将Intune MDM与身份服务引擎集成

目录

简介

本文档介绍如何将Intune移动设备管理(MDM)与思科身份服务引擎(ISE)集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE中的MDM服务知识
- 了解Microsoft Azure Intune服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎3.0
- Microsoft Azure Intune应用程序

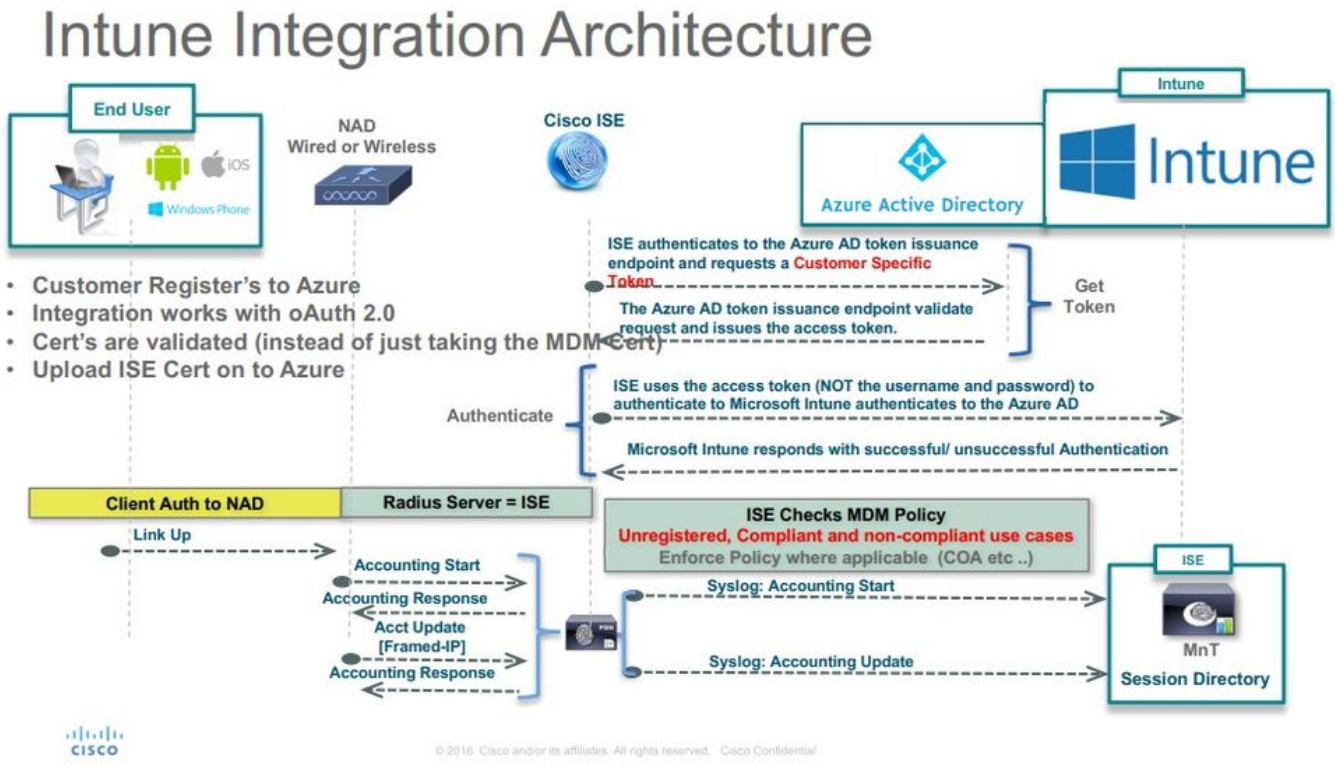
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

MDM服务器可保护、监控、管理和支持跨移动运营商、服务提供商和企业部署的移动设备。这些服务器充当策略服务器，控制部署环境中移动设备上的某些应用（例如电子邮件应用）的使用。但是，网络是唯一能够根据访问控制列表(ACL)提供对终端的精细访问的实体。ISE查询MDM服务器以获取必要的设备属性，以便创建为这些设备提供网络访问控制的ACL。思科ISE与Microsoft Intune MDM服务器集成，以便在设备尝试访问本地资源时帮助组织保护企业数据。

配置

网络图



配置Microsoft Intune

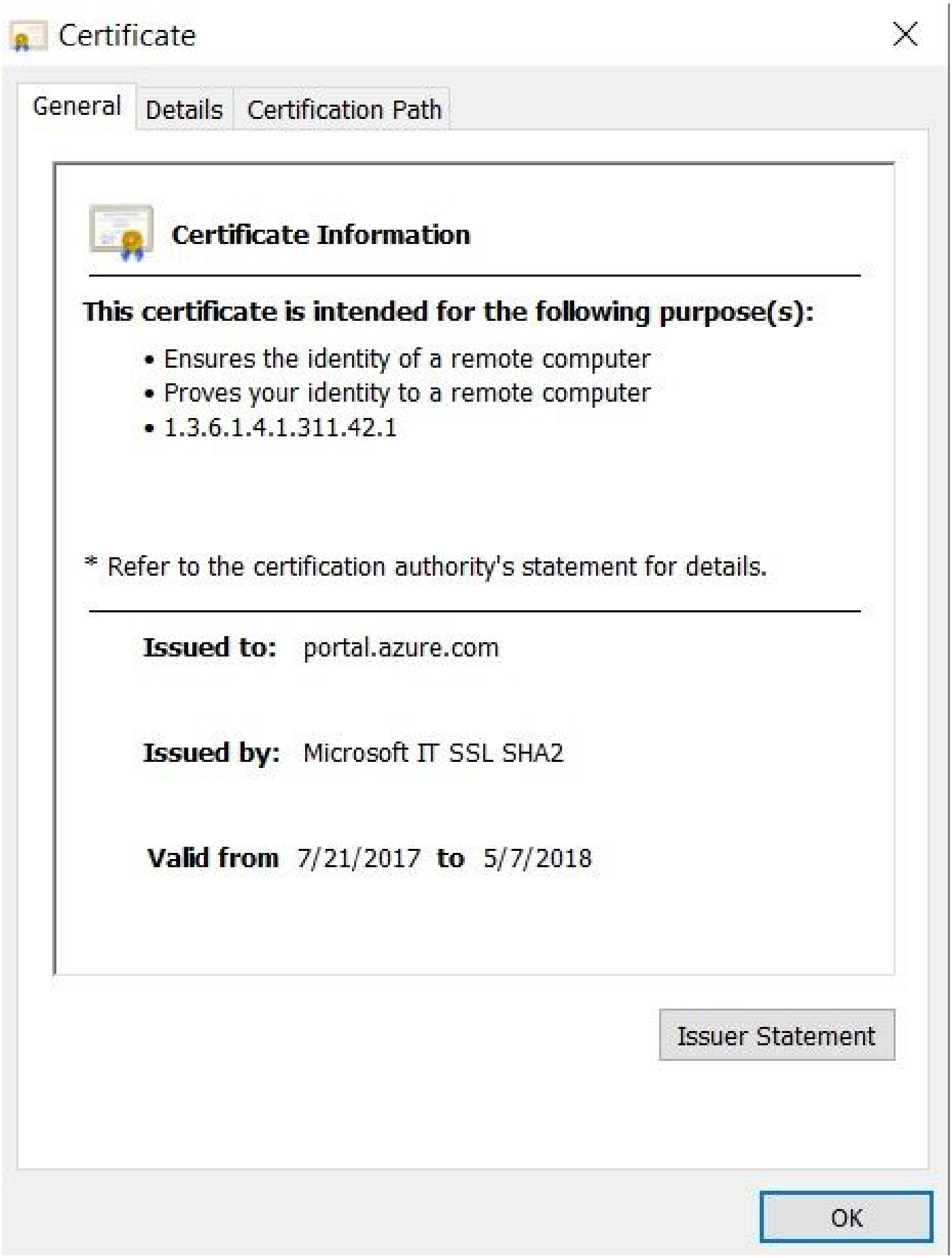
将证书从Intune门户导入到ISE受信任库

登录到Intune管理控制台或Azure管理控制台，无论哪个网站有你的租户。使用浏览器获取证书详细信息：

步骤1:打开 Microsoft Azure portal 从Web浏览器。

第二步：单击浏览器工具栏中的锁定符号，然后单击 View Certificates.

第三步：在Certificate（证书）窗口中，单击 Certification Path 选项卡。示例如下所示：



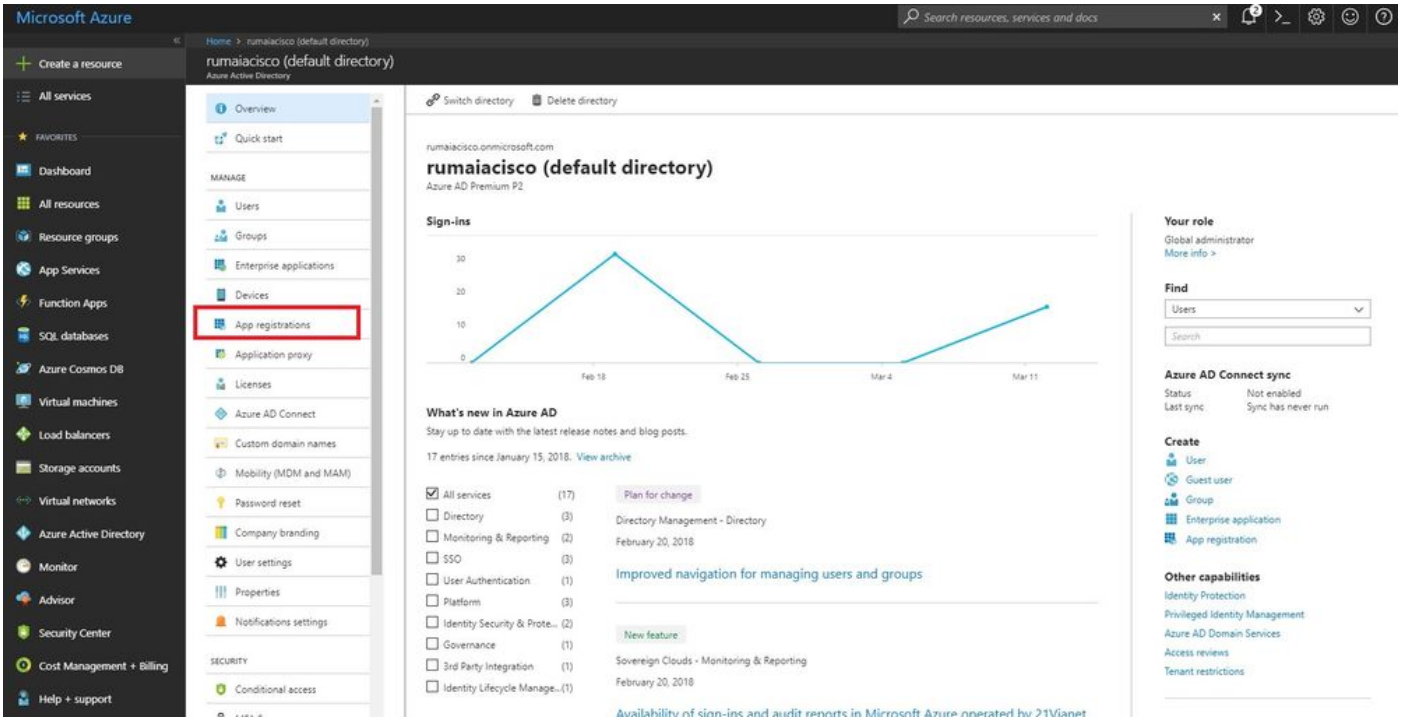
第四步：查找 Baltimore Cyber Trust root，这是通常的根CA。但是，如果存在任何其他不同的根CA，请点击该根CA证书。在该根CA证书的Details（详细信息）选项卡上，可以将其复制到文件并将其另存

为BASE64证书。

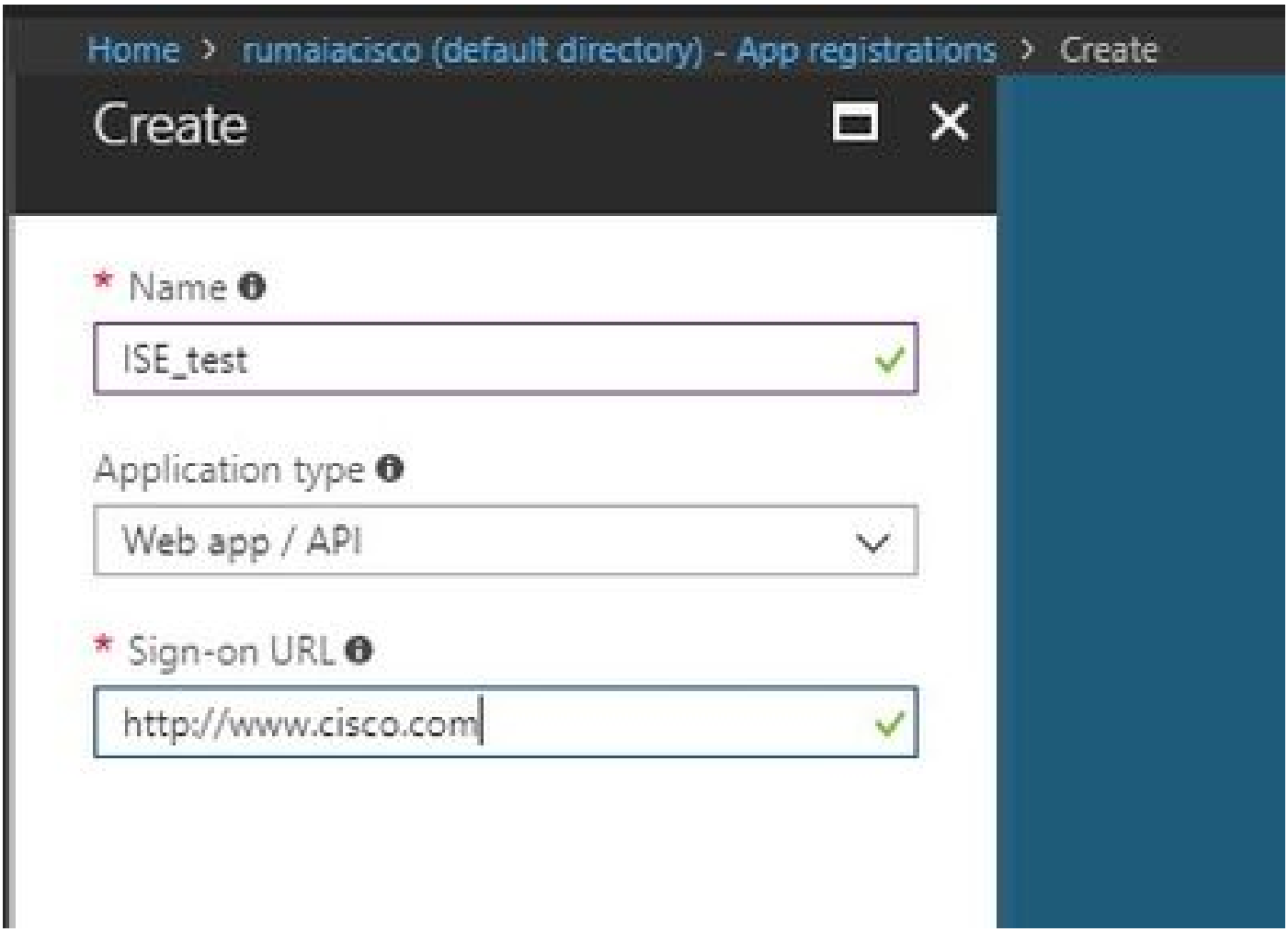
第五步：在ISE中，导航至 Administration > System > Certificates > Trusted Certificates ，并导入刚保存的根证书。为证书指定一个有意义的名称，例如 Azure MDM.对中间CA证书也重复此过程。

在Azure门户中将ISE部署为应用程序

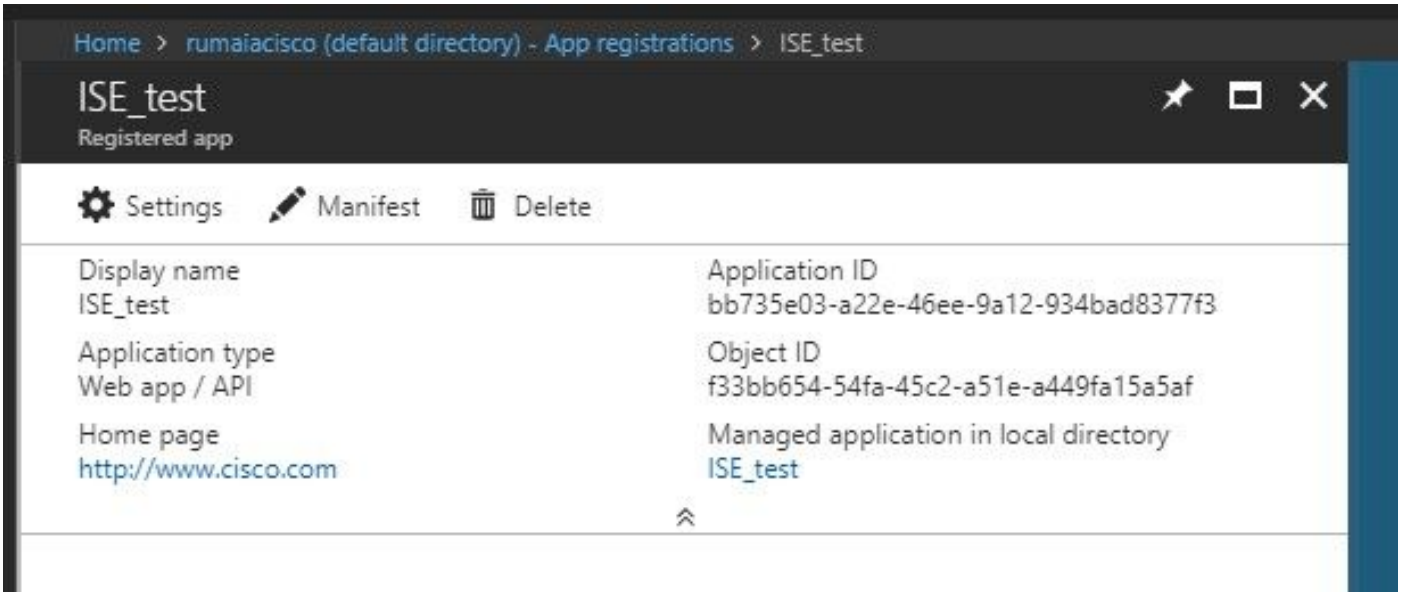
步骤1:导航至 Azure Active Directory 选择 App registrations.



第二步：如果 App registrations ，使用ISE名称创建新的应用注册。点击 Create 如本图所示。



第三步：选择 Settings 以编辑应用程序并添加所需的组件。



第四步：低于 Settings，选择所需的权限，并应用以下选项：

1. Microsoft图形
    - 应用程序权限
        - 读取目录数据

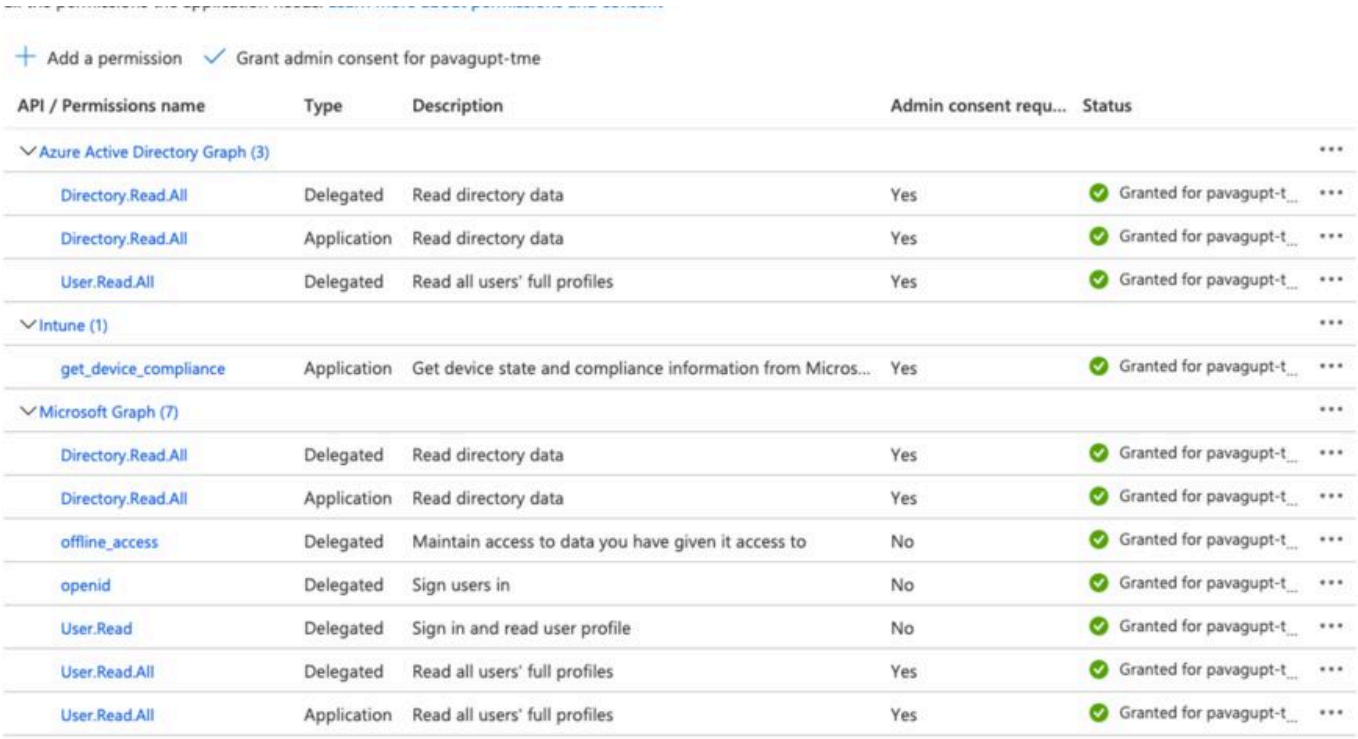
- 授权的权限
  - 阅读Microsoft Intune设备配置和策略
  - 阅读Microsoft Intune配置
  - 登录用户
  - 随时访问用户数据

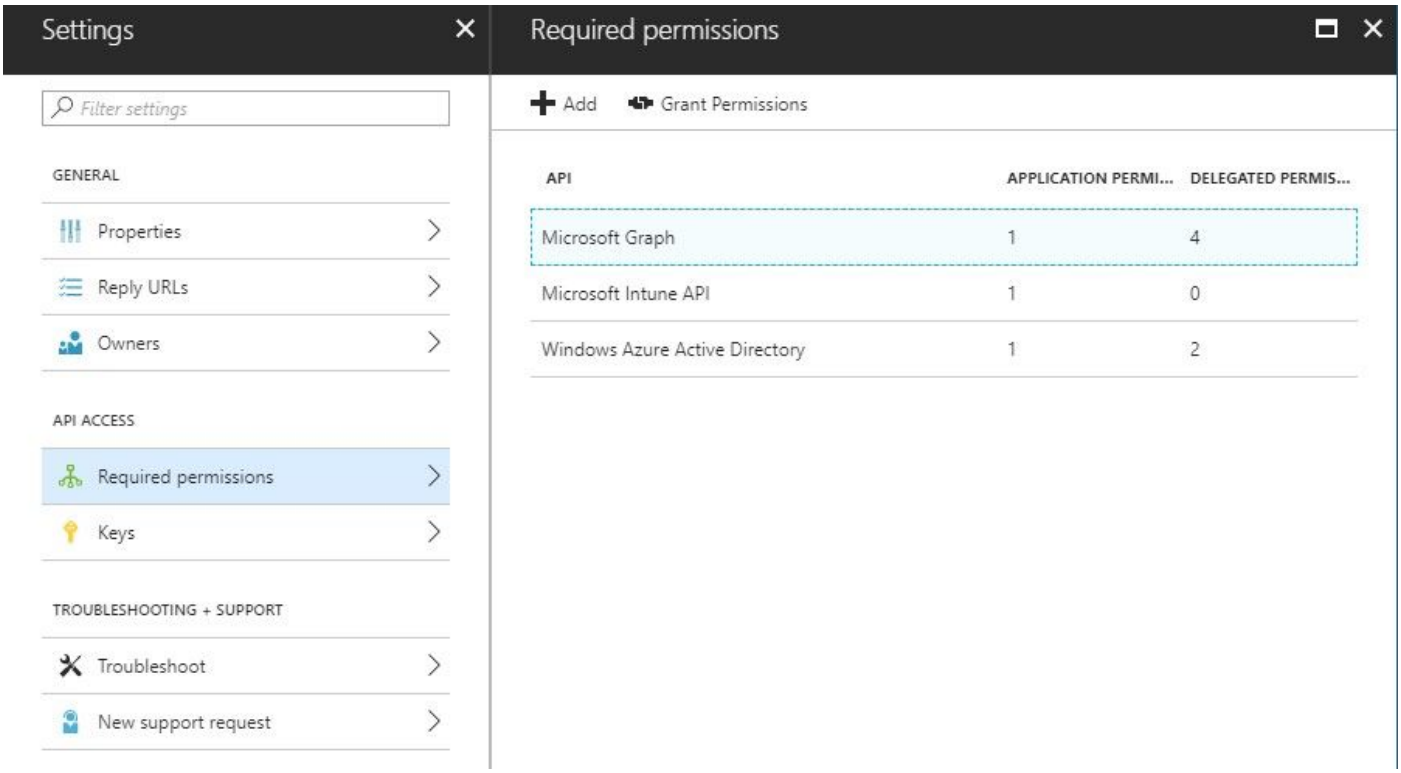
2. Microsoft Intune API
   - 应用程序权限
     - 从Microsoft Intune获取设备状态和合规性信息

3. Windows Azure Active Directory
   - 应用程序权限
     - 读取目录数据

   - 授权的权限
     - 读取目录数据
     - 登录并读取用户配置文件

配置结果类似于如下所示的内容：

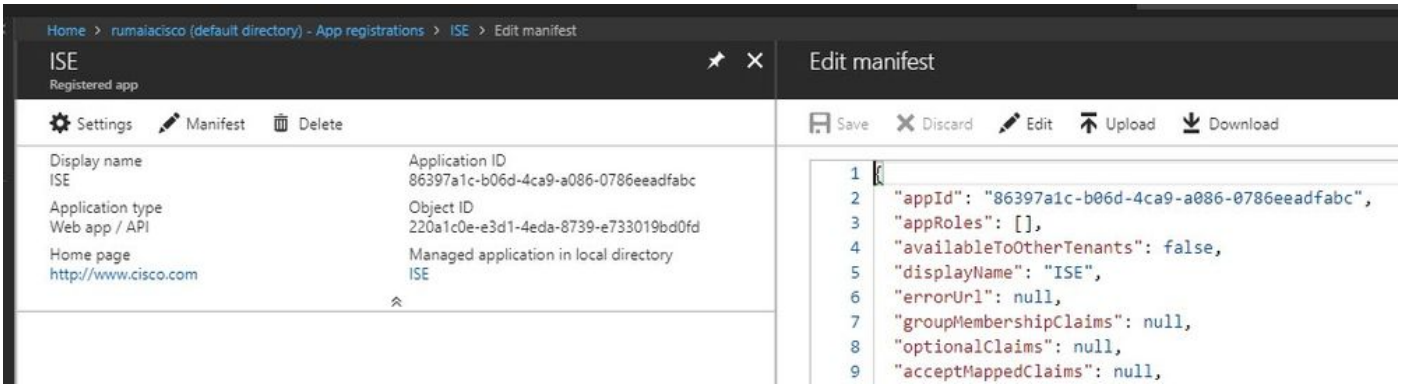




第五步：点击 Grant Permissions 以确认所有应用程序权限。此过程需要5-10分钟才能生效。编辑 Azure Manifest 为导入内部ISE CA证书创建的应用创建的文件。

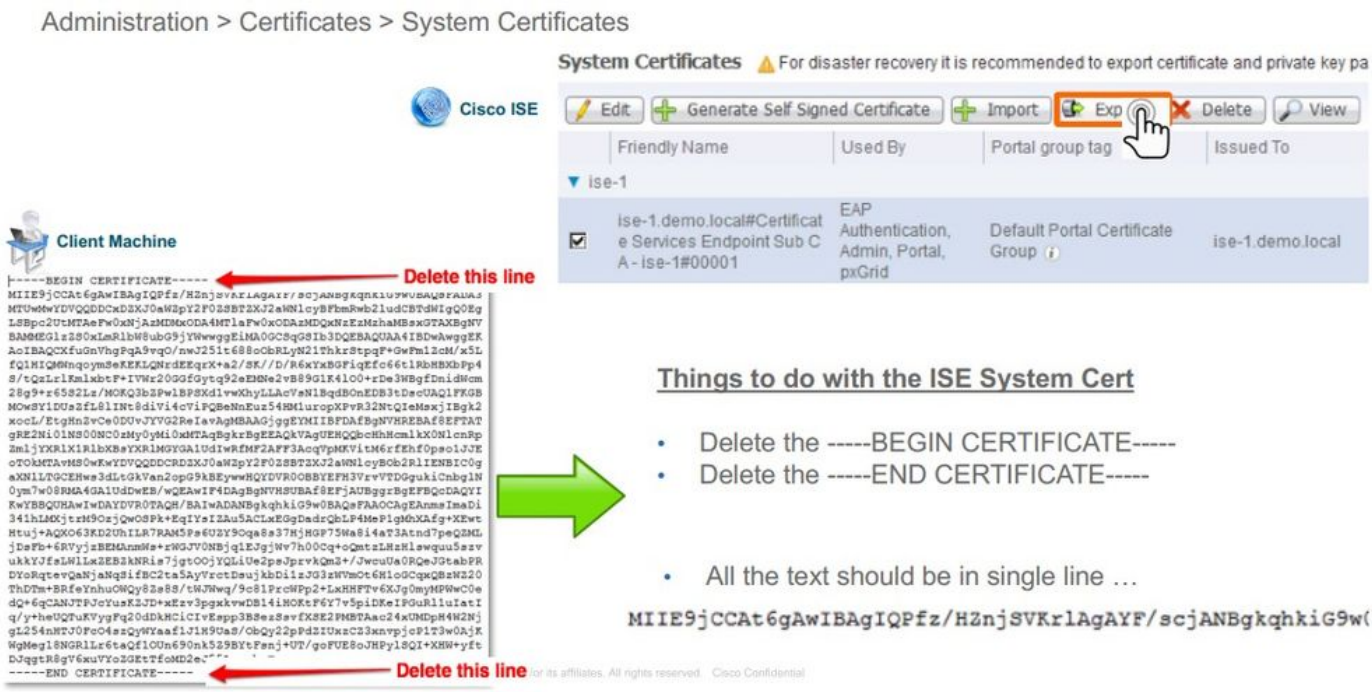
将ISE证书导入Azure中的应用程序

步骤1:下载应用程序的清单文件。

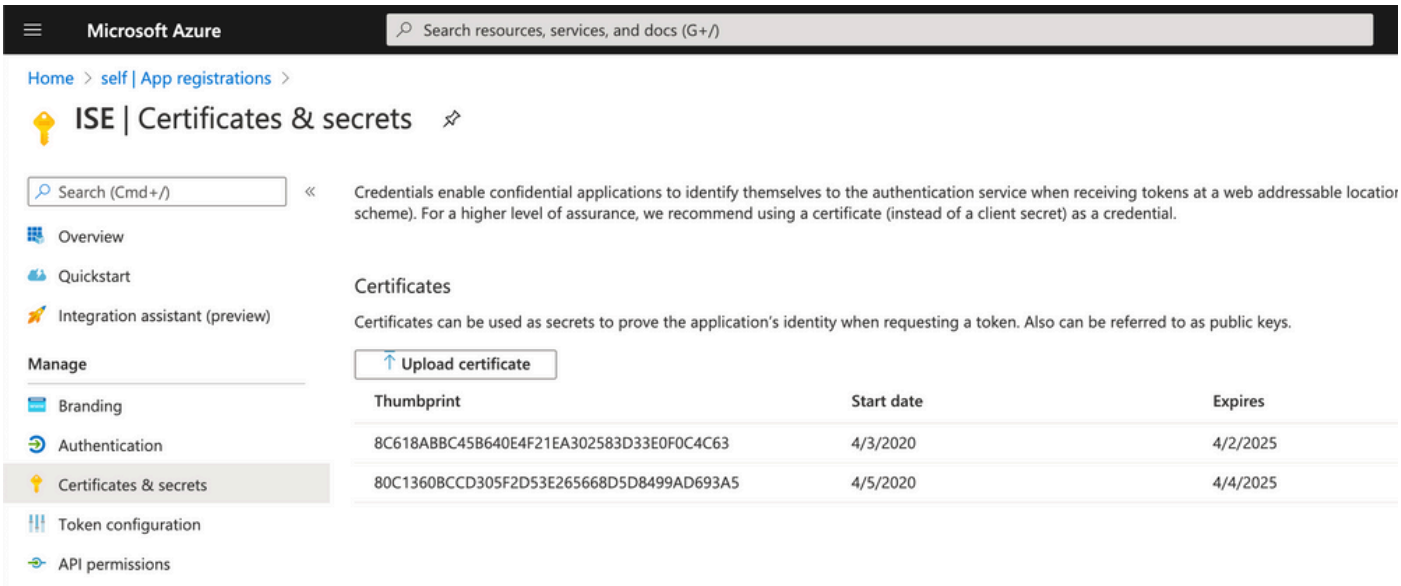


注：它是一个扩展名为JSON的文件。请勿编辑文件名或扩展名，否则会失败。

第二步：从所有节点导出ISE系统证书。在PAN上，导航至 Administration > System > Certificates > System Certificates，选择Default self-signed server certificate，然后单击 Export.选择 Export Certificate Only （默认），并选择一个保存位置。从证书中删除BEGIN和END标记，并将其余文本作为一行进行复制。这适用于旧版选项部分所述的2020年6月之前的版本。



截至2020年6月，门户允许您直接上传证书。



传统选项：

步骤1:运行PowerShell过程以将证书转换为BASE64并正确将其导入Azure JSON清单文件。从Windows使用Windows PowerShell或Windows PowerShell ISE应用程序。使用下列命令：

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

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

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

第二步：保留值 $base64Thumbprint, $base64Value,和 $keyid，用于下一步骤。所有这些值都将添加到JSON字段 keyCredentials 由于默认情况下如下所示：

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

为此，请确保按以下顺序使用值：

```
"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"
  }
],
```

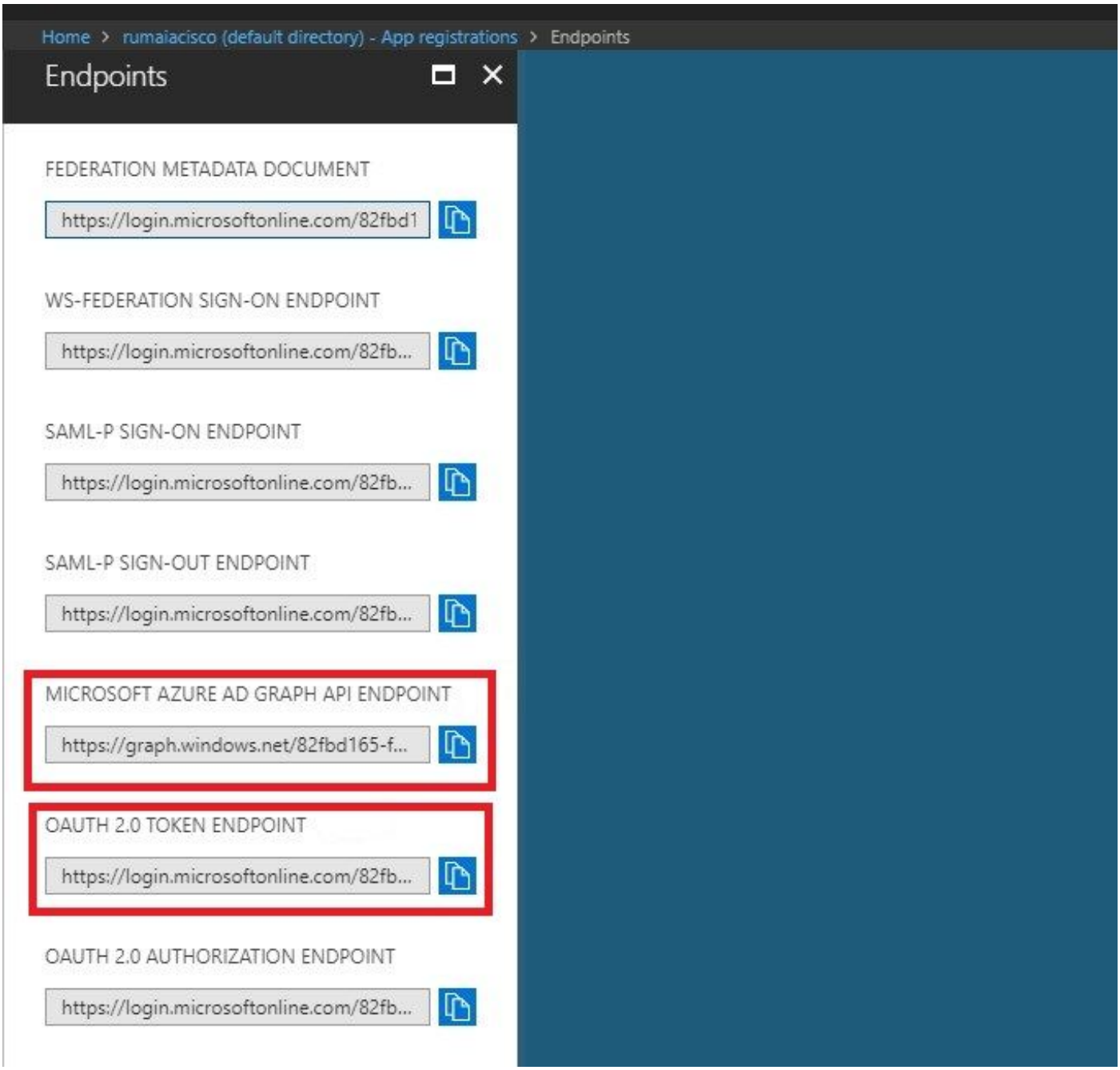
第三步：上传已编辑的 JSON 文件到Azure门户，以便验证 keyCredentials 从ISE上使用的证书。

其外观必须类似于：

```
"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
  },
```

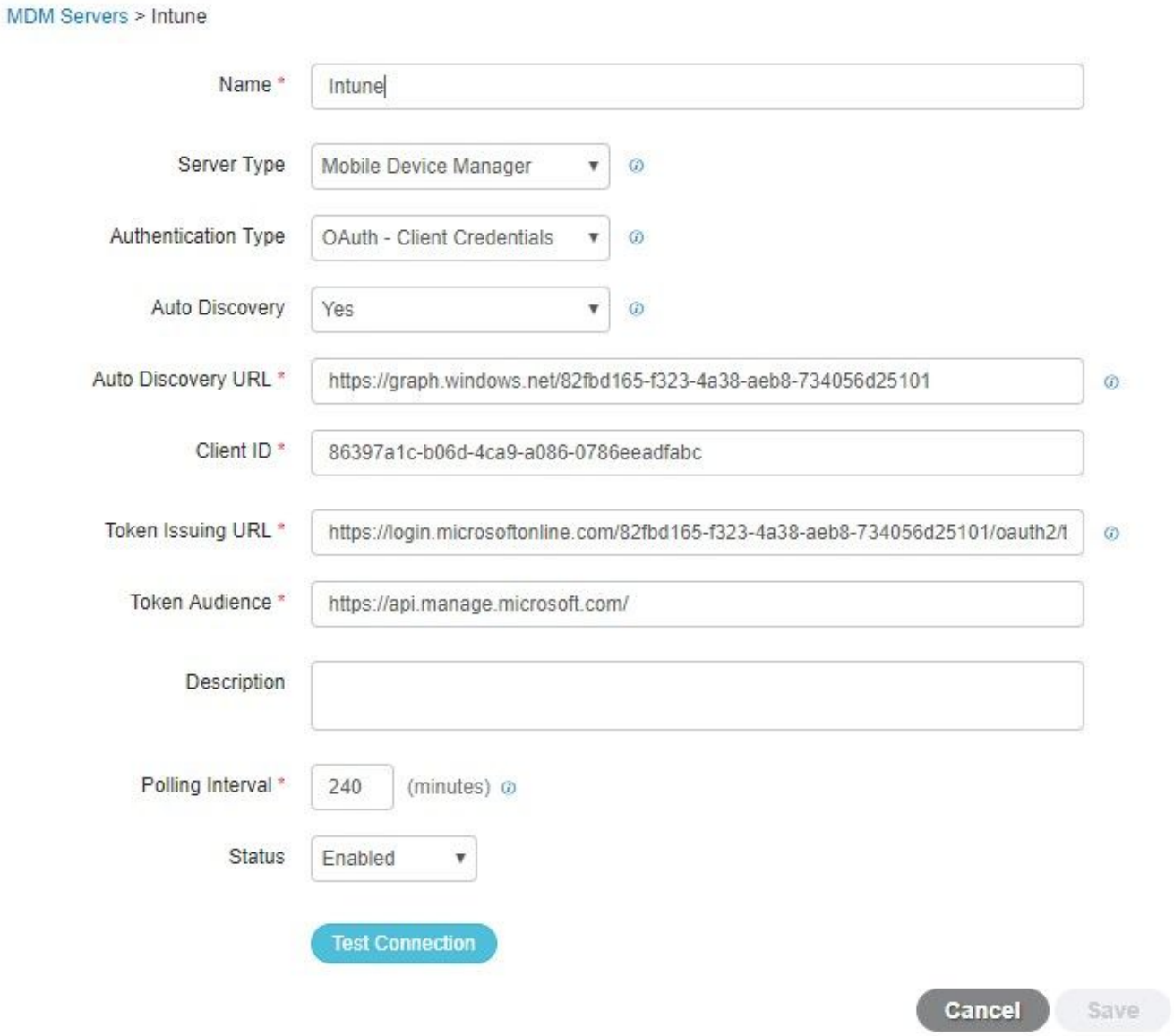

第四步：请注意，上传后， value 以下字段 keyCredentials 显示 null 因为这是Microsoft端强制执行的，不允许在第一次上传后看到这些值。

从ISE中添加MDM服务器所需的值可以复制 Microsoft Azure AD Graph API Endpoint 和 OAUTH 2.0 Token Endpoint.

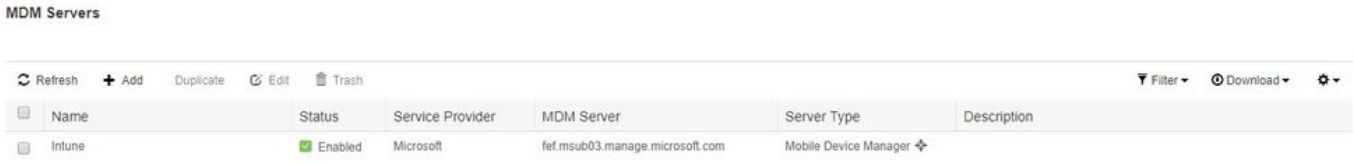


必须在ISE GUI中输入这些值。导航至 Administration > Network Resources > External MDM 并添加新服务器：

ISE	Intune
自动发现网址	终端> Microsoft Azure AD Graph API终端
客户端ID	{Registered-App-Name} >应用ID
令牌颁发URL	终端> OAuth 2.0令牌终端

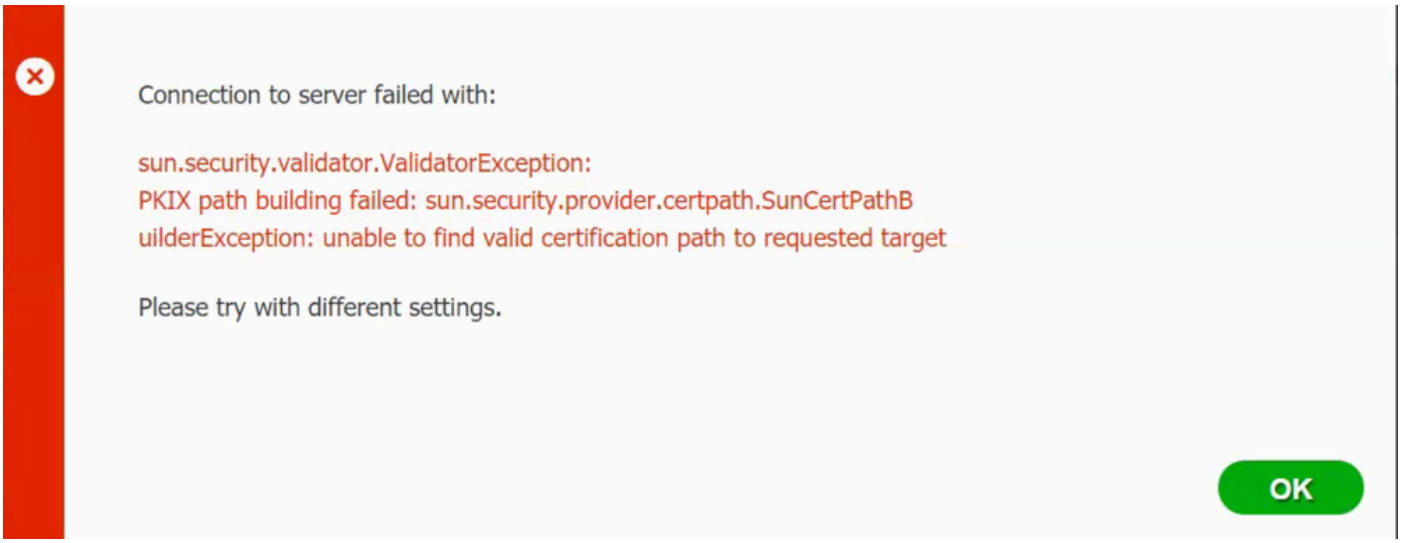


配置完成后，状态显示为enabled。



验证与故障排除

基于sun.security.validatorException的“Connection to the server failed”



步骤1:在TRACE级别使用以下日志收集支持捆绑包：

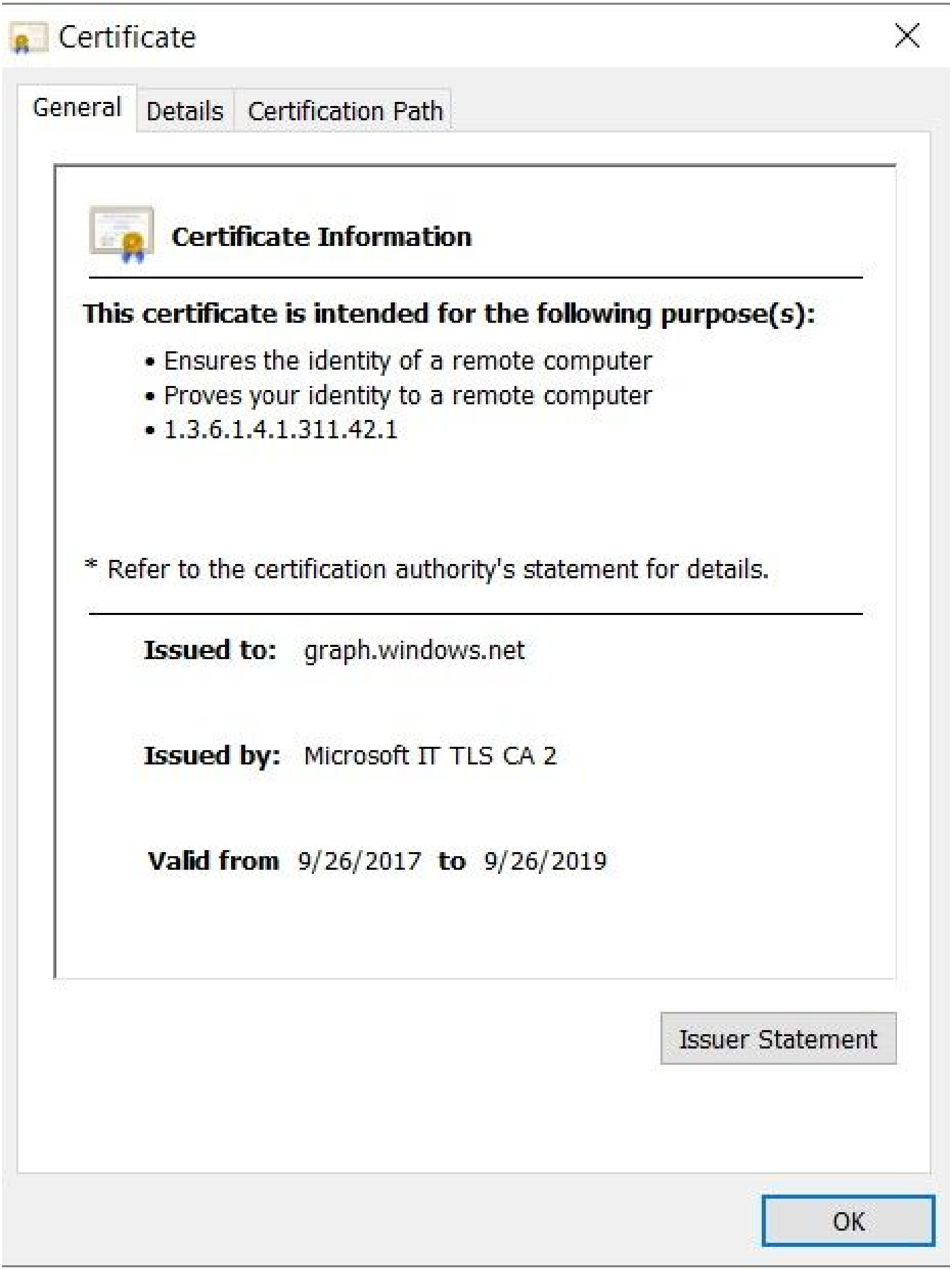
- portal (guest.log)
- mdmportal (ise-psc.log)
- external-mdm (ise-psc.log)

第二步：检查 ise-psc.log 对于这些日志：

- 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

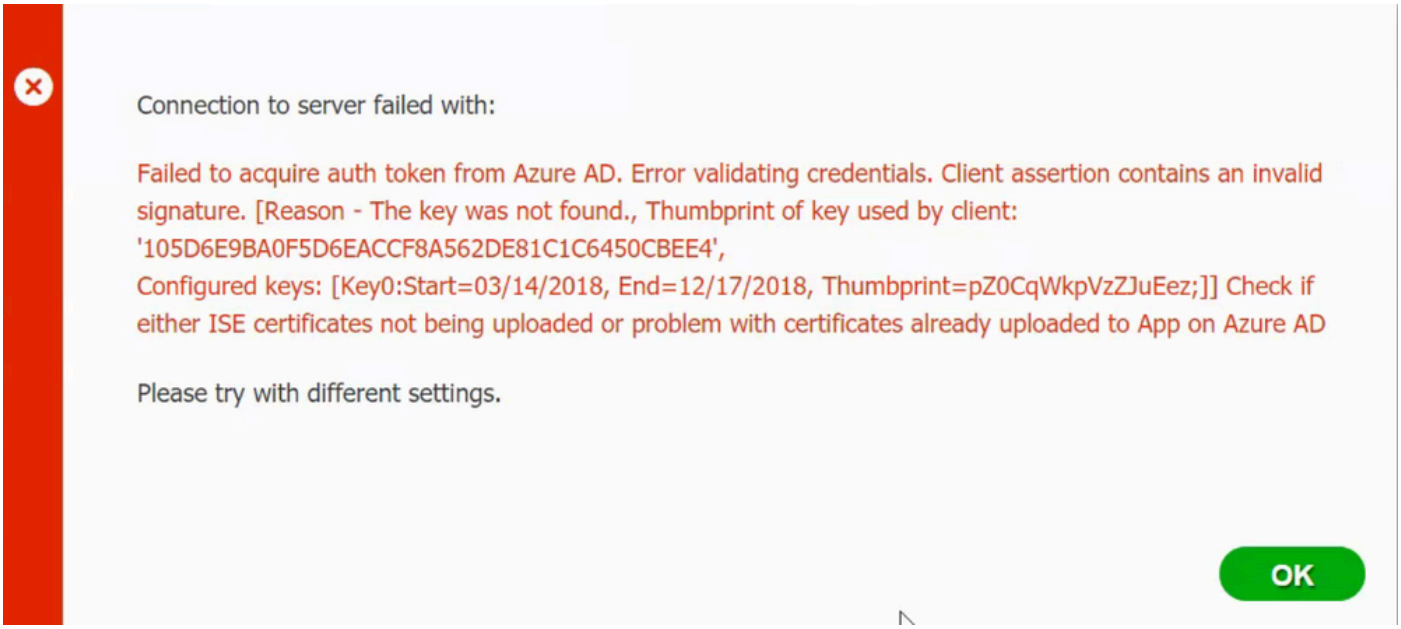
这表示需要导入 graph.microsoft.com 证书，出现在此页面上。

第三步：单击 locker 图标并检查证书详细信息。



第四步：将其保存为BASE64格式的文件，并将其导入到ISE受信任存储。确保导入完整的证书链。然后，再次测试与MDM服务器的连接。

无法从Azure AD获取身份验证令牌



通常，当清单出现时 JSON 文件包含错误的ISE证书链。在将清单文件上载到Azure之前，请验证是否至少存在此配置：

```
"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"
  }
}
],
```

上一个示例基于存在PAN和SAN的场景。再次从PowerShell运行脚本并导入正确的BASE64值。尝试上载清单文件，并且不能遇到任何错误。

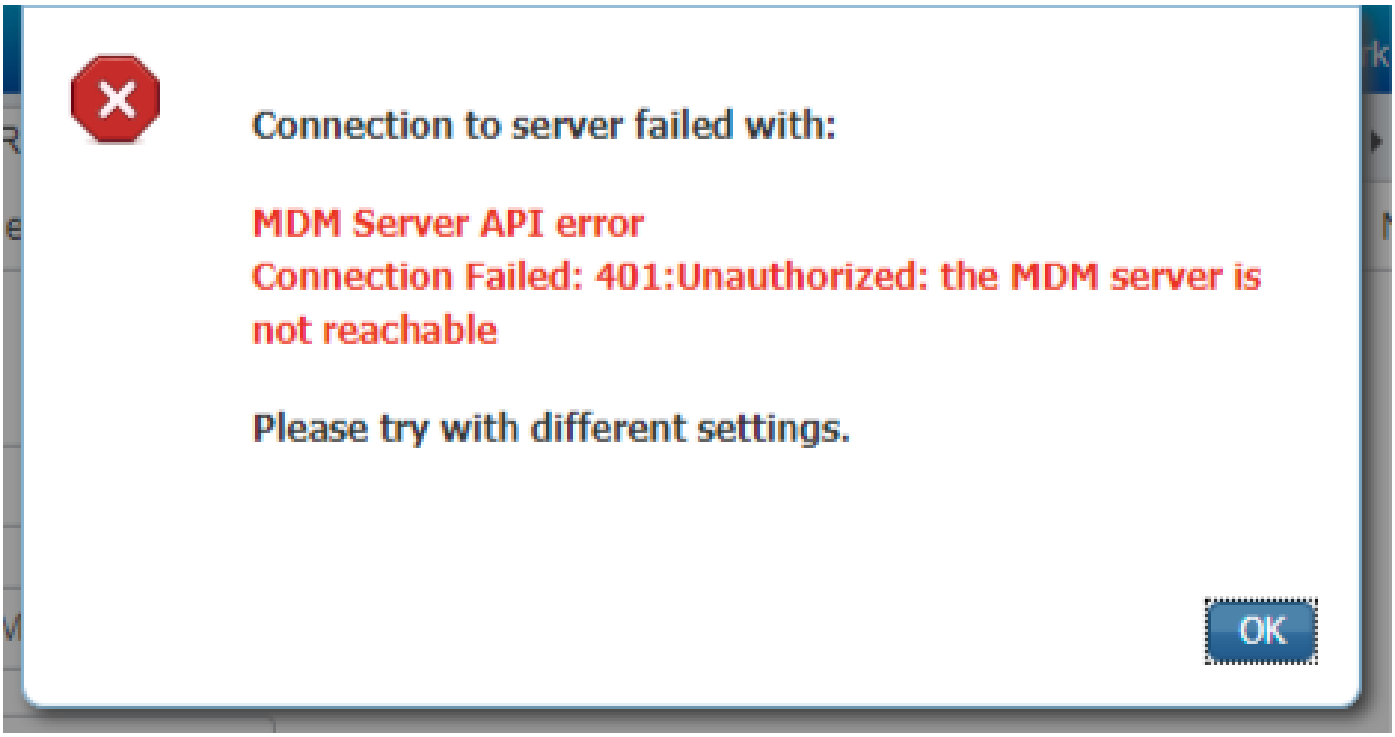
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(“mycer.cer”)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

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

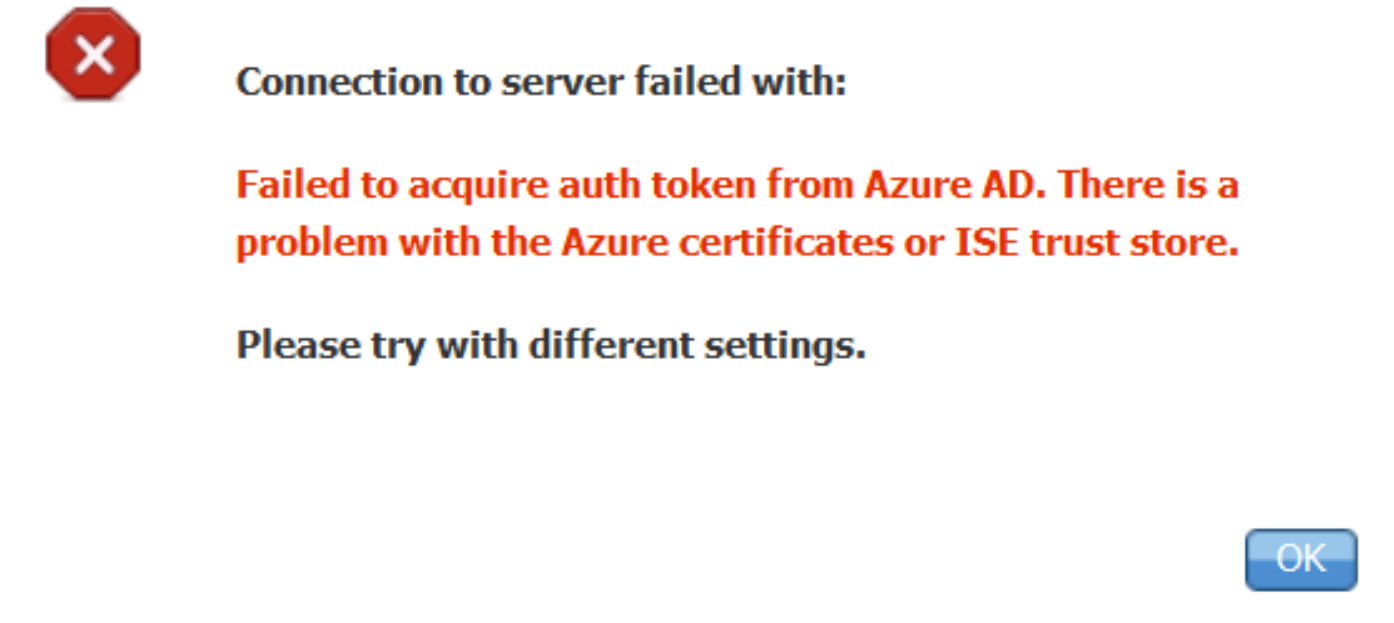
```
$keyid = [System.Guid]::NewGuid().ToString()
```

请记住应用这些值 $base64Thumbprint, $base64Value 和 $keyid 如“配置”一节中的步骤中所述。

无法从Azure AD获取身份验证令牌



通常，当在中为Azure应用授予了正确的权限时，会发生此错误 portal.azure.com.验证你的应用具有正确的属性，并确保你单击 Grant Permissions 每次改变之后。



当ISE尝试访问令牌颁发URL并返回ISE未返回的证书时，会出现此消息。确保完整的CA链在ISE信

任库中。如果在ISE的受信任存储中安装正确的证书后问题仍然存在，请执行数据包捕获并测试连接，以便查看发送的内容。

相关信息

- 使用客户端凭证的服务到服务呼叫
- Azure — 身份验证与授权
- Azure - Quickstart：向Microsoft身份平台注册应用程序
- Azure Active Directory应用清单
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。