將Intune MDM與身份服務引擎整合

目錄
· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>設定</u>
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
<u>驗證和疑難排解</u>
基於sun.security.validator.ValidatorException的「連線到伺服器失敗」
<u>無法從Azure AD獲取身份驗證令牌</u>
無法從Azure AD獲取身份驗證令牌

<u>相關資訊</u>

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:

🐖 Certificate

This certificate	is intended for the following purpose(s):
• Ensures th	e identity of a remote computer
 Proves you 136141 	Ir identity to a remote computer
* Refer to the ce	tification authority's statement for details.
Issued to:	portal.azure.com
Issued by:	Microsoft IT SSL SHA2
Issued by: Valid from	Microsoft IT SSL SHA2 7/21/2017 to 5/7/2018
Issued by: Valid from	Microsoft IT SSL SHA2 7/21/2017 to 5/7/2018

Х

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.

Microsoft Azure			${\cal P}$ Search resources, services and docs	× 🗘 >_ 🎕 😳 Ø
+ Create a resource	rumaiacisco (default directory Azure Active Directory			
i≣ All services	Overview	e ^o Switch directory	ectory	
* FAVORITES	😅 🖞 Quick start	rumaiacisco.onmicrosoft.com		
Dashboard	MANAGE	rumaiacisco (defa	ult directory)	
All resources	🛓 Users	Abure Ab Premium P2		No. of Control of Cont
Resource groups	22 Groups	Sign-ins		Global administrator
🔇 App Services	B Enterprise applications	30		More into >
🐓 Function Apps	Devices	20		Find Users V
🗧 SQL databases	App registrations	10		Search
🧟 Azure Cosmos DB	Application proxy	0 Fait	518 Feb 25 Mar 3 Mar 11	Azure AD Connect sync
Virtual machines	Licenses			Status Not enabled Last sync Sync has never run
🚸 Load balancers	Azure AD Connect	Stay up to date with the latest release	notes and blog posts.	Create
Storage accounts	(b) Mehility (MDM and MAM)	17 entries since January 15, 2018. View	w archive	user 🔒
🐡 Virtual networks	Password reset	All services (17)	Plan for change	Guestuser
Azure Active Directory	Company branding	Directory (3)	Directory Management - Directory	Enterprise application
Monitor	User settings	□ sso (3)	February 20, 2016	e vypregonioni
Advisor	III Properties	User Authentication (1)	improved navigation for managing users and groups	Other capabilities Identity Protection
Security Center	Notifications settings	Identity Security & Prote (2)	New feature	Privileged Identity Management Azure AD Domain Services
O Cost Management + Billing	SECURITY	Governance (1)	Sovereign Clouds - Monitoring & Reporting	Access reviews
Lefo + support	Conditional access	Identity Lifecycle Manage(1)	February 20, 2018	renant restrictions
	aa		Availability of sion-ins and audit renorts in Microsoft Azure operated by 21Vianet	

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。

* Name 🖲	
ISE_test	✓
Application type 0	
Web app / API	~
* Sign-on URL 🛛	
http://www.cisco.com	✓

步驟 3.選擇Settings,以編輯應用程式並新增所需的元件。

ISE_test Registered app	*
🏟 Settings 💉 Manifest 🗴 🗊 (Delete
Display name	Application ID
ISE_test	bb735e03-a22e-46ee-9a12-934bad8377f3
Application type	Object ID
Web app / API	f33bb654-54fa-45c2-a51e-a449fa15a5af
Home page	Managed application in local directory
http://www.cisco.com	ISE_test
	A

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	
Vintune (1)					••••
get_device_compliance	Application	Get device state and compliance information from Micros	Yes	Sranted for pavagupt-t	
✓Microsoft Graph (7)					
Directory.Read.All	Delegated	Read directory data	Yes	Sranted 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	Sranted for pavagupt-t	
User.Read	Delegated	Sign in and read user profile	No	Sranted 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 Solution Owners > API ACCESS 🔏 Required permissions > > 📍 Keys TROUBLESHOOTING + SUPPORT X 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。

ISE Registered app	* ×	Edit manifest
🏟 Settings 💉 Manifest 🗴 🖻 De	lete	🕀 Save 🗶 Discard 💉 Edit 🗍 Upload 坐 Download
Display name ISE Application type Web app / API	Application ID 86397a1c-b06d-4ca9-a086-0786eeadfabc Object ID 220a1c0e-e3d1-4eda-8739-e733019bd0fd	<pre>1 [2 "appId": "86397a1c-b06d-4ca9-a086-0786eeadfabc", 3 "appRoles": [],</pre>
Home page http://www.cisco.com	Managed application in local directory ISE ☆	<pre>4 "availableToOtherTenants": false, 5 "displayName": "ISE", 6 "errorUrl": null, 7 "groupMembershipClaims": null, 8 "optionalClaims": null, 9 "acceptMappedClaims": null,</pre>

💊 註:該檔案具有JSON副檔名。請勿編輯檔名或副檔名,否則它將失敗。

步驟 2.從所有節點匯出ISE系統證書。在PAN上,導航至Administration > System > Certificates > System Certificates, 選擇**Default self**signed server certificate,然後點選Export.。選擇Export Certificate Only(預設),然後選擇要儲存的位置。從證書中刪除BEGIN和 END標籤,並將其余文本作為一行進行複製。這適用於舊版選項部分所述的2020年6月之前的版本。

Administration > Certificates > System Certificates



從2020年6月起,門戶允許您直接上傳證書。

≡ Microsoft Azure	${ ho}$ Search resources, services, and docs (G+/)		
Home > self App registrations > ISE Certificates & se	ecrets 🖈		
Search (Cmd+/) « Øverview	Credentials enable confidential applications to identify themselves scheme). For a higher level of assurance, we recommend using a ce	to the authentication service when receiving tokens trificate (instead of a client secret) as a credential.	at a web addressable locat
 Quickstart Integration assistant (preview) 	Certificates Certificates can be used as secrets to prove the application's identit	y when requesting a token. Also can be referred to	as public keys.
Manage Branding	T Upload certificate	Start date	Expires
Authentication	8C618ABBC45B640E4F21EA302583D33E0F0C4C63	4/3/2020	4/2/2025
📍 Certificates & secrets	80C1360BCCD305F2D53E265668D5D8499AD693A5	4/5/2020	4/4/2025
Token configuration			
-> API permissions			

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() \$base64Va

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 "identifierUris": [
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": "A

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

其外觀必須如下所示:

```
"keyCredentials": [
18
19
       {
         "customKeyIdentifier": "wteOPVePuM0wUeFNB9s22fkDYZE=",
20
         "endDate": "2019-01-22T11:41:01Z",
21
         "keyId": "eb7b1833-3240-4203-98a6-c3ccc6790d9d",
22
23
         "startDate": "2018-01-22T11:41:01Z",
         "type": "AsymmetricX509Cert",
24
        "usage": "Verify",
25
         "value": null
26
27
       },
28
       {
         "customKeyIdentifier": "B5Zz60fZKHGN6qAMvt43swIZQko=",
29
         "endDate": "2019-01-05T14:32:30Z",
30
         "keyId": "86462728-544b-423d-8e5e-22adf3521d23",
31
32
        "startDate": "2018-01-05T14:32:30Z",
         "type": "AsymmetricX509Cert",
33
        "usage": "Verify",
34
        "value": null
35
36
       },
37
       {
         "customKeyIdentifier": "GMlDp/1DYiNknFIJkgjnTbjo9nk=",
38
         "endDate": "2018-12-06T10:46:32Z",
39
         "keyId": "2ed5b262-ced6-4c1a-8a1a-c0abb82ae3c1",
40
        "startDate": "2017-12-06T10:46:32Z",
41
         "type": "AsymmetricX509Cert",
42
        "usage": "Verify",
43
       "value": null
44
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。

Home > rumaiacisco (default director Endpoints	y) - App registrations	> Endpoints	
FEDERATION METADATA DOCUME	NT		
https://login.microsoftonline.com	/82fbd1		
WS-FEDERATION SIGN-ON ENDPO	INT		
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/82fbd	165-f		
OAUTH 2.0 TOKEN ENDPOINT			
https://login.microsoftonline.com	/82fb		
OAUTH 2.0 AUTHORIZATION ENDP	OINT		
https://login.microsoftonline.com	/82fb		

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

MDM Servers > Intune

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

組態完成後,狀態顯示已啟用。

MDM Servers								
C Refresh + Add Duplicate & Edit	🗂 Trash					Ţ Filter →	O Download -	۰.
Name	Status	Service Provider	MDM Server	Server Type	Description			
Intune	Enabled	Microsoft	fef.msub03.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:

X

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.

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 - <u>https://login</u>

OK

- microsoftonline.com/273106dc-2878-42eb-b7c8-069dcf334687/oauth2/token, ResourceId/App Id uri <u>https://graph.windows.net</u>
- 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

٠ : 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。

← → C 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.

步驟 3.點選圖標locker並檢查證書詳細資訊。

This certificate	is intended for the following purpose(s):
 Ensures tri Proves voi 	le identity of a remote computer ur identity to a remote computer
• 1.3.6.1.4.1	1.311.42.1
* Refer to the ce	rtification 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

步驟 4.以BASE64格式將其儲存到檔案,並匯入到ISE受信任儲存。確保匯入完整的證書鏈。然後,再次測試與MDM伺服器的連線。

無法從Azure AD獲取身份驗證令牌



"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。嘗試上載清單檔案,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() \$base64Va

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。



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.



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內容。

相關資訊

- 使用客戶端憑據的服務到服務呼叫
- <u>Azure 身份驗證與授權</u>

- <u>Azure Quickstart: 向Microsoft身份平台註冊應用程式</u>
- <u>Azure Active Directory應用清單</u>
- <u>技術支援與文件 Cisco Systems</u>

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)。