

Integrazione di MDM di Intune con Identity Services Engine

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configura Microsoft Intune](#)

[Importa i certificati dal portale Intune nell'archivio attendibile ISE](#)

[Distribuire ISE come applicazione nel portale di Azure](#)

[Importa certificati ISE nell'applicazione in Azure](#)

[Verifica e risoluzione dei problemi](#)

["Connessione al server non riuscita" basata su sun.security.validatorException](#)

[Non è stato possibile acquisire il token Auth da Azure AD](#)

[Non è stato possibile acquisire il token Auth da Azure AD](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come integrare Intune Mobile Device Management (MDM) con Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza dei servizi MDM in Cisco ISE
- Conoscenza dei servizi di Microsoft Azure Intune

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine 3.0
- Applicazione Microsoft Azure Intune

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

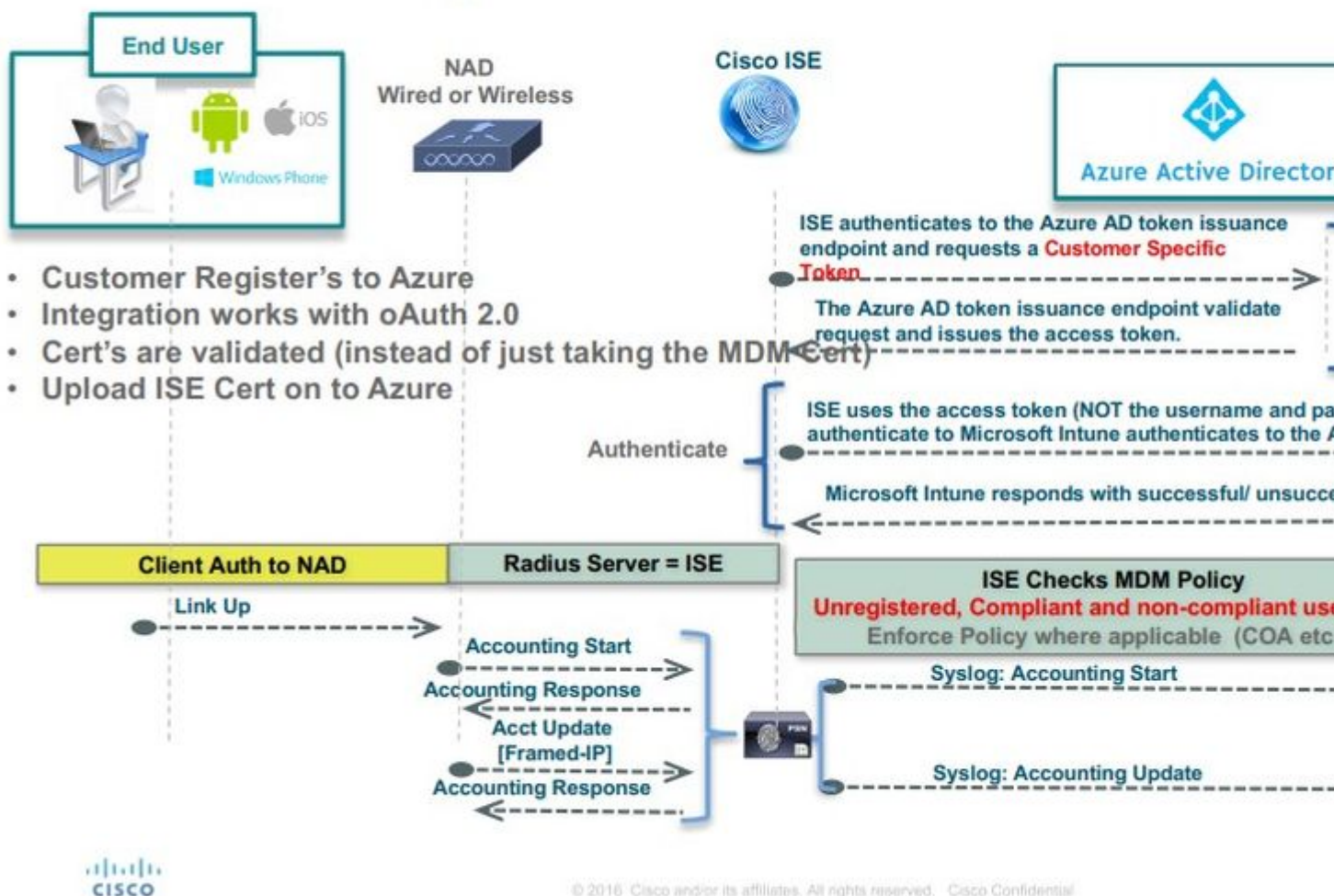
Premesse

I server MDM proteggono, monitorano, gestiscono e supportano i dispositivi mobili distribuiti tra gli operatori mobili, i provider di servizi e le aziende. Questi server fungono da policy server che controlla l'utilizzo di alcune applicazioni su un dispositivo mobile (ad esempio, un'applicazione di posta elettronica) nell'ambiente distribuito. Tuttavia, la rete è l'unica entità in grado di fornire accesso granulare agli endpoint in base agli Access Control Lists (ACL). ISE richiede ai server MDM gli attributi dei dispositivi necessari per creare ACL che offrano ai dispositivi il controllo dell'accesso alla rete. Cisco ISE si integra con Microsoft Intune MDM Server per aiutare le organizzazioni a proteggere i dati aziendali quando i dispositivi tentano di accedere alle risorse locali.

Configurazione

Esempio di rete

Intune Integration Architecture



Configura Microsoft Intune

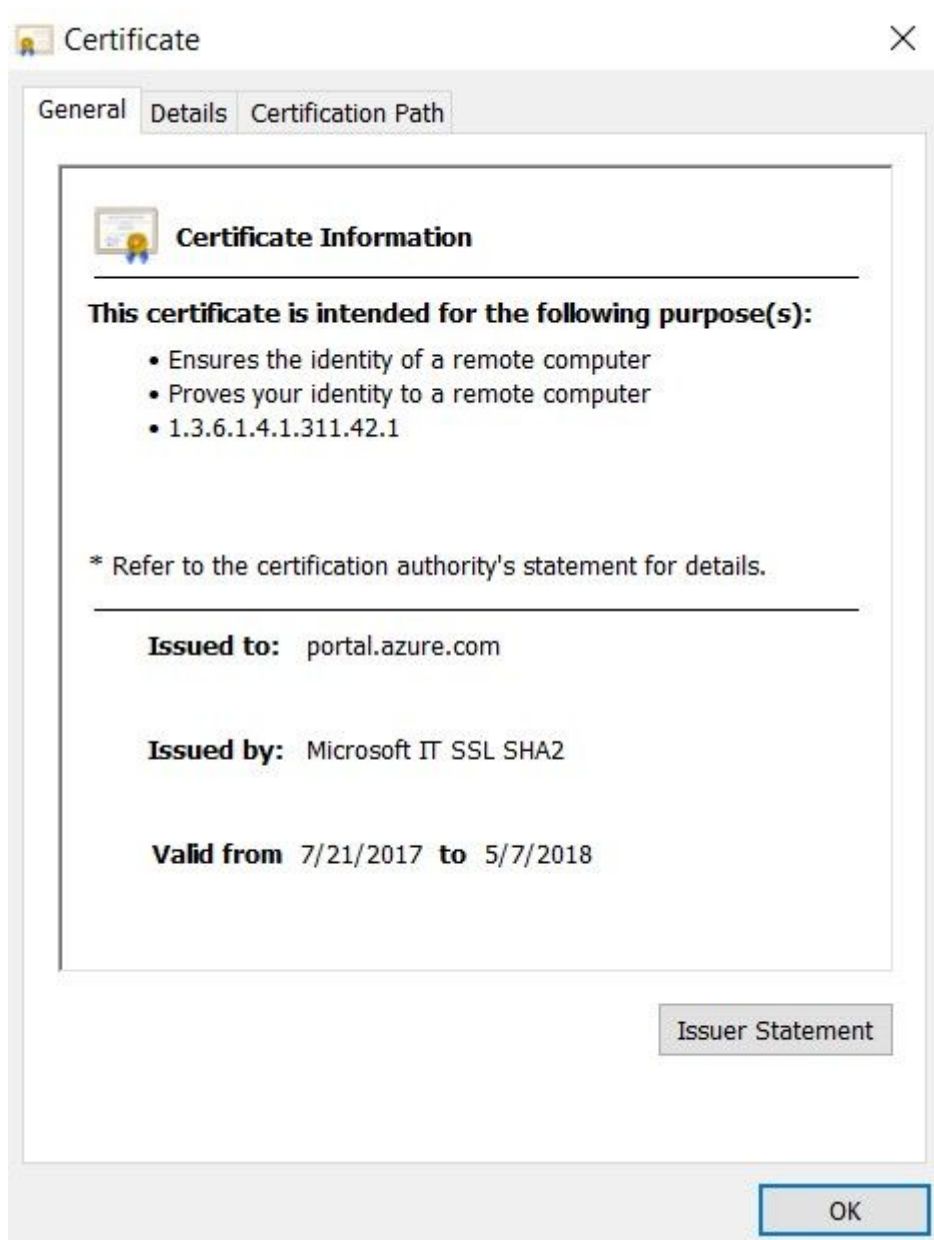
Importa i certificati dal portale Intune nell'archivio attendibile ISE

Accedere alla console di amministrazione di Intune o alla console di amministrazione di Azure, a seconda del sito in cui si trova il tenant. Utilizzare il browser per ottenere i dettagli del certificato:

Passaggio 1. Aprire il Microsoft Azure portal da un browser Web.

Passaggio 2. Fare clic sul simbolo di blocco nella barra degli strumenti del browser, quindi fare clic su View Certificates.

Passaggio 3. Nella finestra Certificato, fare clic sul pulsante Certification Path scheda. Di seguito è riportato un esempio:

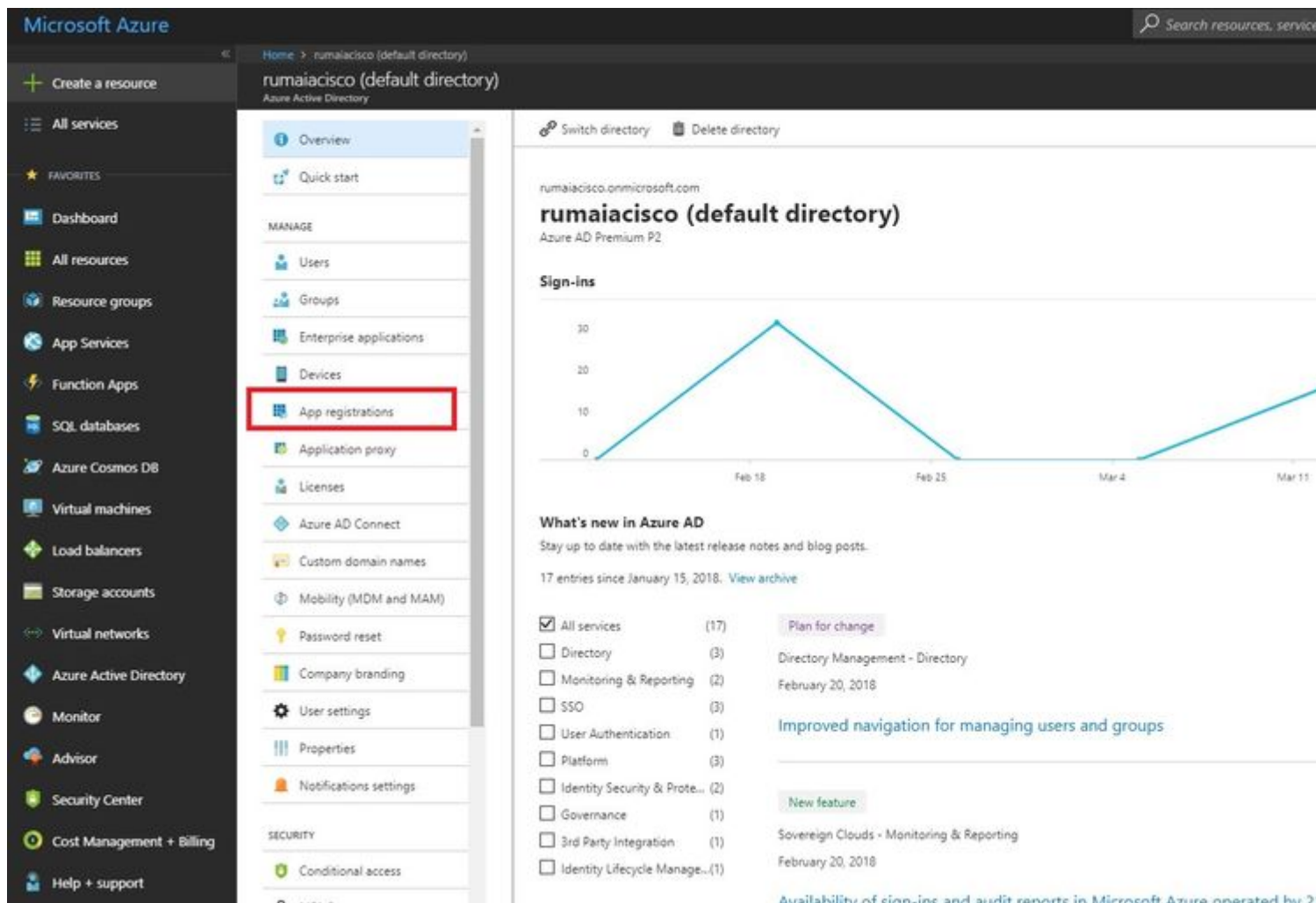


Passaggio 4. Cerca Baltimore Cyber Trust root, che è la normale CA radice. Tuttavia, se esiste un'altra CA radice diversa, fare clic su tale certificato. Nella scheda Dettagli del certificato CA radice è possibile copiarlo nel file e salvarlo come certificato BASE64.

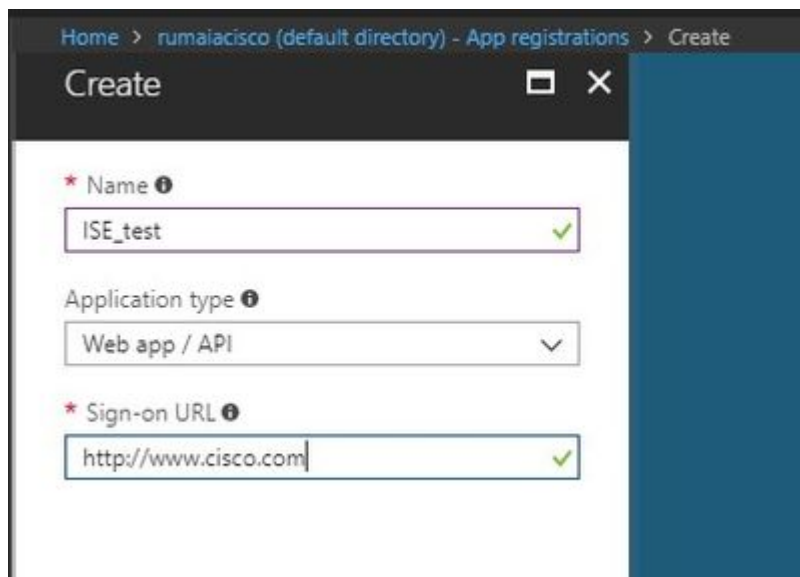
Passaggio 5. Ad ISE, selezionare Administration > System > Certificates > Trusted Certificates e importare il certificato radice appena salvato. Assegnare al certificato un nome significativo, ad esempio Azure MDM. Ripetere la procedura anche per i certificati CA intermedi.

Distribuire ISE come applicazione nel portale di Azure

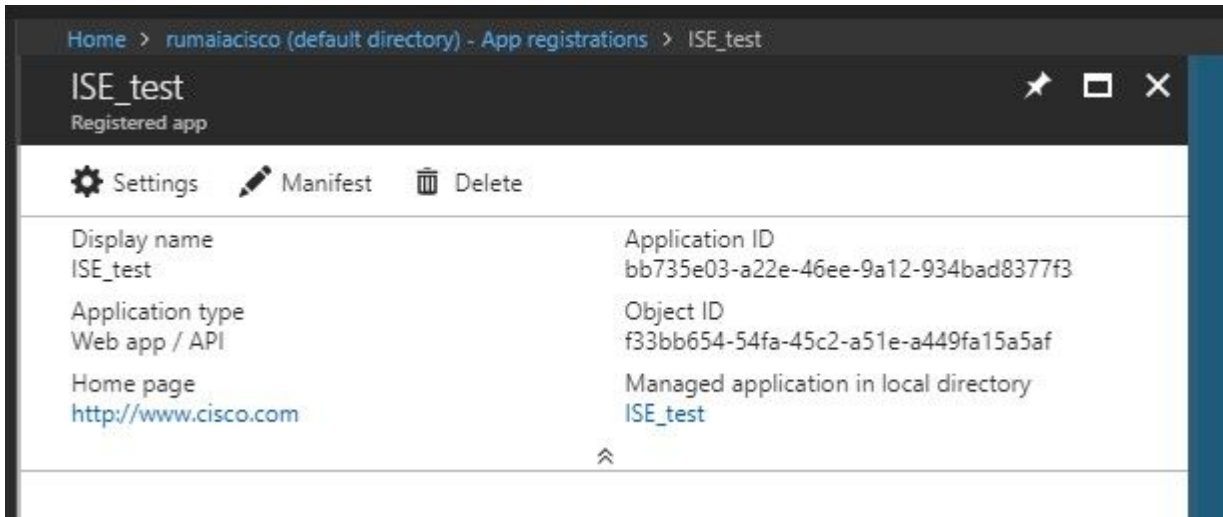
Passaggio 1. Passare alla Azure Active Directory e scegliere App registrations.



Passaggio 2. Nella scheda App registrations, creare una nuova registrazione dell'applicazione con il nome ISE. Fare clic su Create come mostrato nell'immagine.



Passaggio 3. Scegli Settings per modificare l'applicazione e aggiungere i componenti necessari.



Passaggio 4. Inferiore Settings, scegliere le autorizzazioni necessarie e applicare le seguenti opzioni:

1. Microsoft Graph

- Autorizzazioni applicazione
 - Leggi dati directory
- Autorizzazioni delegate
 - Lettura della configurazione e dei criteri dei dispositivi di Microsoft Intune
 - Lettura della configurazione di Microsoft Intune
 - Accedi utenti
 - Accedere ai dati dell'utente in qualsiasi momento

2. API di Microsoft Intune

- Autorizzazioni applicazione
 - Ottieni informazioni sullo stato e sulla conformità del dispositivo da Microsoft Intune

3. Windows Azure Active Directory

- Autorizzazioni applicazione
 - Leggi dati directory
- Autorizzazioni delegate
 - Leggi dati directory
 - Accedi e leggi il profilo utente

Il risultato della configurazione è simile a quello mostrato di seguito:

+ 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 >

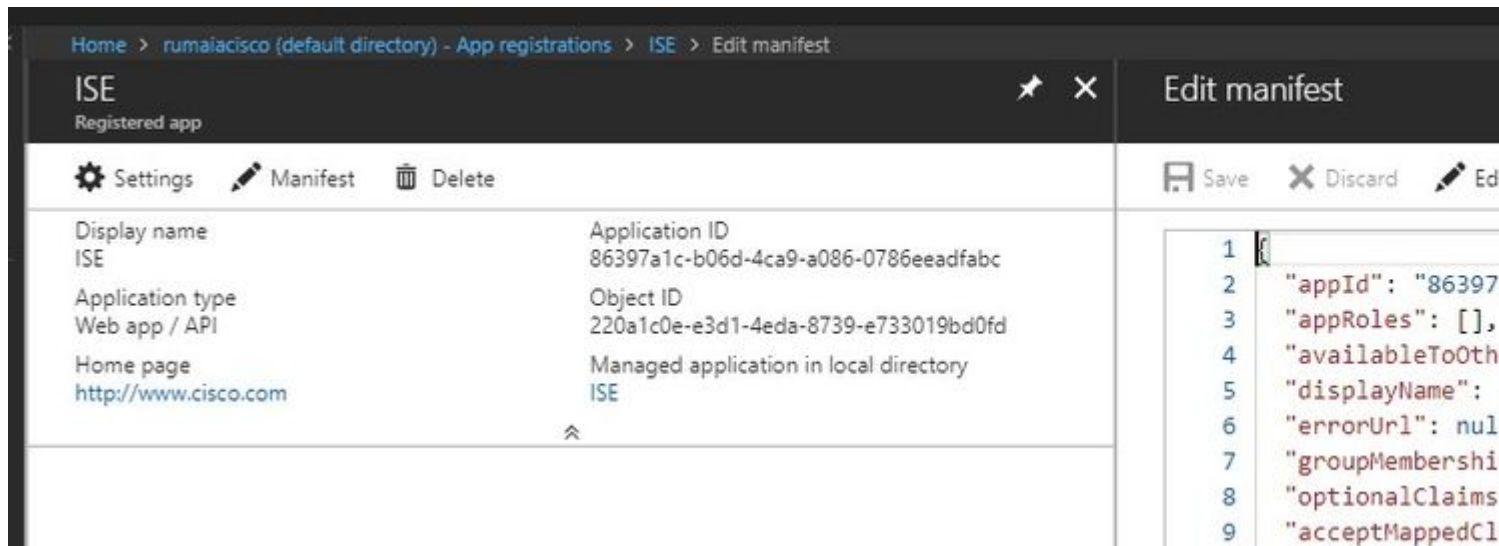
+ Add ↻ Grant Permissions

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

Passaggio 5. Fare clic su **Grant Permissions** per confermare tutte le autorizzazioni dell'applicazione. Per rendere effettiva questa procedura sono necessari 5-10 minuti. Modifica **Azure Manifest** per l'applicazione creata per importare certificati ISE CA interni.

Importa certificati ISE nell'applicazione in Azure

Passaggio 1. Scaricare il file manifesto per l'applicazione.



The screenshot shows the 'Edit manifest' interface in the Azure portal. On the left, there is a summary card for the 'ISE' application, which is a 'Registered app'. The card includes a 'Manifest' button and a 'Delete' button. Below the card, a table lists the application's details:

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

On the right side of the interface, there is a text editor for the manifest file. The visible JSON content is as follows:

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

Nota: è un file con estensione JSON. Non modificare il nome o l'estensione del file, altrimenti non verrà eseguito.

Passaggio 2. Esportare il certificato di sistema ISE da tutti i nodi. Sulla PAN, passare a **Administration > System > Certificates > System Certificates**, scegliere il certificato predefinito del server autofirmato e fare clic su **Export**. Scegli **Export Certificate Only** (impostazione predefinita) e scegliere una posizione in cui salvarlo. Eliminare i tag **BEGIN** e **END** dal certificato e copiare il resto del testo in un'unica riga. Questa opzione è applicabile alle versioni precedenti a giugno 2020 descritte nella sezione **Opzioni legacy**.

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/H2njzsvArIAGaRr/sojANSgkqkxio9wbaqerAUAU
MTUwMwYDVQDDCkxJ0aWZpY2F0ZSBST2XJ2aWNLcyBfbmRwb2ludCBTdWlqQ0Eg
LSBpc2UzMtAeFw0xNjAzMDMxODA4MTlaFw0xODA4MDQxNzEzMDMxMDEwMDA4MDQ
BAMEGlZzS0xLmRlbW8ubG9jYjYwWggEiMA0GC8qSgIb3DQEBAAQAA4ISDwAggEK
AoIBAQCXfuGnVhgPqA9vqO/nwJ251t688oObRlyN21ThkrStpqF+GwFm1ZcM/x5L
fQ1MIQMNqoymSeKEKLQNdEEqrX+a2/SK//D/R6xYxBGFiqEfc66t1RbHXBpP4
S/tQzLrLkmlxbtF+IVWr20GGfGytq92eEMNe2vB89G1K4100+rDe3WBgfdnidWcm
28g9+r6582Lz/WOKQ3b3Pw1BPSXdlvwXhyLLAcVn1BqdBOnEDB3tDecUAQ1FKGB
MowSY1DUa2fL8lINt8diVi4cViFQBeNnEuz54HMLuorXPvR32NtQIeMaxjIBgk2
xocL/EtgHn3vCe0DUvJYVG2ReIavAgMBAAGjggEYMIIBFDafBgNVHREBAf8EFTAT
gRE2Ni01NS00NC0zMy0yMi0xMTAqBgkrBgEEAQkVAguENQCbHhMclKX0N1cnRp
ZmljYXRlX1R1bXBzYXR1MGYGA1UdIwRlMF2AFF3AocqVpMKVitm6rfEhf0peo1JJE
o7OkMTA+MS0wKwYDVQDDCkxJ0aWZpY2F0ZSBST2XJ2aWNLcyBfbmRwb2ludCBTdW
eXN1LTGCERHw3dLtkGkVan2opG9kBEywwHQYDVROBBYEFH3VrVTDGgukiCnbg1N
Oym7w08RMA4GA1UdDwEB/wQEAwIF4DAgBgNVHSUBAf8EFjAUBggrBgEFBQcDAQYI
KwYBBQUHAWIDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQoFAAOCAGeAnmsImaDi
34ihIMXjtrH9OzjQwOSPk+EqIYeI2AU5ACLxEGgDadrQbLP4MePlgMhXAfg+XEWt
HtuJ+AQXO63KD2UhLLR7RAM5Pe6UZy9Oqa8a37HjHGF75Wa8i4aT3Atnd7peQEML
jDeFb+6RVYjzBEMAnMs+rWGJV0NBjqlEJgJw7h00Cq+oQmtzLHzRlswquu5szv
ukkyJfsLWLx2EB2kNRis7jgtOOjYQLiUe2peJprvkQn3+/JwcuUa0RQeJGtabPR
DYoRqteVQaHjaNqSiFBC2ta5AyVrctDaujkbDilzJG3zWVwOt6H1oGCqQ8zWZ20
ThDTm+BRfeYnhuONQy82e88/tWJWwq/9c81PxcWp2+LxHHTv6XJg0myMPWwC0e
dQ+6qCANJTFJcYusE2JD+xEzv3pgxkvwDB14iHOKtF6Y7v5piDKeIFGuR1luIatI
q/y+heUQTuKvYyFq20dDKHCiCivEapp3B8ezSvFKSE2PMBTAac24xUMDpH4W2nj
gL254nHTJ0Fc04ezQyWYaaflJ1H9Ua3/ObQy22pPd3IUxzC33xvvpjcp1T3w0AjK
WgMeg18NGR1Lr6taQf10Un690nk529BYtFenJ+UT/goFUE8oJHPy18QI+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/H2njzsv

A partire da giugno 2020, il portale consente di caricare i certificati direttamente.

☰ 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

Opzione legacy:

Passaggio 1. Eseguire una procedura PowerShell per convertire il certificato in BASE64 e importarlo correttamente nel file manifesto JSON di Azure. Utilizzare l'applicazione Windows PowerShell o Windows PowerShell ISE di Windows. Utilizzare i seguenti comandi:

```
$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()
```

Passaggio 2. Mantieni i valori per \$base64Thumbprint, \$base64Value, e \$keyid, utilizzati nel passaggio successivo. Tutti questi valori vengono aggiunti al campo JSON `keyCredentials` poiché, per impostazione predefinita, ha il seguente aspetto:

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

A tale scopo, assicurarsi di utilizzare i valori nell'ordine seguente:

```
"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"
}
],
```

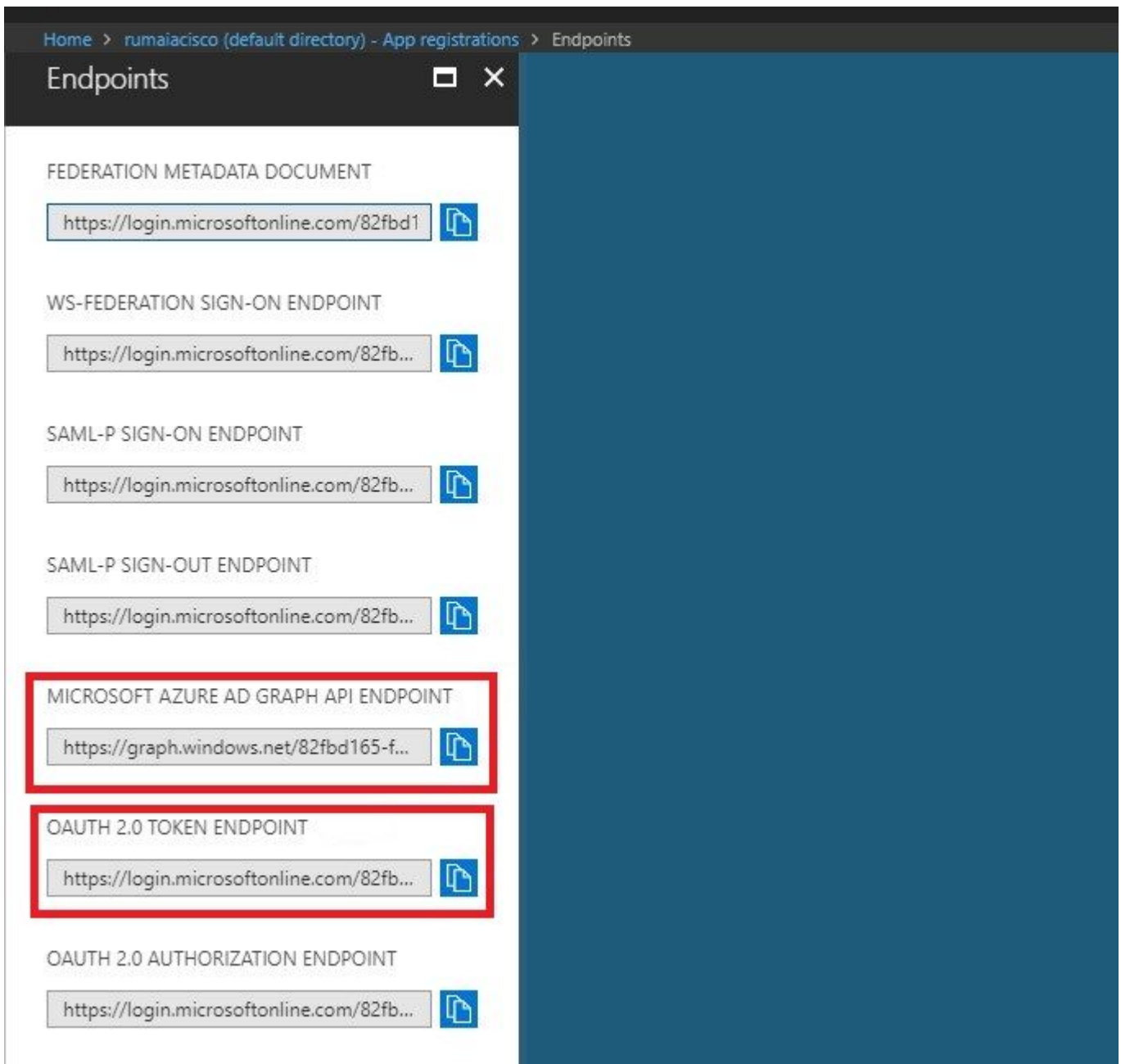
Passaggio 3. Carica il file modificato JSON nel portale di Azure per convalidare il `keyCredentials` dai certificati utilizzati sull'ISE.

Deve avere un aspetto simile al seguente:

```
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  ],
```

Passaggio 4. Tenere presente che dopo il caricamento, `value` campo sotto `keyCredentials` mostra `null` poiché questa opzione viene applicata dal lato Microsoft in modo da non consentire la visualizzazione di questi valori dopo il primo caricamento.

I valori richiesti per aggiungere il server MDM in ISE possono essere copiati da Microsoft Azure AD Graph API Endpoint e OAUTH 2.0 Token Endpoint.



Questi valori devono essere immessi nell'interfaccia grafica di ISE. Passa a Administration > Network Resources > External MDM e aggiungere un nuovo server:

ISE	Intune
URL individuazione automatica	Endpoint > Endpoint API di Microsoft Azure AD Graph
ID client	{Registered-App-Name} > ID applicazione
URL di emissione token	Endpoint > Endpoint token OAuth 2.0

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](#)

Una volta completata la configurazione, lo stato risulta abilitato.

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	

Verifica e risoluzione dei problemi

"Connessione al server non riuscita" basata su 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.

Passaggio 1. Raccogliere il bundle di supporto con questi log a livello TRACE:

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

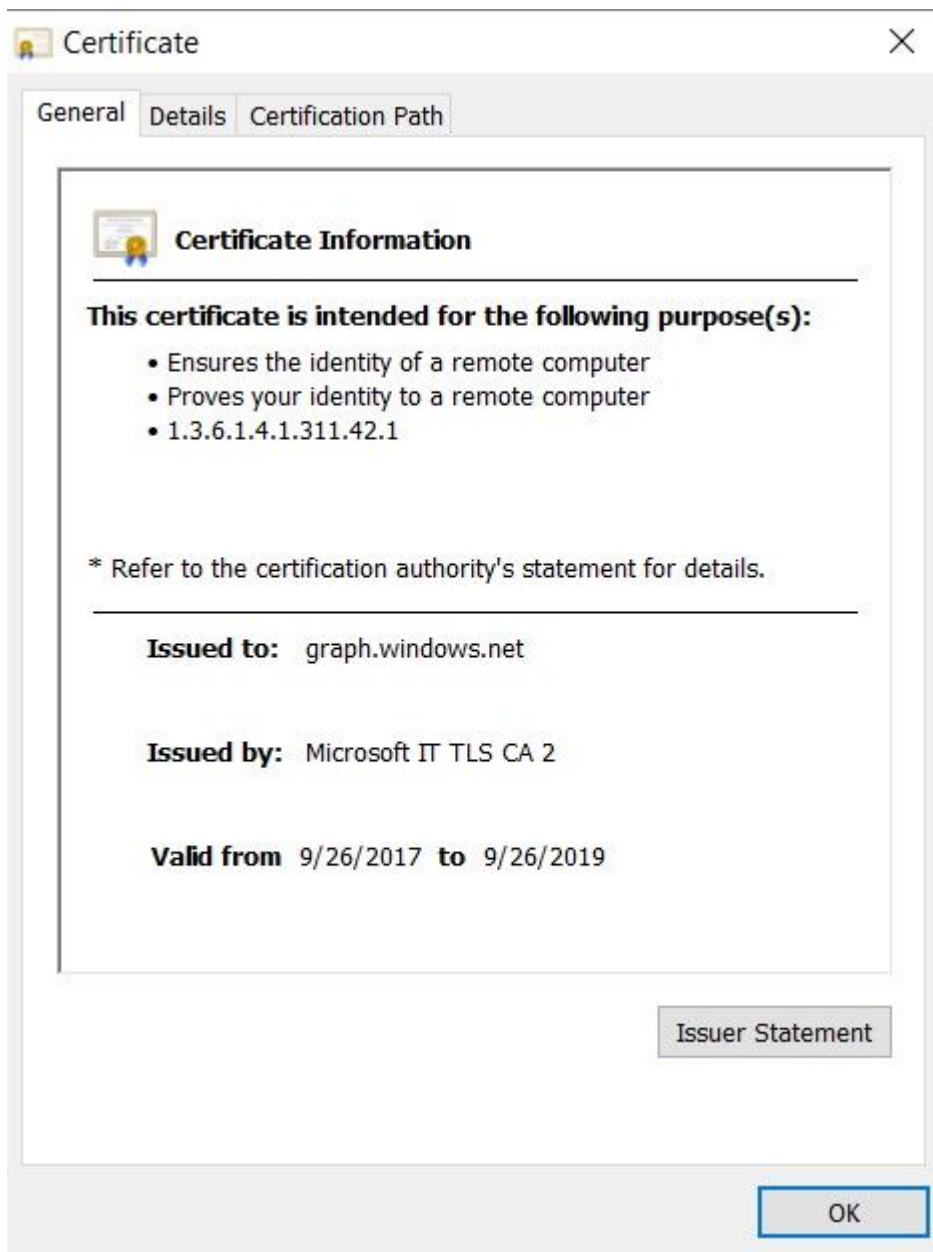
Passaggio 2. Assegno ise-psc.log per questi registri:

- 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

Ciò indica che è necessario importare `graph.microsoft.com` presente in questa pagina.

```
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>
```

Passaggio 3. Fare clic sul pulsante `locker` e controllare i dettagli del certificato.



Passaggio 4. Salvarlo in un file in formato BASE64 e importarlo in ISE Trusted Store. Assicurarsi di importare l'intera catena di certificati. Quindi, eseguire nuovamente il test della connessione al server MDM.

Non è stato possibile acquisire il token Auth da Azure AD



Connection to server failed with:

Failed to acquire auth token from Azure AD. Error validating credentials. Client authentication failed. [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.

Questo errore si verifica in genere quando il manifesto JSON contiene la catena di certificati ISE errata. Prima di caricare il file manifesto in Azure, verificare se è presente almeno questa configurazione:

```
"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"
  }
],
```

L'esempio precedente si basa su uno scenario in cui sono presenti una PAN e una SAN. Eseguire nuovamente gli script da PowerShell e importare i valori BASE64 corretti. Provare a caricare il file manifesto e non si devono riscontrare errori.

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

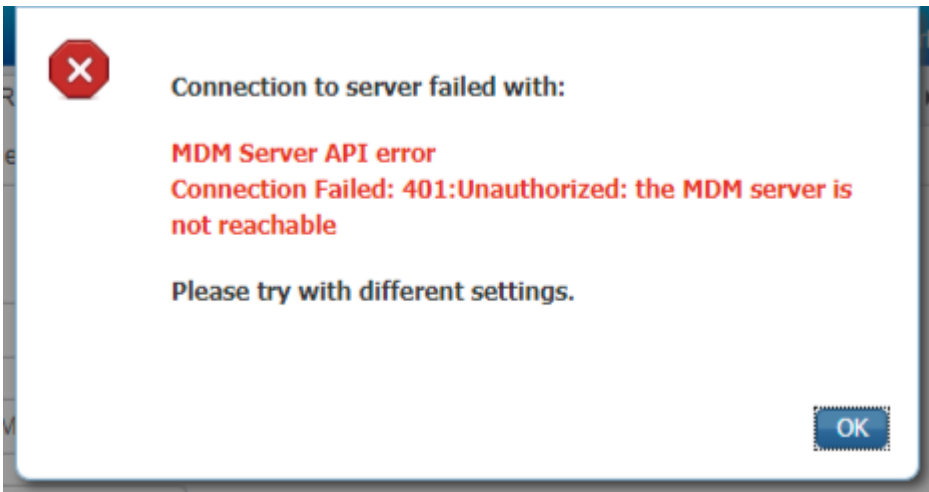
```
$cer.Import(â€œmycer.cerâ€œ)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

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

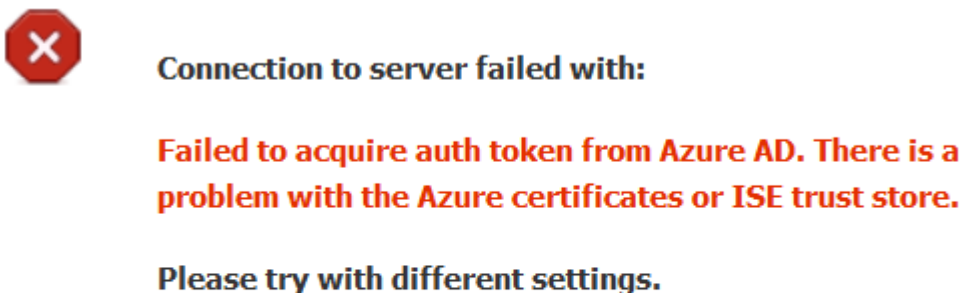
$keyid = [System.Guid]::NewGuid().ToString()
```

Ricordare di applicare i valori per \$base64Thumbprint, \$base64Value e \$keyid come indicato nella sezione Configura.

Non è stato possibile acquisire il token Auth da Azure AD



Questo errore si verifica spesso quando non vengono concesse le autorizzazioni corrette all'app Azure in portal.azure.com. Verificare che l'app disponga degli attributi corretti e fare clic su Grant Permissions dopo ogni cambiamento.



OK

Questo messaggio viene visualizzato quando ISE tenta di accedere all'URL di emissione del token e restituisce un certificato che ISE non restituisce. Verificare che l'intera catena di CA si trovi nell'archivio di attendibilità ISE. Se il problema persiste anche dopo l'installazione del certificato corretto nell'archivio attendibile di ISE, eseguire l'acquisizione dei pacchetti e verificare la connettività per verificare gli elementi inviati.

Informazioni correlate

- [Chiamate da servizio a servizio con credenziali client](#)
- [Azure - Autenticazione e autorizzazione](#)
- [Azure - Quickstart: registra un'applicazione con la piattaforma delle identità Microsoft](#)
- [manifesto dell'app Azure Active Directory](#)
- [Documentazione e supporto tecnico " Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).