

將Intune MDM與身份服務引擎整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[配置Microsoft Intune](#)

[將證書從Intune門戶匯入到ISE受信任儲存](#)

[將ISE部署為Azure門戶中的應用程式](#)

[將ISE證書匯入Azure中的應用程式](#)

[驗證和疑難排解](#)

[基於sun.security.validator.ValidatorException的「連線到伺服器失敗」](#)

[無法從Azure AD獲取身份驗證令牌](#)

[無法從Azure AD獲取身份驗證令牌](#)

[相關資訊](#)

簡介

本文說明如何將Intune流動裝置管理(MDM)與思科身份服務引擎(ISE)整合。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE中的MDM服務知識
- 瞭解Microsoft Azure Intune服務

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎3.0
- Microsoft Azure Intune應用程式

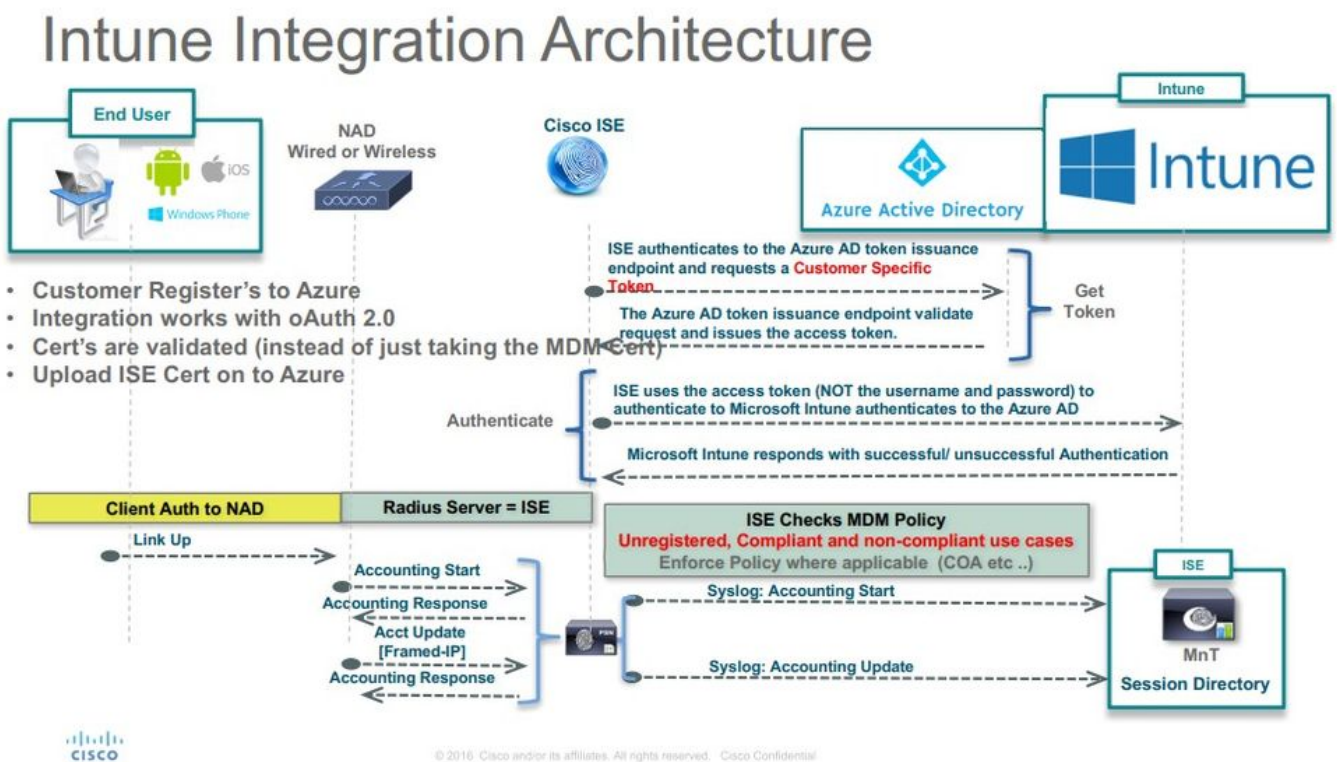
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

MDM伺服器可保護、監控、管理並支援跨移動運營商、服務提供商和企業部署的流動裝置。這些伺服器充當策略伺服器，控制部署環境中流動裝置上的某些應用程式（例如電子郵件應用程式）的使用。但是，網路是唯一可以根據存取控制清單(ACL)提供終端精細存取的實體。ISE向MDM伺服器查詢必要的裝置屬性，以便建立為這些裝置提供網路訪問控制的ACL。思科ISE與Microsoft Intune MDM伺服器整合，在裝置嘗試訪問本地資源時幫助組織保護企業資料。

設定

網路圖表



配置Microsoft Intune

將證書從Intune門戶匯入到ISE受信任儲存

登入到Intune管理控制檯或Azure管理控制檯，無論哪個網站有你的租戶。使用瀏覽器以取得憑證詳細資訊：

步驟 1. 從Web瀏覽器開啟Microsoft Azure portal。

步驟 2. 按一下瀏覽器工具欄中的鎖定符號，然後按一下 View Certificates.

步驟 3. 在「證書」視窗中，按一下選Certification Path 項卡。以下提供範例：

General Details Certification Path



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

Issuer Statement

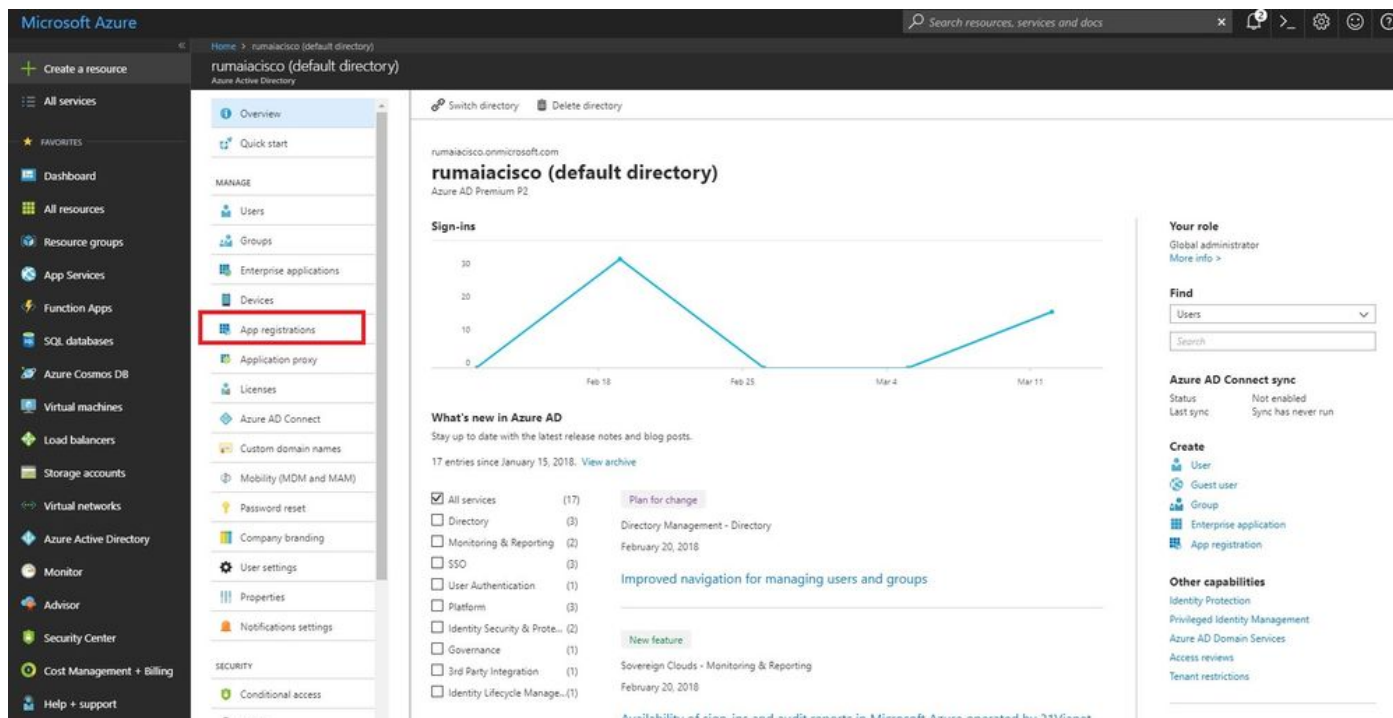
OK

步驟 4. 尋找Baltimore Cyber Trust root, 哪個是通常的根CA。但是, 如果存在任何其他不同的根CA, 請點選該根CA證書。在該根CA證書的Details (詳細資訊) 頁籤上, 可以將其複製到該檔案, 並將其另存為BASE64證書。

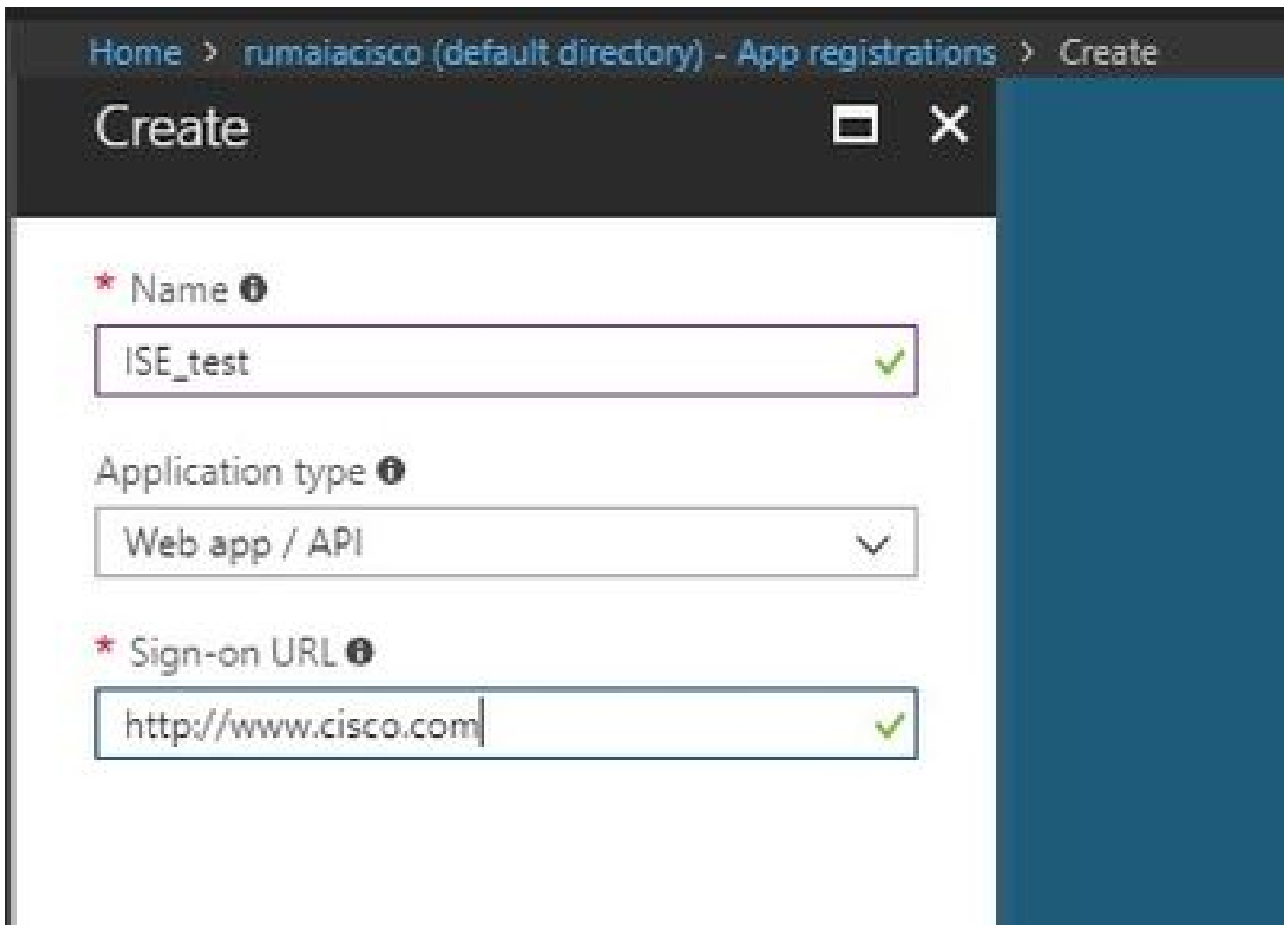
步驟 5. 在ISE中，導航到Administration > System > Certificates > Trusted Certificates, 並匯入剛儲存的根證書。為證書指定一個有意義的名稱， Azure MDM例如。對中間CA憑證也重複此程式。

將ISE部署為Azure門戶中的應用程式

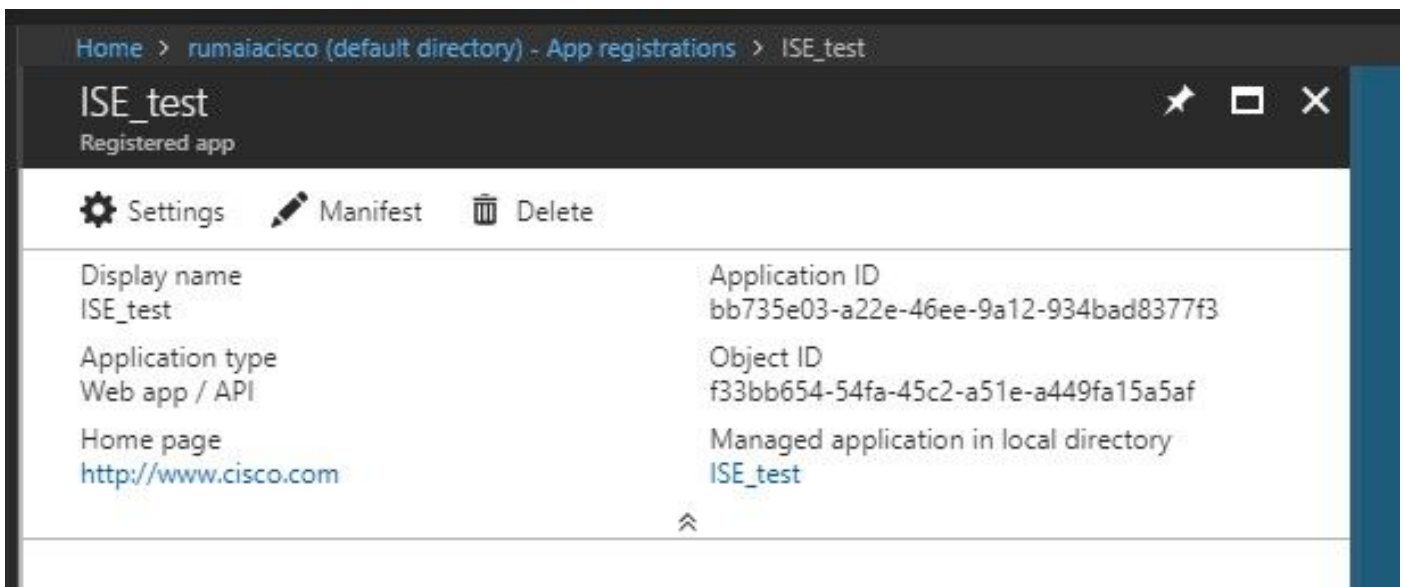
步驟 1. 導航到Azure Active Directory，然後選擇 App registrations.



步驟 2. 在中App registrations, 使用ISE名稱建立新的應用程式註冊。按一下Create，如下圖所示。



步驟 3. 選擇 Settings，以編輯應用程式並新增所需的元件。



步驟 4. 在下 Settings，選擇所需的許可權，並應用以下選項：

- Microsoft Graph

- 應用程式許可權

- 讀取目錄資料

- 授權的許可權

- 閱讀Microsoft Intune裝置配置和策略

- 讀取Microsoft Intune配置

- 使用者登入

- 隨時訪問使用者資料

- Microsoft Intune API

- 應用程式許可權

- 從Microsoft Intune獲取裝置狀態和合規性資訊

- Windows Azure Active Directory

- 應用程式許可權

- 讀取目錄資料

- 授權的許可權

- 讀取目錄資料

- 登入並讀取使用者配置檔案

組態的結果與以下所示類似：

+ 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... ...

Settings

GENERAL

- Properties >
- Reply URLs >
- Owners >

API ACCESS

- Required permissions >**
- Keys >

TROUBLESHOOTING + SUPPORT

- Troubleshoot >
- New support request >

Required permissions

+ Add Grant Permissions

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

步驟 5. 按一下 Grant Permissions，確認所有應用程式許可權。此過程需要 5-10 分鐘才能生效。編輯創建的應用程式的檔案，以匯入內部 ISE CA 證書 Azure Manifest。

將 ISE 證書匯入 Azure 中的應用程式

步驟 1. 下載應用程式的清單檔案。

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

Home > self | App registrations >

ISE | Certificates & secrets

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

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 can be referred to as public keys.

[Upload certificate](#)

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

舊版選項：

步驟 1. 運行 PowerShell 過程以將證書轉換為 BASE64 並正確將其匯入到 Azure JSON 清單檔案。從 Windows 使用 Windows PowerShell 或 Windows PowerShell ISE 應用程式。使用以下命令：

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

步驟 2. 保留、和 \$base64Thumbprint, \$base64Value 的值， \$keyid 這些值將在下一步中使用。所有這些值都將新增到 JSON 欄位 keyCredentials 中，因為預設情況下如下所示：

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

為此，請確保按以下順序使用值：

```
"keyCredentials": [ { "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN", "keyId": "$keyid_from_above_PPAN", "type": "AsymmetricX509Cert"
```

步驟 3. 將編輯的 JSON 檔案上傳到 Azure 門戶，以便從 keyCredentials ISE 上使用的證書中驗證。

其外觀必須如下所示：

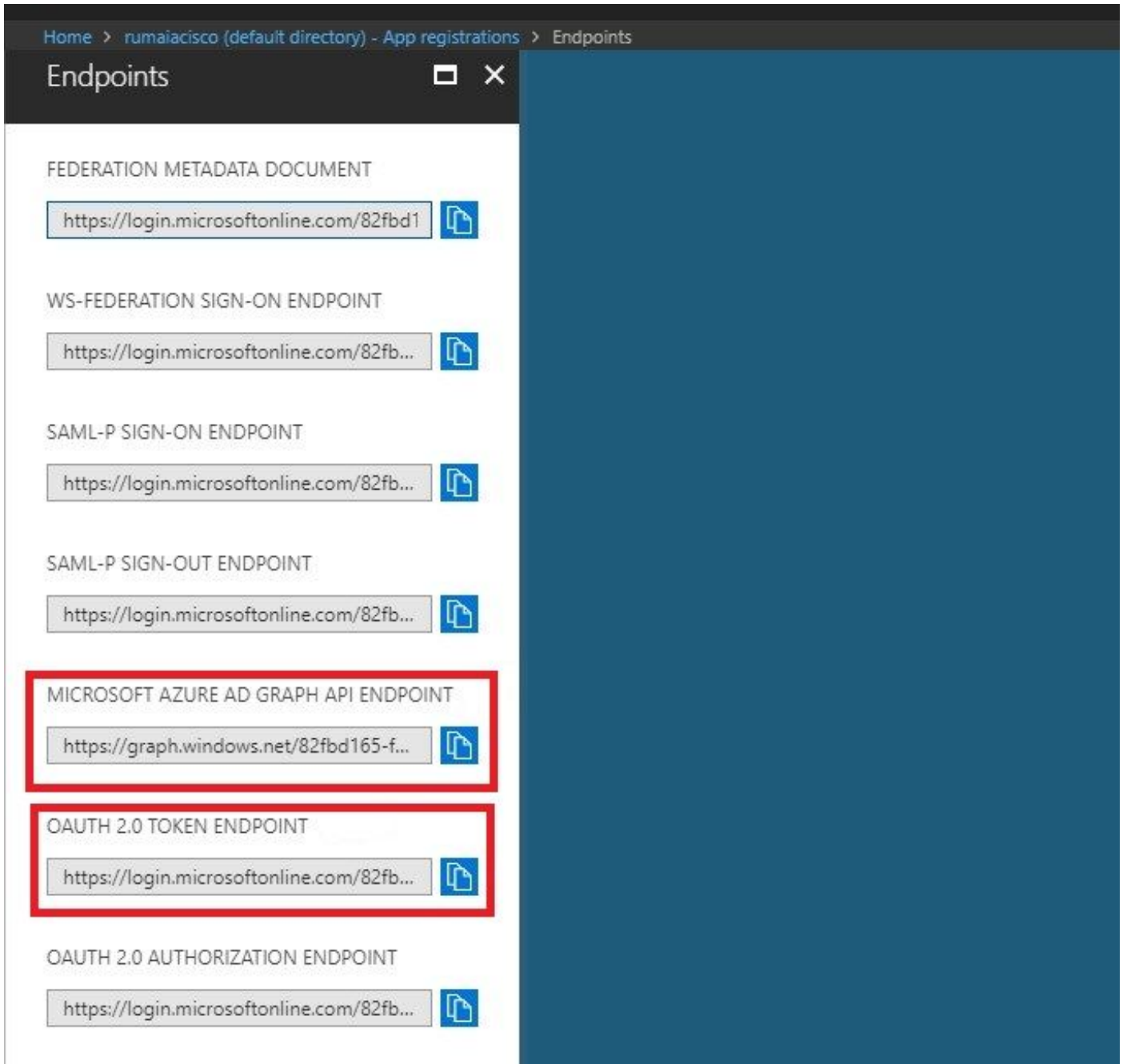
```

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": "GMlDp/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   },

```

步驟 4.請注意，上傳後，系統會顯示下面的字 value 段，因為Microsoft端會強制執行該操 keyCredentials 作，以便在第一次上傳後不允許看到這些值 null 值。

ISE中新增MDM伺服器所需的值可從和 Microsoft Azure AD Graph API Endpoint 復 OAUTH 2.0 Token Endpoint制。



必須在ISE GUI中輸入這些值。導覽至Administration > Network Resources > External MDM 並新增伺服器：

ISE	Intune
自動發現URL	終結點> Microsoft Azure AD Graph API終結點
客戶端ID	{Registered-App-Name} >應用程式ID
令牌頒發URL	終結點> OAuth 2.0令牌終結點

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/"/> ⓘ
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](#)

組態完成後，狀態顯示已啟用。

MDM Servers

<input type="checkbox"/>	Name	Status	Service Provider	MDM Server	Server Type	Description
<input type="checkbox"/>	Intune	■ Enabled	Microsoft	fef.msusub03.manage.microsoft.com	Mobile Device Manager ↕	

驗證和疑難排解

基於sun.security.validator.ValidatorException的「連線到伺服器失敗」



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.

OK

步驟 1.在TRACE級別使用以下日誌收集支援捆綁包：

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

步驟 2.檢查 ise-psc.log 以下日誌：

- 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.com#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

這表示需要匯入此頁graph.microsoft.com 上的證書。



The screenshot shows a web browser window with the address bar displaying "Secure | https://graph.windows.net". Below the address bar, a message states: "This XML file does not appear to have any style information associated with it. The document tree is shown below." The XML content is as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<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>
```

步驟 3. 點選圖標locker並檢查證書詳細資訊。

General Details Certification Path



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

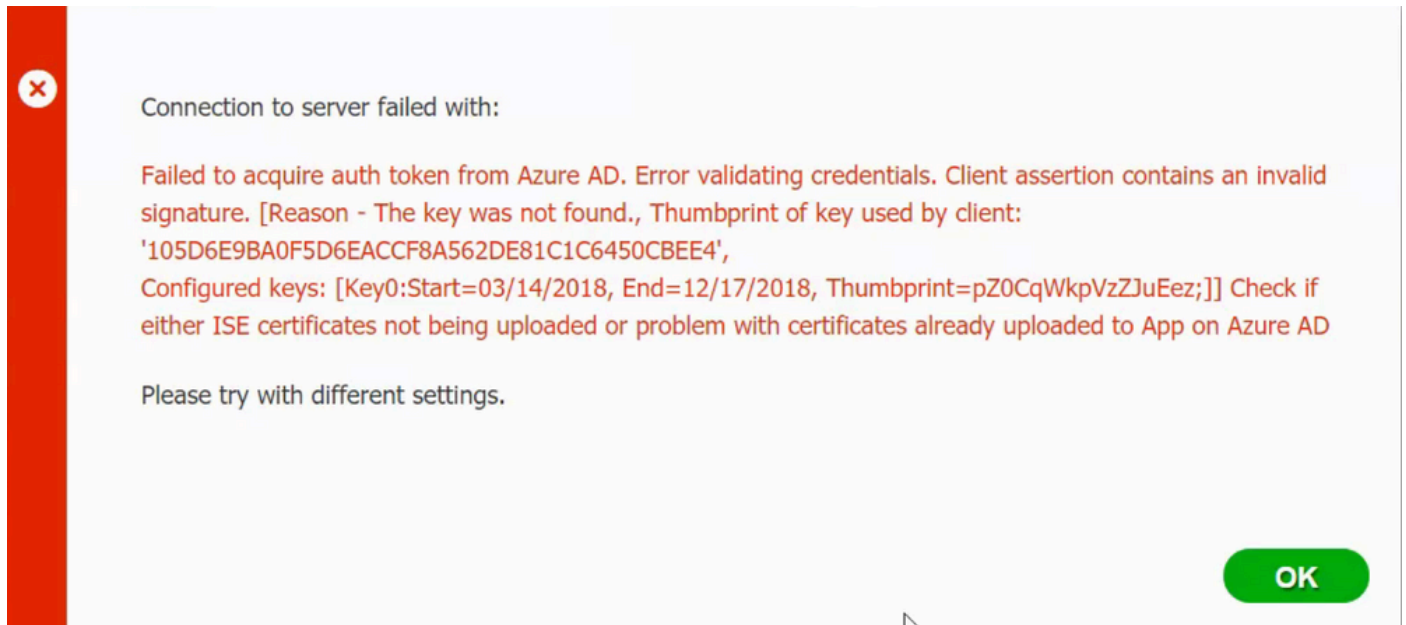
Issued by: Microsoft IT TLS CA 2

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

Issuer Statement

OK

無法從Azure AD獲取身份驗證令牌



通常，當清單檔案包含錯誤JSON的ISE證書鏈時會發生此錯誤。在將清單檔案上傳到Azure之前，請驗證是否至少存在此配置：

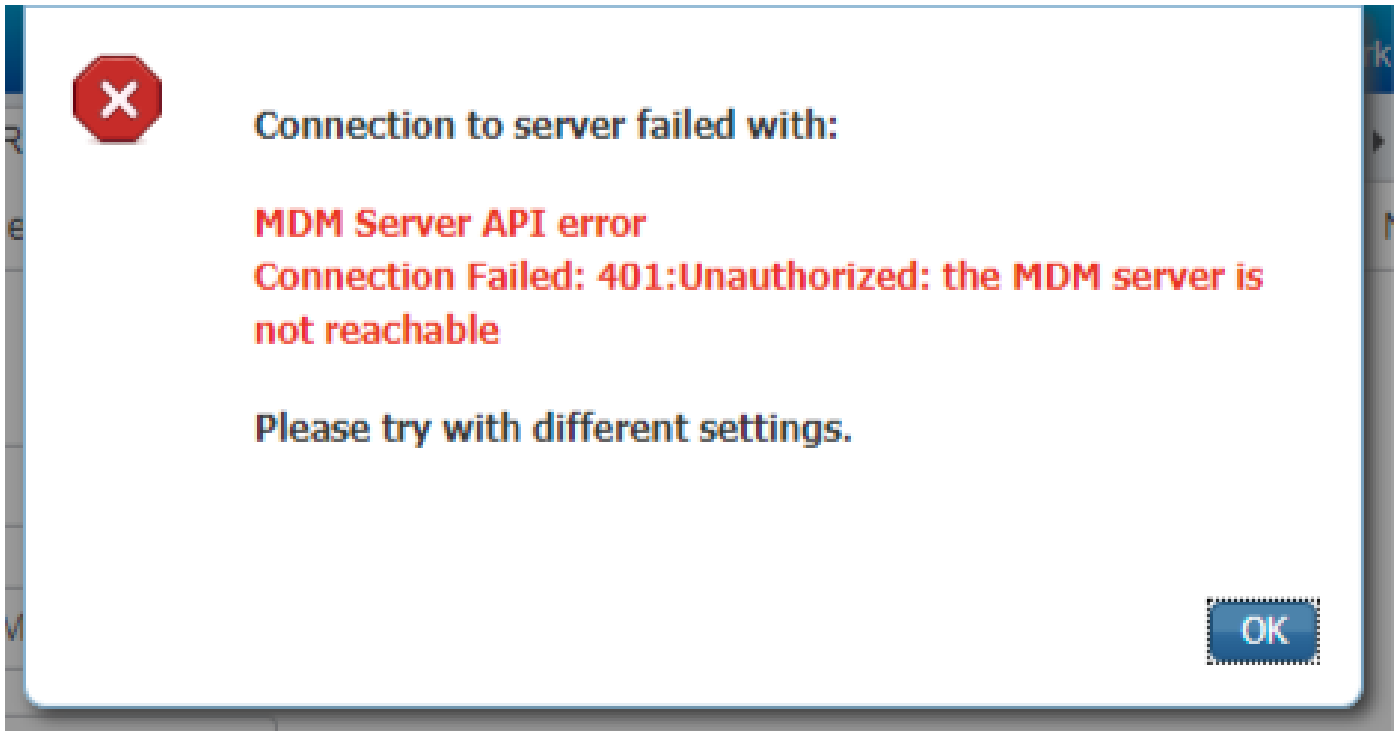
```
"keyCredentials": [ { "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN", "keyId": "$keyid_from_above_PPAN", "type": "Asym"
```

上一個示例基於存在PAN和SAN的場景。再次從PowerShell運行指令碼並導入正確的BASE64值。嘗試上傳清單檔案，並且不能面臨任何錯誤。

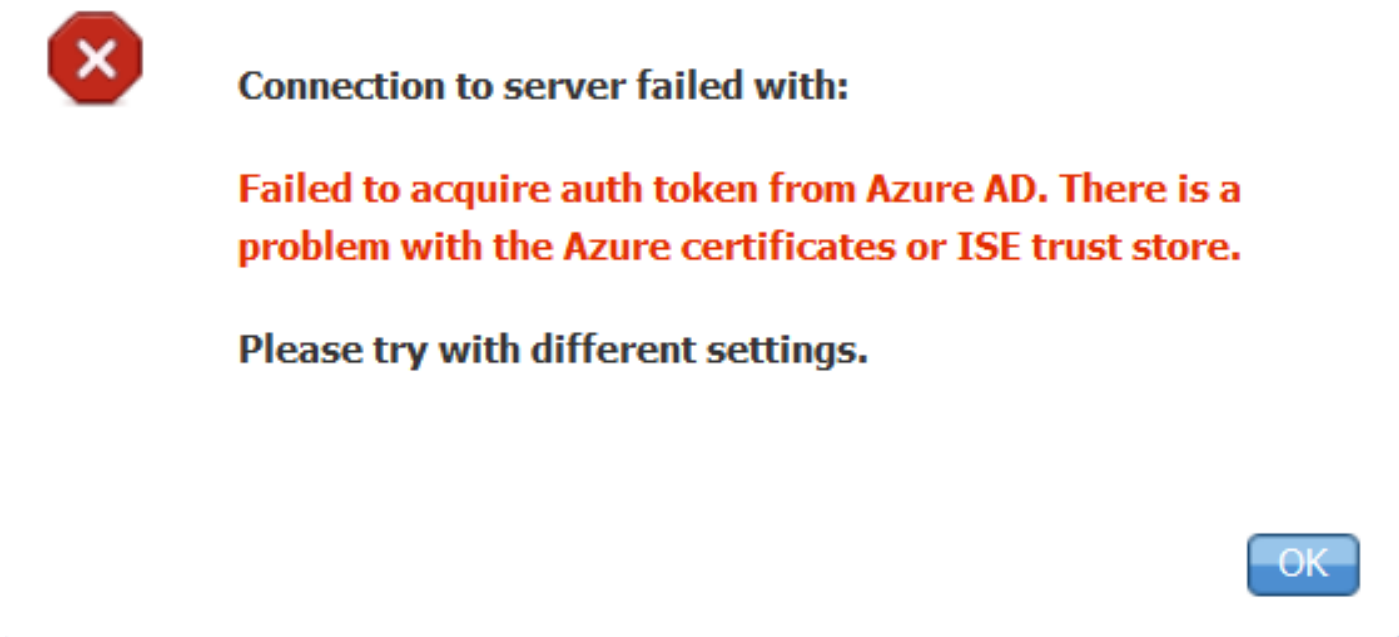
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import("mycer.cer") $bin = $cer.GetRawCertData() $base64V
```

請記得應用「配置」 \$base64Thumbprint, \$base64Value 部 \$keyid 分中步驟中提到的和的值。

無法從Azure AD獲取身份驗證令牌



通常，當中沒有為Azure應用授予正確的許可權時，會發生此錯 portal.azure.com 誤。驗證你的應用具有正確的屬性，並確保每次更改後都按一下Grant Permissions。



當ISE嘗試訪問令牌頒發URL並返回ISE沒有的證書時，會出現此消息。確保完整CA鏈位於ISE信任儲存中。如果在ISE的受信任儲存中安裝了正確的證書後問題仍然存在，請執行資料包捕獲並測試連線，以便檢視正在傳送的内容。

相關資訊

- [使用客戶端憑據的服務到服務呼叫](#)
- [Azure — 身份驗證與授權](#)

- [Azure - Quickstart : 向Microsoft身份平台註冊應用程式](#)
- [Azure Active Directory應用清單](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。