Integrate Intune MDM with Identity Services Engine

Contents

Introduction

This document describes how to integrate Intune Mobile Device Management (MDM) with Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of MDM Services in Cisco ISE
- Knowledge of Microsoft Azure Intune Services

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine 3.0
- Microsoft Azure Intune Application

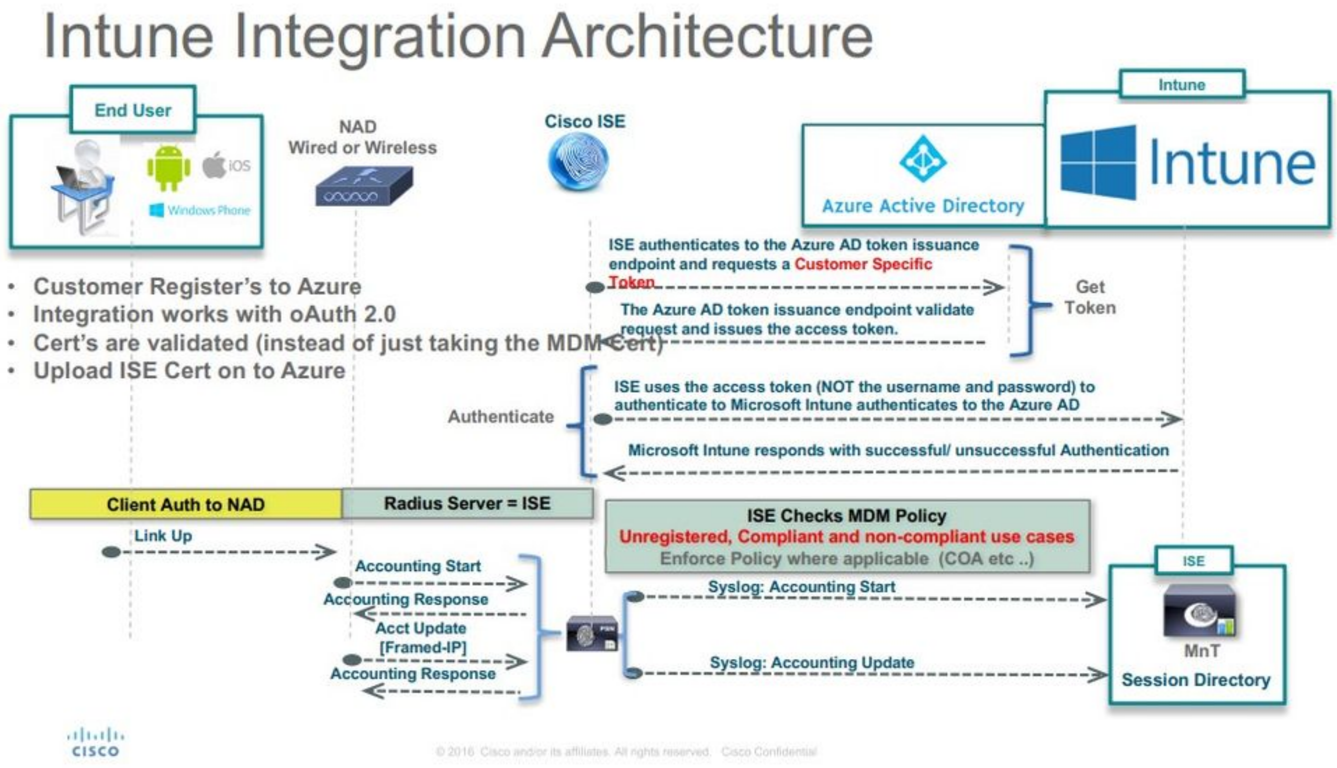
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

MDM servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. These servers act as the policy server that controls the use of some applications on a mobile device (for example, an email application) in the deployed environment. However, the network is the only entity that can provide granular access to endpoints based on Access Control Lists (ACLs). ISE queries the MDM servers for the necessary device attributes in order to create ACLs that provide network access control for those devices. Cisco ISE integrates with Microsoft Intune MDM Server in order to help organizations secure corporate data when devices try to access on-premises resources.

Configure

Network Diagram



Intune Integration Architecture

- Customer Register's to Azure
- Integration works with oAuth 2.0
- Cert's are validated (instead of just taking the MDM Cert)
- Upload ISE Cert on to Azure

ISE authenticates to the Azure AD token issuance endpoint and requests a Customer Specific Token

The Azure AD token issuance endpoint validate request and issues the access token.

ISE uses the access token (NOT the username and password) to authenticate to Microsoft Intune authenticates to the Azure AD

Microsoft Intune responds with successful/ unsuccessful Authentication

ISE Checks MDM Policy
Unregistered, Compliant and non-compliant use cases
Enforce Policy where applicable (COA etc ..)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Microsoft Intune

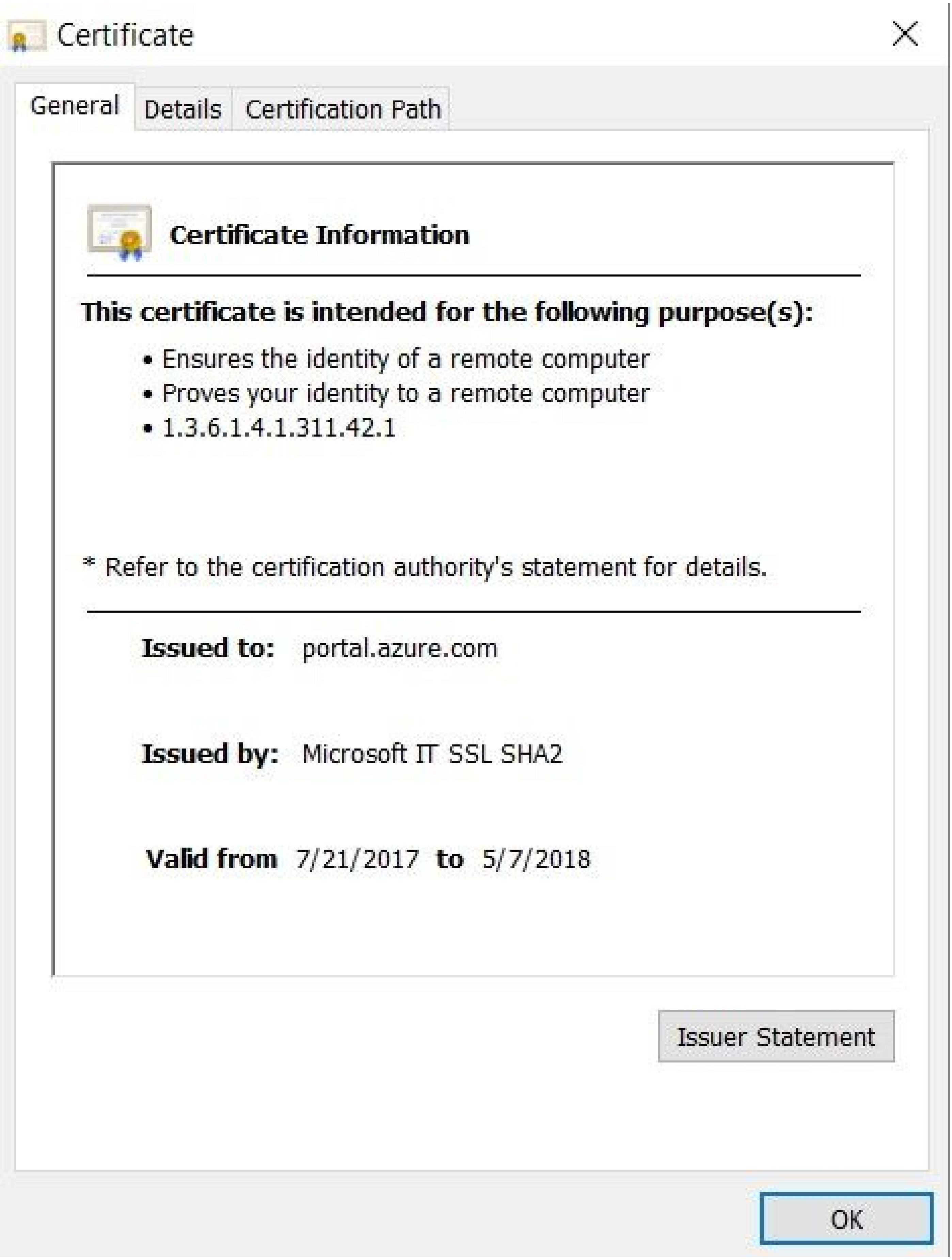
Import the Certificates from the Intune Portal to the ISE Trusted Store

Log in to the Intune Admin Console or Azure Admin console, whichever site has your tenant. Use the browser in order to get the certificate details:

Step 1. Open the Microsoft Azure portal from a web browser.

Step 2. Click the **lock symbol** in the browser toolbar, then click View Certificates.

Step 3. In the Certificate window, click the Certification Path tab. An example is shown here:



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.311.42.1

* Refer to the certification authority's statement for details.

Issued to: portal.azure.com

Issued by: Microsoft IT SSL SHA2

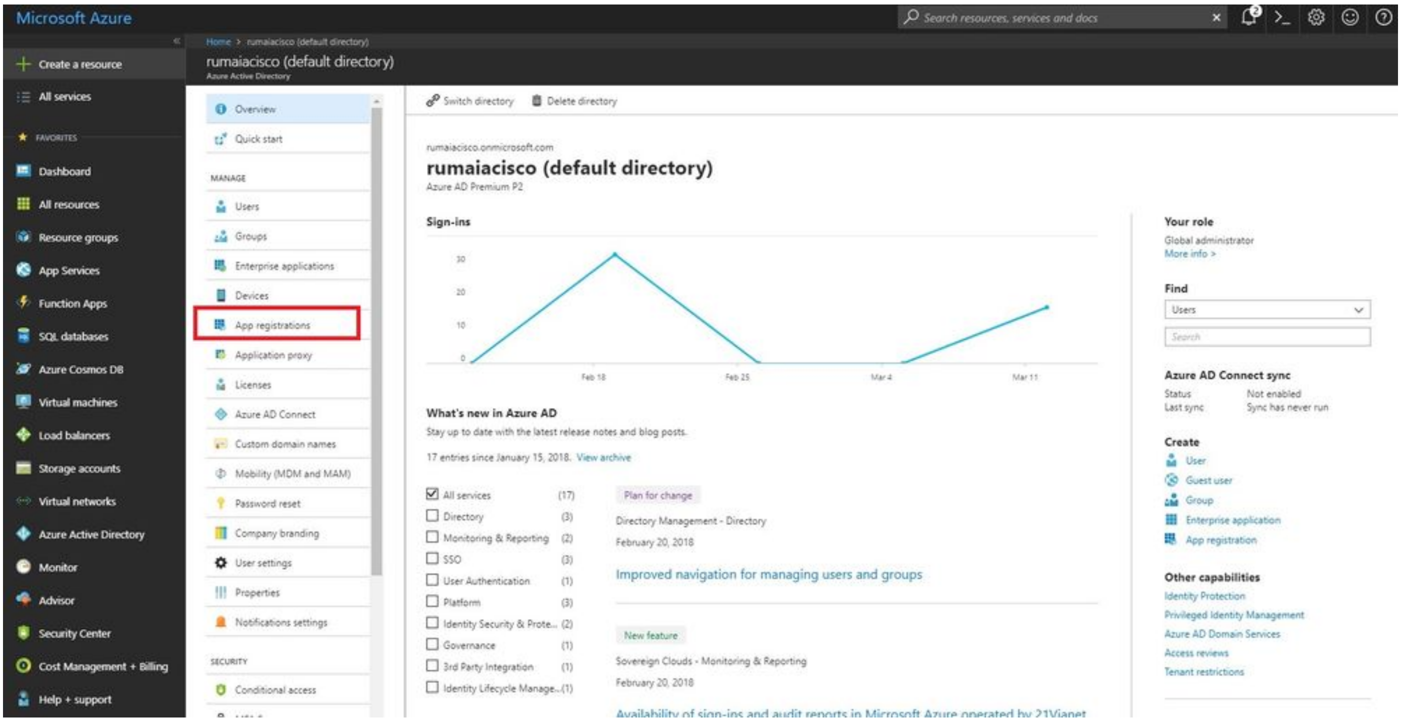
Valid from 7/21/2017 **to** 5/7/2018

Step 4. Find Baltimore Cyber Trust root, which is the usual Root CA. However, if there is any other different Root CA, click that Root CA certificate. On the Details tab of that Root CA certificate, you can **copy** it to the file and **save** it as BASE64 cert.

Step 5. In ISE, navigate to Administration > System > Certificates > Trusted Certificates, and import the root certificate that was just saved. Give the certificate a meaningful name, such as Azure MDM. Repeat the procedure for the intermediate CA certificates as well.

Deploy ISE as an Application in the Azure Portal

Step 1. Navigate to the Azure Active Directory and choose App registrations.



Stay up to date with the latest release notes and blog posts.

17 entries since January 15, 2018. View archive

Directory Management - Directory

February 20, 2018

Improved navigation for managing users and groups

Sovereign Clouds - Monitoring & Reporting

February 20, 2018

Availability of sign-ins and audit reports in Microsoft Azure operated by 21Vianet

Global administrator

More info >

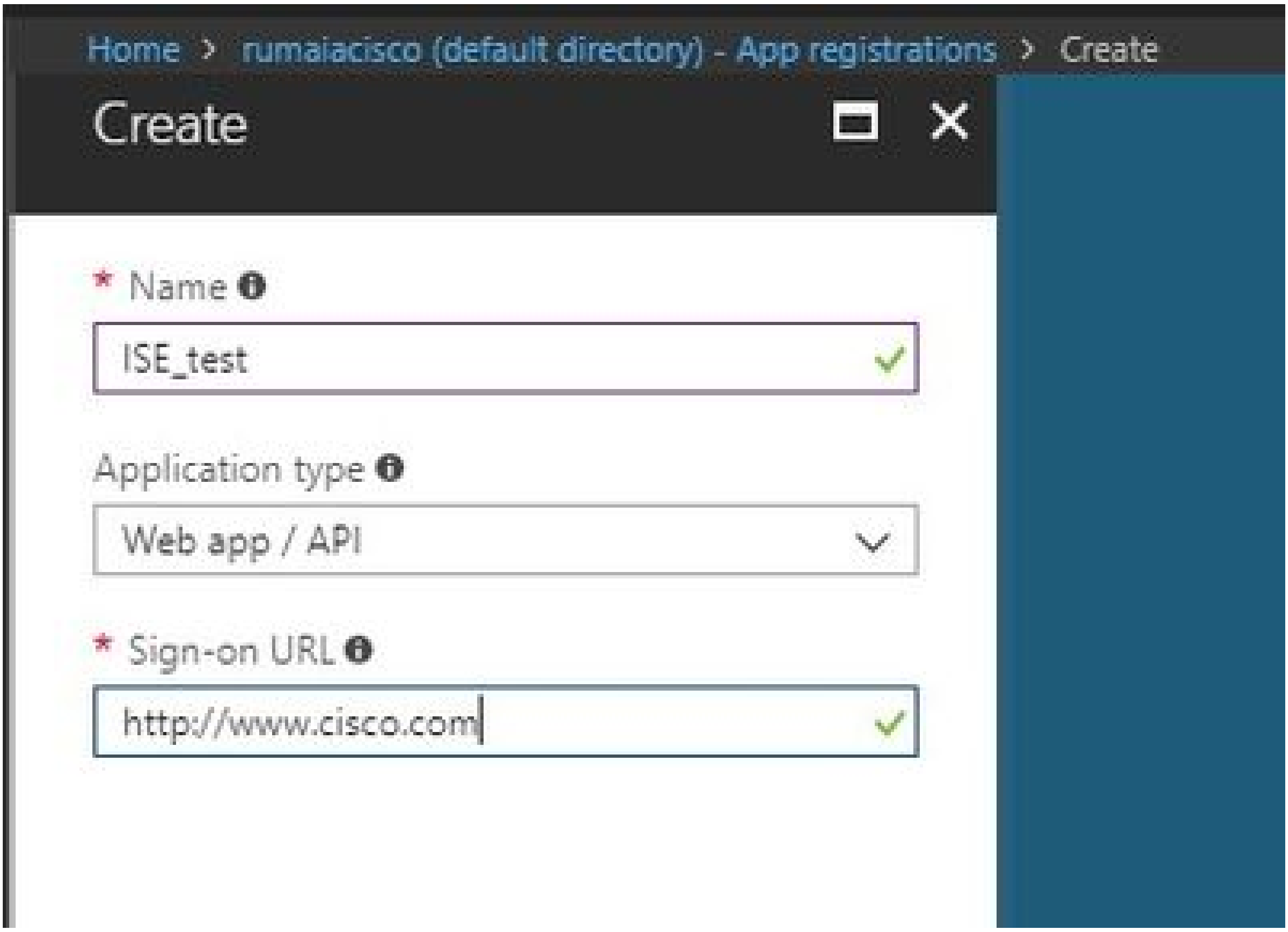
Users

Search

Status: Not enabled

Last sync: Sync has never run

Step 2. In App registrations, create a new application registration with the ISE name. Click Create as shown in this image.



Home > rumaiacisco (default directory) - App registrations > Create

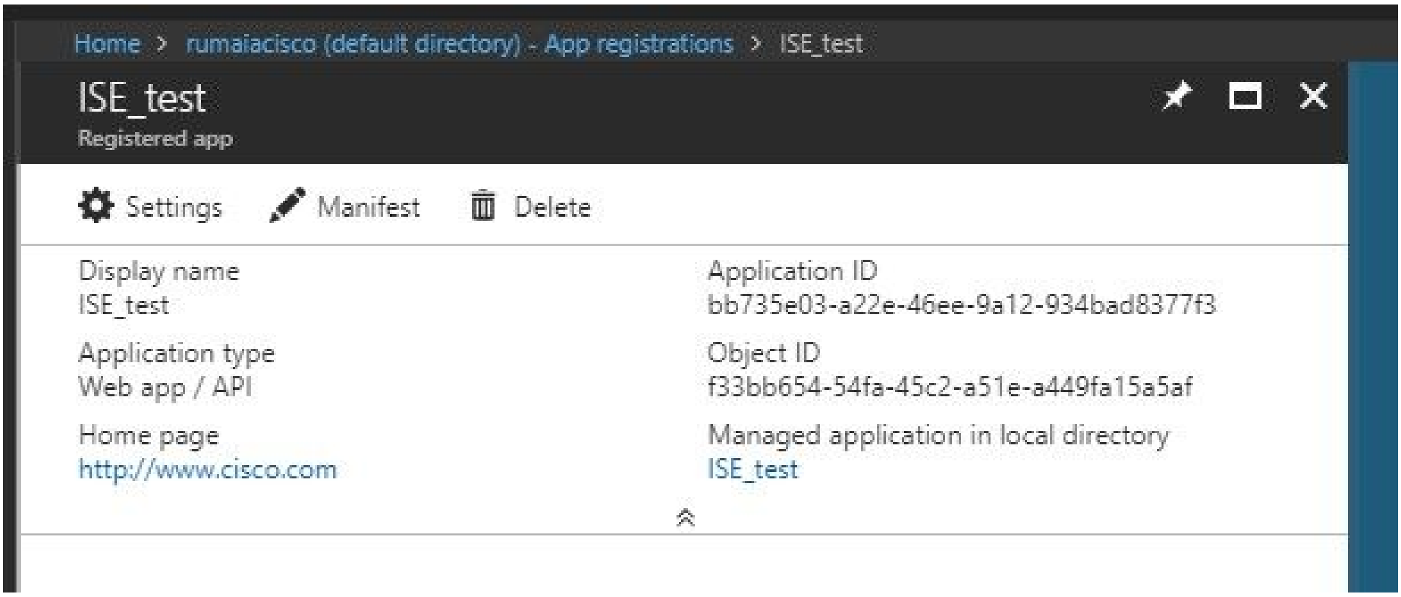
Create

* Name: ISE_test

Application type: Web app / API

* Sign-on URL: http://www.cisco.com

Step 3. Choose Settings in order to edit the application and add the required components.



Home > rumaiacisco (default directory) - App registrations > ISE_test

ISE_test

Registered app

Display name: ISE_test

Application type: Web app / API

Home page: http://www.cisco.com

Application ID: bb735e03-a22e-46ee-9a12-934bad8377f3

Object ID: f33bb654-54fa-45c2-a51e-a449fa15a5af

Managed application in local directory: ISE_test

Step 4. Under Settings, choose the required permissions, and **apply** these options:

1. Microsoft Graph
   - Application Permissions
     - Read directory data
   - Delegated Permissions

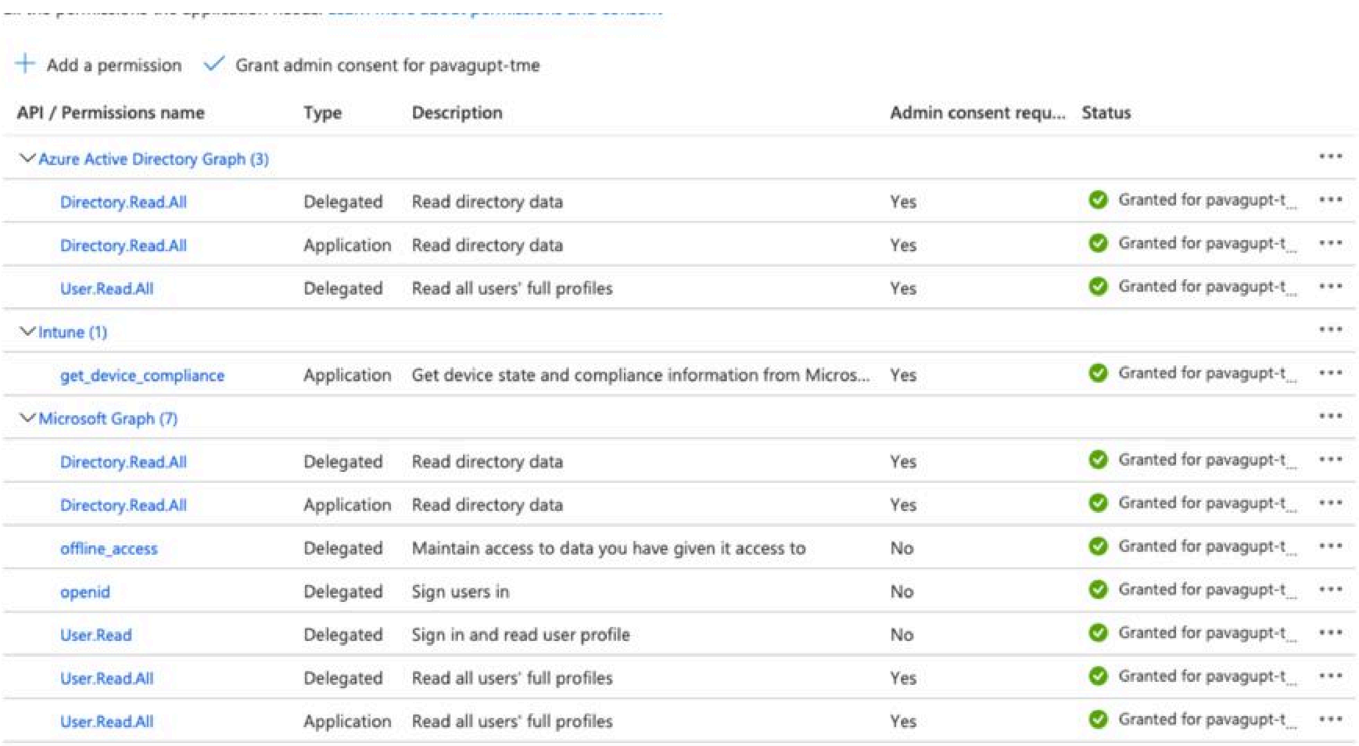
    - Read Microsoft Intune Device Configuration and Policies
    - Read Microsoft Intune Configuration
    - Sign users in
    - Access the data of the user anytime

2. Microsoft Intune API
    - Application Permissions
        - Get device state and compliance information from Microsoft Intune

3. Windows Azure Active Directory
    - Application Permissions
        - Read directory data

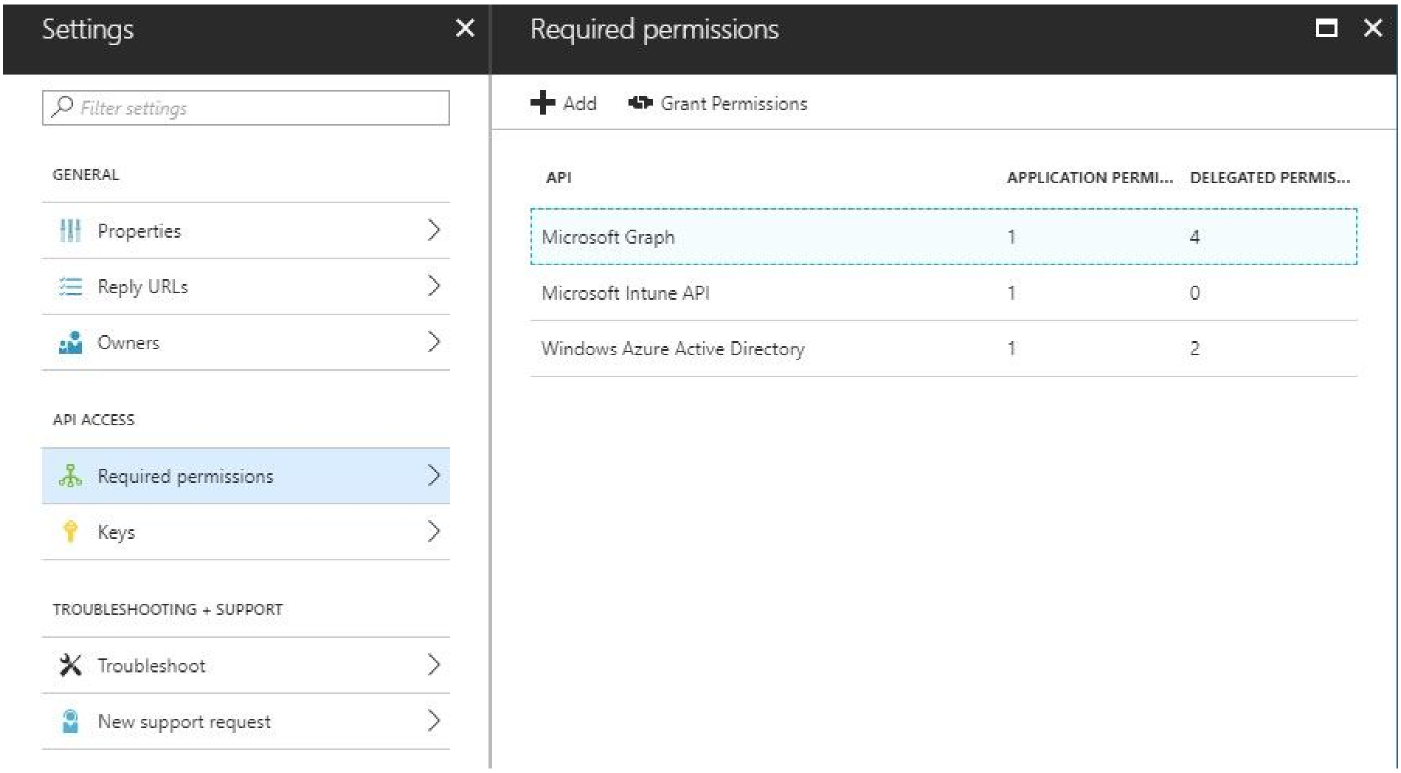
    - Delegated Permissions
        - Read directory data
        - Sign in and read the user profile

The result of the configuration looks similar to what is shown here:



+ 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	✓ Granted for pavagupt-t...	···
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for pavagupt-t...	···
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for pavagupt-t...	···
∨ Intune (1)					···
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	✓ Granted for pavagupt-t...	···
∨ Microsoft Graph (7)					···
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for pavagupt-t...	···
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for pavagupt-t...	···
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for pavagupt-t...	···
openid	Delegated	Sign users in	No	✓ Granted for pavagupt-t...	···
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for pavagupt-t...	···
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for pavagupt-t...	···
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for pavagupt-t...	···

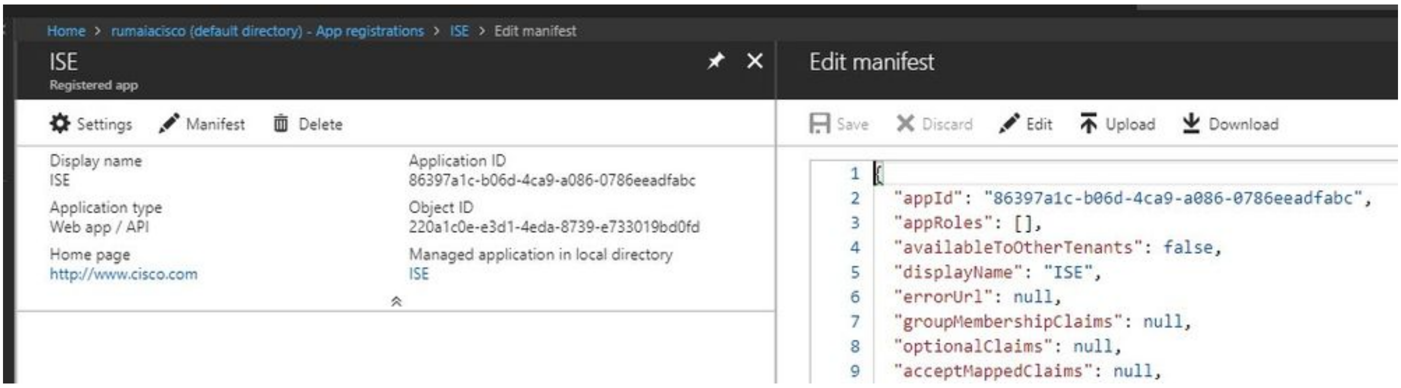


API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	1	4
Microsoft Intune API	1	0
Windows Azure Active Directory	1	2

Step 5. Click Grant Permissions in order to confirm all the application permissions. This process takes 5-10 minutes to take effect. Edit the Azure Manifest file for the application created in order to import internal ISE CA certificates.

Import ISE Certificates to the Application in Azure

Step 1. **Download** the manifest file for the application.



Display name
ISE

Application type
Web app / API

Home page
http://www.cisco.com

Application ID
86397a1c-b06d-4ca9-a086-0786eeadfabc

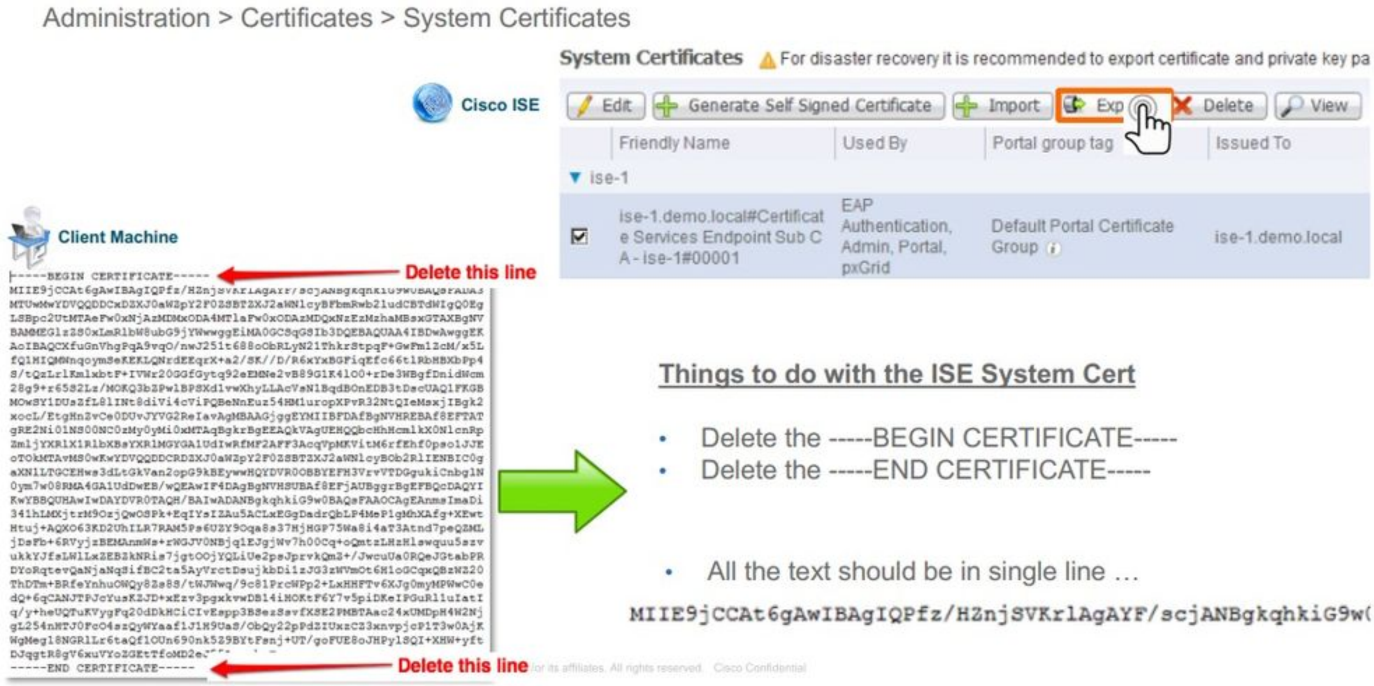
Object ID
220a1c0e-e3d1-4eda-8739-e733019bd0fd

Managed application in local directory
ISE

```
{
  "appId": "86397a1c-b06d-4ca9-a086-0786eeadfabc",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "ISE",
  "errorUrl": null,
  "groupMembershipClaims": null,
  "optionalClaims": null,
  "acceptMappedClaims": null,
```

Note: It is a file with a JSON extension. Do not edit the file name or the extension, otherwise, it fails.

Step 2. Export the ISE system certificate from all the nodes. On the PAN, navigate to Administration > System > Certificates > System Certificates, choose the **Default self-signed server certificate**, and click Export.. Choose Export Certificate Only(default), and choose a place to **save** it. **Delete** the BEGIN and END tags from the certificate and **copy** the rest of the text as a single line. This is applicable for versions before June 2020 described in the Legacy Option section.



Administration > Certificates > System Certificates

Cisco ISE
System Certificates
For disaster recovery it is recommended to export certificate and private key pa
Edit
Generate Self Signed Certificate
Import
Exp
Delete
View
Client Machine
Delete this line
Delete this line

	Friendly Name	Used By	Portal group tag	Issued To
▼ ise-1				
☑	ise-1.demo.local#Certificate Services Endpoint Sub CA - ise-1#00001	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group ⓘ	ise-1.demo.local

```
-----BEGIN CERTIFICATE-----
MIIE9jCCAt6gAwIBAgIQPfz/HZnjSVKrlAgAYF/scjANBgkqhkiG9w0BAQsFADAz
MTUwMwYDVQQDDCxDZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBFbmRwb2ludCBTdWIgQ0Eg
LSBpc2UtMTAeFw0xNjAzMDMxODA4MTlaFw0xODAzMDQxNzEzMzhaMBsxGTAXBgNV
BAMMEGlzZS0xLmRlbW8ubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCXfuGnVhgPqA9vqO/nwJ25lt688oObRLyN21ThkrStpqF+GwFm1ZcM/x5L
fQ1MIQMWnqoymSeKEKLQNrdEEqrX+a2/SK//D/R6xYxBGFiqEfc66tlRbMBXbPp4
S/tQzLrlKmlxbtF+IVWr20GGfGytq92eEMNe2vB89G1K41O0+rDe3WBgfDnidWcm
28g9+r65S2Lz/MOKQ3bZPw1BPSXd1vwXhyLLAcVsN1BqdBOnEDB3tDscUAQ1FKGB
MOwSY1DUsZfL8lINt8diVi4cViPQBeNnEuz54HM1uropXPvR32NtQIeMsxjIBgk2
xocL/EtgHnZvCe0DUvJYVG2ReIavAgMBAAGjggEYMIIBFDAfBgNVHREBAf8EFTAT
gRE2Ni01NS00NC0zMy0yMi0xMTAqBgkrBgEEAQkVAgUEHQQbcHhHcmlkX0NlcnRp
ZmljYXRlX1RlbXBsYXRlMGYGA1UdIwRfMF2AFF3AcqVpMKVitM6rfEhf0pso1JJE
oTOkMTAvMS0wKwYDVQQDDCRDZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBOb2RlIENBIC0g
aXNlLTGCEHws3dLtGkVan2opG9kBEywwHQYDVR0OBBYEFH3VrvVTDGgukiCnbg1N
0ym7w08RMA4GA1UdDwEB/wQEAwIF4DAgBgNVHSUBAf8EFjAUBggrBgEFBQcDAQYI
KwYBBQUHAwIwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAgEAnmsImaDi
341hLMXjtrM9OzjQwO8Pk+EqIYsIZAu5ACLxEGgDadrQbLP4MeP1gMhXAfg+XEwt
Htuj+AQXO63KD2UhILR7RAM5Ps6UZY9Oqa8s37HjHGP75Wa8i4aT3Atnd7peQZML
jDsFb+6RVyjzBEMAnmWs+rWGJV0NBjq1EJgjWv7h00Cq+oQmtzLHzHlswquu5szv
ukkYJfsLWlLxZEBZkNRis7jgtOOjYQLiUe2psJprvkQmZ+/JwcuUa0RQeJGtabPR
DYoRqtevQaNjaNqSifBC2ta5AyVrctDsujkbDi1zJG3zWVmOt6M1oGCqxQBzWZ20
ThDTm+BRfeYnhuOWQy8Zs88/tWJWwq/9c81PrcWPp2+LxHHFTv6XJg0myMPWwC0e
dQ+6qCANJTPJcYusKZJD+xEzv3pgxkvwDB14iMOKtF6Y7v5piDKeIPGuRl1uIatI
q/y+heUQTuKVygFq20dDkHCiCIvEspp3BSezSsvfXSE2PMBTAac24xUMDpH4W2Nj
gL254nMTJ0FcO4szQyWYaaf1J1M9UaS/ObQy22pPdZIUxzCZ3xnvpjcP1T3w0AjK
WgMeg18NGRlLr6taQf1OUn690nk529BYtFsnj+UT/goFUE8oJHPy18QI+XHW+yft
DJqgtR8gV6xuVYoZGEtTfoMD2e
-----END CERTIFICATE-----
```

Things to do with the ISE System Cert

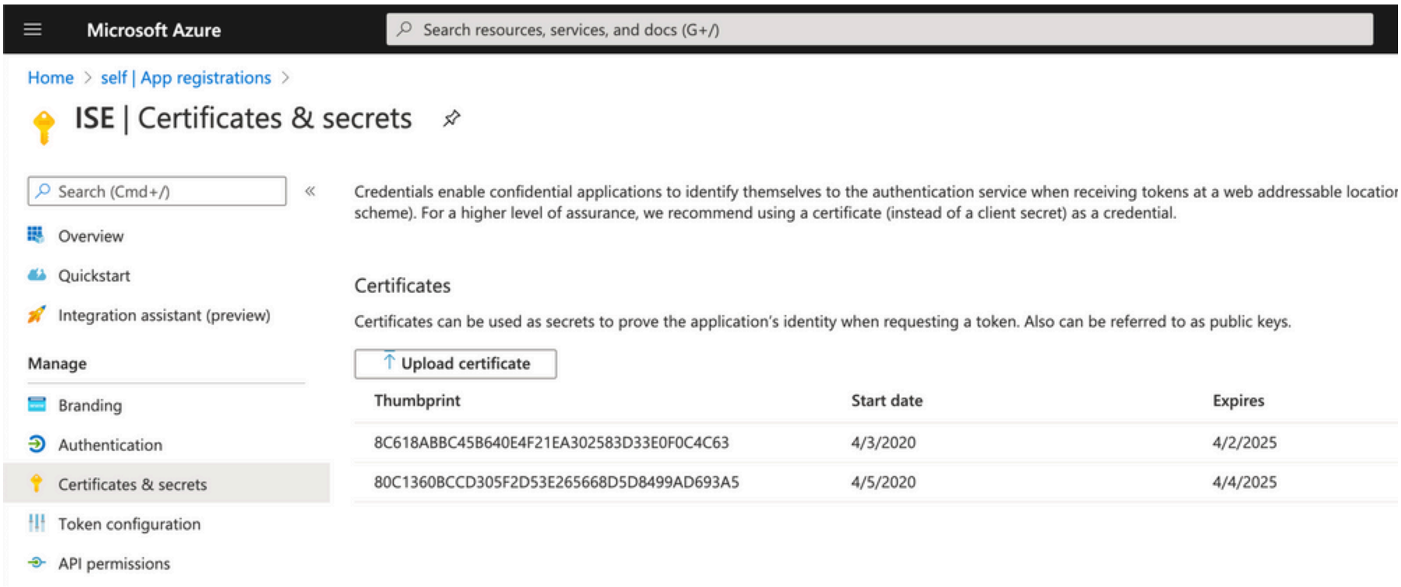
- Delete the -----BEGIN CERTIFICATE-----
- Delete the -----END CERTIFICATE-----

- All the text should be in single line …

MIIE9jCCAt6gAwIBAgIQPfz/HZnjSVKrlAgAYF/scjANBgkqhkiG9w(

or its affiliates. All rights reserved. Cisco Confidential

As of June 2020, The Portal allows you to upload certificates directly.



ISE | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable locatio scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

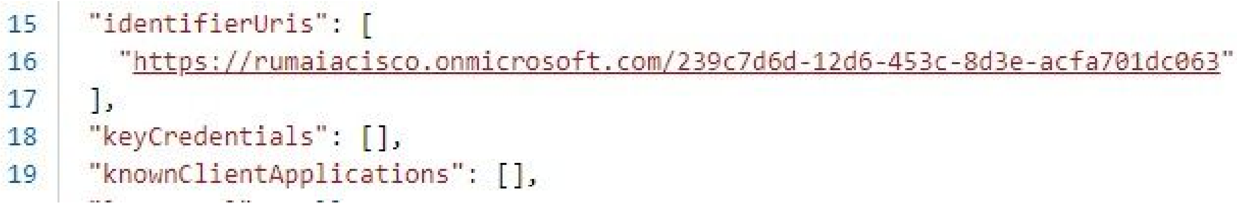
Thumbprint	Start date	Expires
8C618ABBC45B640E4F21EA302583D33E0F0C4C63	4/3/2020	4/2/2025
80C1360BCCD305F2D53E265668D5D8499AD693A5	4/5/2020	4/4/2025

Legacy Option:

Step 1. Run a PowerShell procedure in order to turn the certificate to BASE64 and properly import it to the Azure JSON manifest file. Use the Windows PowerShell or Windows PowerShell ISE application from Windows. Use these commands:

```
$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()
```

Step 2. Keep the values for $base64Thumbprint, $base64Value, and $keyid, which are used in the next step. All these values are added to the JSON field keyCredentialssince by default, it looks like this:



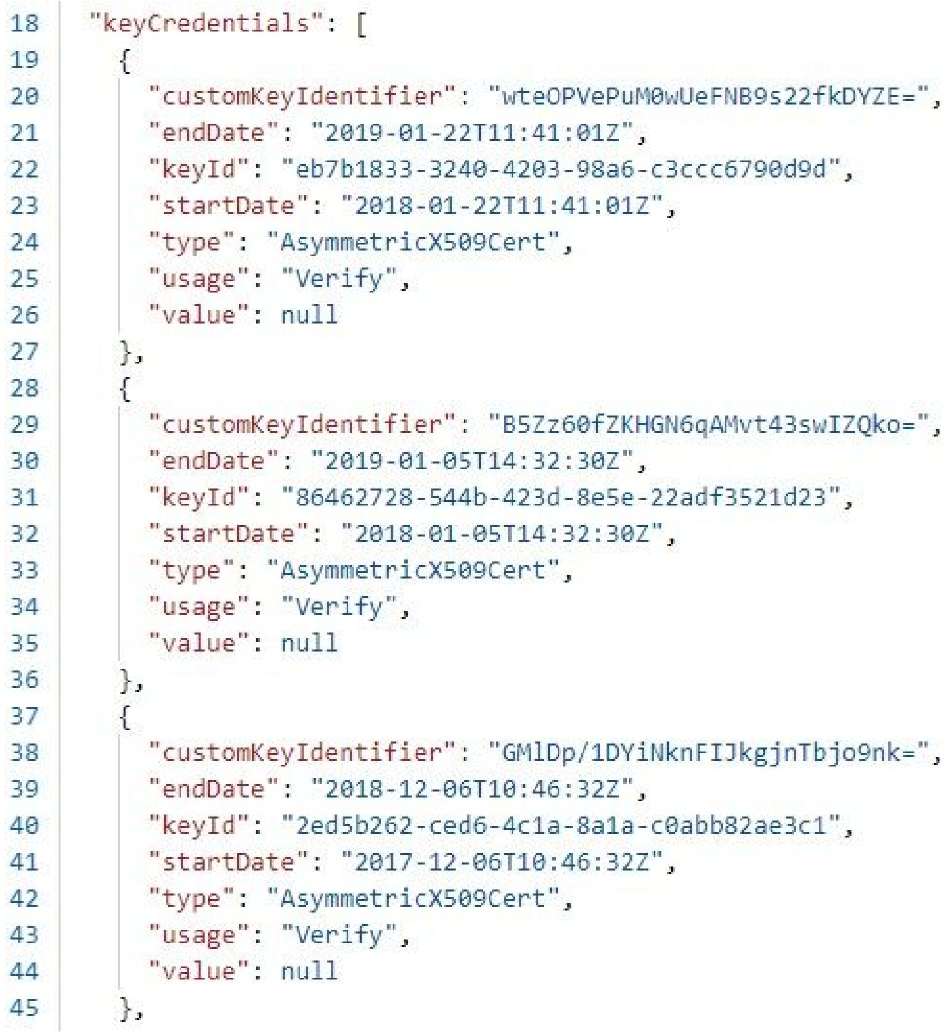
```
"identifierUris": [
  "https://rumaiacisco.onmicrosoft.com/239c7d6d-12d6-453c-8d3e-acfa701dc063"
],
"keyCredentials": [],
"knownClientApplications": [],
```

In order to do so, ensure you use the values in this order:

```
"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"

  }
],
```

Step 3. **Upload** the edited JSON file to Azure Portal in order to validate the keyCredentials from the certificates used on ISE.

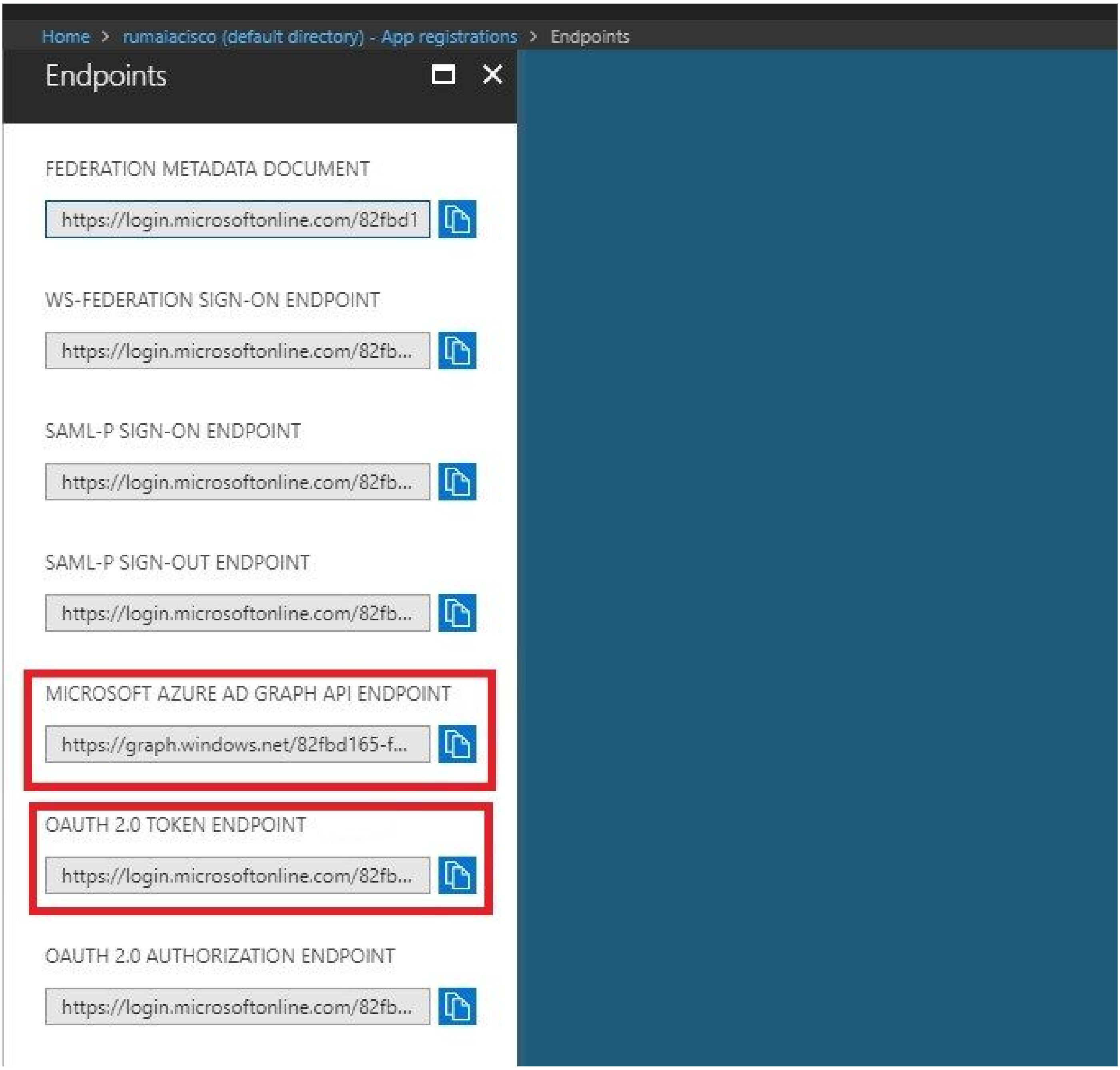
It must look similar to this:



```
  "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
    },
```

Step 4. Be aware that after the Upload, the value field under keyCredentials shows null since this is enforced by the Microsoft side to not allow these values to be seen after the first Upload.

The values required to add the MDM server in ISE can be copied from Microsoft Azure AD Graph API Endpoint and OAUTH 2.0 Token Endpoint.



Home > rumaiacisco (default directory) - App registrations > Endpoints

Endpoints

FEDERATION METADATA DOCUMENT

https://login.microsoftonline.com/82fbd1

WS-FEDERATION SIGN-ON ENDPOINT

https://login.microsoftonline.com/82fb...

SAML-P SIGN-ON ENDPOINT

https://login.microsoftonline.com/82fb...

SAML-P SIGN-OUT ENDPOINT

https://login.microsoftonline.com/82fb...

MICROSOFT AZURE AD GRAPH API ENDPOINT

https://graph.windows.net/82fbd165-f...

OAUTH 2.0 TOKEN ENDPOINT

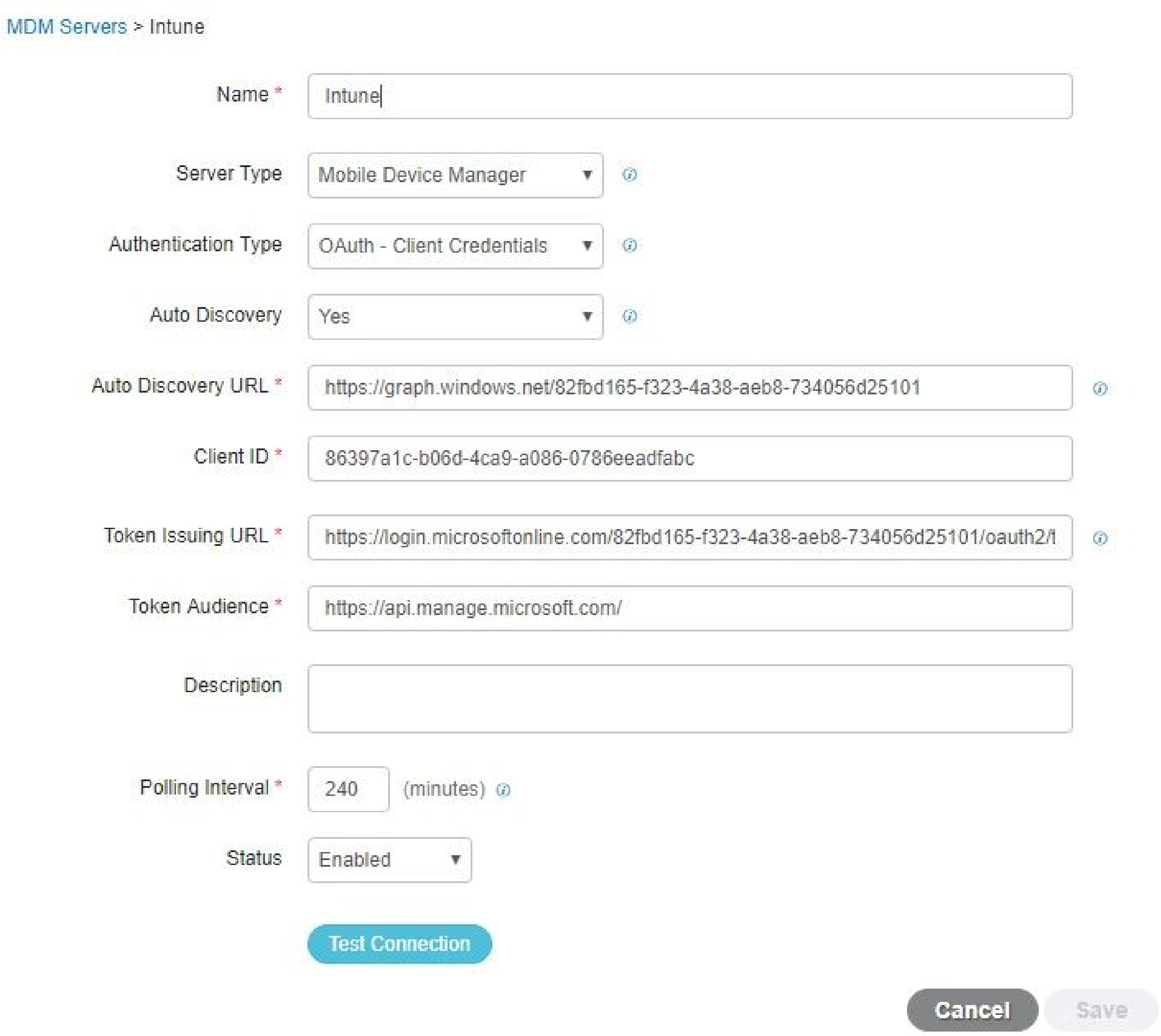
https://login.microsoftonline.com/82fb...

OAUTH 2.0 AUTHORIZATION ENDPOINT

https://login.microsoftonline.com/82fb...

These values must be entered in the ISE GUI. Navigate to Administration > Network Resources > External MDM and **add** a new server:

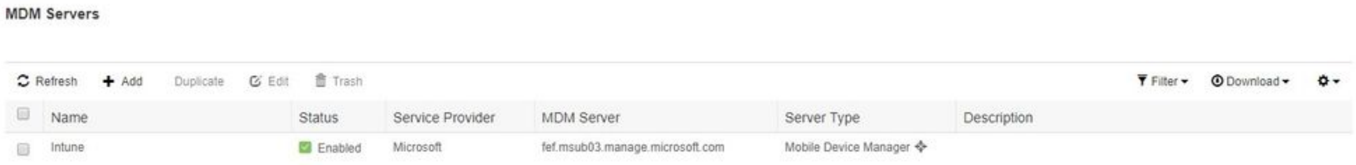
ISE	Intune
Auto Discovery URL	Endpoints > Microsoft Azure AD Graph API Endpoint
Client ID	{Registered-App-Name} > Application ID
Token Issuing URL	Endpoints > OAuth 2.0 Token Endpoint



MDM Servers > Intune

Name *	Intune
Server Type	Mobile Device Manager
Authentication Type	OAuth - Client Credentials
Auto Discovery	Yes
Auto Discovery URL *	https://graph.windows.net/82fbd165-f323-4a38-aeb8-734056d25101
Client ID *	86397a1c-b06d-4ca9-a086-0786eeadfabc
Token Issuing URL *	https://login.microsoftonline.com/82fbd165-f323-4a38-aeb8-734056d25101/oauth2/t
Token Audience *	https://api.manage.microsoft.com/
Description	
Polling Interval *	240 (minutes)
Status	Enabled

After the configuration is complete, the status shows enabled.

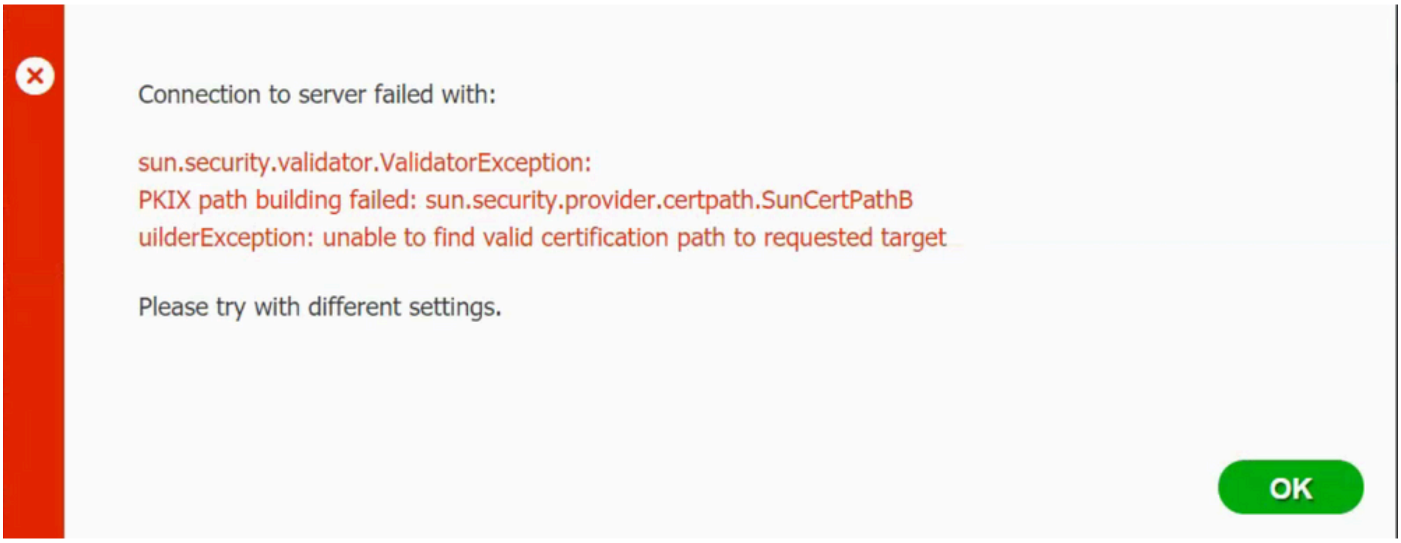


MDM Servers

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

Verify and Troubleshoot

"Connection to the server failed" based on sun.security.validator.ValidatorException



Connection to server failed with:

sun.security.validator.ValidatorException:
PKIX path building failed: sun.security.provider.certpath.SunCertPathB
uilderException: unable to find valid certification path to requested target

Please try with different settings.

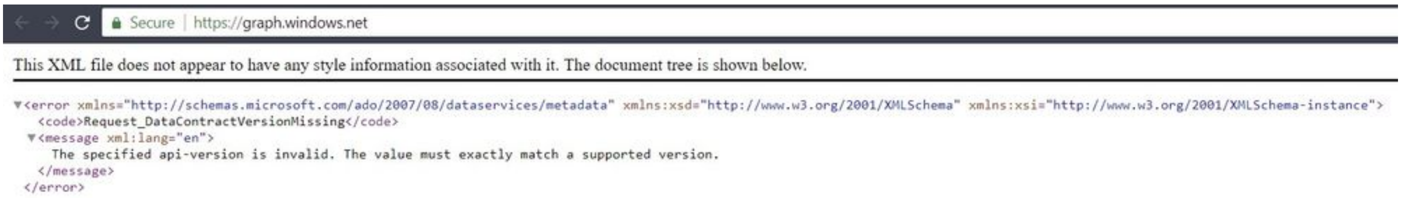
Step 1. Collect the support bundle with these logs at the TRACE level:

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

Step 2. Check ise-psc.log for these 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 -::::- 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

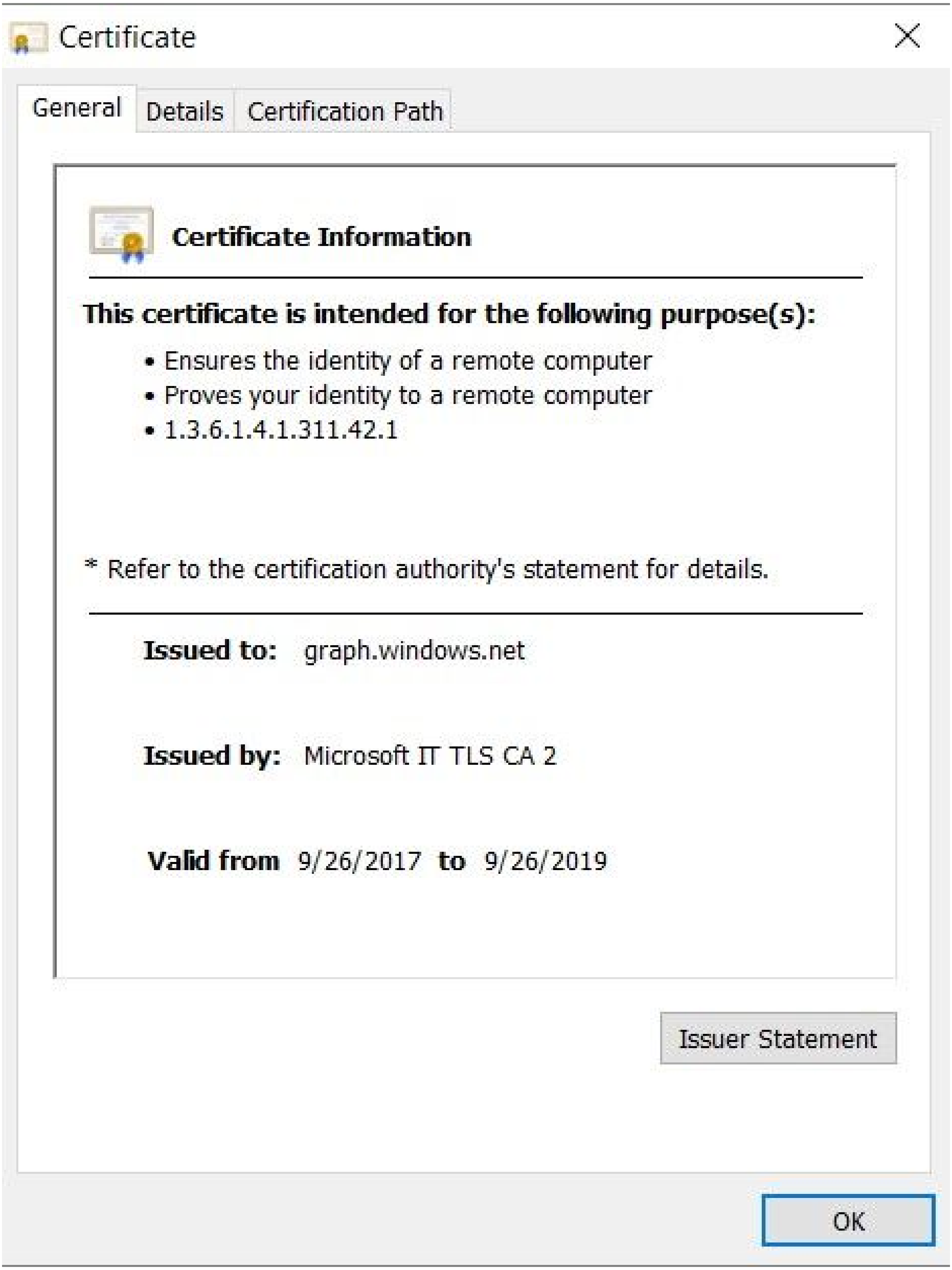
This indicates that there is a need to import the graph.microsoft.com certificate, present on this page.



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>
```

Step 3. Click the lockericon and check the certificate details.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.311.42.1

* Refer to the certification authority's statement for details.

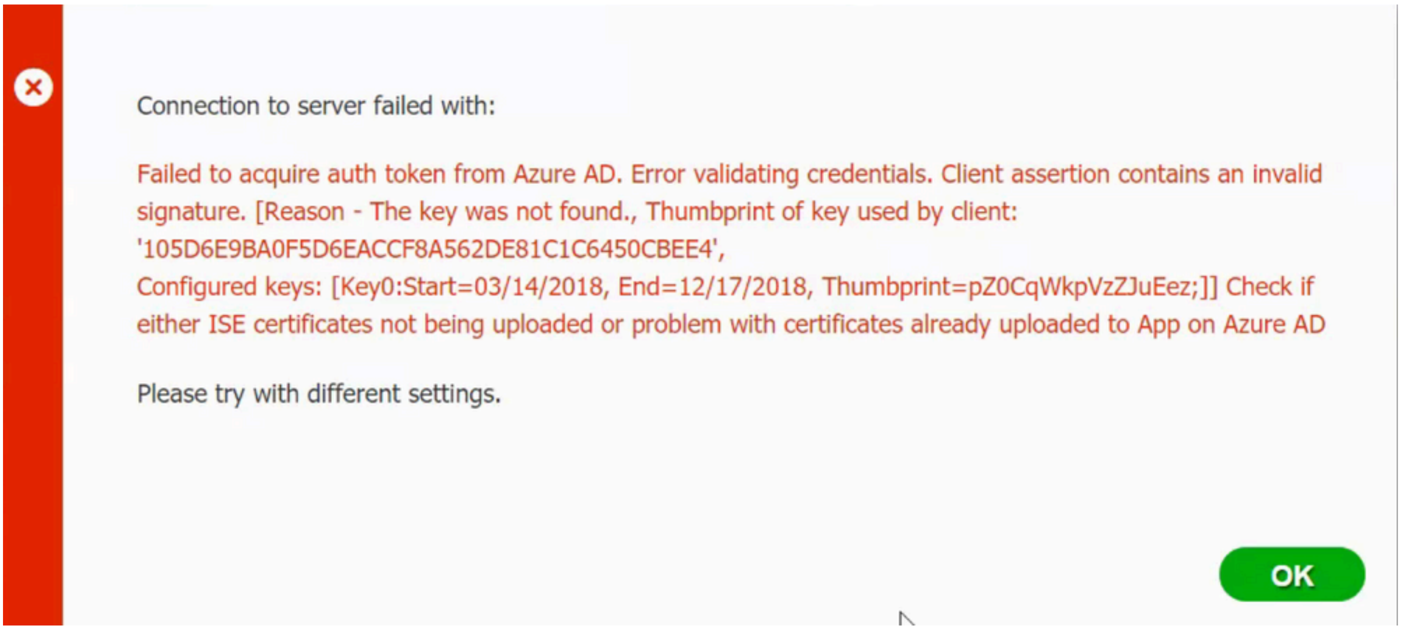
Issued to: graph.windows.net

Issued by: Microsoft IT TLS CA 2

Valid from 9/26/2017 **to** 9/26/2019

Step 4. **Save** it to a file in BASE64 format and **import** it to ISE Trusted Store. Ensure you import the full certificate chain. After this, **test the connection** to the MDM server again.

Failed to Acquire Auth Token from Azure AD



Connection to server failed with:

Failed to acquire auth token from Azure AD. Error validating credentials. Client assertion contains an invalid 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=pZ0CqWkpVzZJuEez;]] Check if either ISE certificates not being uploaded or problem with certificates already uploaded to App on Azure AD

Please try with different settings.

Usually, this error occurs when the manifest JSON file contains the wrong ISE certificate chain. Before you upload the manifest file to Azure, verify if at least this configuration is present:

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

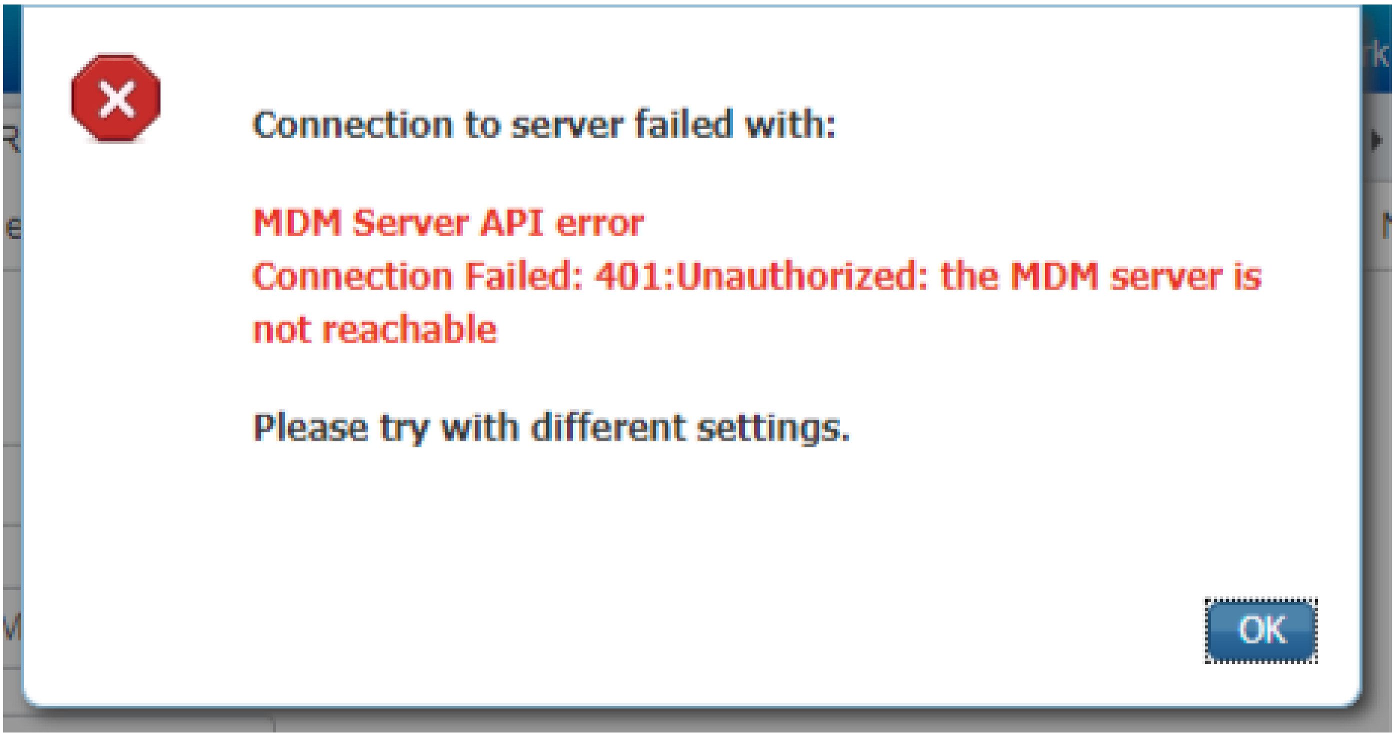
The previous example is based on a scenario where there is a PAN and SAN. **Run** the scripts from PowerShell again and **import** the proper BASE64 values. Try to upload the manifest file and you must not face any errors.

```
$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()
```

Remember to apply the values for $base64Thumbprint, $base64Value and $keyid as mentioned in the steps in the Configure section.

Failed to Acquire Auth Token from Azure AD

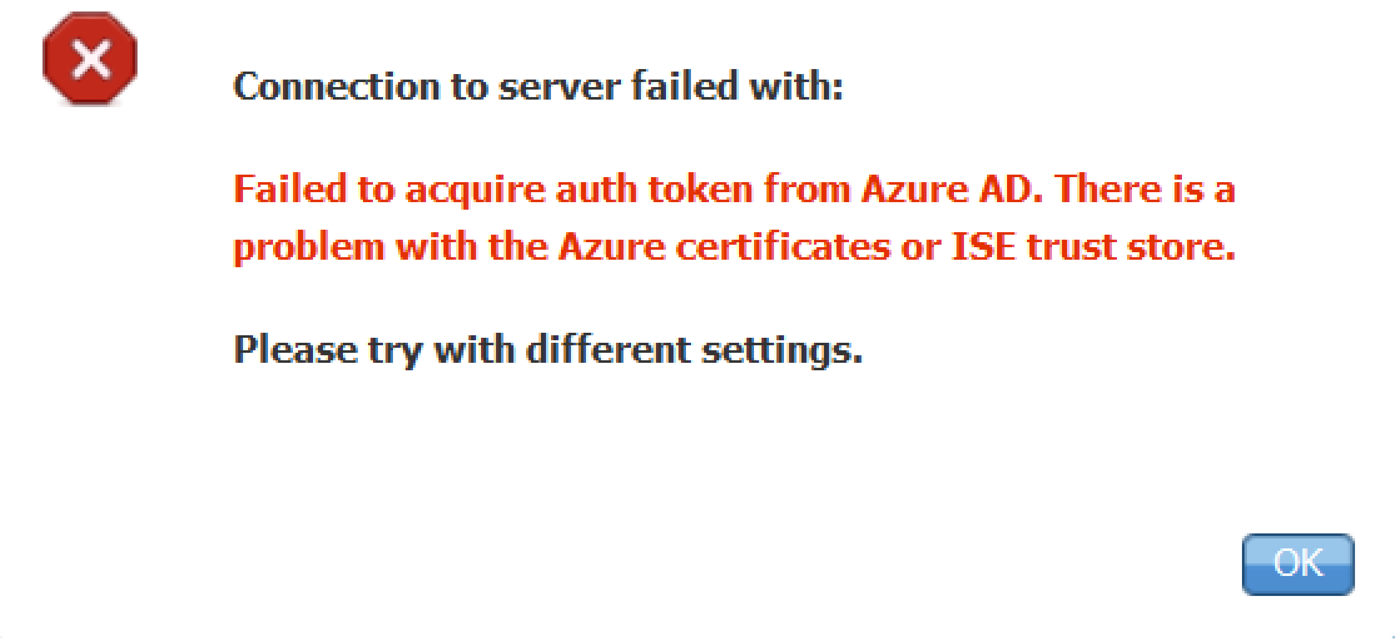


Connection to server failed with:

MDM Server API error
Connection Failed: 401:Unauthorized: the MDM server is not reachable

Please try with different settings.

Often this error occurs when the right permissions are not given to the Azure app in portal.azure.com. Verify that your app has the correct attributes and ensure that you click Grant Permissions after every change.



Connection to server failed with:

Failed to acquire auth token from Azure AD. There is a problem with the Azure certificates or ISE trust store.

Please try with different settings.

This message occurs when ISE tries to access the Token Issuing URL and it returns a certificate that the ISE does not. Ensure the full CA chain is in the ISE trust store. If the issue still persists after the correct certificate is installed in the trusted store of ISE, perform packet captures and test connectivity in order to see what is being sent.

Related Information

- Service to Service Calls Using Client Credentials
- Azure - Authentication vs. Authorization
- Azure - Quickstart: Register an Application with the Microsoft Identity Platform
- Azure Active Directory App Manifest
- Technical Support & Documentation - Cisco Systems