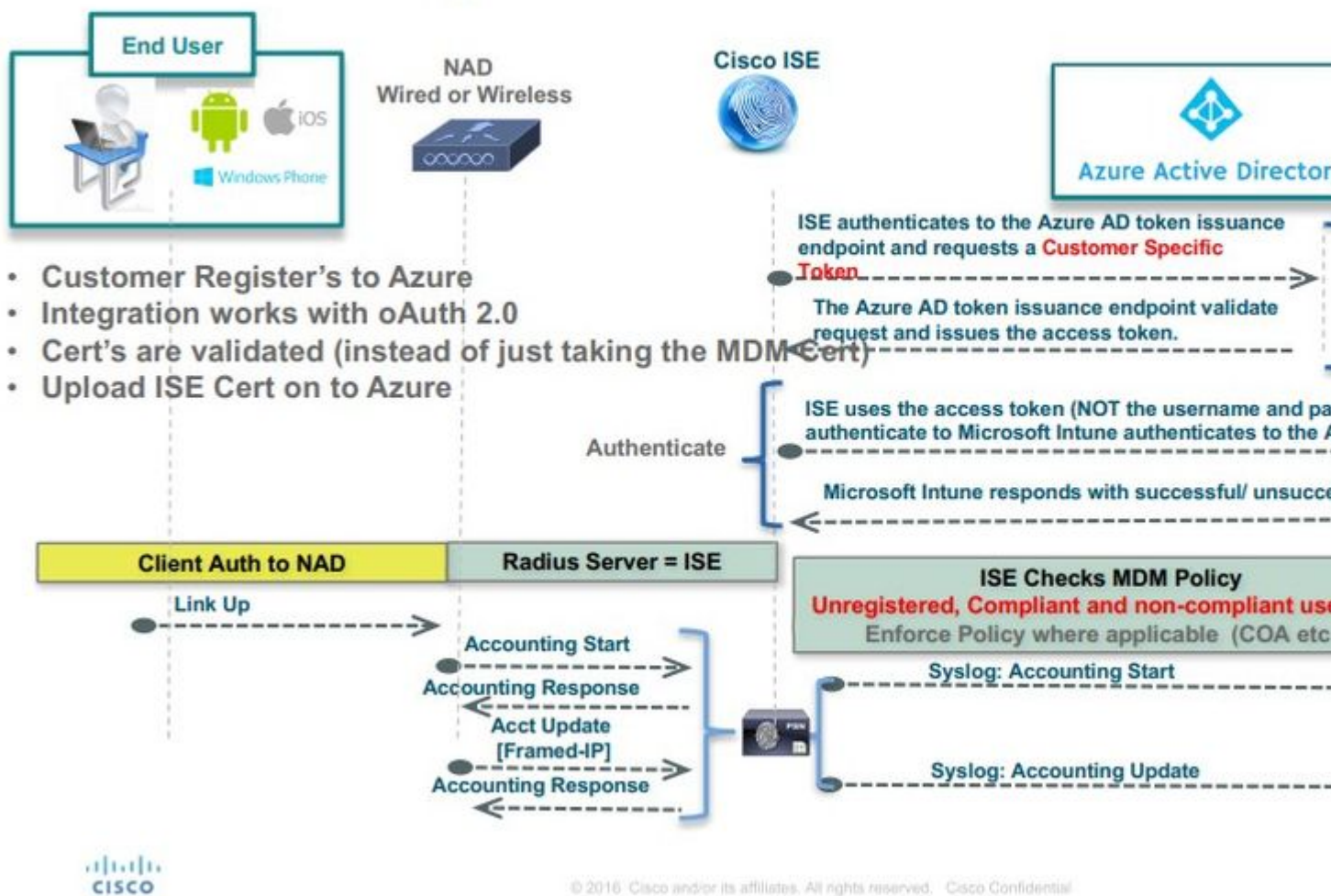
Os servidores MDM protegem, monitoram, gerenciam e dão suporte a dispositivos móveis implantados em

operadoras móveis, provedores de serviços e empresas. Esses servidores atuam como o servidor de políticas que controla o uso de alguns aplicativos em um dispositivo móvel (por exemplo, um aplicativo de e-mail) no ambiente implantado. No entanto, a rede é a única entidade que pode fornecer acesso granular a endpoints com base em Listas de Controle de Acesso (ACLs). O ISE consulta os servidores MDM quanto aos atributos de dispositivo necessários para criar ACLs que fornecem controle de acesso à rede para esses dispositivos. O Cisco ISE integra-se ao Microsoft Intune MDM Server para ajudar as organizações a proteger dados corporativos quando os dispositivos tentam acessar recursos locais.

## Configurar

### Diagrama de Rede

# Intune Integration Architecture



## Configurar o Microsoft Intune

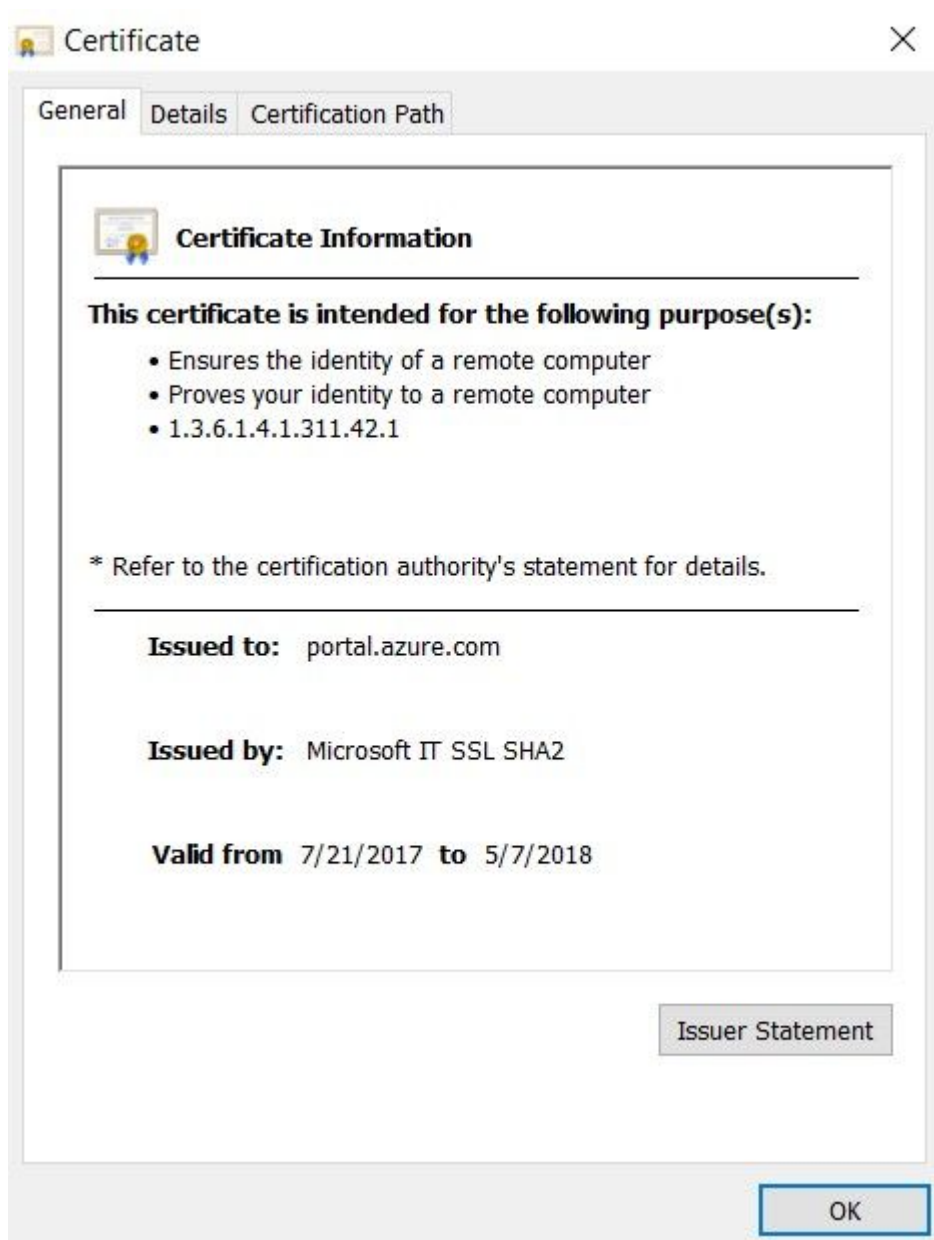
### Importar os Certificados do Portal do Intune para o Repositório Confiável do ISE

Faça login no Console de Administração do Intune ou no console de Administração do Azure, qualquer que seja o site que tenha seu locatário. Use o navegador para obter os detalhes do certificado:

Etapa 1. Abra o Microsoft Azure portal a partir de um navegador da Web.

Etapa 2. Clique no símbolo de bloqueio na barra de ferramentas do navegador e, em seguida, clique em View Certificates.

Etapa 3. Na janela Certificado, clique no botão Certification Path guia. Um exemplo é mostrado abaixo:

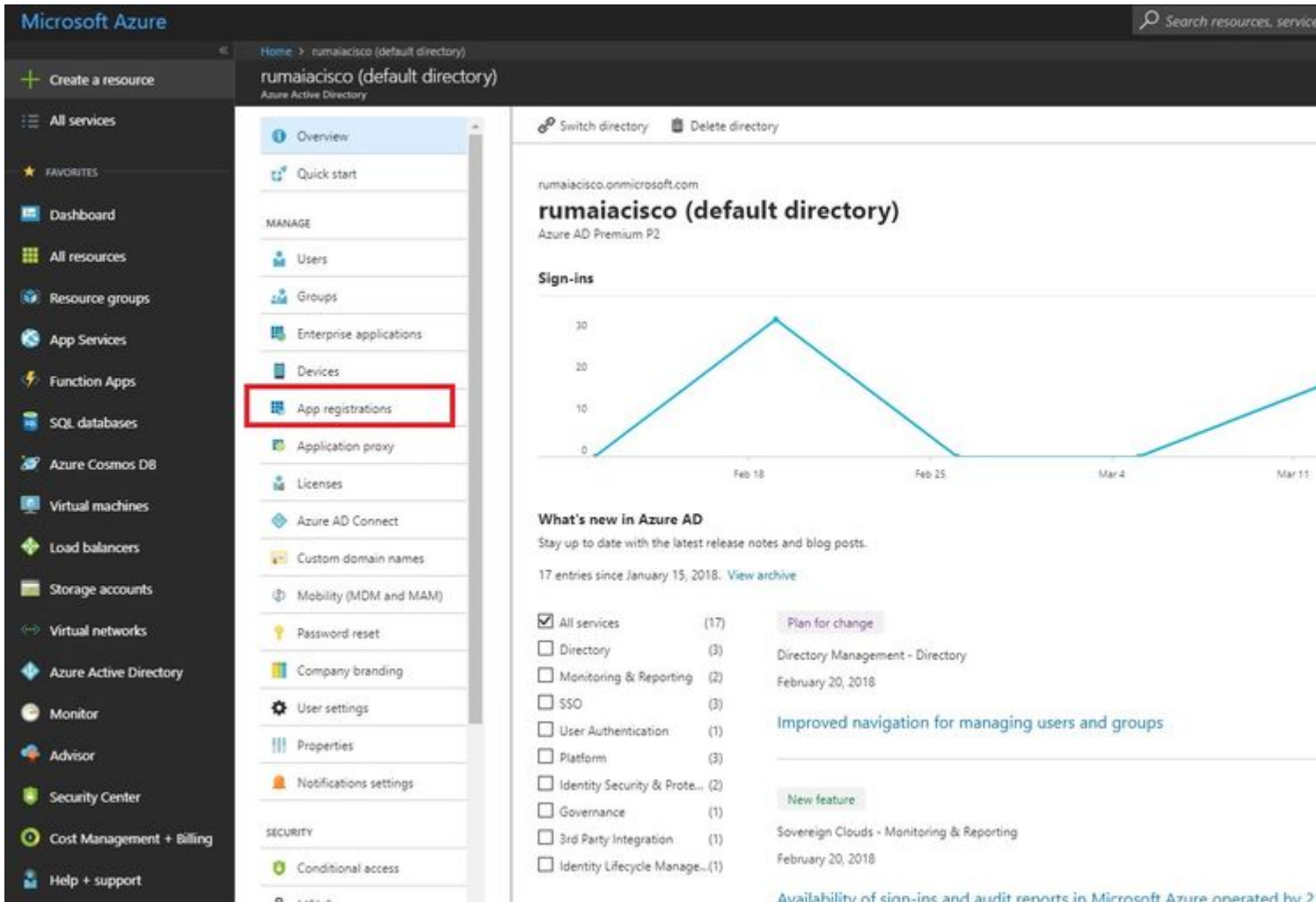


Etapa 4. Localizar Baltimore Cyber Trust root, que é a CA raiz comum. No entanto, se houver outra CA raiz diferente, clique no certificado dessa CA raiz. Na guia Details (Detalhes) desse certificado de CA raiz, você pode copiá-lo para o arquivo e salvá-lo como certificado BASE64.

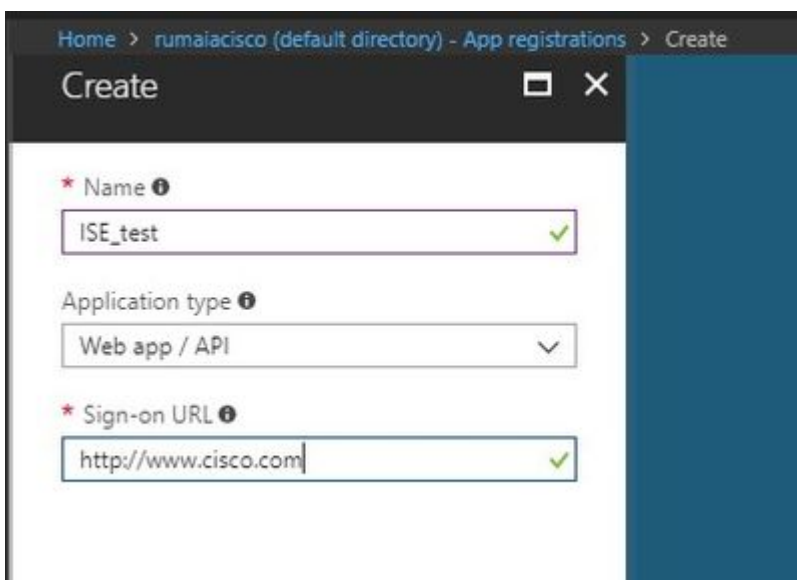
Etapa 5. No ISE, navegue até Administration > System > Certificates > Trusted Certificates e importe o certificado raiz que acabou de ser salvo. Dar ao certificado um nome significativo, como Azure MDM. Repita também o procedimento para os certificados CA intermediários.

## Implantar o ISE como um Aplicativo no Portal do Azure

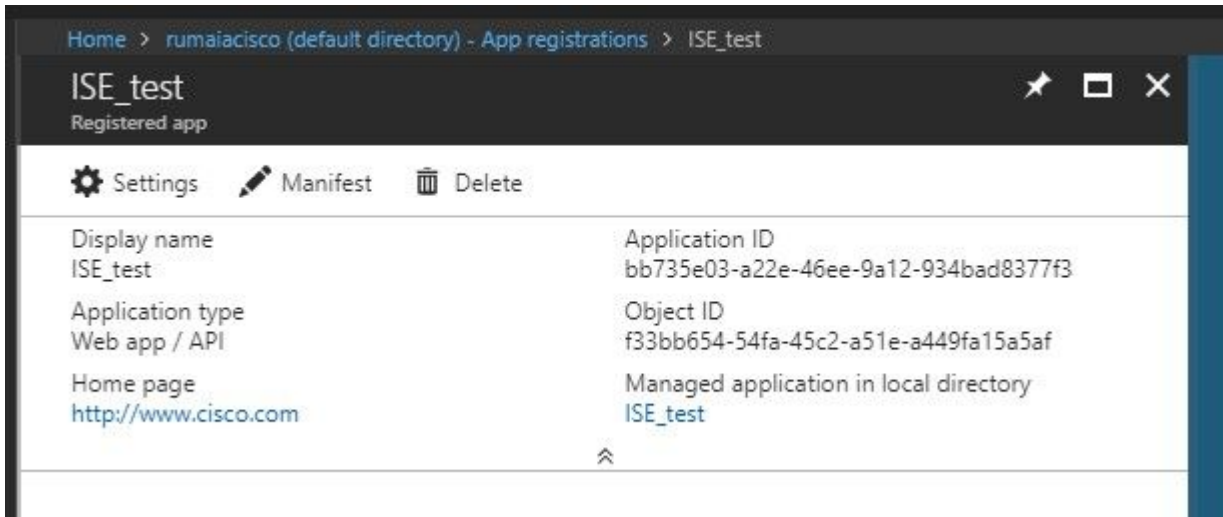
Etapa 1. Navegue até a página Azure Active Directory e escolher App registrations.



Etapa 2. No App registrations, crie um novo registro de aplicativo com o nome ISE. Clique em Create como mostrado nesta imagem.



Etapa 3. Escolher Settings para editar o aplicativo e adicionar os componentes necessários.



Etapa 4. Sob Settings, escolha as permissões necessárias e aplique estas opções:

#### 1. Microsoft Graph

- Permissões de Aplicativo
  - Ler dados do diretório
- Permissões delegadas
  - Leia a Configuração e as Políticas de Dispositivo do Microsoft Intune
  - Leia a Configuração do Microsoft Intune
  - Entrar usuários
  - Acessar os dados do usuário a qualquer momento

#### 2. API do Microsoft Intune

- Permissões de Aplicativo
  - Obter informações de estado e conformidade do dispositivo do Microsoft Intune

#### 3. Ative Directory do Microsoft Azure

- Permissões de Aplicativo
  - Ler dados do diretório
- Permissões delegadas
  - Ler dados do diretório
  - Entre e leia o perfil do usuário

O resultado da configuração é semelhante ao mostrado aqui :

+ 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



## Required permissions

🔍 Filter settings

### GENERAL

📄 Properties >

🔗 Reply URLs >

👤 Owners >

### API ACCESS

🌐 Required permissions >

🔑 Keys >

### TROUBLESHOOTING + SUPPORT

🛠 Troubleshoot >

👤 New support request >

+ Add ↻ Grant Permissions

### API

### APPLICATION PERMI

Microsoft Graph 1

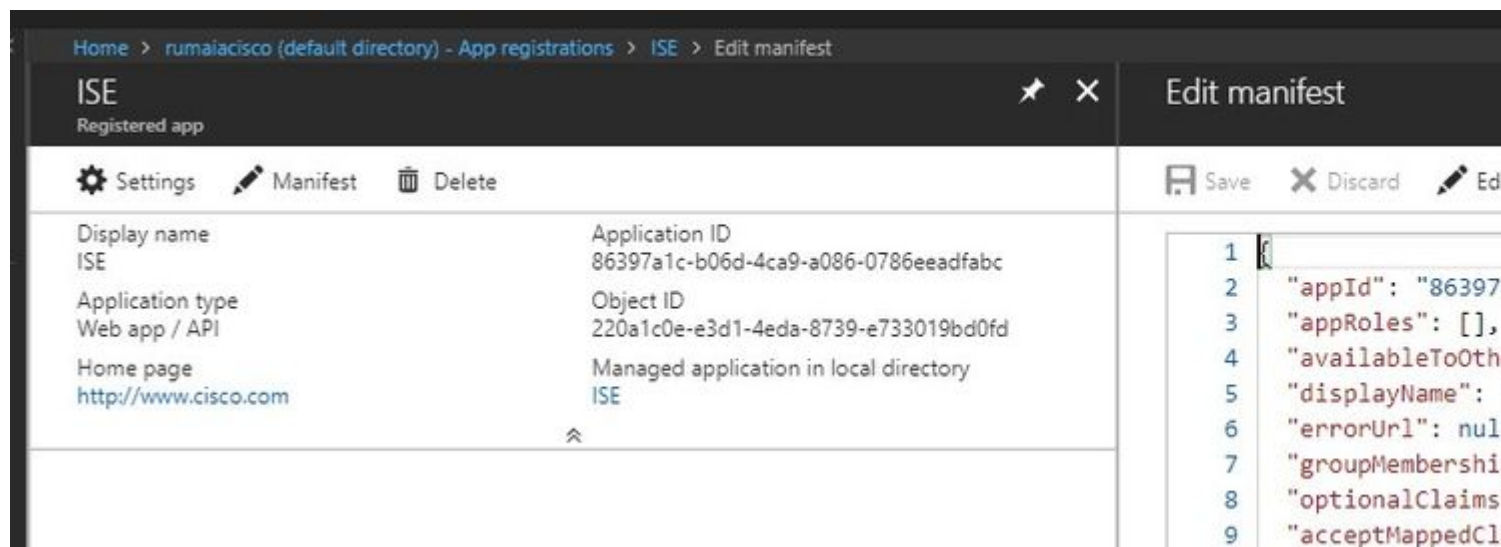
Microsoft Intune API 1

Windows Azure Active Directory 1

Etapa 5. Clique em **Grant Permissions** para confirmar todas as permissões do aplicativo. Esse processo leva de 5 a 10 minutos para entrar em vigor. Edite o **Azure Manifest** para o aplicativo criado para importar certificados internos de CA do ISE.

## Importar Certificados ISE para o Aplicativo no Azure

Etapa 1. Baixe o arquivo de manifesto do aplicativo.



**Observação:** é um arquivo com uma extensão JSON. Não edite o nome do arquivo ou a extensão, caso contrário, haverá falha.

Etapa 2. Exporte o certificado do sistema ISE de todos os nós. No PAN, navegue até **Administration > System > Certificates > System Certificates**, escolha o certificado de servidor autoassinado padrão e clique em **Export**. Escolher **Export Certificate Only** (padrão) e escolha um local para salvá-lo. Exclua as marcas **BEGIN** e **END** do certificado e copie o restante do texto como uma única linha. Isso se aplica às versões anteriores a junho de 2020 descritas na seção **Opção legada**.

# Administration > Certificates > System Certificates

## System Certificates ⚠ For disaster recovery it is recom



[Edit](#) [Generate Self Signed Certificate](#) [Import](#)

Friendly Name	Used By	Porta
ise-1		
<input checked="" type="checkbox"/> ise-1.demo.local#Certificate Services Endpoint Sub C A - ise-1#00001	EAP Authentication, Admin, Portal, pxGrid	Defau Group



```
-----BEGIN CERTIFICATE-----
MIIE9jCCAt6gAwIBAgIQPffz/HZnjzsvArIAGaRr/sojANSgkqkxiU9wbaqerAUAU
MTUwMwYDVQQDDCkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkz
LSBpc2UzMTAeFw0xNjAzMDMxODA4MTlaFw0xODAzMDQxNzEzZDQzODkzODkzODkzODkz
BAMzEzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkz
AoIBAQCXfuGnVhgPqA9vqO/nwJ251t688oObRlyN21ThkrStpqF+GwFm1ZcM/x5L
fQ1MIQMNqoymSeKEKLQNdEEqrX+a2/SK//D/R6xYxBGFiqEfc66t1RbHXBpP4
S/tQzLrLkmlxhtF+IVwr20GGfGytq92eEMNe2vB89G1E4100+rDe3WBgfdnidWcm
28g9+r6582Lz/WOKQ3b3Pw1BPSXdlvwXhyLLAcVn1BqdBOnEDB3tDecUAQ1FKGB
MowSY1DUa2fL8lINt8diVi4cViFQBeNnEuz54HMLuorXPvR32NtQieMaxjIBgk2
xocL/EtgHn2vCe0DUvJYVG2ReIavAgMBAAGjggEYMIIBFDafBgNVHREBAf8EFTAT
gRE2Ni01NS00NC0zMy0yMi0xMTAqBgkrBgEEAQkVAQUENQbcHhMclKX0N1cnRp
ZmljYXRlX1R1bXBzYXR1MGYGA1UdIwRlMF2AFF3AocqVpMKVtTM6rfEhf0peo1JJE
o7OkMTAVMSowKwYDVQQDDCkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkzODkz
aXNLLTGCeHw3dLtkGkVan2opG9kBEywwHQYDVROBBYEFH3VrVTDGguKiCnbg1N
Oym7w08RMA4GA1UdDwEB/wQEAwIF4DAgBgNVHSUBAf8EFjAUBgggrBgEFBQcDAQYI
KwYBBQUHAwIwDAYDVROTAQH/BAIwADANBgkqhkiG9w0BAQEFAAOCAgEAnmsImaDi
34ihIMXjtrrh9OzjQwOSPk+EqIYeI2Au5ACLxEgGdadrQbLP4MePlgMhXAfg+Xewt
HtuJ+AQXO63KD2UhLLR7RAM5Pe6UZy9Oqa8a37HjHGF75Wa8i4aT3Atnd7peQEML
jDeFb+6RVYjzBEMAnMs+rWGJV0NBjqlEJgJw7h00Cq+oQmzLHzRlswquu5szv
ukkyJfsLWLkzEB2kNRis7jgtOOjYQLiUe2peJprvkQn3+/JwcuUa0RQeJGtabPR
DYoRqtevQanJaNqSiFBC2ta5AyVrctDaujkbDi1zJG3zWVwOt6H1oGcQqBzWz20
ThDTm+BRfeYnhuQWQy82e8S/tWJWwq/9c81PxcWp2+LxHHTv6XJg0myMPWwC0e
dQ+6qCANJTFJcYusEzJD+xEzv3pgxkvwDB14iHOKtF6Y7v5piDKeIFGuR1luIatI
q/y+heUQTuKvYyFq20dDKHCiCivEapp3B8ezSvFXSE2PMBTAac24xUMDpH4W2nj
gL254nHTJ0Fc04szQyWaaflJ1H9Ua3/ObQy22pPd3IUxzC33xvvpjcp1T3w0AjK
WqMeg18NGR1Lr6taQf10Un690nk529BYtFenJ+UT/goFUESoJHPy18QI+XHW+yft
DJqgtR8gV6xuVYoZGktTfomD2e-----
-----END CERTIFICATE-----
```

Delete this line

Delete this line

### Things to do with the ISE Sys

- Delete the -----BEGIN CERT
- Delete the -----END CERTIF
- All the text should be in sing

MIIE9jCCAt6gAwIBAgIQPffz/HZnjzsvArIAGaRr/sojANSgkqkxiU9wbaqerAUAU



A partir de junho de 2020, o Portal permite que você carregue certificados diretamente.

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

Home > self | App registrations >

### ISE | Certificates & secrets

Search (Cmd+)

- 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

[Upload certificate](#)

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



Opção herdada:

Etapa 1. Execute um procedimento do PowerShell para transformar o certificado em BASE64 e importá-lo corretamente para o arquivo de manifesto JSON do Azure. Use o aplicativo Windows PowerShell ou Windows PowerShell ISE do Windows. Use estes comandos:

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

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

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

Etapa 2. Manter os valores para \$base64Thumbprint, \$base64Value,e \$keyid, que serão usados na próxima etapa. Todos esses valores são adicionados ao campo JSON keyCredentials já que, por padrão, ele se parece com isto:

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

Para fazer isso, certifique-se de usar os valores nesta ordem:

```
"keyCredentials": [
  {
    "customKeyIdentifier": "â€œ$base64Thumbprint_from_powerShell_for_PPANâ€",
    "keyId": "â€œ$keyid_from_above_PPANâ€",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": "Base64 Encoded String of ISE PPAN cert"
  },
  {
    "customKeyIdentifier": "â€œ$base64Thumbprint_from_powerShell_for_SPANâ€",
    "keyId": "â€œ$keyid_from_above_SPANâ€",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
```

```
"value": "Base64 Encoded String of ISE SPAN cert"
}
],
```

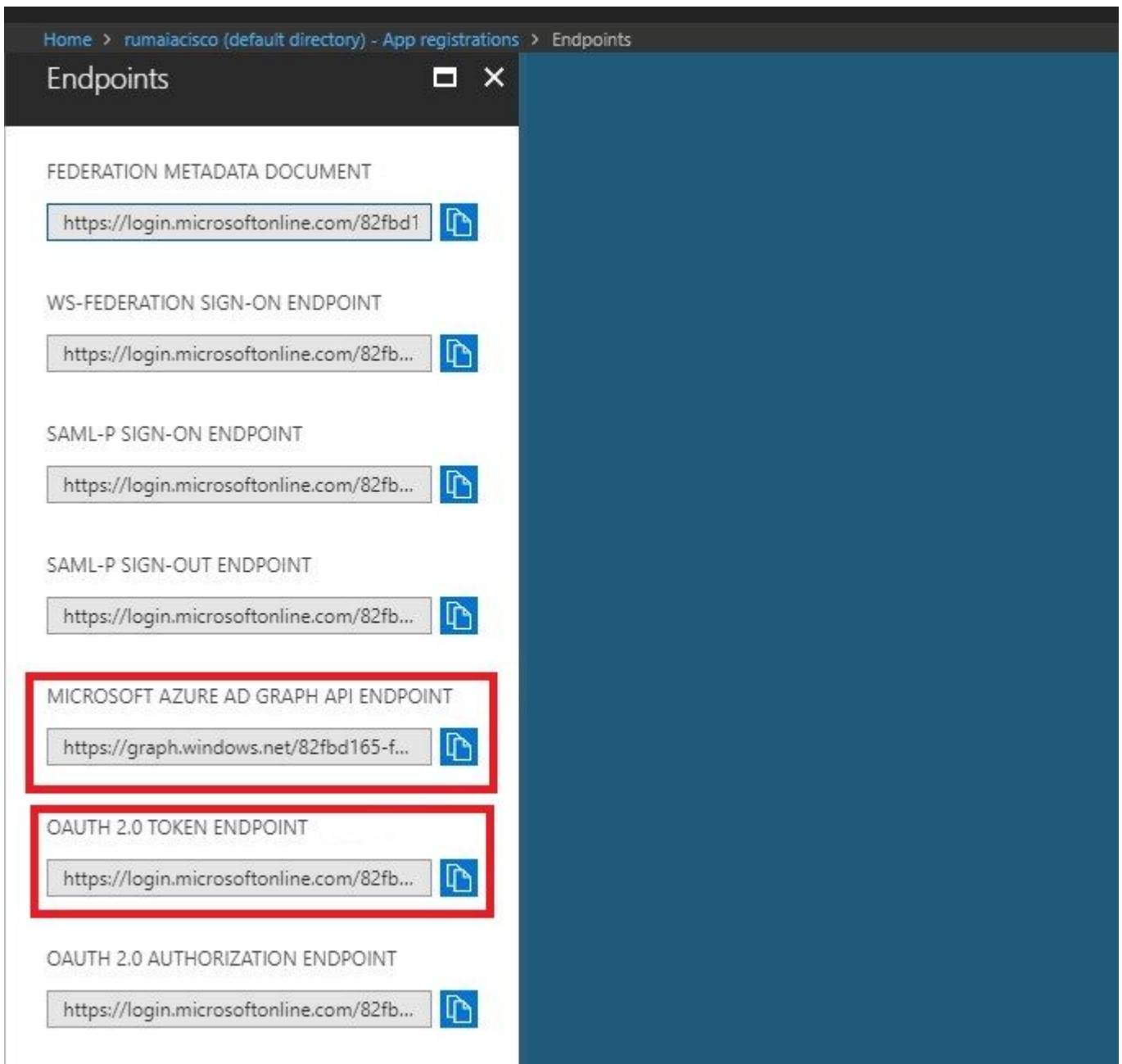
Etapa 3. Carregar o arquivo JSON para o Portal do Azure para validar o keyCredentials dos certificados usados no ISE.

Ele deve ser semelhante a:

```
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": "GM1Dp/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    },
46  ],
```

Etapa 4. Esteja ciente de que, após o upload, o value sob keyCredentials mostra null pois isso é imposto pelo lado da Microsoft para não permitir que esses valores sejam vistos após o primeiro carregamento.

Os valores necessários para adicionar o servidor MDM no ISE podem ser copiados de Microsoft Azure AD Graph API Endpoint e OAUTH 2.0 Token Endpoint.



Esses valores devem ser inseridos na GUI do ISE. Navegue até Administration > Network Resources > External MDM e adicionar um novo servidor:

ISE	Intune
URL de descoberta automática	Pontos de Extremidade > Ponto de Extremidade da API do Microsoft Azure AD Graph
ID do cliente	{Registered-App-Name} > ID do Aplicativo
URL de Emissão de Token	Pontos de Extremidade > Ponto de Extremidade de Token OAuth 2.0

Name *	<input type="text" value="Intune"/>
Server Type	Mobile Device Manager <span>ⓘ</span>
Authentication Type	OAuth - Client Credentials <span>ⓘ</span>
Auto Discovery	Yes <span>ⓘ</span>
Auto Discovery URL *	<input type="text" value="https://graph.windows.net/82fbd165-f323-4a38-aeb8-734056d25101"/> ⓘ
Client ID *	<input type="text" value="86397a1c-b06d-4ca9-a086-0786eeadfab"/>
Token Issuing URL *	<input type="text" value="https://login.microsoftonline.com/82fbd165-f323-4a38-aeb8-734056d25101/oauth2/1"/> ⓘ
Token Audience *	<input type="text" value="https://api.manage.microsoft.com/"/>
Description	<input type="text"/>
Polling Interval *	<input type="text" value="240"/> (minutes) ⓘ
Status	Enabled <span>▼</span>

[Test Connection](#)

[Cancel](#) [Save](#)

Depois que a configuração for concluída, o status mostrará enabled (habilitado).

#### MDM Servers

Refresh + Add Duplicate Edit Trash

Name	Status	Service Provider	MDM Server	Server Type	Description
Intune	Enabled	Microsoft	fef.msub03.manage.microsoft.com	Mobile Device Manager	

## Verificar e solucionar problemas

"Falha na conexão com o servidor" com base em `sun.security.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.

Etapa 1. Colete o pacote de suporte com estes logs no nível TRACE:

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

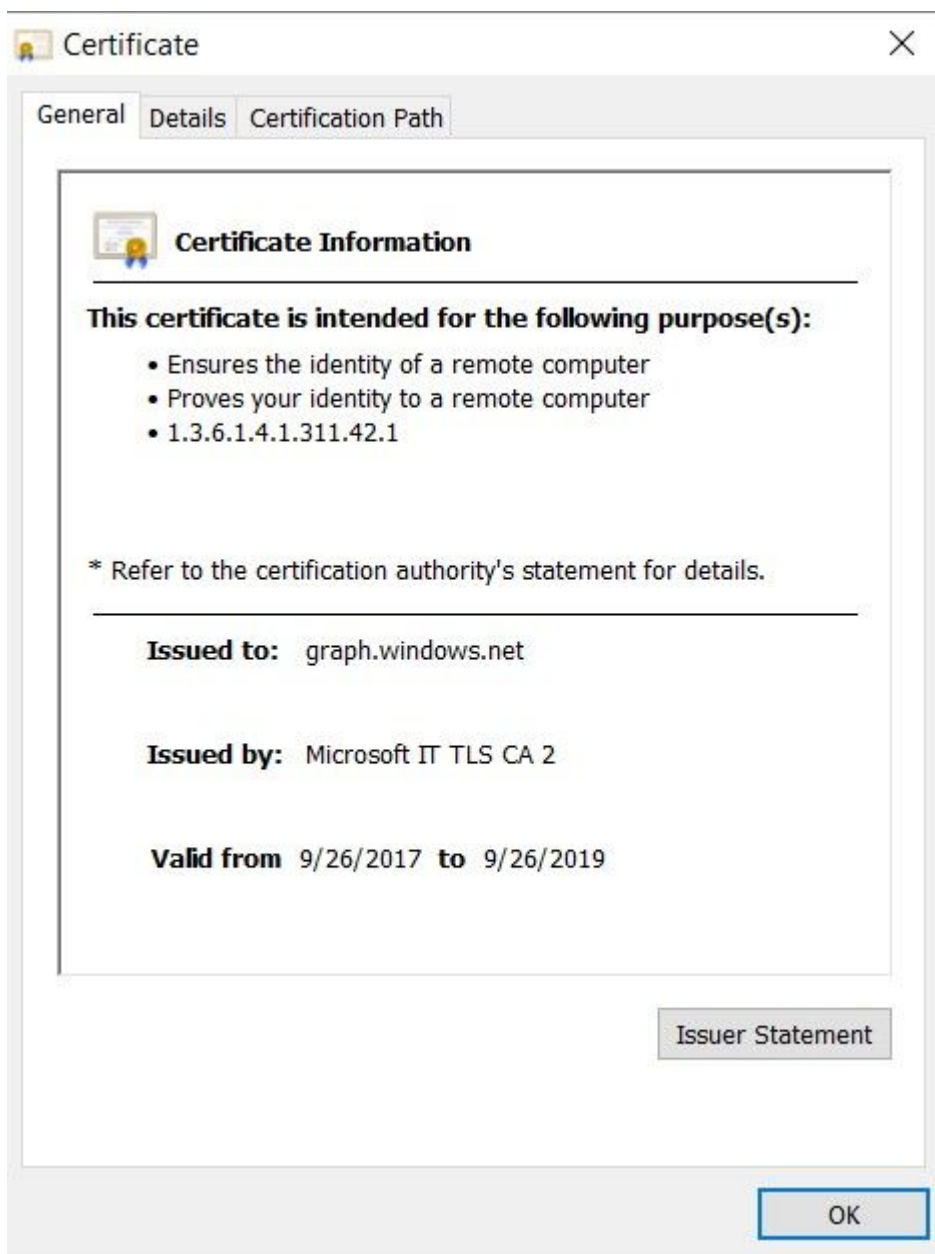
Etapa 2. Verificar ise-psc.log para estes logs:

- 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

Isso indica que há necessidade de importar o [graph.microsoft.com](https://graph.microsoft.com) presente nesta página.

```
Secure | https://graph.windows.net
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<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>
```

Etapa 3. Clique no botão locker e verifique os detalhes do certificado.



Etapa 4. Salve-o em um arquivo no formato BASE64 e importe-o para o ISE Trusted Store. Certifique-se de importar a cadeia completa de certificados. Depois disso, teste a conexão com o servidor MDM novamente.

### Falha ao Adquirir o Token de Autenticação do Azure AD



Connection to server failed with:

Failed to acquire auth token from Azure AD. Error validating credentials. Client assertion signature. [Reason - The key was not found., Thumbprint of key used by client: '105D6E9BA0F5D6EACCF8A562DE81C1C6450CBEE4', Configured keys: [Key0:Start=03/14/2018, End=12/17/2018, Thumbprint=pZ0CqV either ISE certificates not being uploaded or problem with certificates already uplo

Please try with different settings.

Geralmente, esse erro ocorre quando o manifesto JSON contém a cadeia de certificados ISE incorreta. Antes de carregar o arquivo de manifesto para o Azure, verifique se pelo menos esta configuração está presente:

```
"keyCredentials": [
  {
    "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN",
    "keyId": "$keyid_from_above_PPAN",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": "Base64 Encoded String of ISE PPAN cert"
  },
  {
    "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_SPAN",
    "keyId": "$keyid_from_above_SPAN",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": "Base64 Encoded String of ISE SPAN cert"
  }
],
```

O exemplo anterior é baseado em um cenário em que há um PAN e uma SAN. Execute os scripts do PowerShell novamente e importe os valores BASE64 apropriados. Tente carregar o arquivo de manifesto e você não deve enfrentar nenhum erro.

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
```

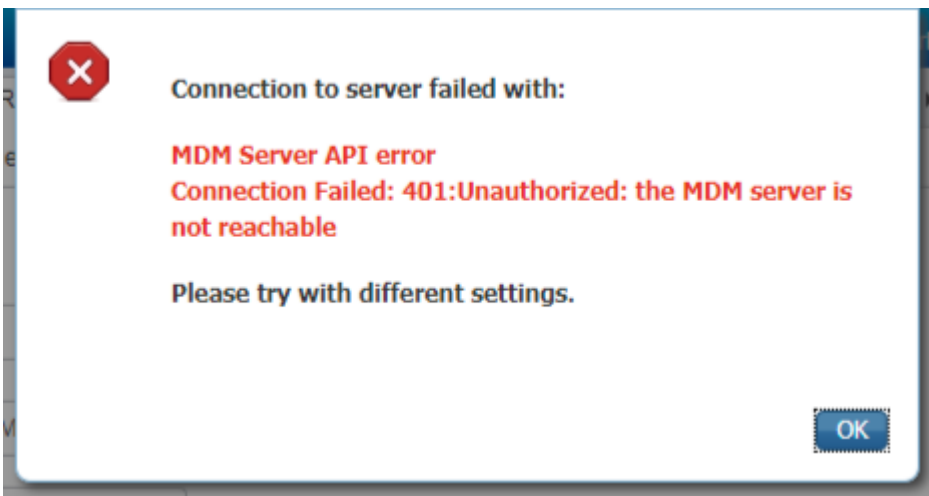
```
$cer.Import(â€œmycer.cerâ€œ)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

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

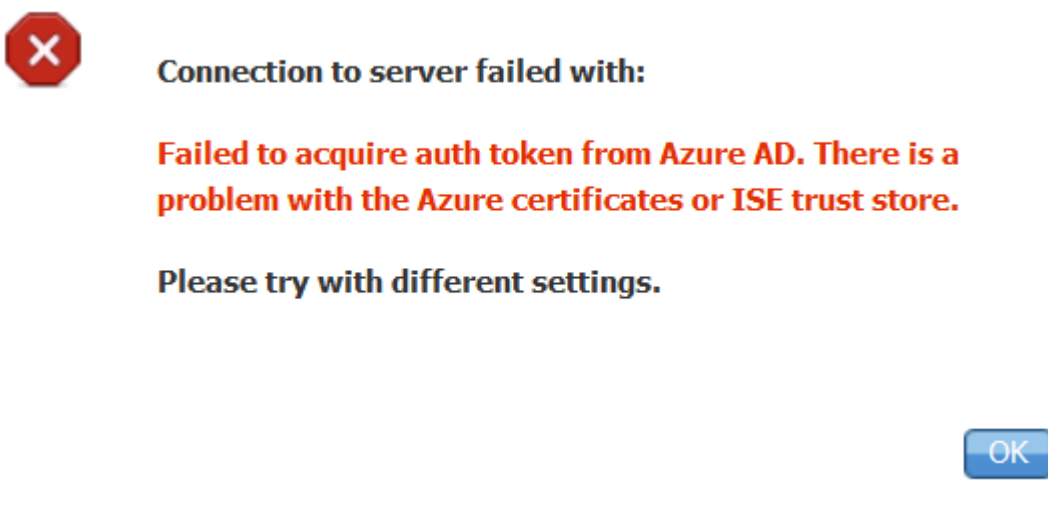
$keyid = [System.Guid]::NewGuid().ToString()
```

Lembre-se de aplicar os valores para \$base64Thumbprint, \$base64Value e \$keyid conforme mencionado nas etapas da seção Configurar.

## Falha ao Adquirir o Token de Autenticação do Azure AD



Geralmente, esse erro ocorre quando as permissões certas não são concedidas ao aplicativo do Azure no portal.azure.com. Verifique se o aplicativo tem os atributos corretos e certifique-se de clicar em Grant Permissions após cada alteração.



Essa mensagem ocorre quando o ISE tenta acessar a URL de emissão de token e retorna um certificado que o ISE não oferece. Verifique se toda a cadeia de CA está no armazenamento confiável do ISE. Se o problema ainda persistir após a instalação do certificado correto no armazenamento confiável do ISE, execute capturas de pacotes e teste a conectividade para ver o que está sendo enviado.



## Informações Relacionadas

- [Chamadas de Serviço para Serviço Usando Credenciais de Cliente](#)
- [Azure - Autenticação vs. autorização](#)
- [Azure - Quickstart: Registrar um aplicativo com a plataforma de identidade da Microsoft](#)
- [Manifesto de aplicativo do Azure Active Directory](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.