Intune MDM을 Identity Services Engine과 통합

목차

소개

이 문서에서는 Intune MDM(Mobile Device Management)을 Cisco ISE(Identity Services Engine)와 통합하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE의 MDM 서비스에 대한 지식
- Microsoft Azure Intune 서비스에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 3.0
- Microsoft Azure Intune 응용 프로그램

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

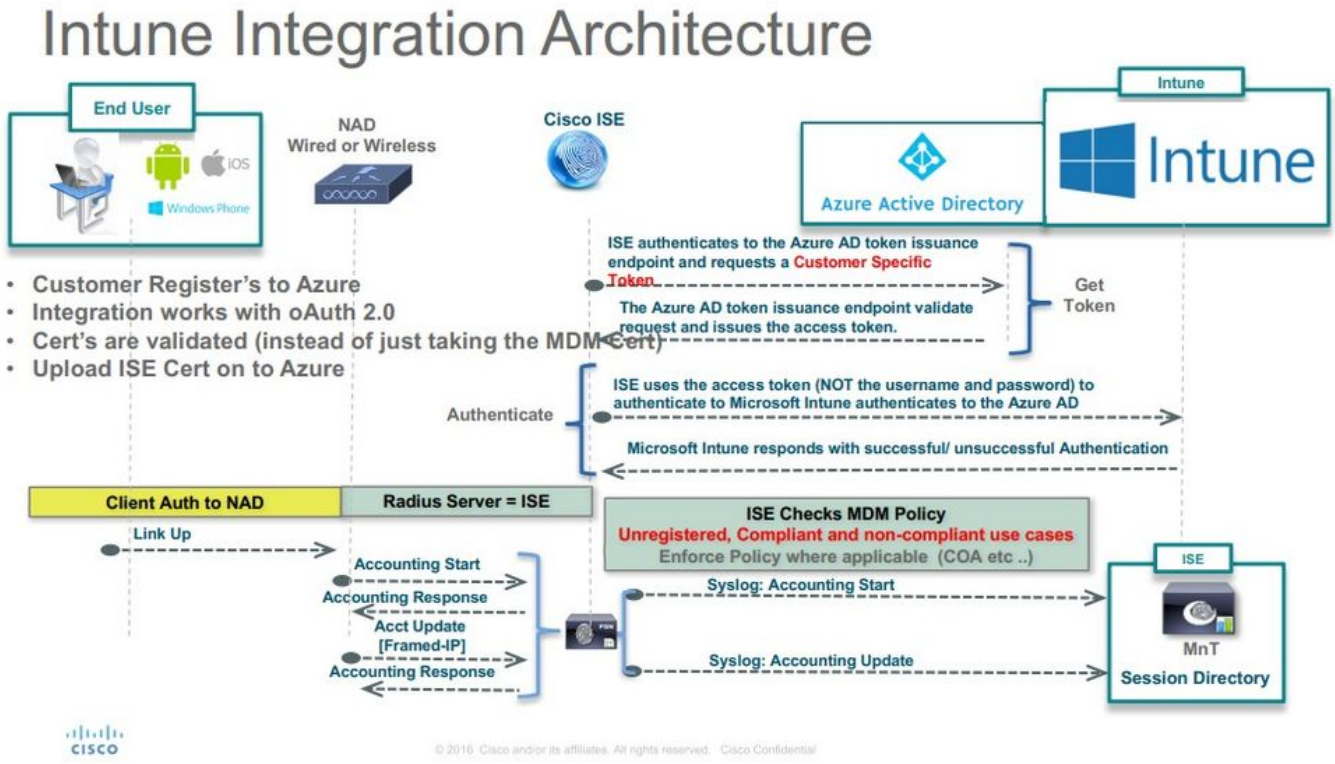
명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

MDM 서버는 모바일 운영자, 통신 사업자, 기업 전체에 구축된 모바일 디바이스를 보안, 모니터링, 관리 및 지원합니다. 이러한 서버는 구축된 환경에서 모바일 디바이스(예: 이메일 애플리케이션)의 일부 애플리케이션 사용을 제어하는 정책 서버 역할을 합니다. 그러나 네트워크는 ACL(Access Control List)을 기반으로 엔드포인트에 대한 세분화된 액세스를 제공할 수 있는 유일한 엔티티입니다. ISE는 MDM 서버에 필요한 디바이스 특성을 쿼리하여 해당 디바이스에 대한 네트워크 액세스 제어를 제공하는 ACL을 생성합니다. Cisco ISE는 Microsoft Intune MDM Server와 통합되어 장치가 온프레미스 리소스에 액세스하려고 할 때 조직이 기업 데이터를 보호할 수 있도록 지원합니다.

구성

네트워크 다이어그램



Microsoft Intune 구성

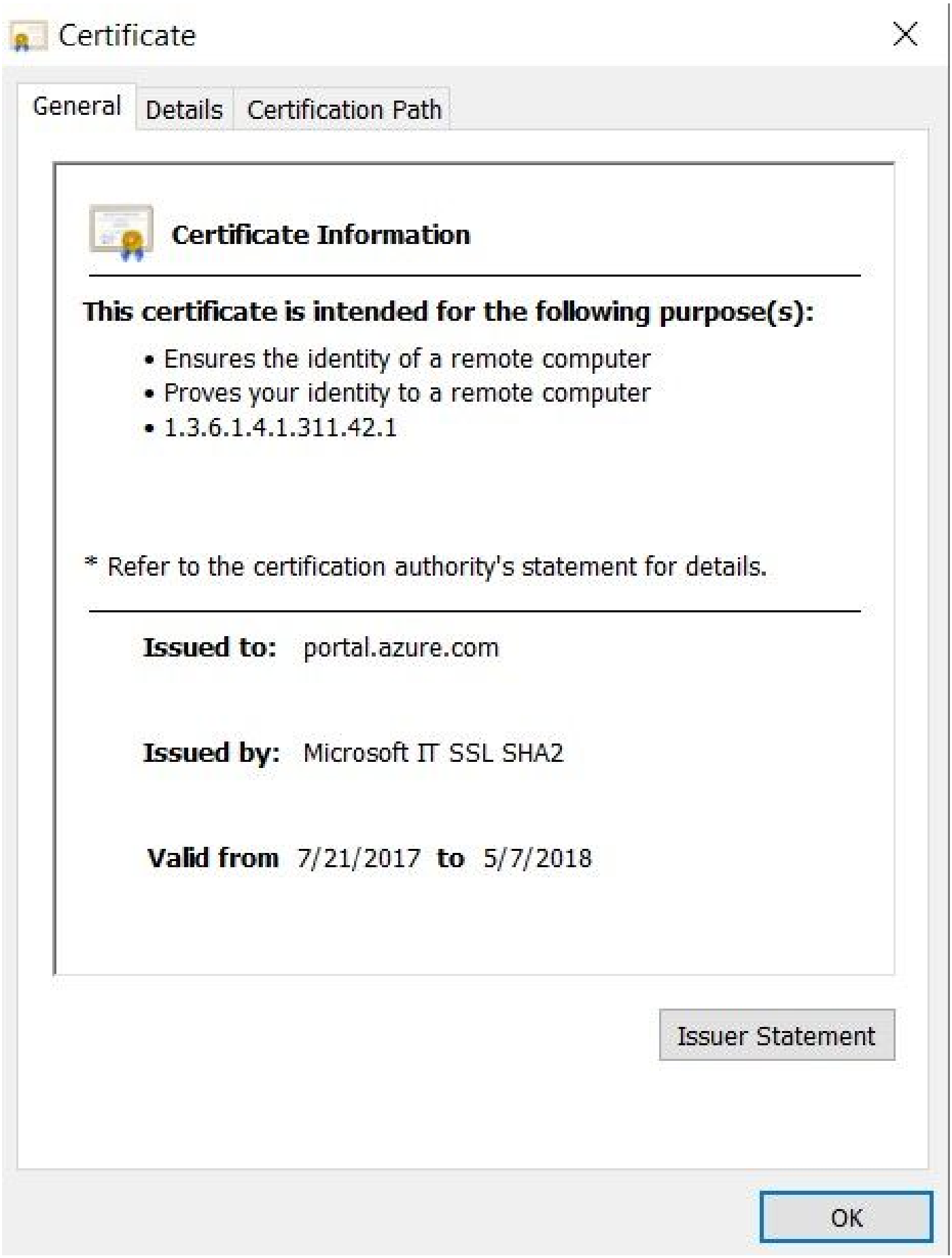
Intune 포털에서 ISE 트러스트된 저장소로 인증서 가져오기

테넌트가 있는 사이트에서 Intune 관리 콘솔 또는 Azure 관리 콘솔에 로그인합니다. 인증서 세부사항을 가져오려면 브라우저를 사용하십시오.

1단계. 열기 Microsoft Azure portal 웹 브라우저에서 다운로드합니다.

2단계. 브라우저 도구 모음에서 잠금 기호를 클릭한 다음 View Certificates.

3단계. Certificate 창에서 Certification Path 탭을 클릭합니다. 예를 들면 다음과 같습니다.



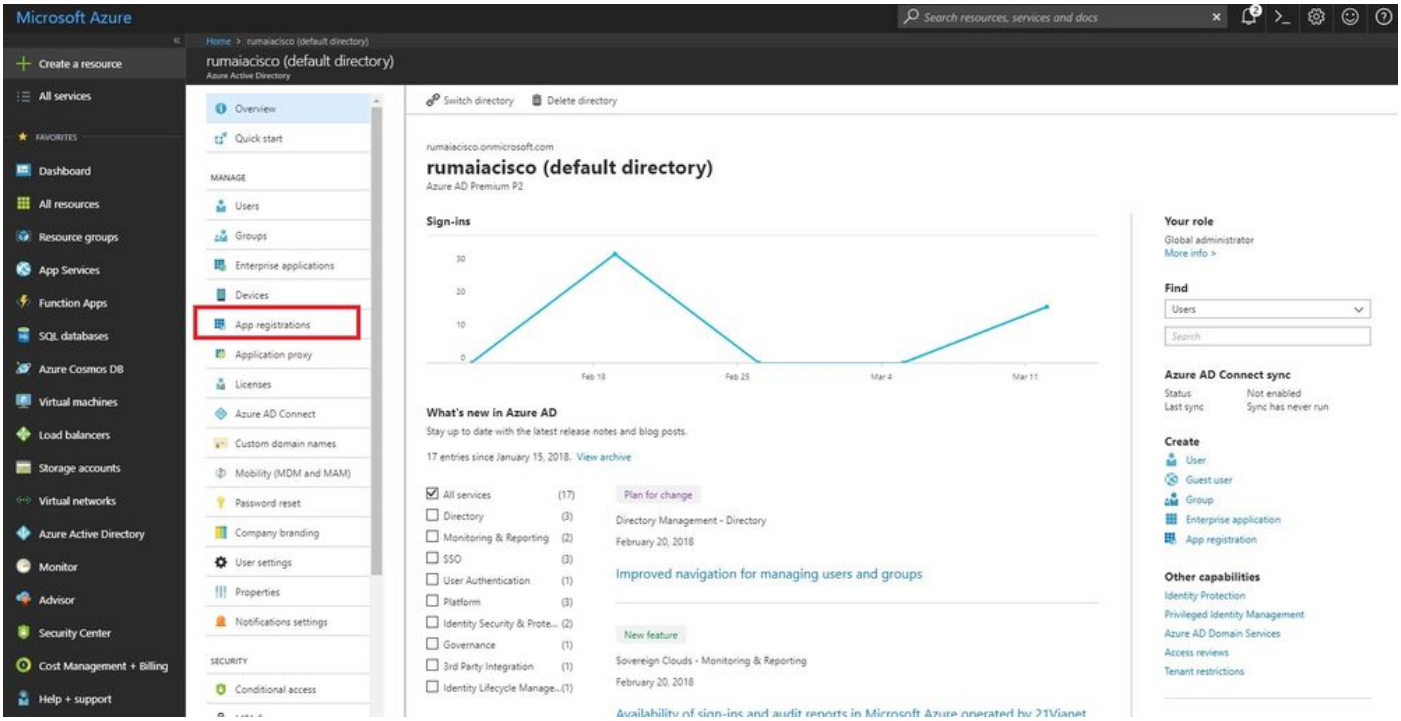
4단계. 찾기 Baltimore Cyber Trust root- 일반적인 루트 CA. 그러나 다른 루트 CA가 있으면 해당 루트 CA 인증서를 클릭합니다. 해당 루트 CA 인증서의 Details(세부사항) 탭에서 파일에 복사하여 BASE64

인증서로 저장할 수 있습니다.

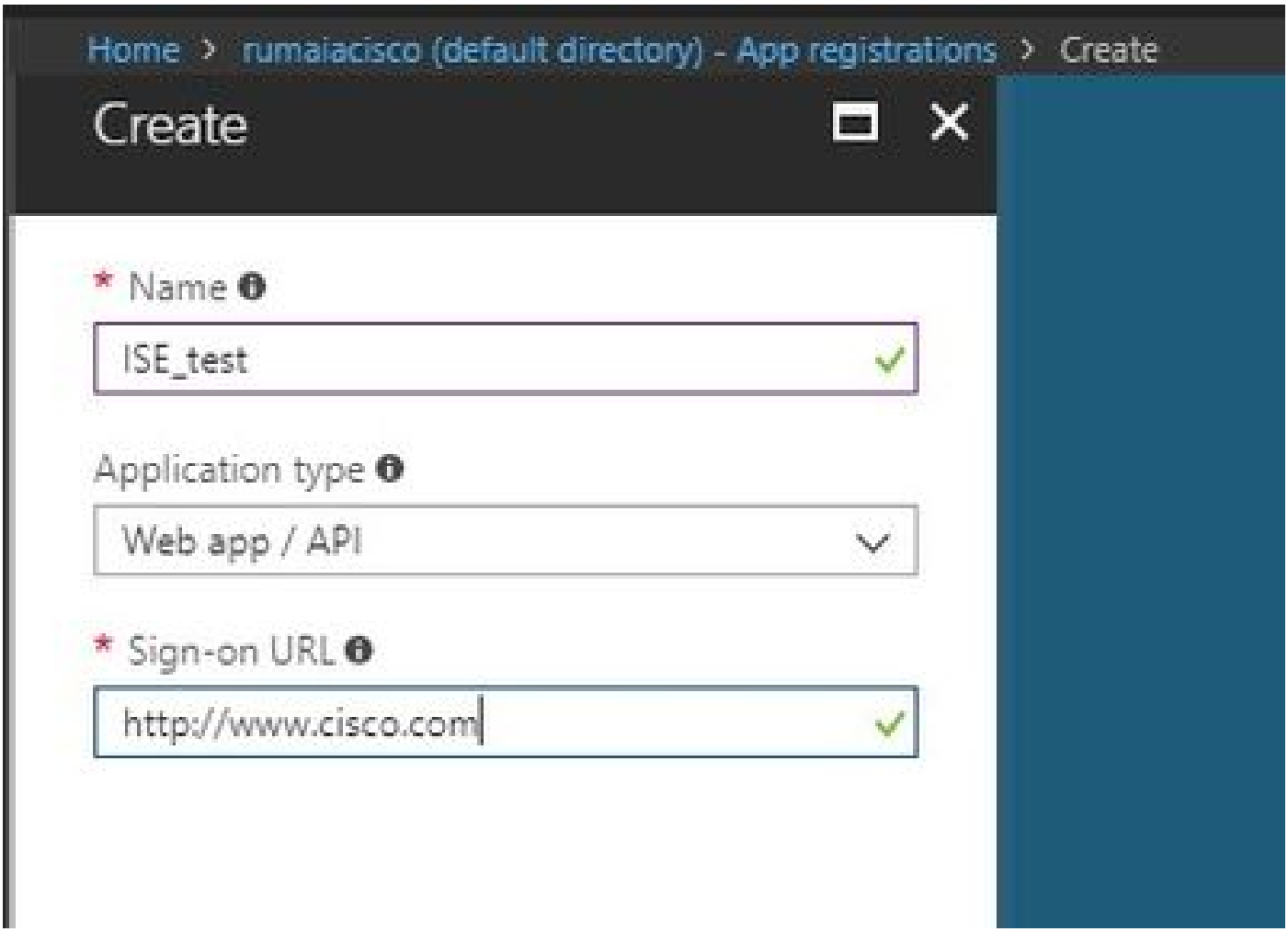
5단계. ISE에서 Administration > System > Certificates > Trusted Certificates방금 저장한 루트 인증서를 가져옵니다. 인증서에 다음과 같이 의미 있는 이름을 지정합니다. Azure MDM. 중간 CA 인증서에 대해서도 이 절차를 반복합니다.

Azure 포털에서 ISE를 애플리케이션으로 배포

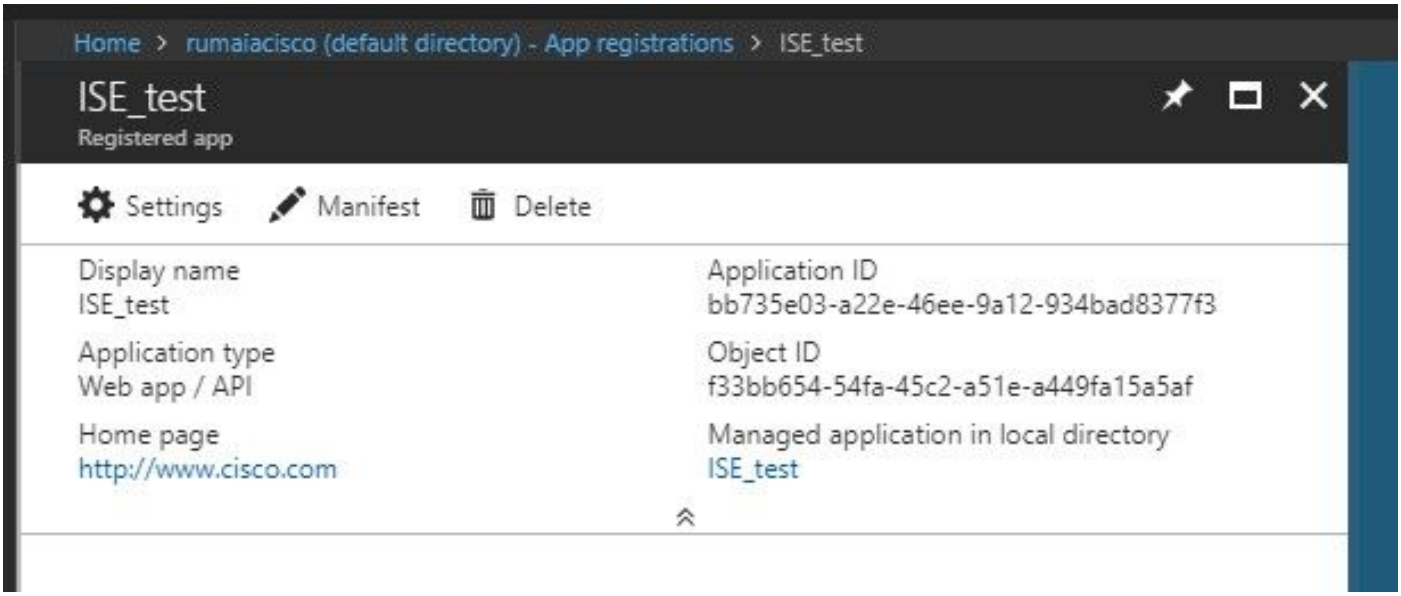
1단계. 탐색: Azure Active Directory 선택 App registrations.



2단계. 의 App registrations에서 ISE 이름으로 새 애플리케이션 등록을 생성합니다. 클릭 Create 이 그림에 표시된 것과 같습니다.



3단계. 선택 Settings 애플리케이션을 수정하고 필요한 구성 요소를 추가합니다.



4단계. 아래 Settings에서 필요한 권한을 선택하고 다음 옵션을 적용합니다.

1. Microsoft Graph
    - 응용 프로그램 권한
        - 디렉토리 데이터 읽기

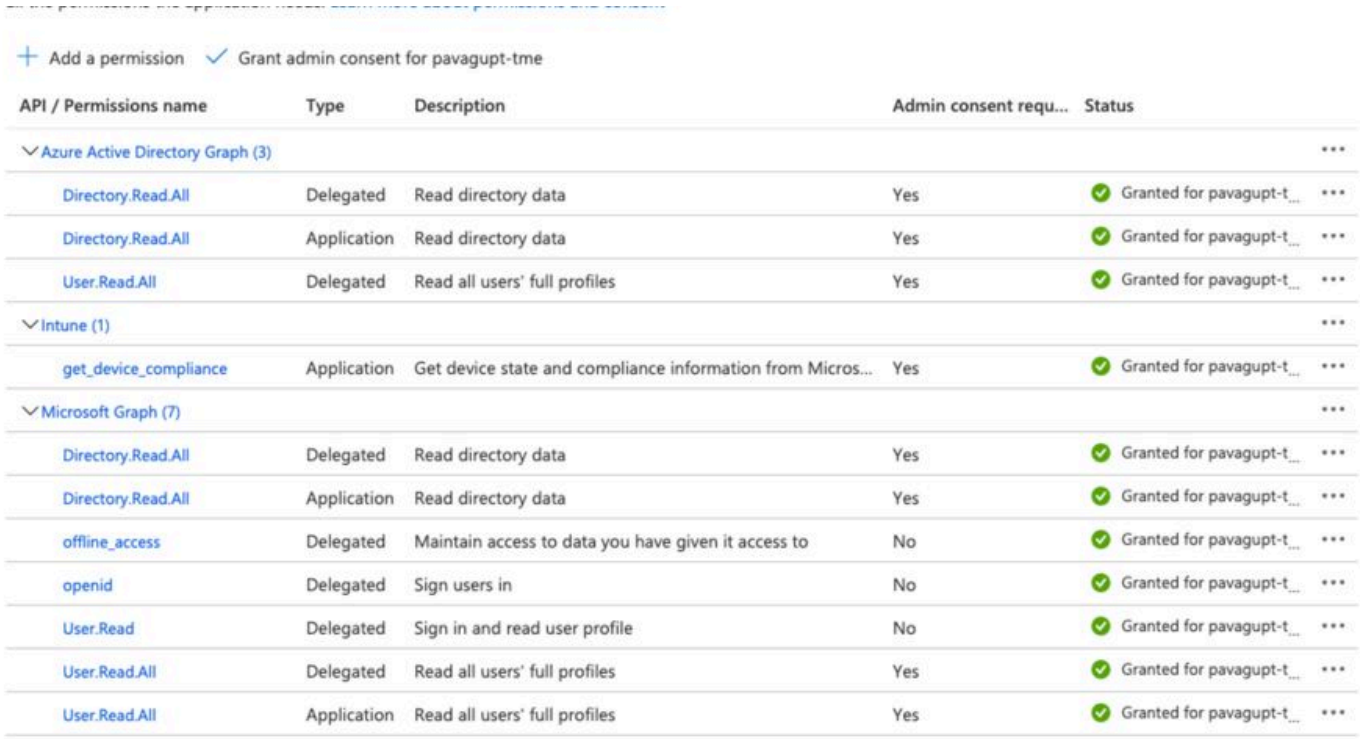
- 위임된 권한
    - Microsoft Intune 장치 구성 및 정책 읽기
    - Microsoft Intune 구성 읽기
    - 사용자 로그인
    - 언제든지 사용자의 데이터에 액세스

2. Microsoft Intune API
    - 응용 프로그램 권한
        - Microsoft Intune에서 장치 상태 및 규정 준수 정보 가져오기

3. Windows Azure Active Directory
    - 응용 프로그램 권한
        - 디렉토리 데이터 읽기

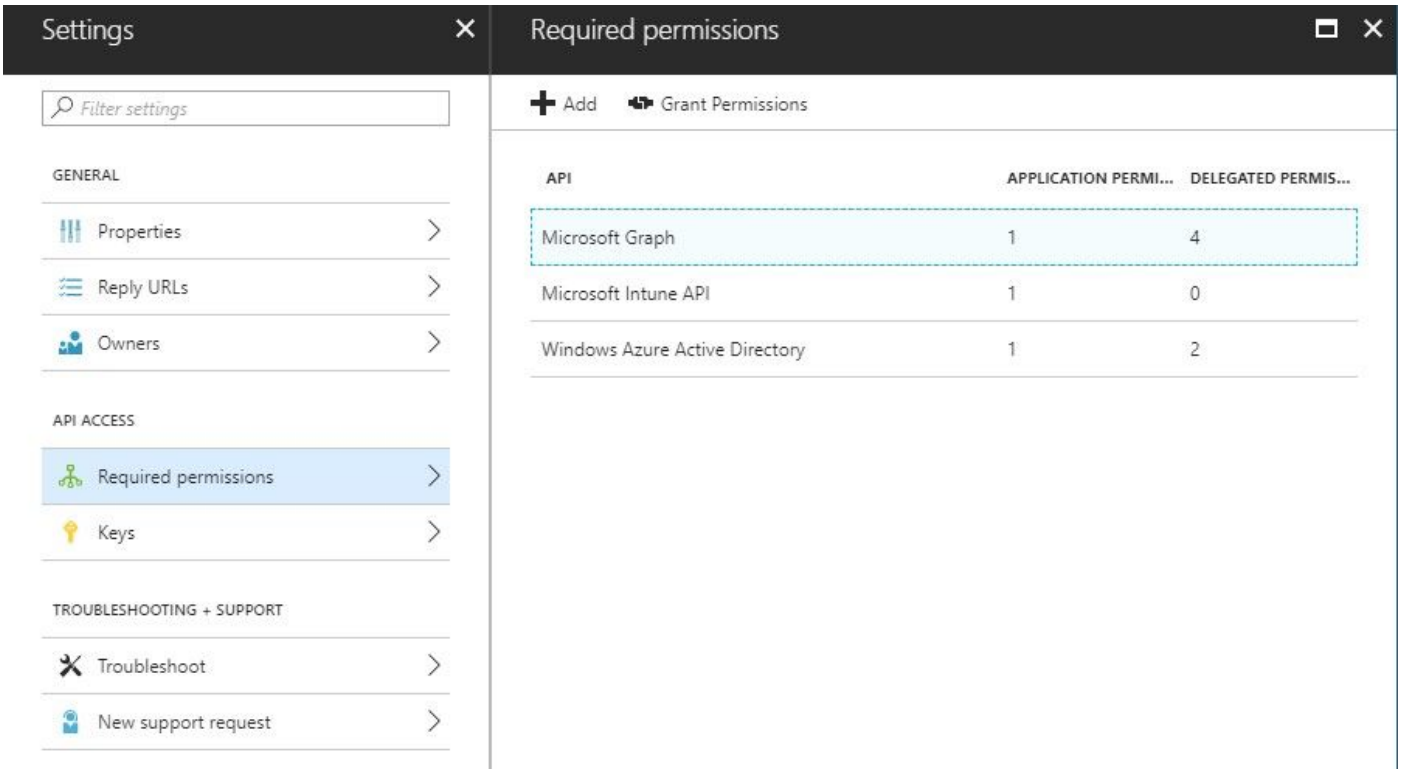
    - 위임된 권한
        - 디렉토리 데이터 읽기
        - 로그인하고 사용자 프로필 읽기

컨피그레이션의 결과는 여기에 표시된 것과 유사합니다.



+ Add a permission ✓ Grant admin consent for pavagupt-tme

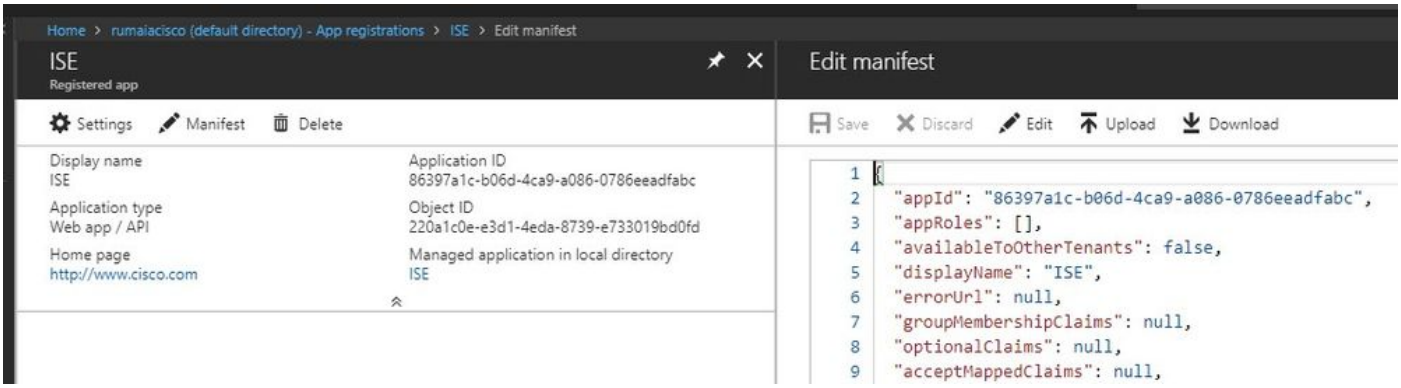
API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted for pavagupt-t...
Directory.Read.All	Application	Read directory data	Yes	Granted for pavagupt-t...
User.Read.All	Delegated	Read all users' 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...



5단계. 클릭 Grant Permissions 모든 응용 프로그램 권한을 확인합니다. 이 프로세스는 5~10분 정도 소요됩니다. 편집 Azure Manifest 내부 ISE CA 인증서를 가져오기 위해 생성된 애플리케이션 파일입니다.

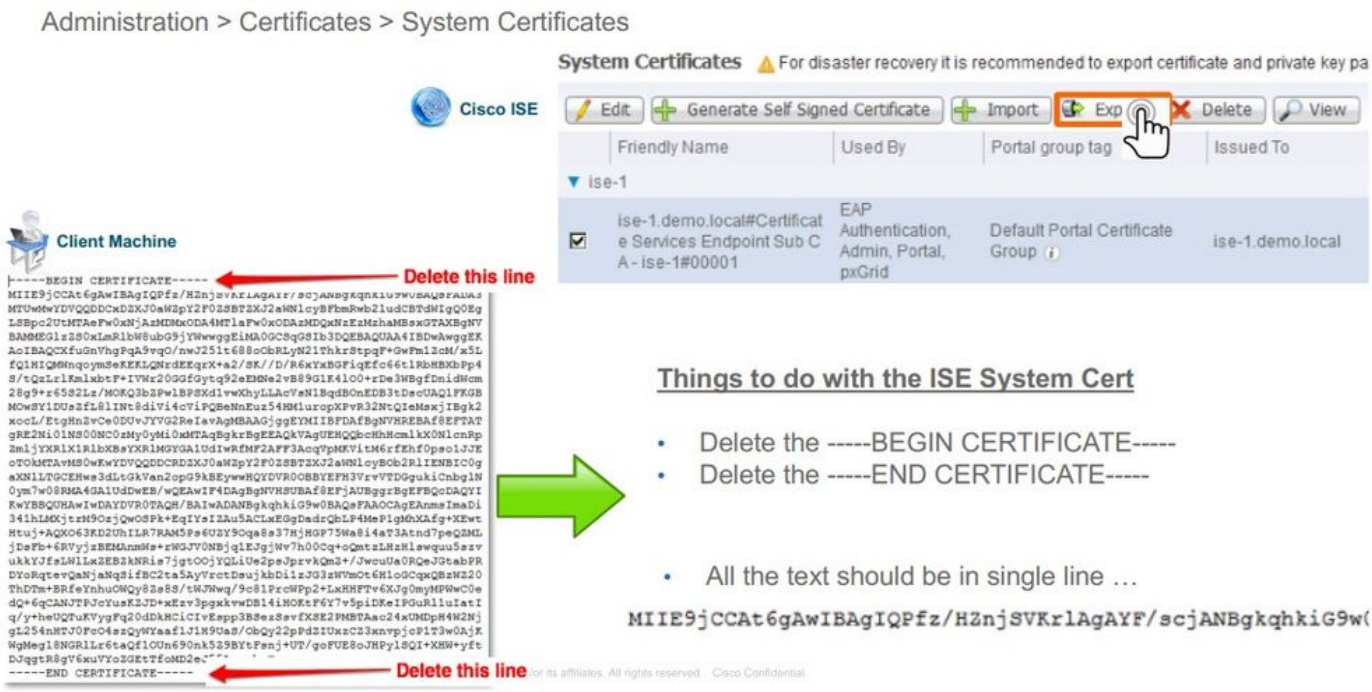
Azure의 응용 프로그램으로 ISE 인증서 가져오기

1단계. 응용 프로그램의 매니페스트 파일을 다운로드합니다.

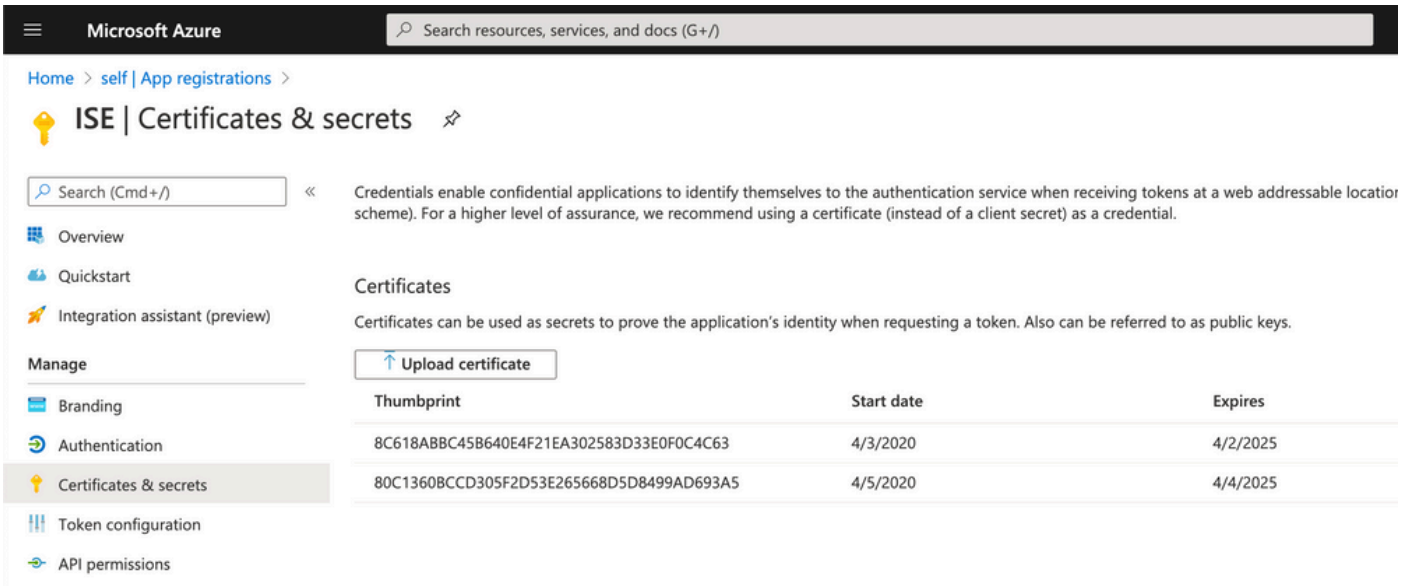


참고: JSON 확장명을 가진 파일입니다. 파일 이름 또는 확장명을 편집하지 마십시오. 그렇지 않으면 실패합니다.

2단계. 모든 노드에서 ISE 시스템 인증서를 내보냅니다. PAN에서 Administration > System > Certificates > System Certificates에서 기본 자체 서명 서버 인증서를 선택하고 Export. 선택 Export Certificate Only (기본값)을 선택하고 저장할 위치를 선택합니다. 인증서에서 BEGIN 및 END 태그를 삭제하고 나머지 텍스트를 한 줄로 복사합니다. 이는 Legacy Option(레거시 옵션) 섹션에 설명된 2020년 6월 이전 버전에 적용됩니다.



2020년 6월 현재 포털에서는 인증서를 직접 업로드할 수 있습니다.



레거시 옵션:

1단계. 인증서를 BASE64로 전환하고 Azure JSON 매니페스트 파일로 제대로 가져오려면 PowerShell 프로시저를 실행합니다. Windows의 Windows PowerShell 또는 Windows PowerShell ISE 애플리케이션을 사용합니다. 다음 명령을 사용합니다.

```
$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()
```

2단계. 값 유지 $base64Thumbprint, $base64Value 및 $keyid를 참조하십시오. 이 모든 값이 JSON 필드에 추가됩니다 keyCredentials 기본적으로 다음과 같습니다.

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

이렇게 하려면 다음 순서대로 값을 사용하십시오.

```
"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"

  }
],
```

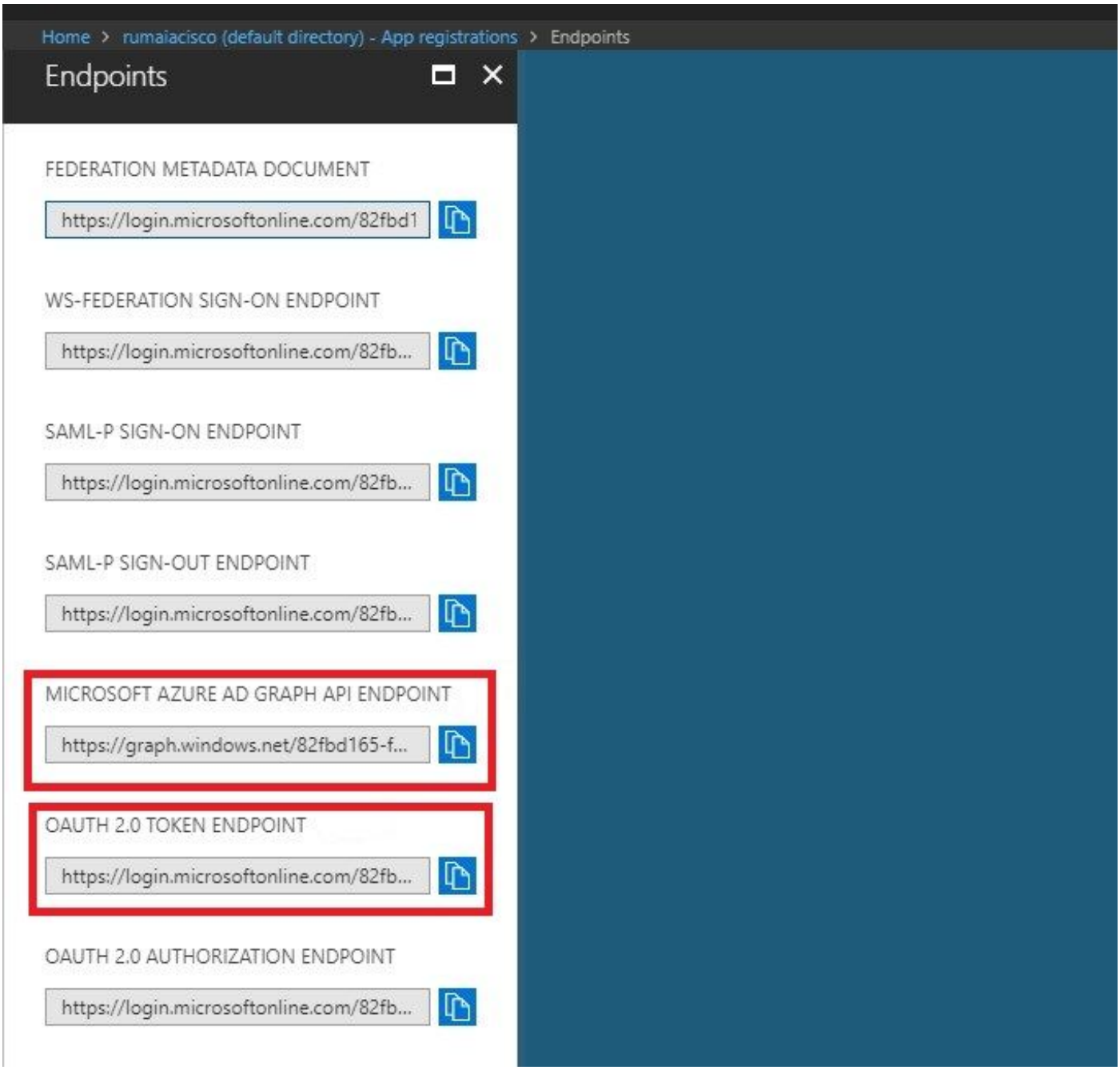
3단계. 편집한 파일 업로드 JSON 파일을 Azure Portal에 추가하여 keyCredentials ISE에서 사용되는 인증서에서 가져옵니다.

다음과 비슷해야 합니다.

```
"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
  },
```

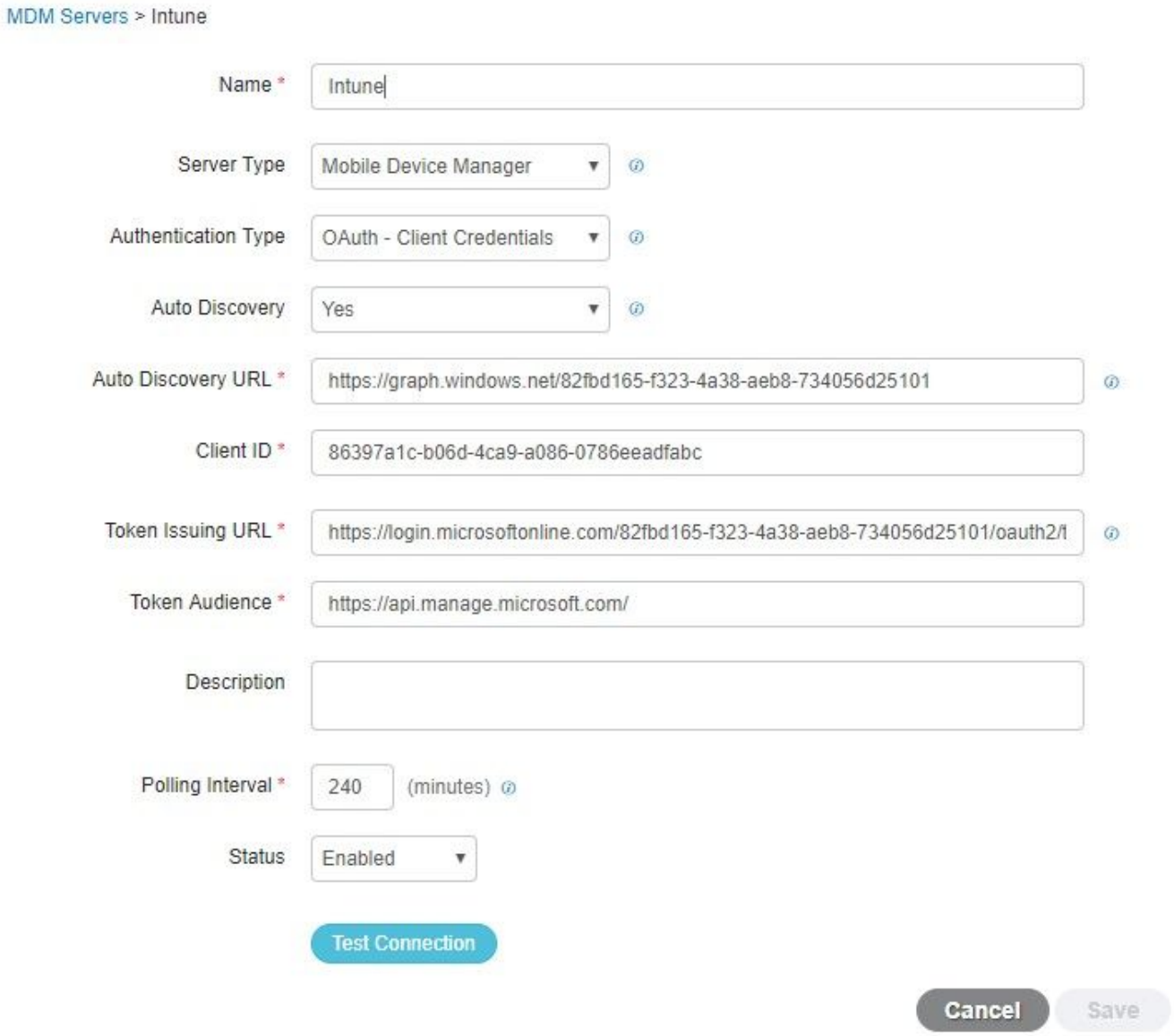

4단계. 업로드 후에는 value 필드 아래 keyCredentials 표시 null 이는 Microsoft 측에서 첫 번째 업로드 이후에 이러한 값을 볼 수 없도록 하기 때문입니다.

ISE에서 MDM 서버를 추가하는 데 필요한 값을 다음에서 복사할 수 있습니다 Microsoft Azure AD Graph API Endpoint 및 OAUTH 2.0 Token Endpoint.

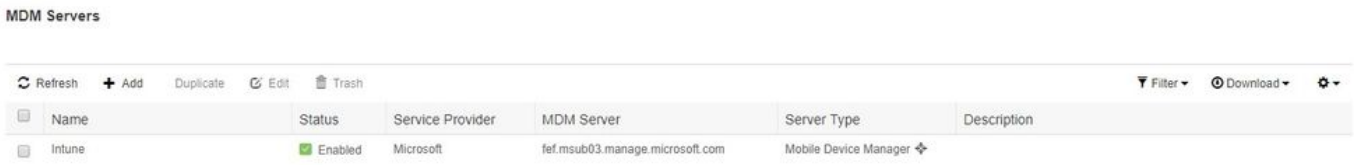


이러한 값은 ISE GUI에 입력해야 합니다. 탐색 Administration > Network Resources > External MDM 새 서버를 추가합니다.

ISE	Intune
자동 검색 URL	엔드포인트 > Microsoft Azure AD Graph API 엔드포인트
클라이언트 ID	{Registered-App-Name} > 애플리케이션 ID
토큰 발급 URL	Endpoints(엔드포인트) > OAuth 2.0 토큰 엔드포인트

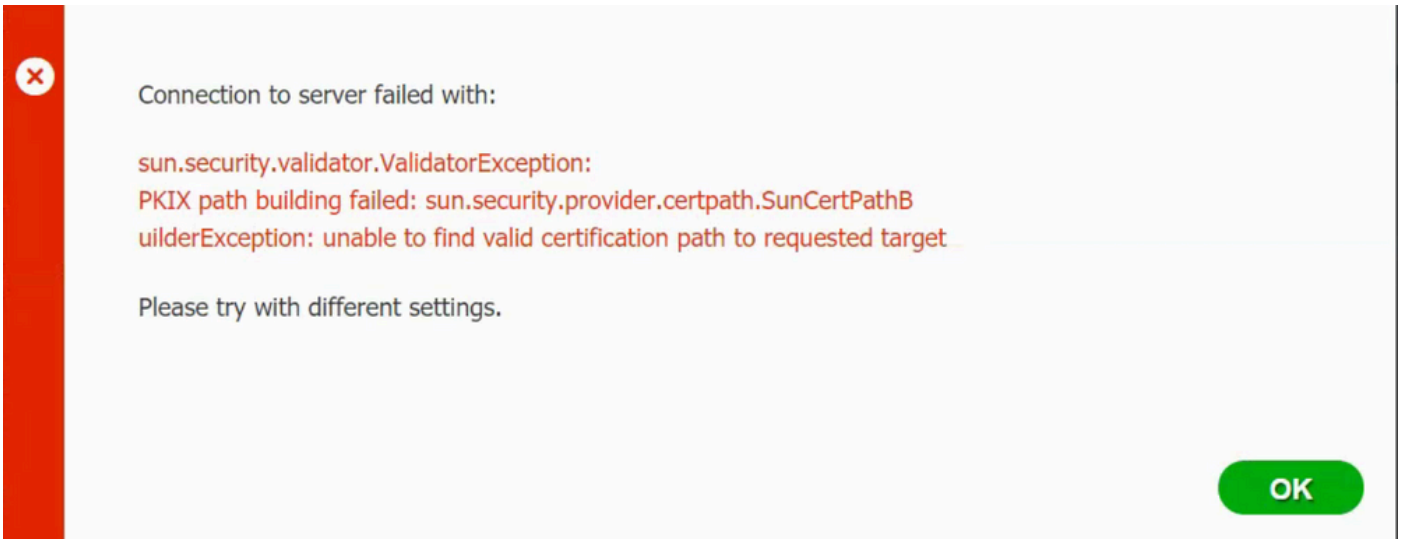


컨피그레이션이 완료되면 상태가 enabled(활성화됨)로 표시됩니다.



확인 및 문제 해결

sun.security.validatorException에 기반한 "서버 연결 실패"



1단계. TRACE 레벨에서 다음 로그와 함께 지원 번들을 수집합니다.

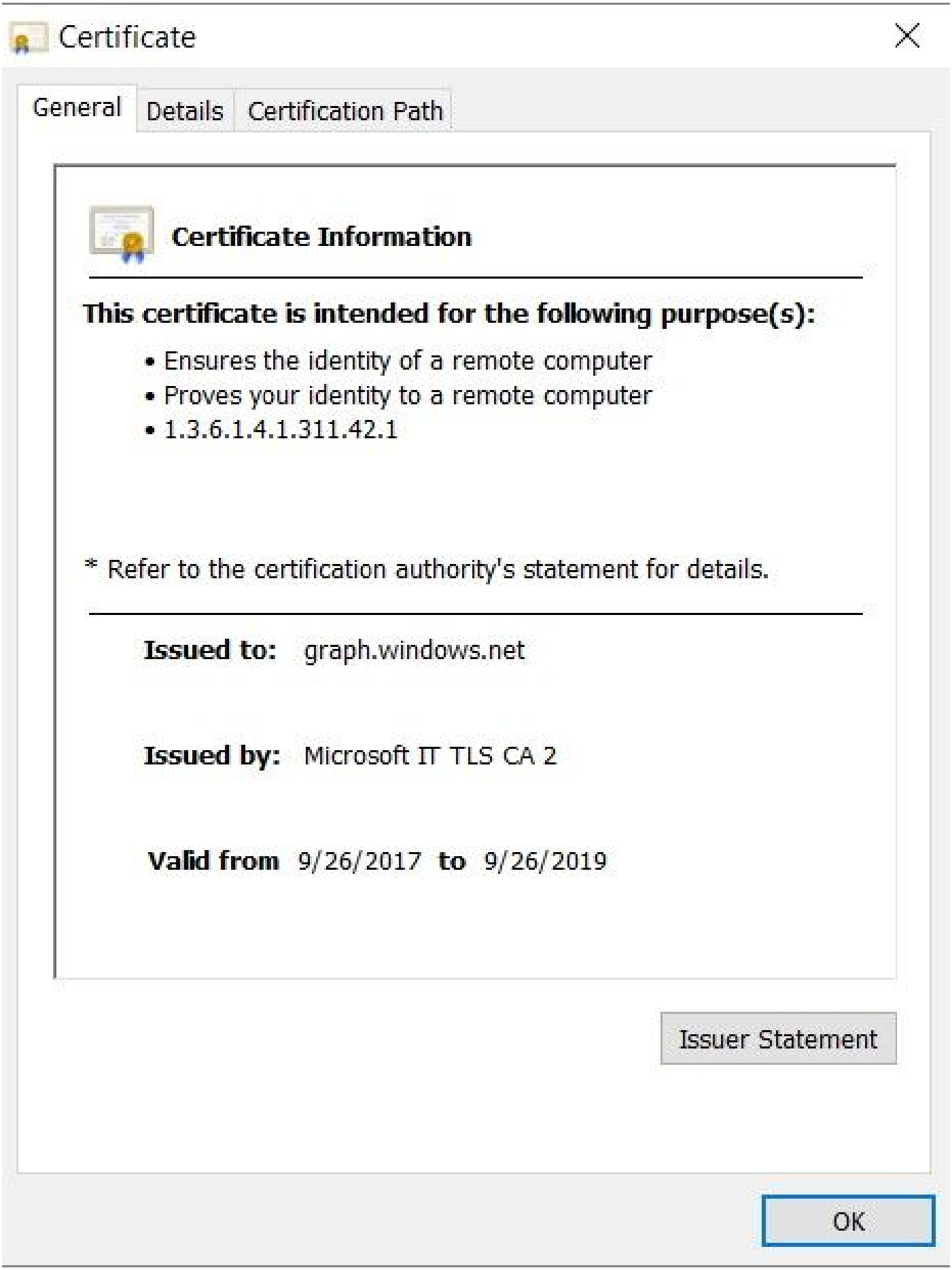
- portal (guest.log)
- mdmportal (ise-psc.log)
- external-mdm (ise-psc.log)

2단계. 수표 ise-psc.log 이러한 로그의 경우:

- 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

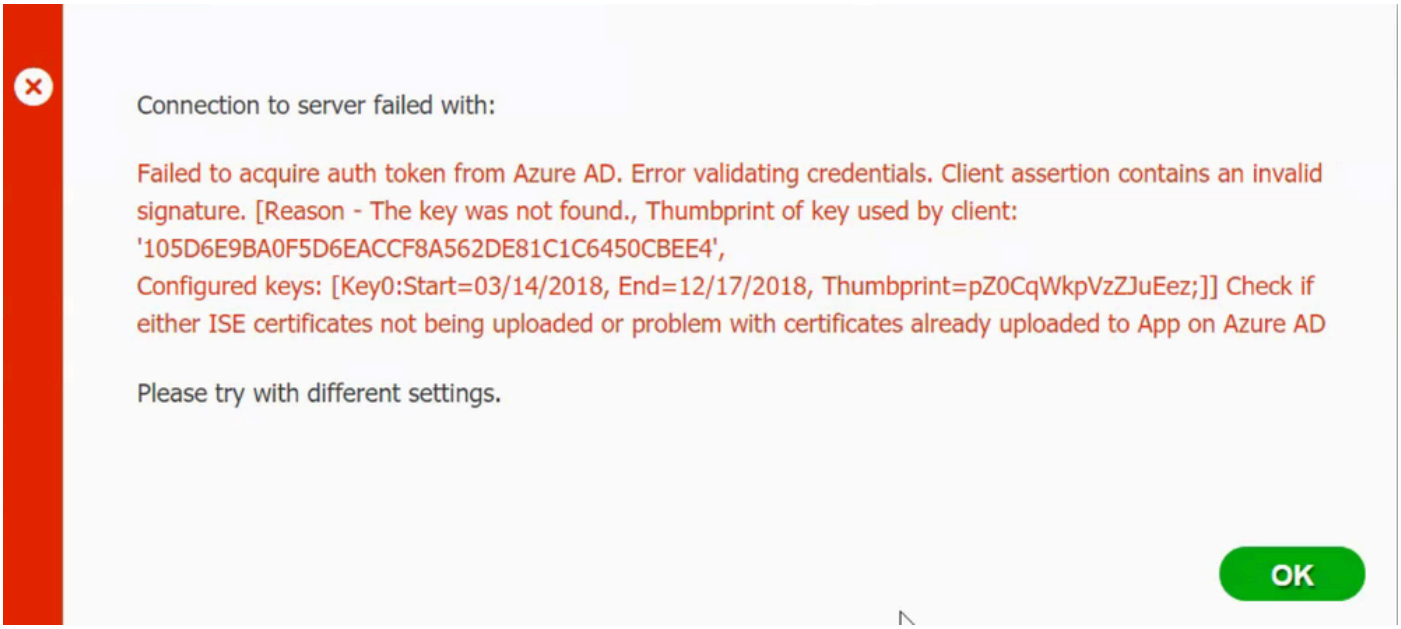
이는 을(를) 가져올 필요가 있음을 나타냅니다 graph.microsoft.com 인증서, 이 페이지에 있음

3단계. 다음을 클릭합니다. locker 아이콘을 클릭하고 인증서 세부사항을 확인합니다.



4단계. BASE64 형식의 파일에 저장하고 ISE Trusted Store로 가져옵니다. 전체 인증서 체인을 가져와야 합니다. 그런 다음 MDM 서버에 대한 연결을 다시 테스트합니다.

Azure AD에서 인증 토큰을 가져오지 못했습니다.



일반적으로 이 오류는 매니페스트가 JSON 파일에 잘못된 ISE 인증서 체인이 포함되어 있습니다. 매니페스트 파일을 Azure에 업로드하기 전에 적어도 이 구성이 있는지 확인하십시오.

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

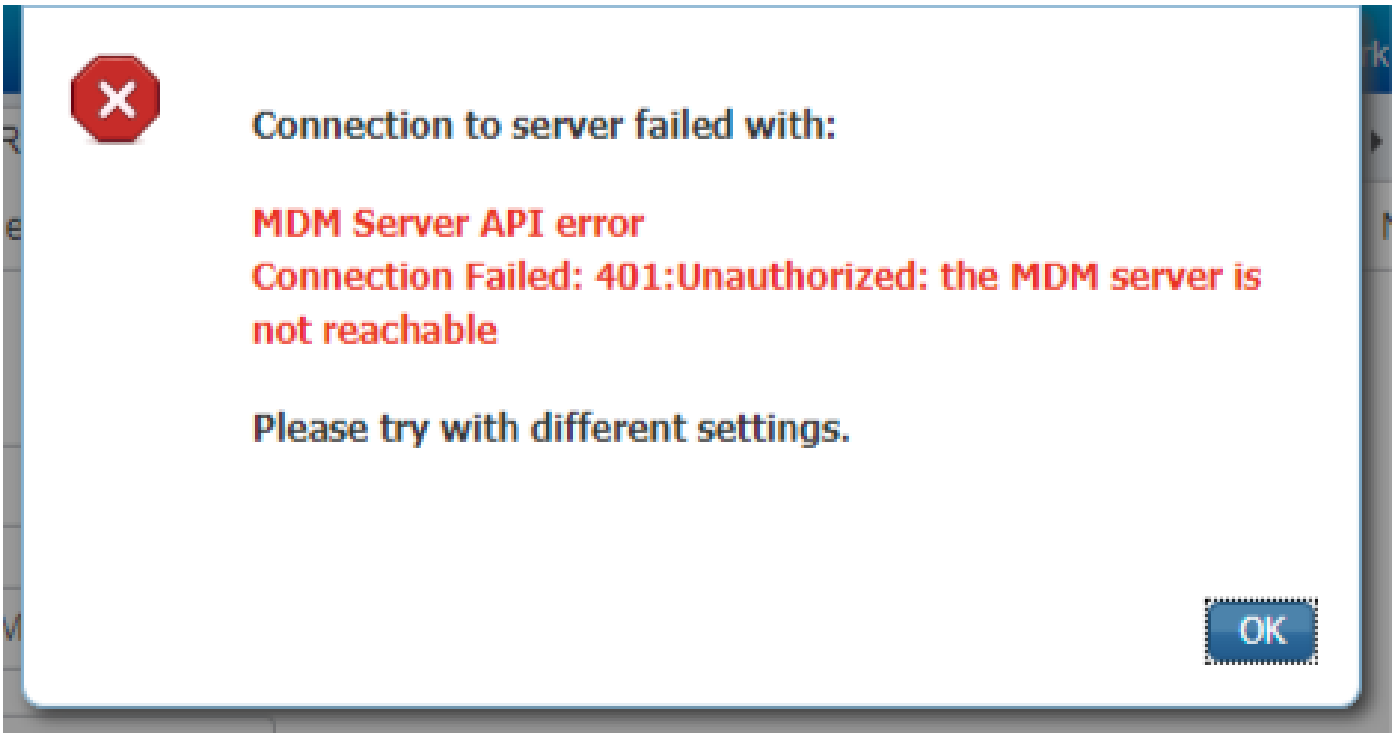
앞의 예는 PAN 및 SAN이 있는 시나리오를 기반으로 합니다. PowerShell에서 스크립트를 다시 실행하고 적절한 BASE64 값을 가져옵니다. 매니페스트 파일을 업로드해 보세요. 오류가 발생하지 않아야 합니다.

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

$bin = $cer.GetCertHash()
```

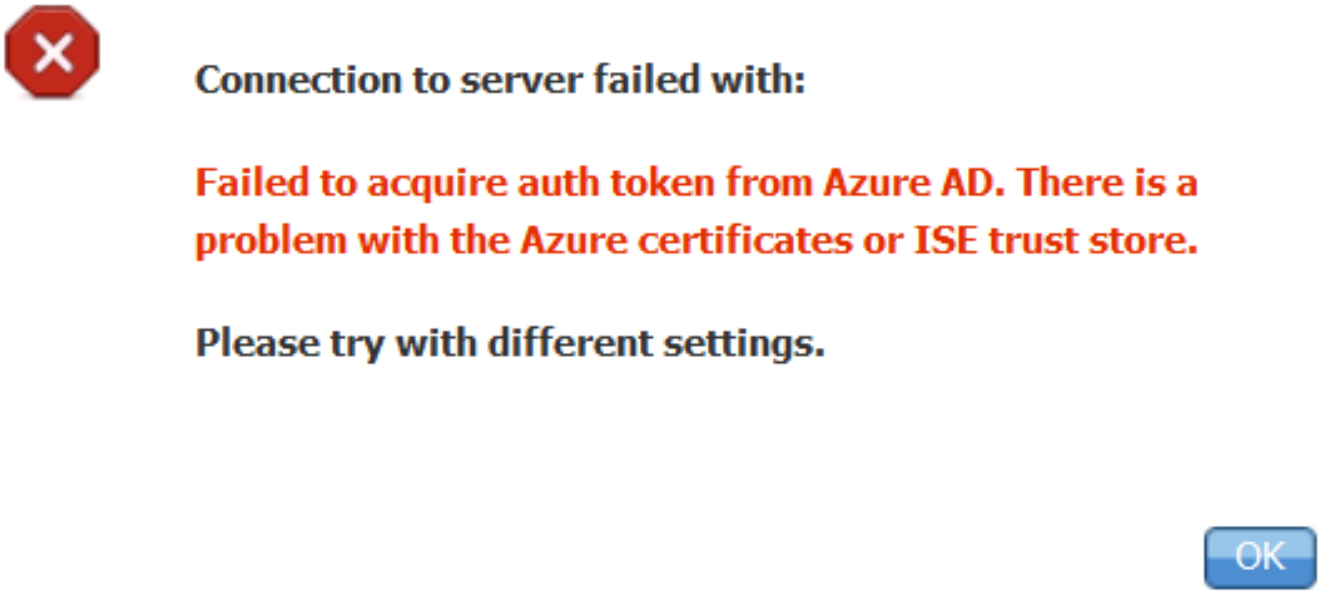
```
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

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

다음에 대한 값을 적용해야 합니다. $base64Thumbprint, $base64Value 및 $keyid 구성 섹션의 단계에서 설명한 대로

Azure AD에서 인증 토큰을 가져오지 못했습니다.



이 오류는 의 Azure 앱에 올바른 권한이 부여되지 않은 경우 자주 발생합니다. portal.azure.com. 앱에 올바른 특성이 있는지 확인하고 Grant Permissions 모든 변화 후에.



이 메시지는 ISE가 토큰 발급 URL에 액세스하려고 할 때 ISE가 반환하지 않는 인증서를 반환할 때 발생합니다. 전체 CA 체인이 ISE 트러스트 저장소에 있는지 확인합니다. ISE의 신뢰할 수 있는 저장소에 올바른 인증서를 설치한 후에도 문제가 지속되면 패킷 캡처를 수행하고 무엇이 전송되는지 확인하기 위해 연결을 테스트합니다.

관련 정보

- 클라이언트 자격 증명을 사용한 서비스 간 통화
- Azure - 인증 대 권한 부여
- Azure - Quickstart: Microsoft ID 플랫폼으로 응용 프로그램 등록
- Azure Active Directory 앱 매니페스트
- 기술 지원 및 문서 − Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.