

Integration von Intune MDM mit Identity Services Engine

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren von Microsoft Intune](#)

[Importieren Sie die Zertifikate aus dem Intune-Portal in den ISE Trusted Store.](#)

[Bereitstellen von ISE als Anwendung im Azure-Portal](#)

[Importieren von ISE-Zertifikaten in die Anwendung in Azure](#)

[Überprüfung und Fehlerbehebung](#)

["Verbindung zum Server fehlgeschlagen", basierend auf sun.security.validatorException](#)

[Fehler beim Abrufen des Auth-Tokens aus Azure AD.](#)

[Fehler beim Abrufen des Auth-Tokens aus Azure AD.](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Integration von Intune Mobile Device Management (MDM) in die Cisco Identity Services Engine (ISE) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der MDM-Services der Cisco ISE
- Kenntnisse von Microsoft Azure Intune Services

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

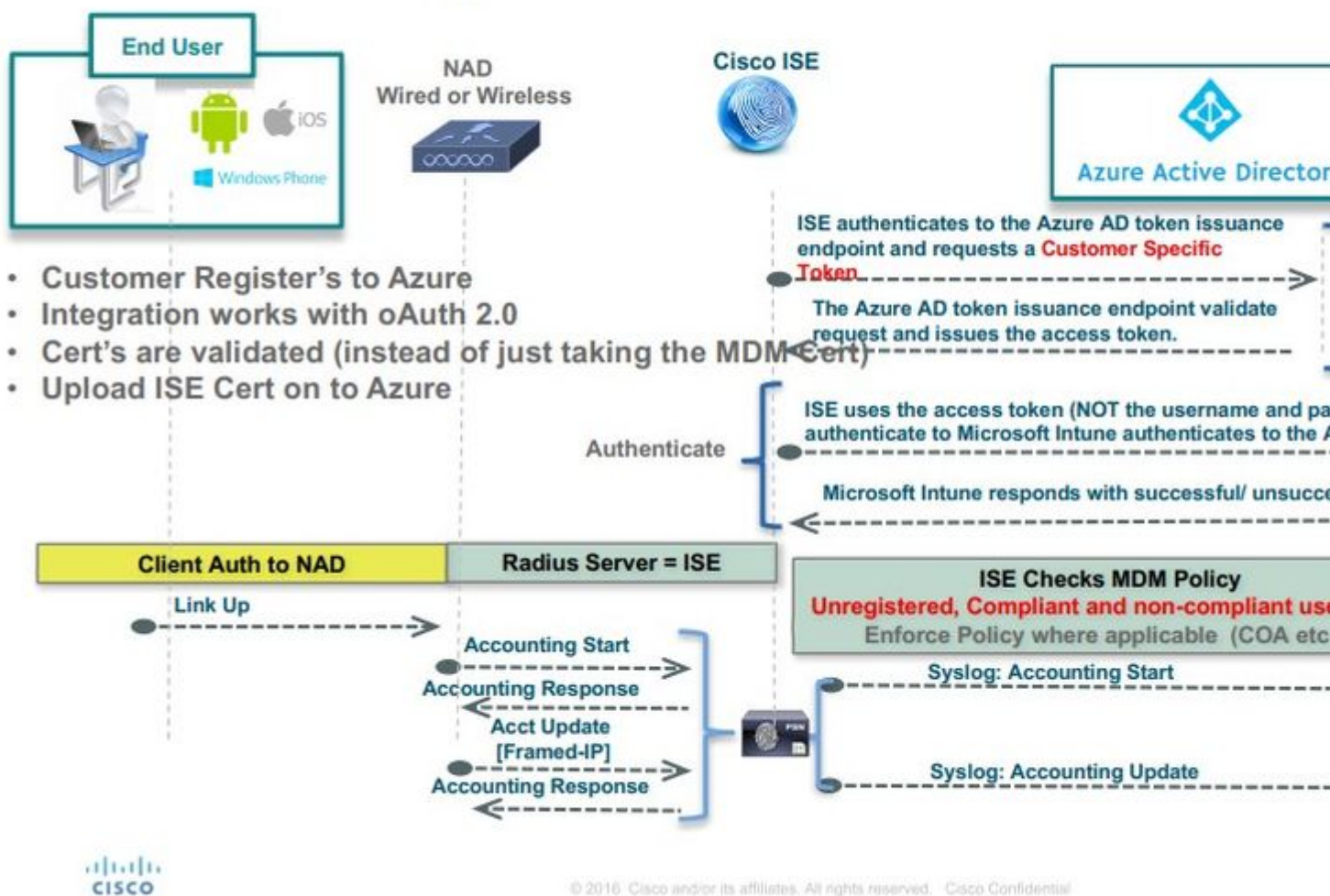
Hintergrundinformationen

MDM-Server sorgen für die Sicherheit, Überwachung, Verwaltung und Unterstützung von Mobilgeräten bei Mobilnetzbetreibern, Service Providern und Unternehmen. Diese Server fungieren als Richtlinienserver, der die Verwendung einiger Anwendungen auf einem Mobilgerät (z. B. einer E-Mail-Anwendung) in der bereitgestellten Umgebung steuert. Das Netzwerk ist jedoch die einzige Einheit, die auf Basis von Zugriffskontrolllisten (Access Control Lists, ACLs) granularen Zugriff auf Endpunkte ermöglichen kann. Die ISE fragt die MDM-Server nach den erforderlichen Geräteattributen ab, um ACLs zu erstellen, die die Netzwerkzugriffskontrolle für diese Geräte ermöglichen. Die Cisco ISE lässt sich mit Microsoft Intune MDM Server integrieren, um Unternehmen beim Zugriff auf Ressourcen vor Ort beim Schutz ihrer Unternehmensdaten zu unterstützen.

Konfigurieren

Netzwerkdiagramm

Intune Integration Architecture



Konfigurieren von Microsoft Intune

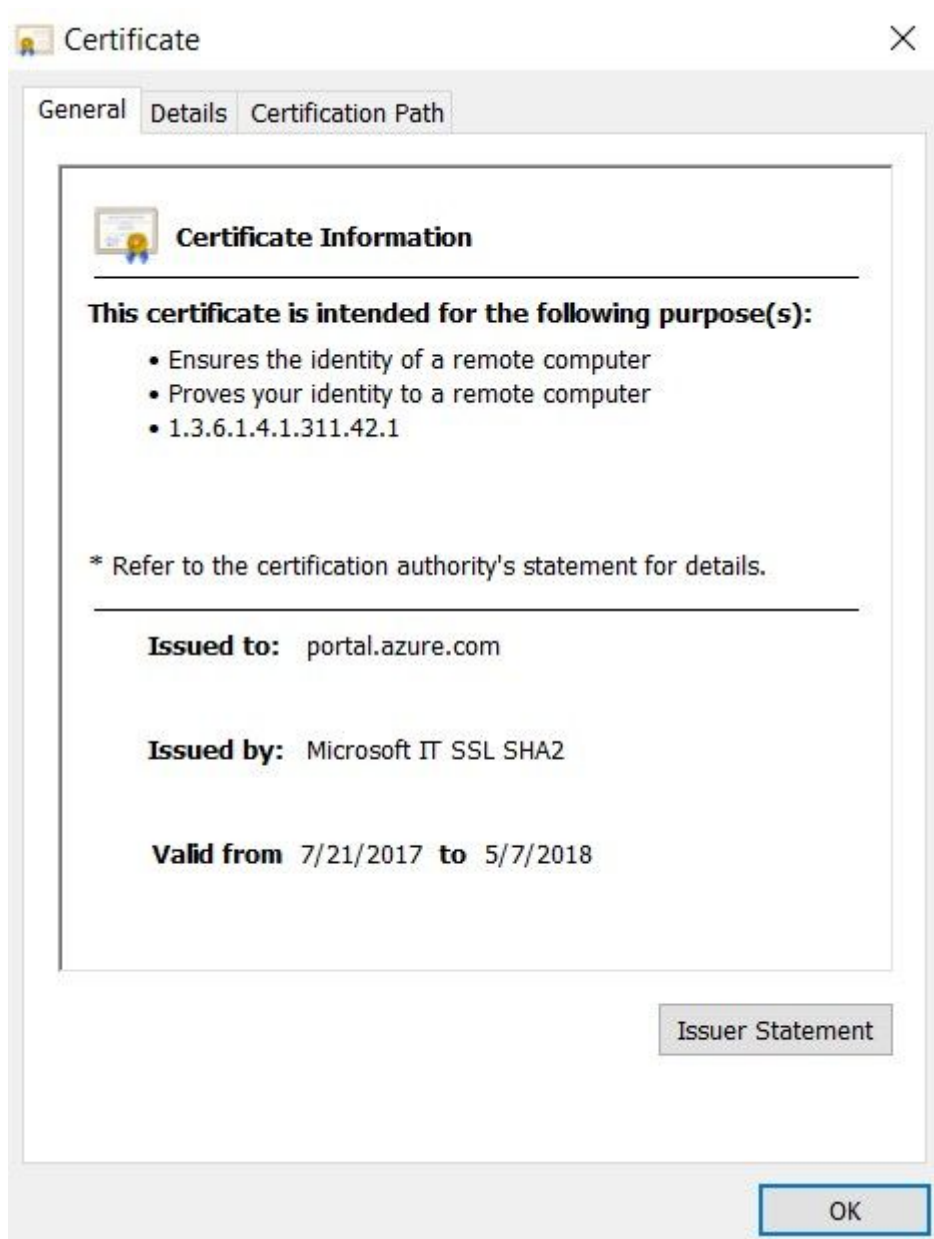
Importieren Sie die Zertifikate aus dem Intune-Portal in den ISE Trusted Store.

Melden Sie sich bei der Intune-Admin-Konsole oder der Azure-Admin-Konsole an, je nachdem, welcher Standort Ihren Tenant hat. Verwenden Sie den Browser, um die Zertifikatdetails abzurufen:

Schritt 1: Öffnen Sie Microsoft Azure portal über einen Webbrowser.

Schritt 2: Klicken Sie in der Browser-Symbolleiste auf das Sperrsymbol und anschließend auf View Certificates.

Schritt 3: Klicken Sie im Fenster Zertifikat auf die Schaltfläche Certification Path aus. Hier sehen Sie ein Beispiel:



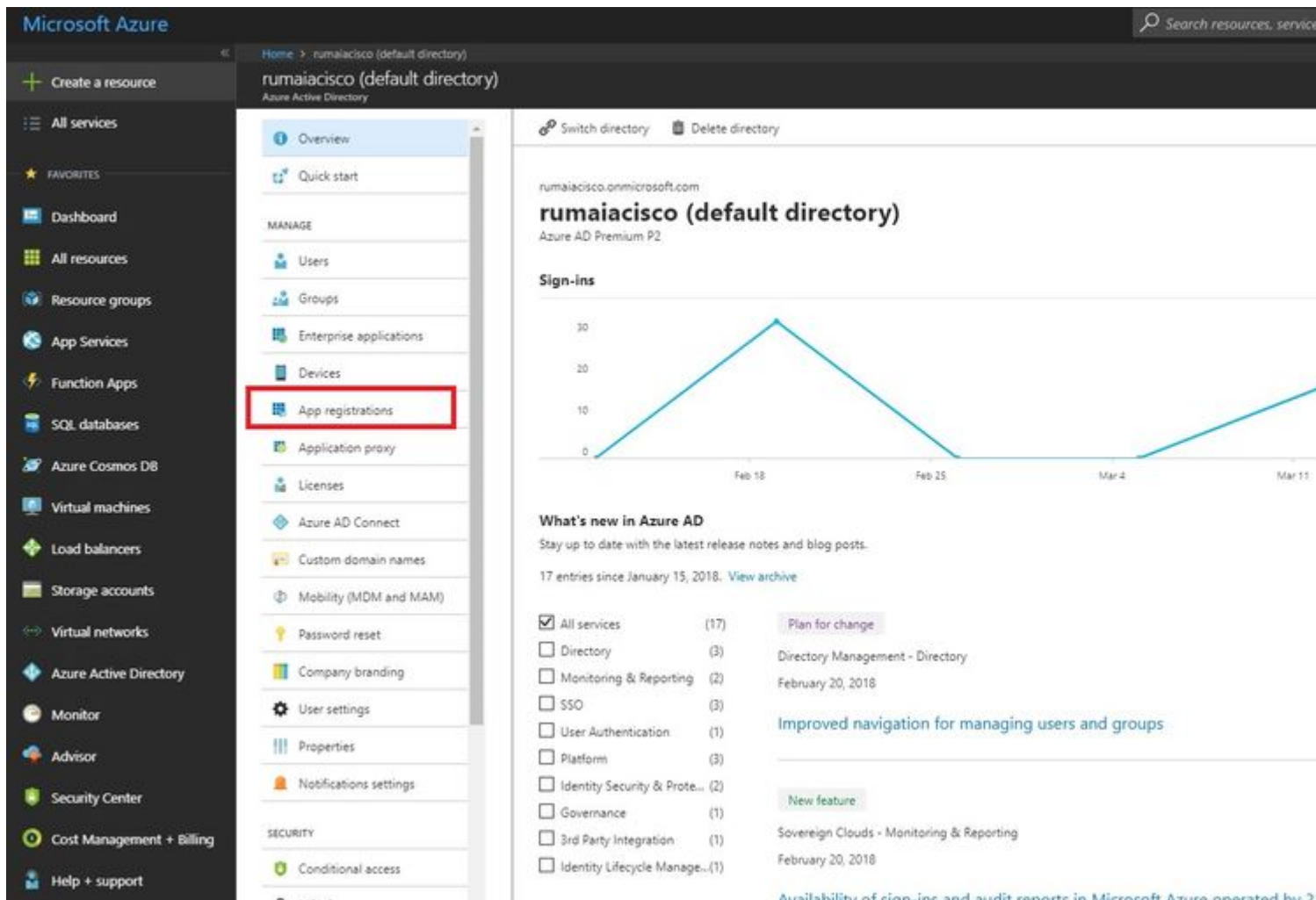
Schritt 4: Suchen Baltimore Cyber Trust root, die die übliche Stammzertifizierungsstelle ist. Wenn jedoch eine andere Stammzertifizierungsstelle vorhanden ist, klicken Sie auf dieses Stammzertifizierungsstelle-Zertifikat. Auf der Registerkarte Details dieses Root-Zertifizierungsstellenzertifikats können Sie es in die Datei kopieren und als BASE64-Zertifikat speichern.

Schritt 5: Navigieren Sie in der ISE zu Administration > System > Certificates > Trusted Certificates, und importieren Sie das soeben gespeicherte Stammzertifikat. Geben Sie dem Zertifikat einen aussagekräftigen Namen, z. B.

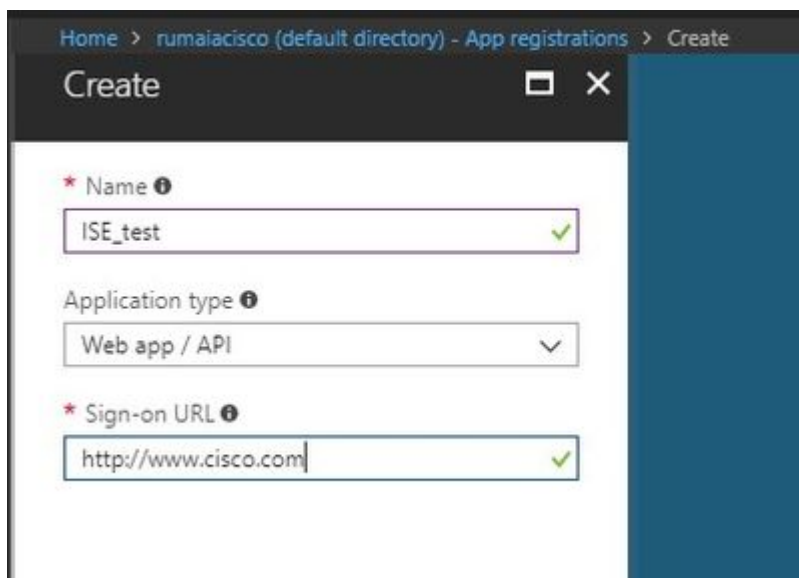
Azure MDM. Wiederholen Sie auch das Verfahren für die Zwischenzertifikate.

Bereitstellen von ISE als Anwendung im Azure-Portal

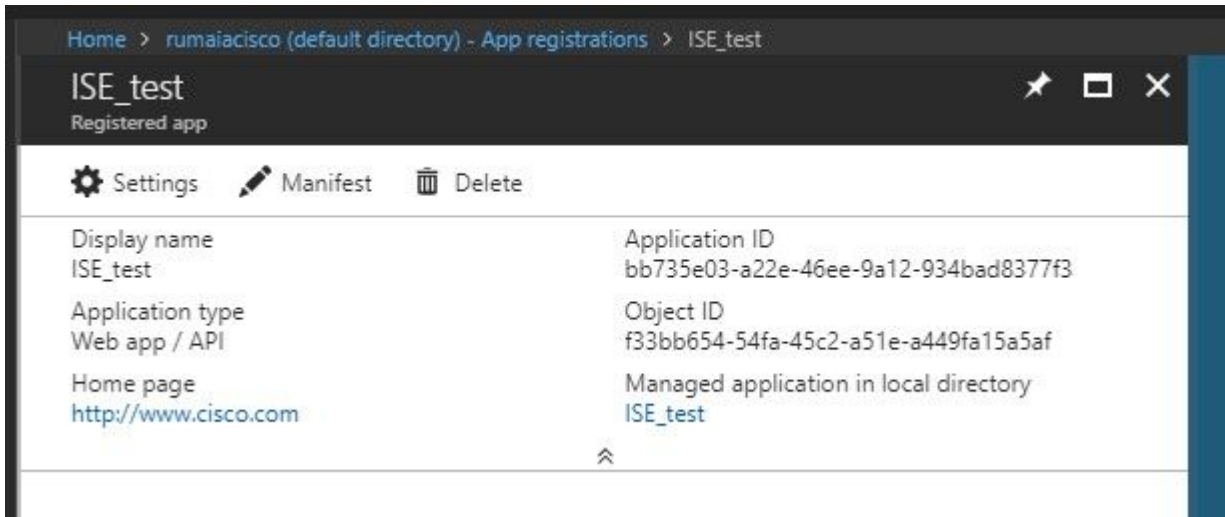
Schritt 1: Navigieren Sie zum Azure Active Directory und wählen App registrations.



Schritt 2: Im App registrations erstellen Sie eine neue Anwendungsregistrierung mit dem ISE-Namen. Klicken Sie auf Create wie in diesem Bild dargestellt.



Schritt 3: Auswählen Settings um die Anwendung zu bearbeiten und die erforderlichen Komponenten hinzuzufügen.



Schritt 4: Unter Settings, wählen Sie die erforderlichen Berechtigungen aus, und wenden Sie die folgenden Optionen an:

1. Microsoft-Diagramm

- Anwendungsberechtigungen
 - Verzeichnisdaten lesen
- Delegierte Berechtigungen
 - Microsoft Intune-Gerätekonfiguration und -richtlinien lesen
 - Microsoft Intune-Konfiguration lesen
 - Benutzer anmelden
 - Jederzeit Zugriff auf die Daten des Benutzers

2. Microsoft Intune-API

- Anwendungsberechtigungen
 - Gerätestatus- und Compliance-Informationen von Microsoft Intune abrufen

3. Windows Azure Active Directory

- Anwendungsberechtigungen
 - Verzeichnisdaten lesen
- Delegierte Berechtigungen
 - Verzeichnisdaten lesen
 - Anmelden und das Benutzerprofil lesen

Das Ergebnis der Konfiguration ähnelt dem hier gezeigten:

+ 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 >

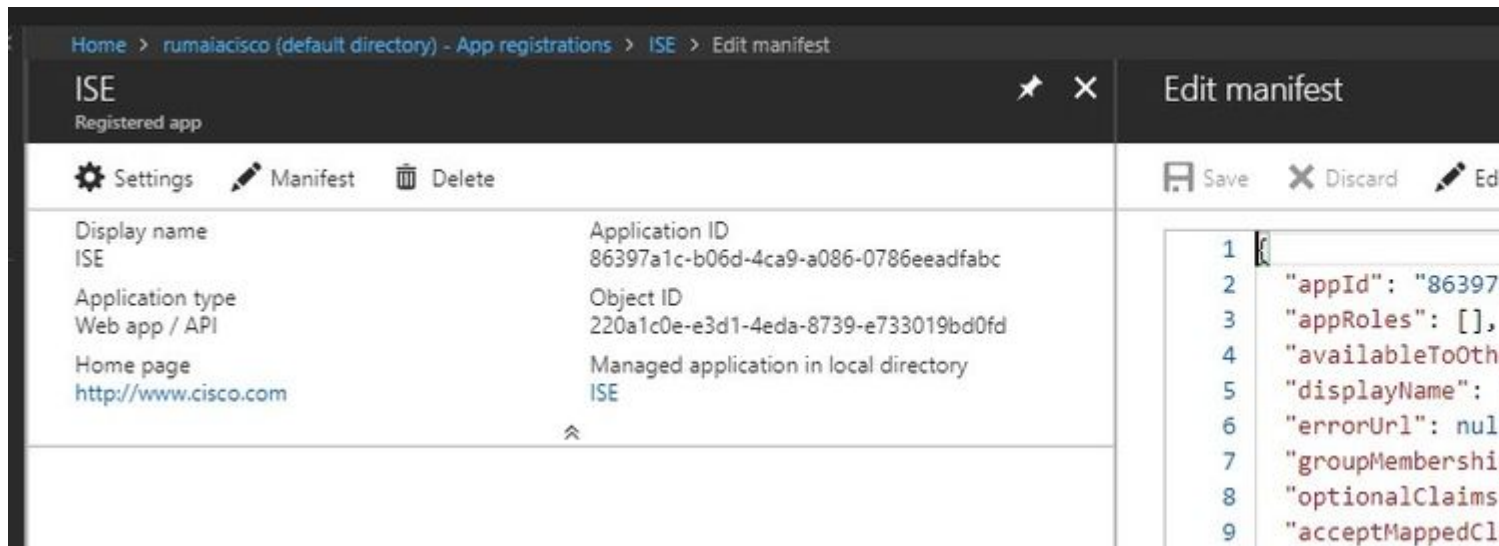
+ Add ↻ Grant Permissions

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

Schritt 5: Klicken Sie auf **Grant Permissions** um alle Anwendungsberechtigungen zu bestätigen. Dieser Vorgang dauert 5-10 Minuten. Bearbeiten Sie die **Azure Manifest** -Datei für die Anwendung, die zum Importieren interner ISE-Zertifizierungsstellenzertifikate erstellt wurde.

Importieren von ISE-Zertifikaten in die Anwendung in Azure

Schritt 1: Die Manifestdatei für die Anwendung herunterladen.



The screenshot shows the 'Edit manifest' page in the Azure portal. The left pane displays the application details for 'ISE' (Registered app). The right pane shows the JSON manifest file being edited.

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

```
1 {
2   "appId": "86397
3   "appRoles": [],
4   "availableToOth
5   "displayName":
6   "errorUrl": nul
7   "groupMembershi
8   "optionalClaims
9   "acceptMappedCl
```

Hinweis: Es handelt sich um eine Datei mit der Erweiterung JSON. Bearbeiten Sie nicht den Dateinamen oder die Erweiterung, andernfalls schlägt sie fehl.

Schritt 2: Exportieren Sie das ISE-Systemzertifikat von allen Knoten. Navigieren Sie auf dem PAN zu **Administration > System > Certificates > System Certificates**, wählen Sie das selbstsignierte Standard-Serverzertifikat aus, und klicken Sie auf **Export**. Auswählen **Export Certificate Only (Standard)**, und wählen Sie einen Speicherort aus. Löschen Sie die **BEGIN-** und **END-**Tags aus dem Zertifikat, und kopieren Sie den Rest des Texts in einer Zeile. Dies gilt für Versionen vor Juni 2020, die im Abschnitt zu Legacy-Optionen beschrieben werden.

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 CA - ise-1#00001	EAP Authentication, Admin, Portal, pxGrid	Defau Group



```

-----BEGIN CERTIFICATE-----
MIIE9jCCAt6gAwIBAgIQPffz/HZnjzsvArIAGaRr/sojANSgkqkxio9wbaqerAUAU
MTUwMwYDVQDDCkxJODAwZjY2F0ZSSTZkxJ2aWNLcyBfbmRwb2ludCBTdWlqQ0Eg
LSBpc2UzMtAeFw0xNjAzMDMxODA4MTlaFw0xODA4MDQxNzEzMDMxMDAwGTAxBgNV
BAMEGlZzS0xLmRlbW8ubG9jYjYwYyYwYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYy
AoIBAQCXfuGnVhgPqA9vqO/nwJ251t688oObRlyN21ThkrStpqF+GwFm1ZcM/x5L
fQ1MIQMNqoymSeKEKLQNdEEqR+a2/SK//D/R6xYxBGFiqEfc66t1RbHXBpP4
S/tQzLrLkmlxbtF+IVwr20GGfGytq92eEMNe2vB89G1K4100+rDe3WBgfdnidWcm
28g9+r6582Lz/WOKQ3b3Pw1BPSXdlvwXhyLLAcVn1BqdbOnEDB3tDecUAQ1FKGB
MowSY1DUa2fL8lINt8diV4cViFQBeNnEuz54HMLuorXPvR32NtQIeMaxjIBgk2
xocL/EtgHn2vCe0DUvJYVG2ReIavAgMBAAGjggEYMIIBFDafBgNVHREBAf8EFTAT
gREZNI01NS00NC0zMy0yMi0xMTAqBgkrBgEEAQkVAQUENQbcHhMcmkxX0N1cnRp
ZmljYXRlX1R1bXBzYXR1MGYGA1UdIwRlMF2AFF3AocVpMKVt6M6rfehF0peo1JJE
o7OkMTA+MS0wKwYDVQDDCkxJODAwZjY2F0ZSSTZkxJ2aWNLcyBfbmRwb2ludCBTdWlq
aXN1LTGCERHw3dLtkGkVan2opG9kBEywwHQYDVROBBYEFH3VrVTDGgukiCnbg1N
Oym7w08RMA4GA1UdDwEB/wQEAwIF4DAgBgNVHSUBAf8EFjAUBggrBgEFBQcDAQYI
KwYBBQUHAWIDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQoFAAOCAGeAnmsImaDi
34ihIMXjtrrh9OzjQwOSPk+EqIYeI2Au5AClxEgGdadrQbLP4MePlgMhXAfg+Xewt
HtuJ+AQX063KD2UHLR7RAM5Pe6UZy9Oqa8a37HjHGF75Wa8i4aT3Atnd7peQEML
jDeFb+6RVYjzBEMAnMs+rWGJV0NBjqlEJgJw7h00Cq+oQmtzLHzRlswquu5szv
ukkyJfsLWLx2EB2kNRis7jgtOOjYQLiUe2peJprvkQn3+/JwcuUa0RQeJGtabPR
DYoRqteVQaHjaNqSiFBC2ta5AyVrctDaujkbD1izJG3zWVwOt6H1oGcQqBzWz20
ThDTm+BRfeYnhuQWQy82e88/tWJWwq/9c81PxcWp2+LxHHTv6XJg0myMPWwC0e
dQ+6qCANJTFJcYusEzJD+xEzv3pgxkvwDB14iHOKtF6Y7v5piDKeIFGuR1luIatI
q/y+heUQTuKvYyFq20dDKHCiCivEapp3B8ezSvFKSE2PMBTAac24xUMDpH4W2nj
gL254nHTJ0Fc04szQyWYaaflJ1H9Uas/ObQy22pPd3IUxzc33xvvpjcp1T3w0AjK
WgMeg18NGR1Lr6taQf1OU690nk529BYtFenJ+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/HZnjzsv

Ab Juni 2020 können Sie Zertifikate direkt über das Portal hochladen.

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

Home > self | App registrations >

ISE | Certificates & secrets

- 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

Legacy-Option:

Schritt 1: Führen Sie eine PowerShell-Prozedur aus, um das Zertifikat in BASE64 umzuwandeln und es ordnungsgemäß in die Azure JSON-Manifestdatei zu importieren. Verwenden Sie die Windows PowerShell- oder Windows PowerShell ISE-Anwendung von Windows aus. Verwenden Sie folgende Befehle:

```
$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()
```

Schritt 2: Werte beibehalten für \$base64Thumbprint, \$base64Value und \$keyid, die im nächsten Schritt verwendet werden. Alle diese Werte werden dem JSON-Feld hinzugefügt. keyCredentials da es standardmäßig wie folgt aussieht:

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

Verwenden Sie dazu die Werte in der folgenden Reihenfolge:

```
"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"
}
],
```

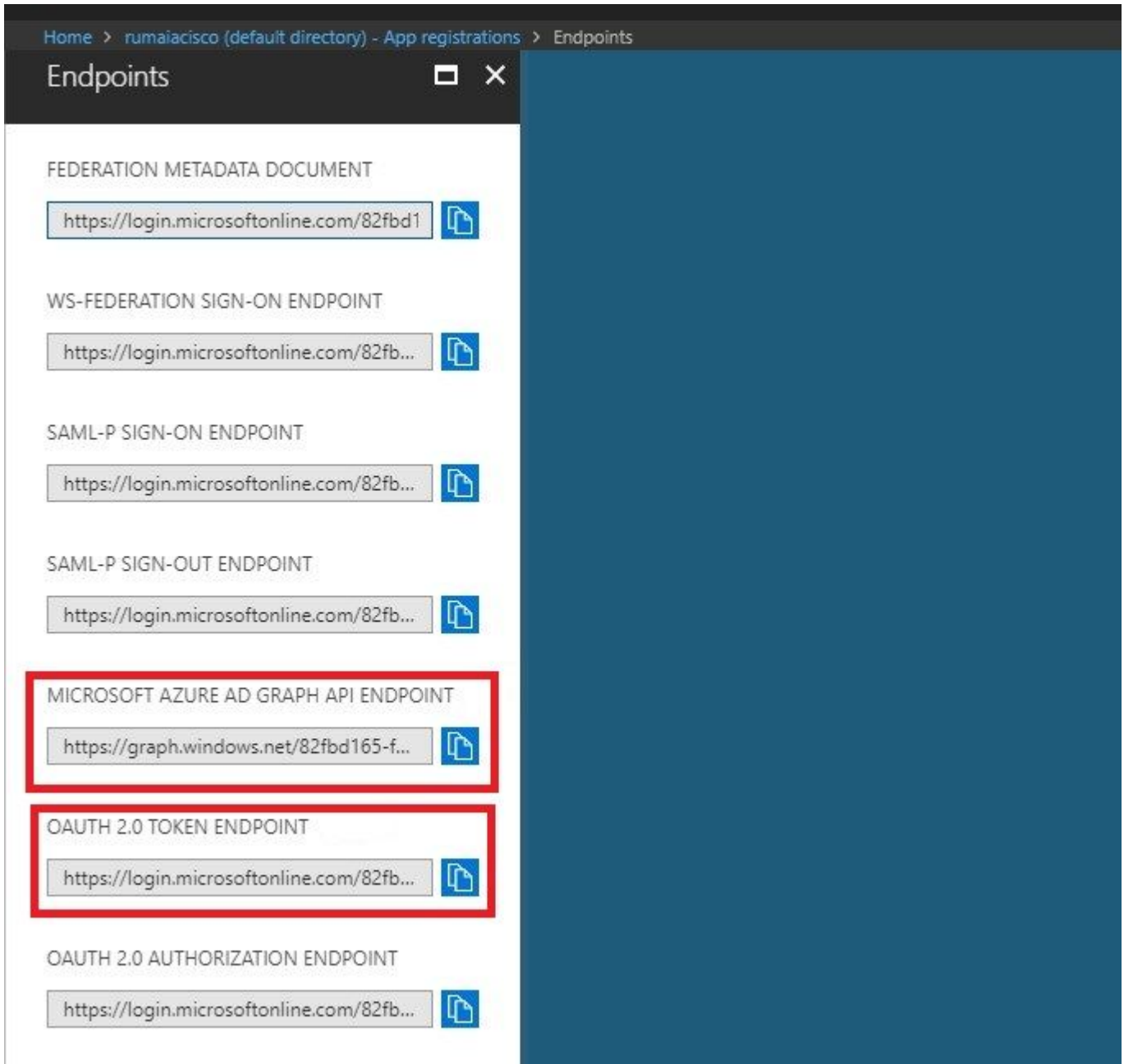
Schritt 3: Hochladen der bearbeiteten JSON in Azure Portal ein, um die `keyCredentials` von den auf der ISE verwendeten Zertifikaten.

Es muss ähnlich aussehen:

```
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  ],
```

Schritt 4: Beachten Sie, dass nach dem Upload `value` Feld unter `keyCredentials` zeigt `null` da dies von der Microsoft-Seite erzwungen wird, damit diese Werte nach dem ersten Upload nicht mehr angezeigt werden.

Die zum Hinzufügen des MDM-Servers in der ISE erforderlichen Werte können kopiert werden von Microsoft Azure AD Graph API Endpoint und OAUTH 2.0 Token Endpoint.



Diese Werte müssen in die ISE-GUI eingegeben werden. Navigieren Sie zu Administration > Network Resources > External MDM und einen neuen Server hinzufügen:

ISE	Intune
URL für automatische Erkennung	Endgeräte > Microsoft Azure AD Graph API-Endgeräte
Client-ID	{ Registered-App-Name } > Anwendungs-ID
Tokenausstellungs-URL	Endpunkte > OAuth 2.0-Token-Endpoint

Name *	<input type="text" value="Intune"/>
Server Type	Mobile Device Manager ⓘ
Authentication Type	OAuth - Client Credentials ⓘ
Auto Discovery	Yes ⓘ
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 ▼

[Test Connection](#)

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

Nach Abschluss der Konfiguration wird der Status als aktiviert angezeigt.

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	

Überprüfung und Fehlerbehebung

"Verbindung zum Server fehlgeschlagen", basierend auf 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.

Schritt 1: Erfassen Sie das Support-Paket mit diesen Protokollen auf TRACE-Ebene:

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

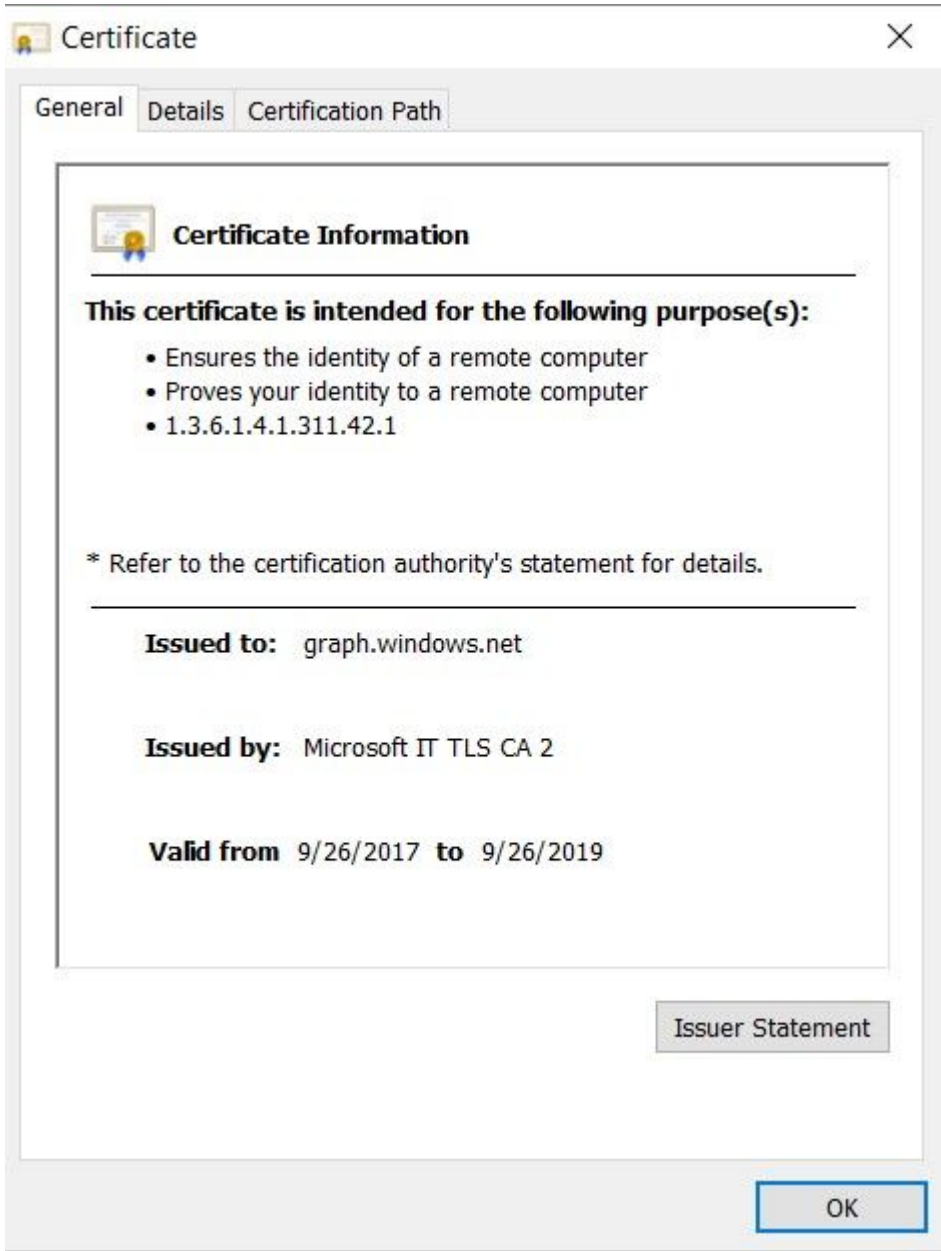
Schritt 2: Überprüfen `ise-psc.log` für diese Protokolle:

- 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

Dies deutet darauf hin, dass die `graph.microsoft.com` -Zertifikat, das auf dieser Seite vorhanden ist.


```
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>
```

Schritt 3: Klicken Sie auf `locker` und überprüfen Sie die Zertifikatdetails.



Schritt 4: Speichern Sie die Datei im BASE64-Format, und importieren Sie sie in den ISE Trusted Store. Stellen Sie sicher, dass Sie die gesamte Zertifikatskette importieren. Testen Sie anschließend die Verbindung zum MDM-Server erneut.

Fehler beim Abrufen des Auth-Tokens aus 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 uploaded]

Please try with different settings.

In der Regel tritt dieser Fehler auf, wenn das Manifest JSON enthält die falsche ISE-Zertifikatkette. Bevor Sie die Manifestdatei in Azure hochladen, überprüfen Sie, ob mindestens diese Konfiguration vorhanden ist:

```
"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"
  }
],
```

Das vorherige Beispiel basiert auf einem Szenario mit PAN und SAN. Führen Sie die Skripte aus PowerShell erneut aus, und importieren Sie die korrekten BASE64-Werte. Versuchen Sie, die Manifestdatei hochzuladen, und es dürfen keine Fehler auftreten.

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

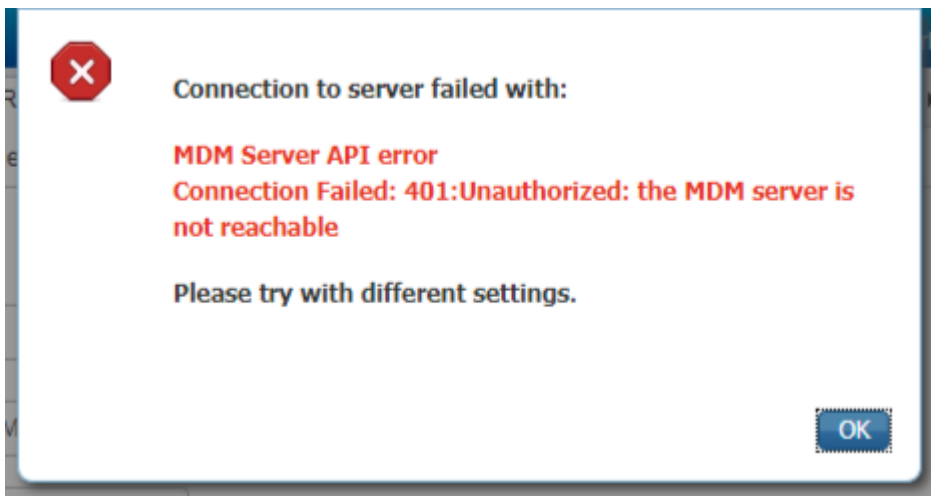
```
$cer.Import(â€œmycer.cerâ€œ)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

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

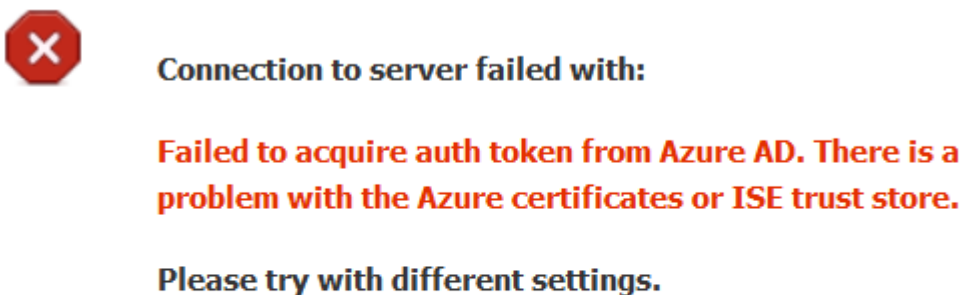
$keyid = [System.Guid]::NewGuid().ToString()
```

Denken Sie daran, die Werte für \$base64Thumbprint, \$base64Value und \$keyid wie in den Schritten im Abschnitt Konfigurieren beschrieben.

Fehler beim Abrufen des Auth-Tokens aus Azure AD.



Häufig tritt dieser Fehler auf, wenn der Azure-App nicht die richtigen Berechtigungen in portal.azure.com. Vergewissern Sie sich, dass Ihre App die richtigen Attribute aufweist, und klicken Sie auf Grant Permissions nach jeder Änderung.



OK

Diese Meldung wird angezeigt, wenn die ISE versucht, auf die Token Issuing URL zuzugreifen, und ein Zertifikat zurückgibt, das die ISE nicht zurückgibt. Stellen Sie sicher, dass sich die vollständige Zertifizierungsstellenkette im ISE-Vertrauensspeicher befindet. Wenn das Problem nach der Installation des richtigen Zertifikats im vertrauenswürdigen ISE-Speicher weiterhin besteht, führen Sie eine Paketerfassung durch, und testen Sie die Verbindung, um festzustellen, was gesendet wird.

Zugehörige Informationen

- [Dienst-zu-Dienst-Anrufe mit Client-Anmeldeinformationen](#)
- [Azure - Authentifizierung und Autorisierung](#)
- [Azure - Quickstart: Registrieren Sie eine Anwendung bei der Microsoft-Identitätsplattform.](#)
- [Azure Active Directory-App-Manifest](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.