Intune MDMとIdentity Services Engineの統合

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

設定

- ネットワーク図
- Microsoft Intuneの構成
  - IntuneポータルからISE信頼ストアへの証明書のインポート
  - ISEをAzureポータルのアプリケーションとして展開する
  - AzureのアプリケーションへのISE証明書のインポート

確認とトラブルシューティング

- sun.security.validator.ValidatorExceptionに基づく「Connection to the server failed」
- Azure ADから認証トークンを取得できませんでした
- Azure ADから認証トークンを取得できませんでした

関連情報

はじめに

このドキュメントでは、Intune Mobile Device Management(MDM)をCisco Identity Services Engine(ISE)と統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ISEのMDMサービスに関する知識
- Microsoft Azure Intuneサービスに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine 3.0
- Microsoft Azure Intuneアプリケーション

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

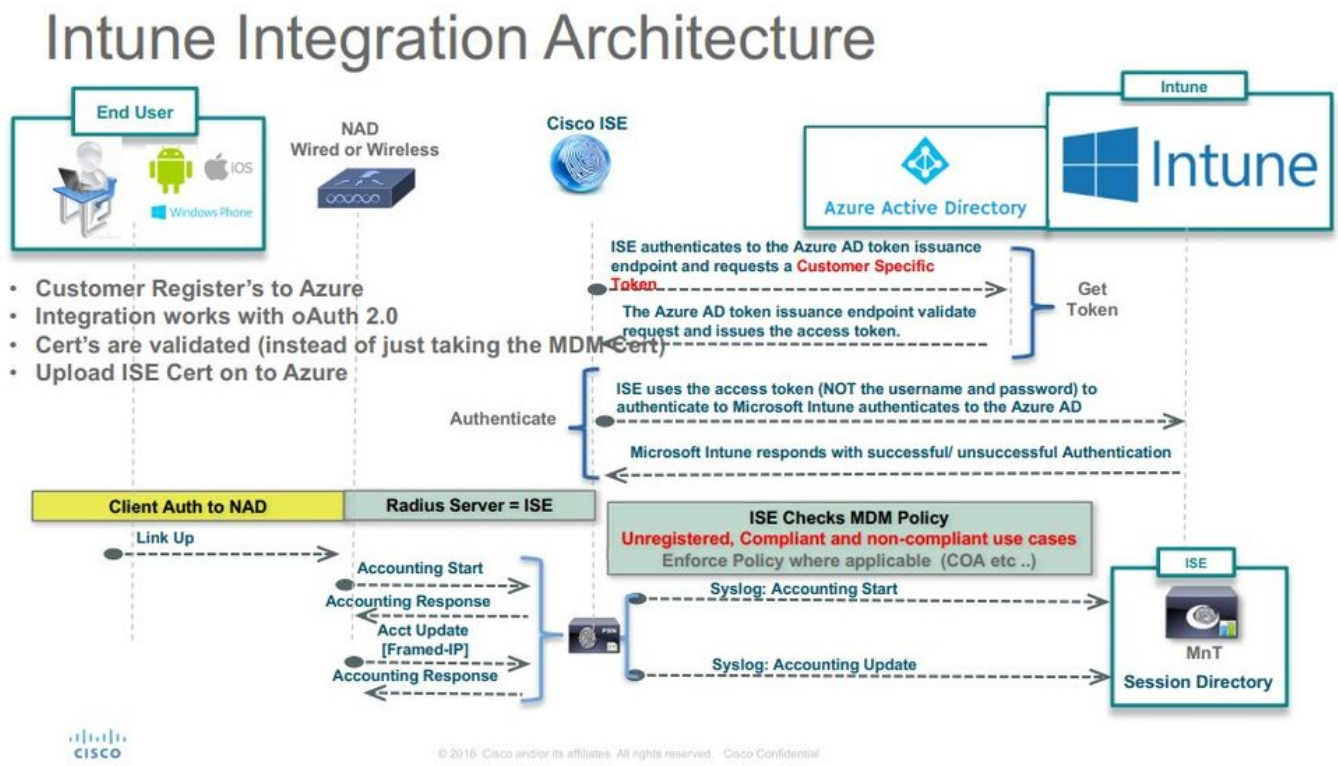
す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

MDMサーバは、モバイル事業者、サービスプロバイダー、およびエンタープライズ全体に導入されたモバイルデバイスを保護、監視、管理、およびサポートします。これらのサーバは、導入された環境でモバイルデバイス上の一部のアプリケーション（Eメールアプリケーションなど）の使用を制御するポリシーサーバとして機能します。ただし、アクセスコントロールリスト(ACL)に基づいてエンドポイントに詳細なアクセスを提供できるエンティティはネットワークだけです。ISEは、MDMサーバに必要なデバイス属性を照会し、それらのデバイスのネットワークアクセス制御を提供するACLを作成します。Cisco ISEはMicrosoft Intune MDM Serverと統合し、デバイスが社内リソースにアクセスしようとしたときに企業データを保護します。

設定

ネットワーク図



Microsoft Intuneの構成

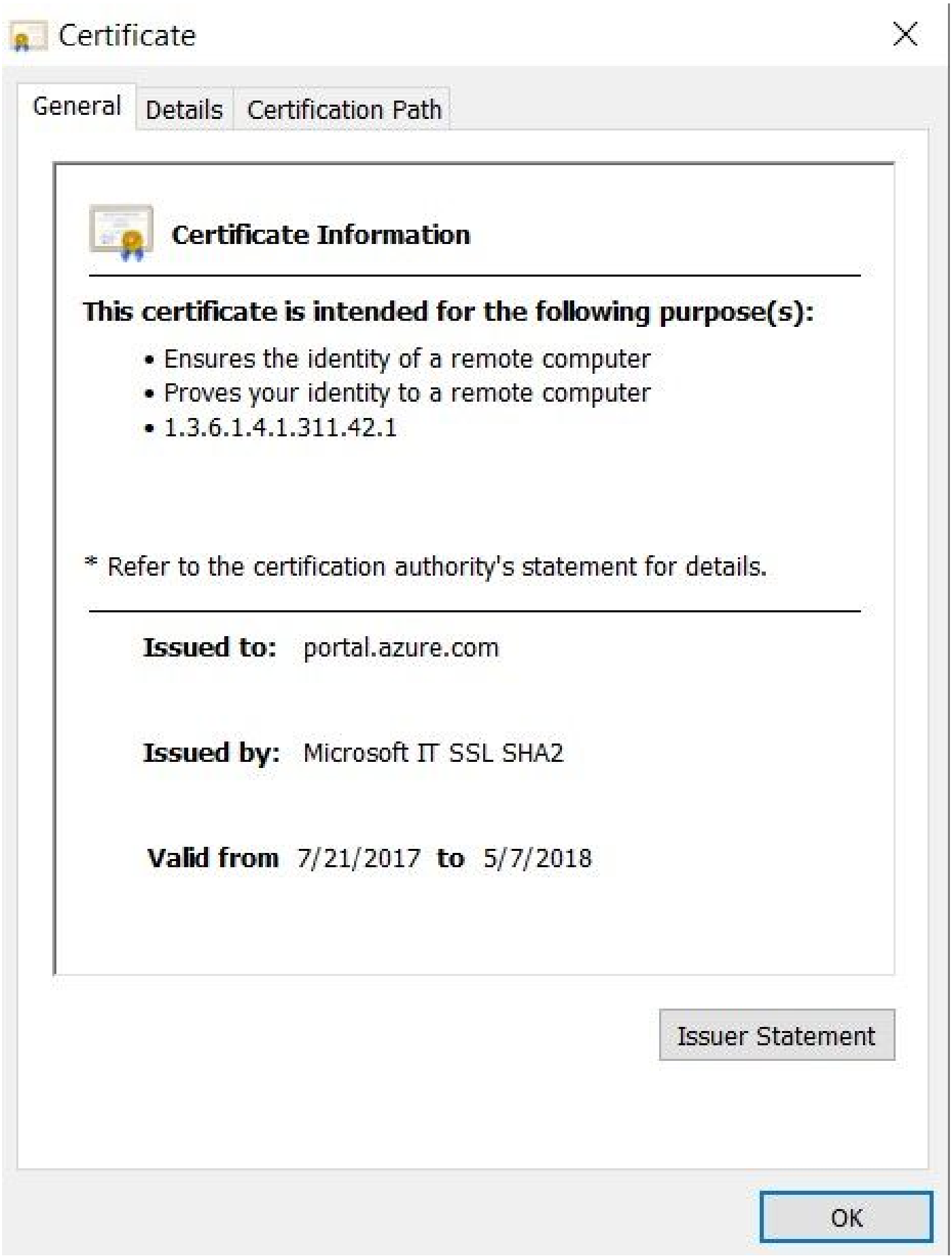
IntuneポータルからISE信頼ストアへの証明書のインポート

Intune管理コンソールまたはAzure管理コンソール（テナントがあるサイト）にログインします。ブラウザを使用して、証明書の詳細を取得します。

ステップ 1：Webブラウザから Microsoft Azure portal、を開きます。

ステップ 2：ブラウザのツールバーでロック記号をクリックし、 View Certificates.

ステップ 3：Certificateウィンドウで、Certification Path タブをクリックします。次に例を示します。



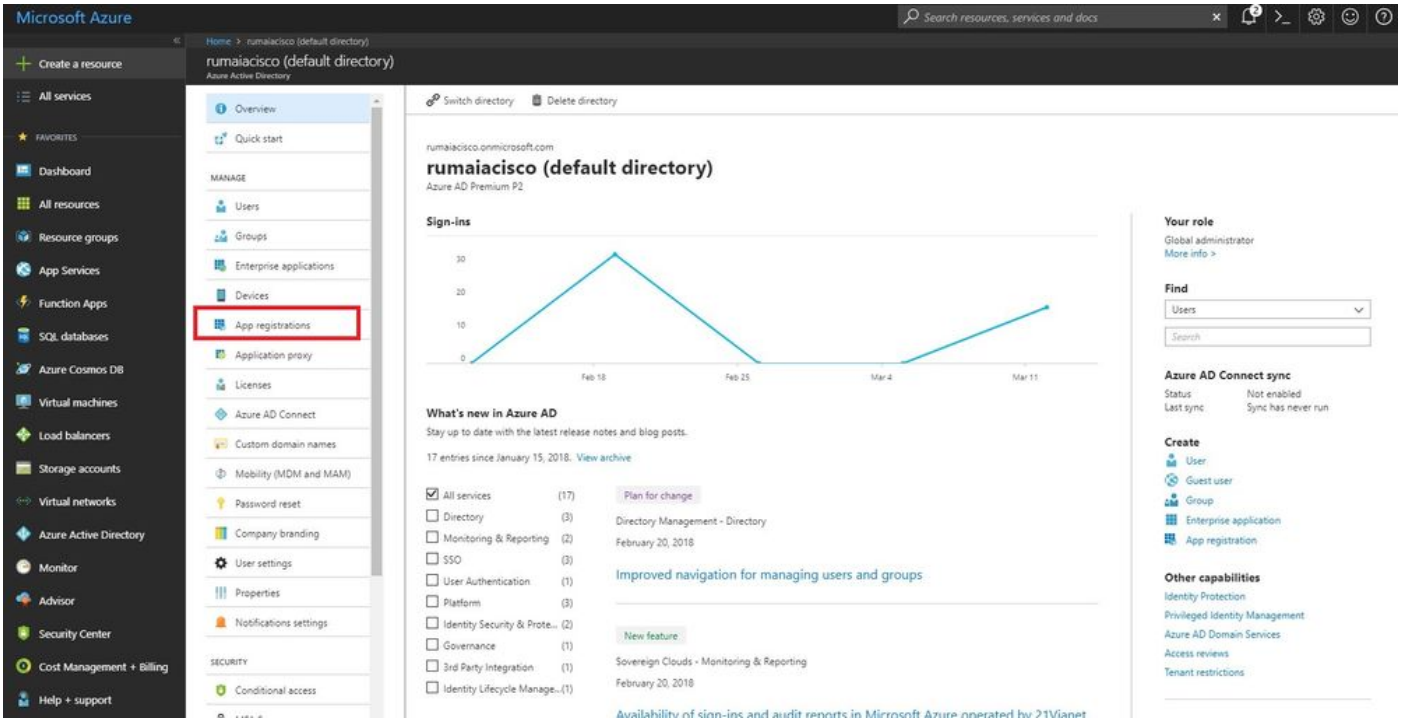
ステップ 4：通常Baltimore Cyber Trust root, のルートCAを検索します。ただし、他に別のルートCAがある場合は、そのルートCA証明書をクリックします。そのルートCA証明書のDetailsタブで、証明書をファイルにコピーし、BASE64証明書として保存で

きます。

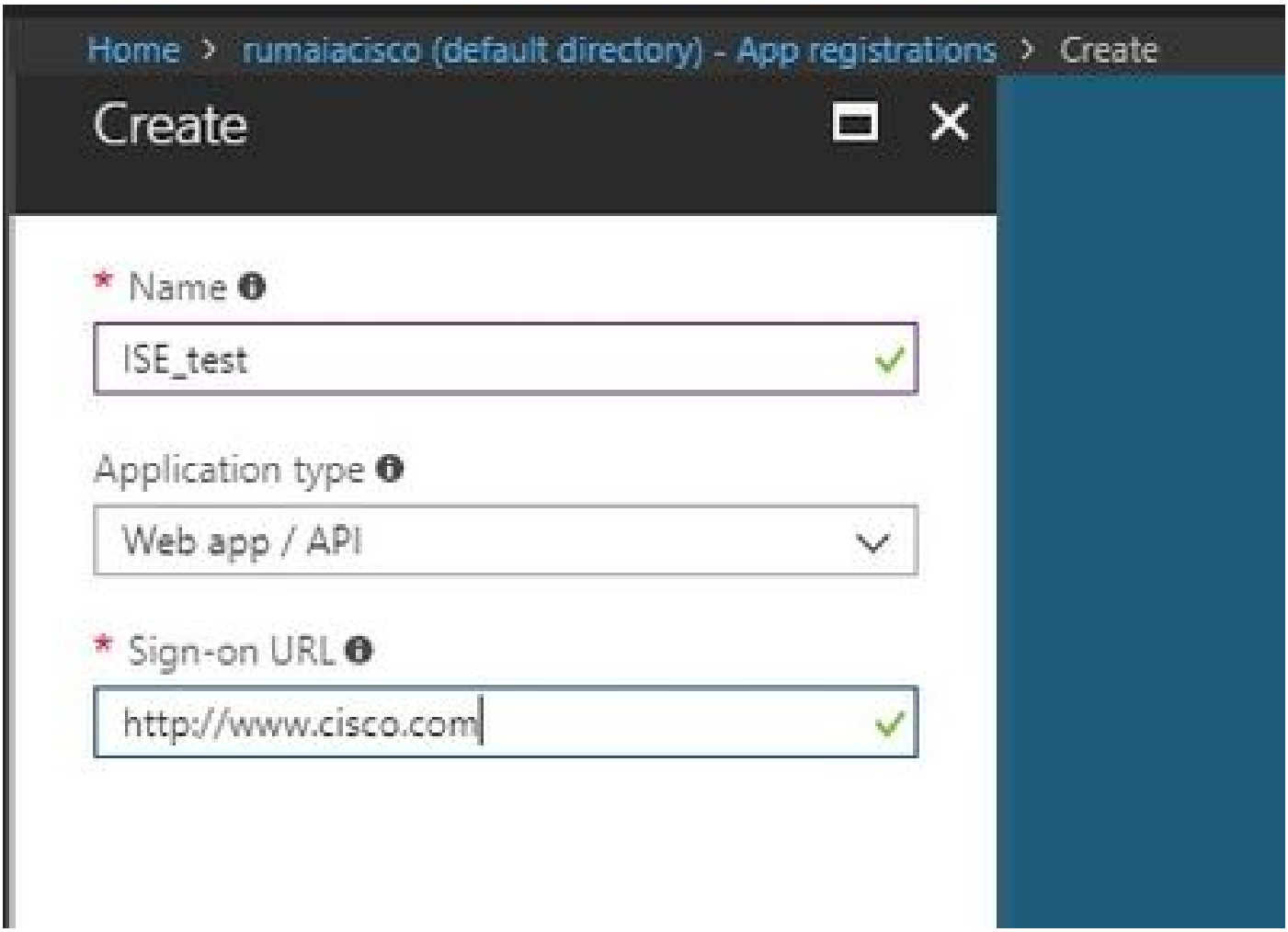
ステップ５：ISEで、保存したルート証明書に移動Administration > System > Certificates > Trusted Certificates, し、インポートします。証明書にわかりやすい名前(Azure MDMなど)を付けます。中間CA証明書についても、この手順を繰り返します。

ISEをAzureポータルのアプリケーションとして展開する

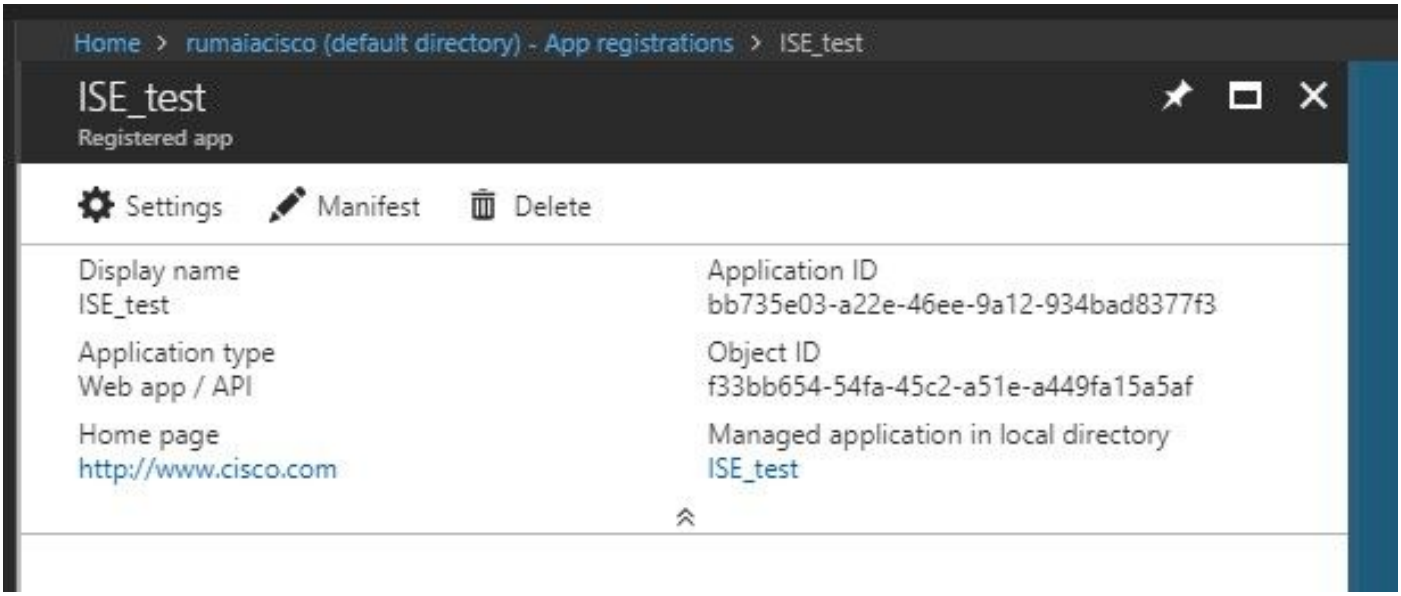
ステップ１：に移動しAzure Active Directory、 App registrations.



ステップ２：で、ISE名を使用して新しいアプリケーション登録をApp registrations, 作成します。次の図に示すようにCreateクリックします。



ステップ 3：を選択してSettings、アプリケーションを編集し、必要なコンポーネントを追加します。



ステップ 4：下で必要な権限をSettings, 選択し、次のオプションを適用します。

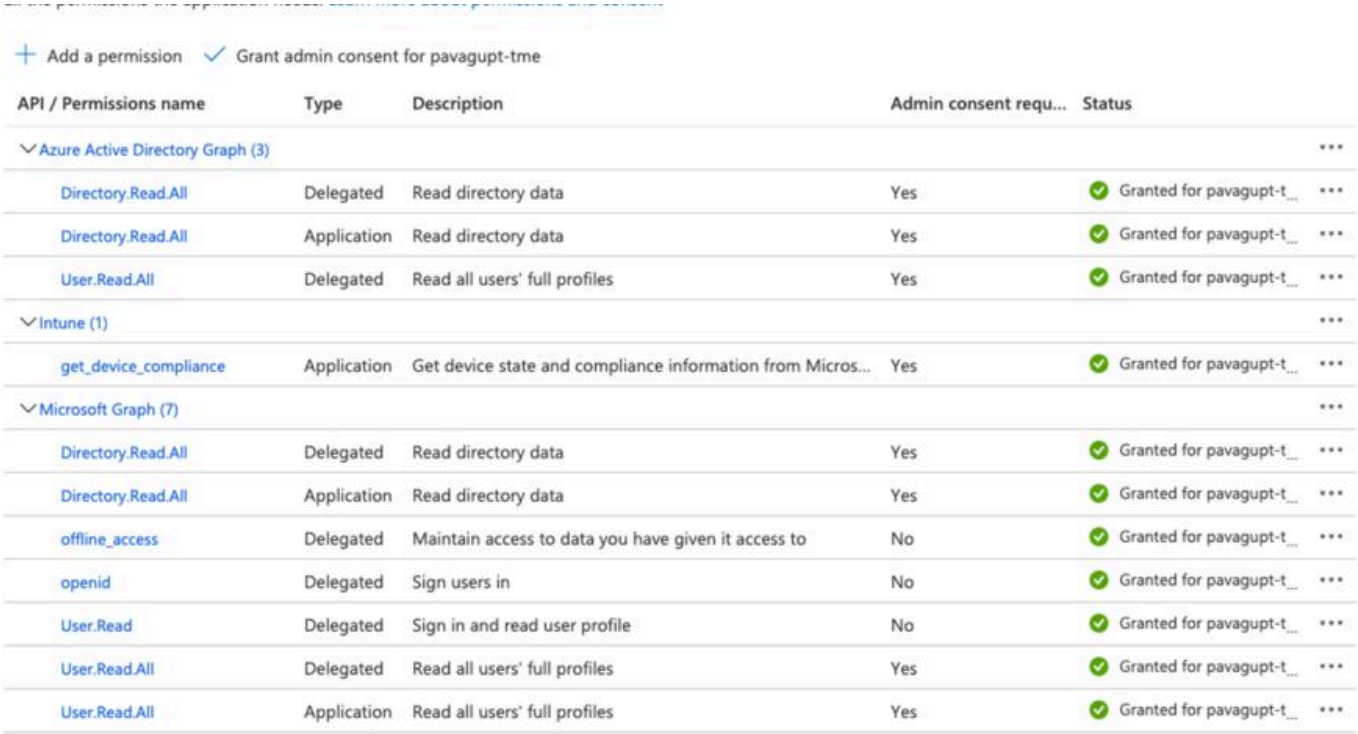
- Microsoft Graph

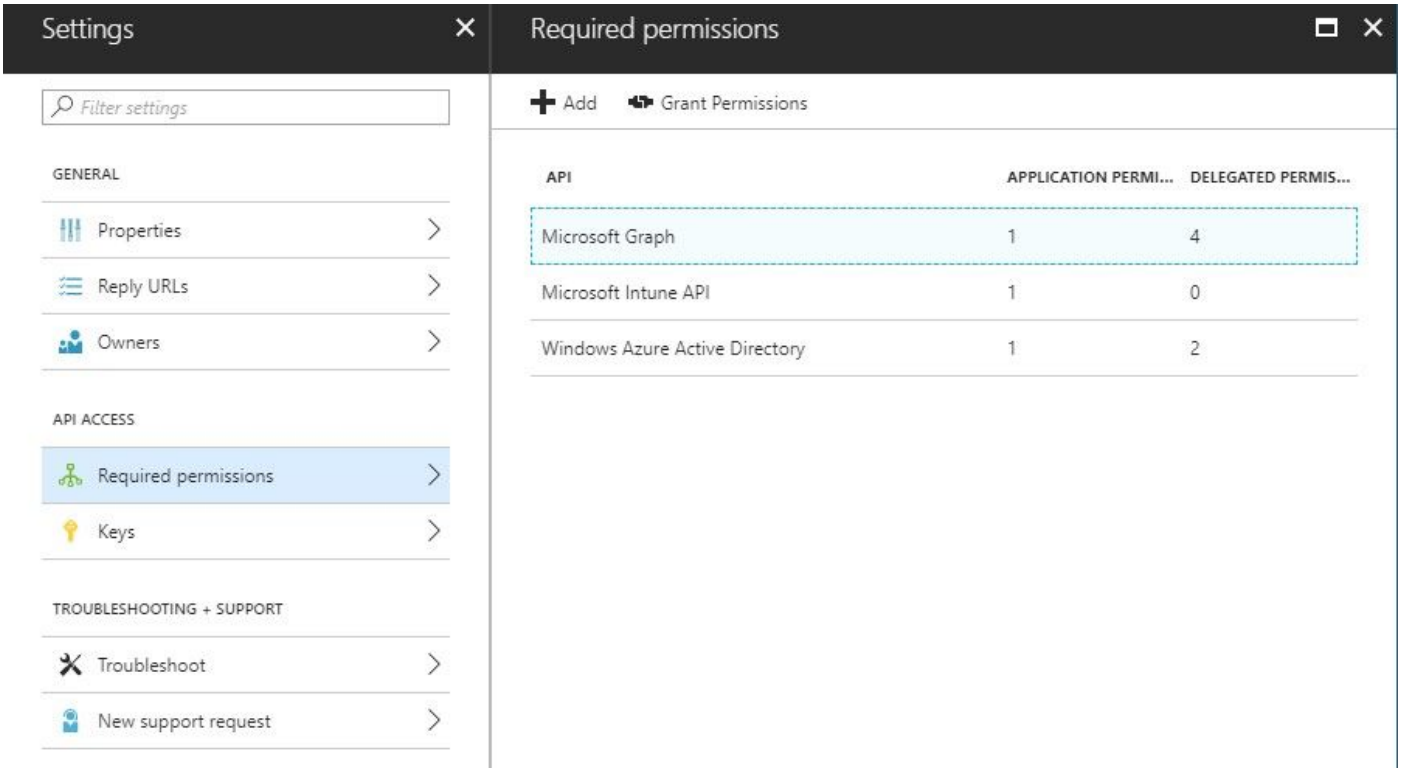
- アプリケーション権限
    - ディレクトリデータの読み取り
- 委任された権限
    - Microsoft Intuneデバイスの構成とポリシーの読み取り
    - Microsoft Intune構成の読み取り
    - サインインする
    - ユーザのデータにいつでもアクセス可能

- Microsoft Intune API
    - アプリケーション権限
        - Microsoft Intuneからデバイスの状態とコンプライアンス情報を取得する

- Windows Azure Active Directory
    - アプリケーション権限
        - ディレクトリデータの読み取り
    - 委任された権限
        - ディレクトリデータの読み取り
        - サインインしてユーザプロファイルを読む

設定の結果は、次のようになります。

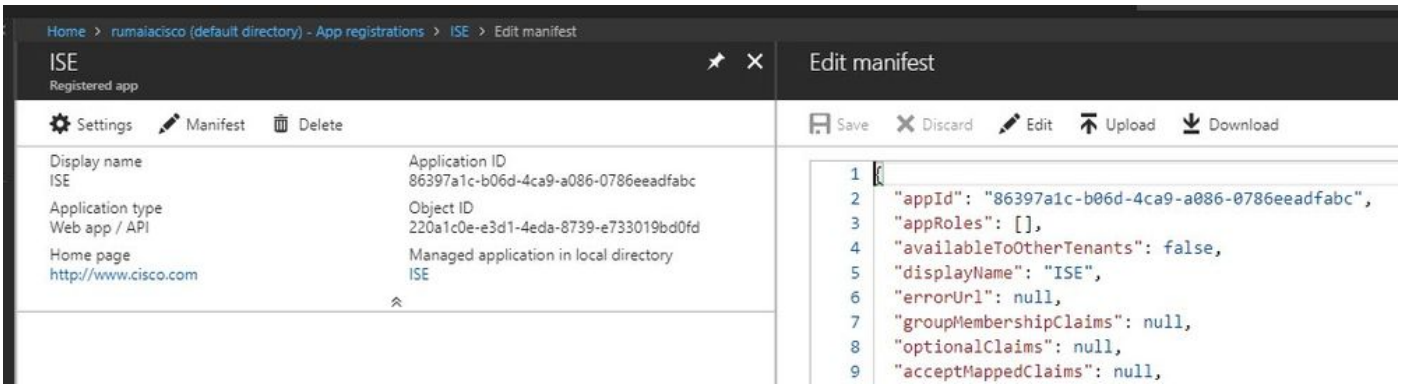




ステップ５：をクリックしてGrant Permissions、すべてのアプリケーション権限を確認します。このプロセスが有効になるには、５～ 10分かかります。内部ISE CA証明書をインポートするために作成されたアプリケーションのファイルを編集しますAzure Manifest。

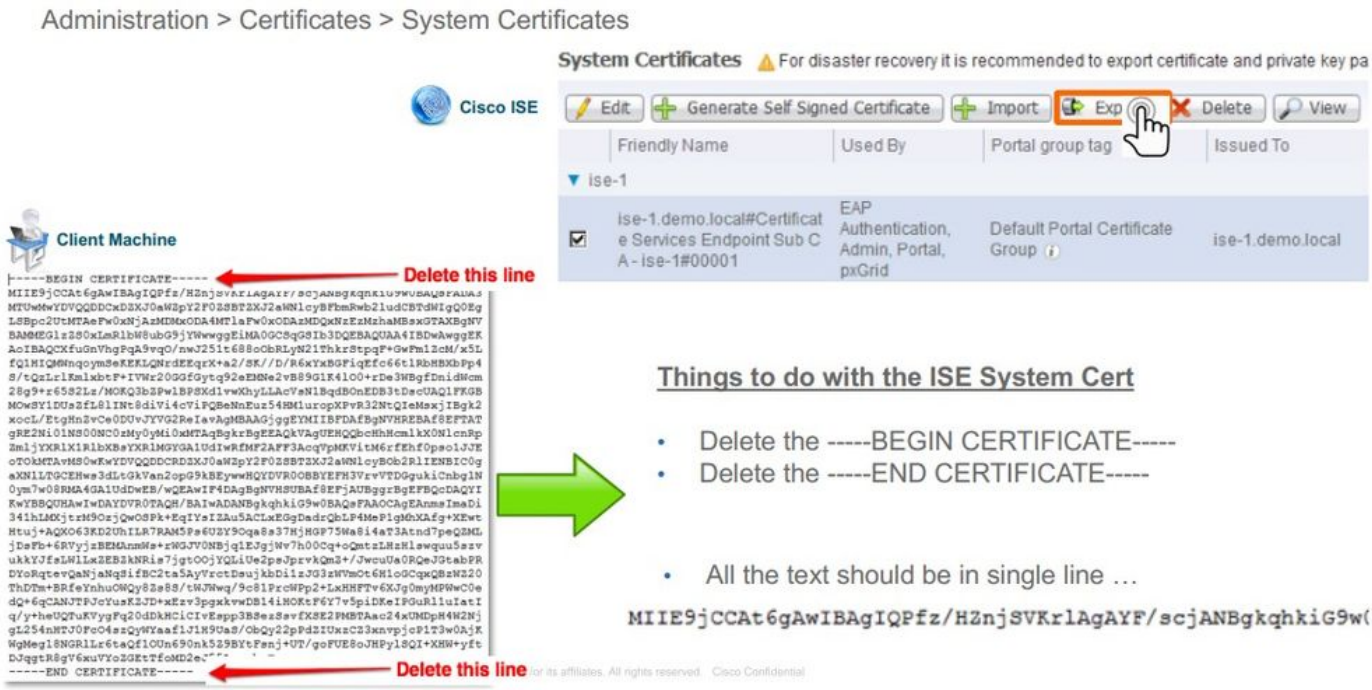
Azureのアプリケーションへの ISE証明書のインポート

ステップ１：アプリケーションのマニフェストファイルをダウンロードします。

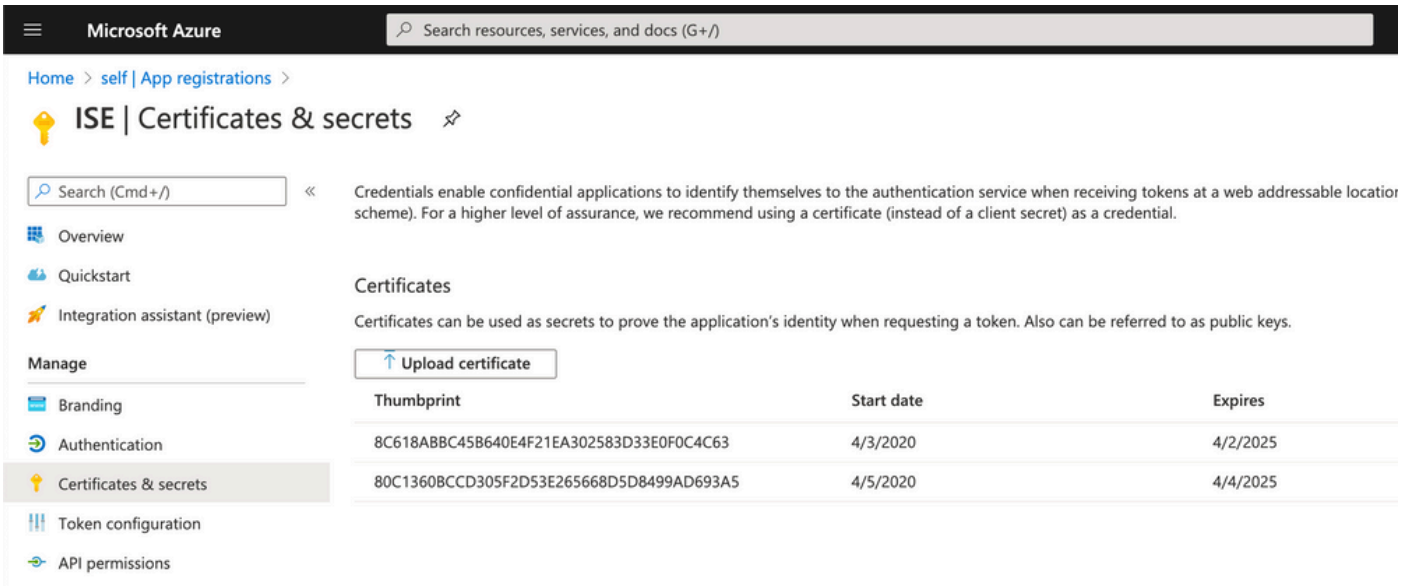


注：これはJSON拡張子を持つファイルです。ファイル名や拡張子は編集しないでください。編集すると失敗します。

ステップ 2：すべてのノードからISEシステム証明書をエクスポートします。PANで、**Default self-signed server certificate**に移動して選択Administration > System > Certificates > System Certificates, し、をクリックしExport.ます。Export Certificate Only（デフォルト）を選択し、保存する場所を選択します。証明書からBEGINタグとENDタグを削除し、残りのテキストを1行でコピーします。これは、「レガシーオプション」セクションで説明されている2020年6月より前のバージョンに適用されます。



2020年6月現在、ポータルでは証明書を直接アップロードできます。



レガシーオプション：

ステップ 1：PowerShellプロシージャを実行して証明書をBASE64に変換し、Azure JSONマニフェストファイルに適切にインポートします。WindowsからWindows PowerShellまたはWindows PowerShell ISEアプリケーションを使用します。次のコマンドを使用します。

$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import(“mycer.cer”) $bin = $cer.GetRawCertData() $base64Va

ステップ 2：次の手順で使用する $base64Thumbprint, $base64Valueおよび $keyidの値を保持します。これらの値はすべてJSONフィールドに追加されます。keyCredentialsこれは、デフォルトでは次のように表示されるためです。

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

そのためには、次の順序で値を使用してください。

"keyCredentials": [{ “customKeyIdentifier“: “$base64Thumbprint_from_powerShell_for_PPAN”, “keyId“: “$keyid_from_above_PPAN“, "type": "A

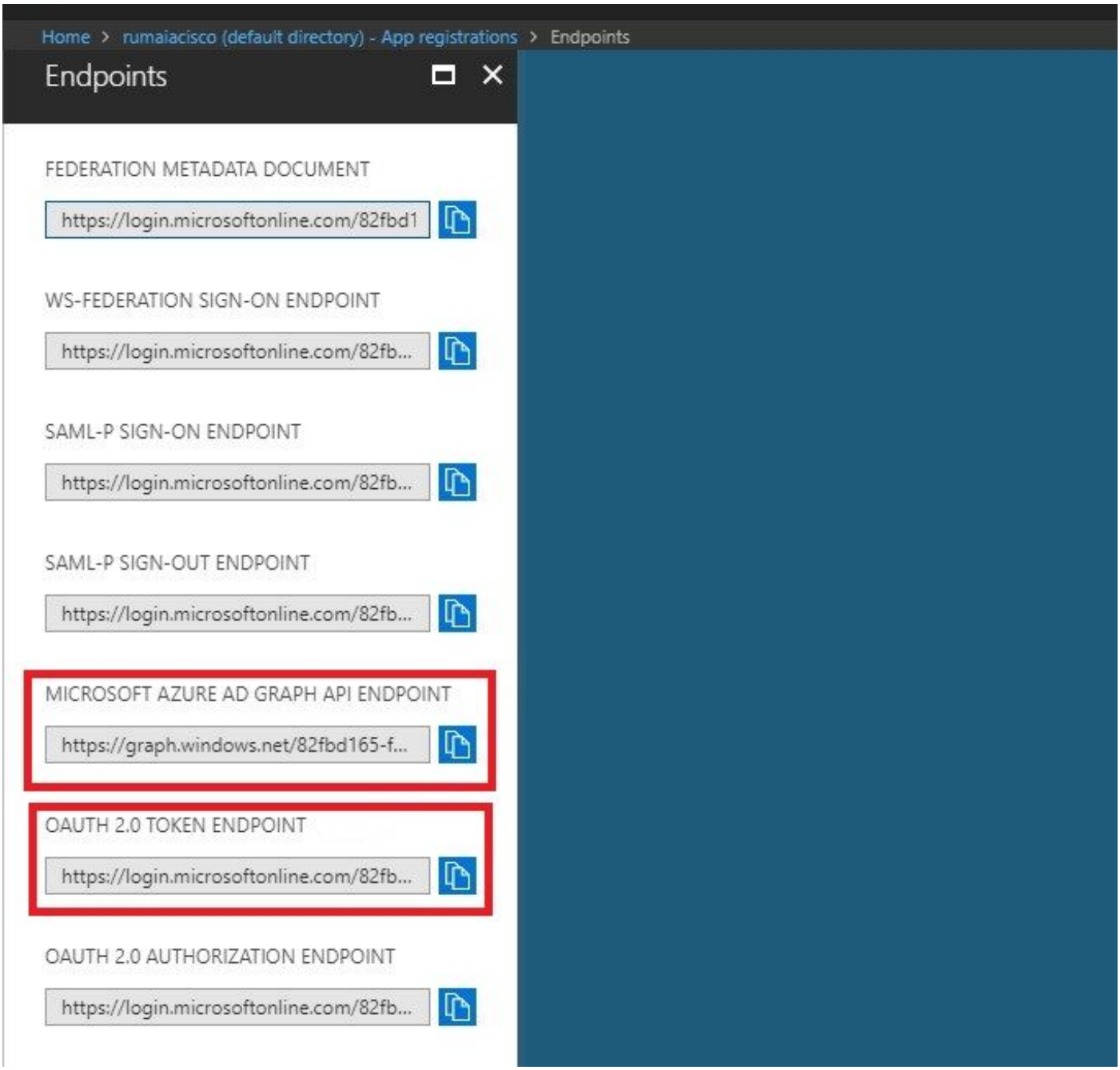
ステップ 3：ISEで使用される証明書を検証するために、編集したJSONファイルをAzureポータルkeyCredentialsにアップロードします。

次のように表示されるはずです。

```
"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
  },
```

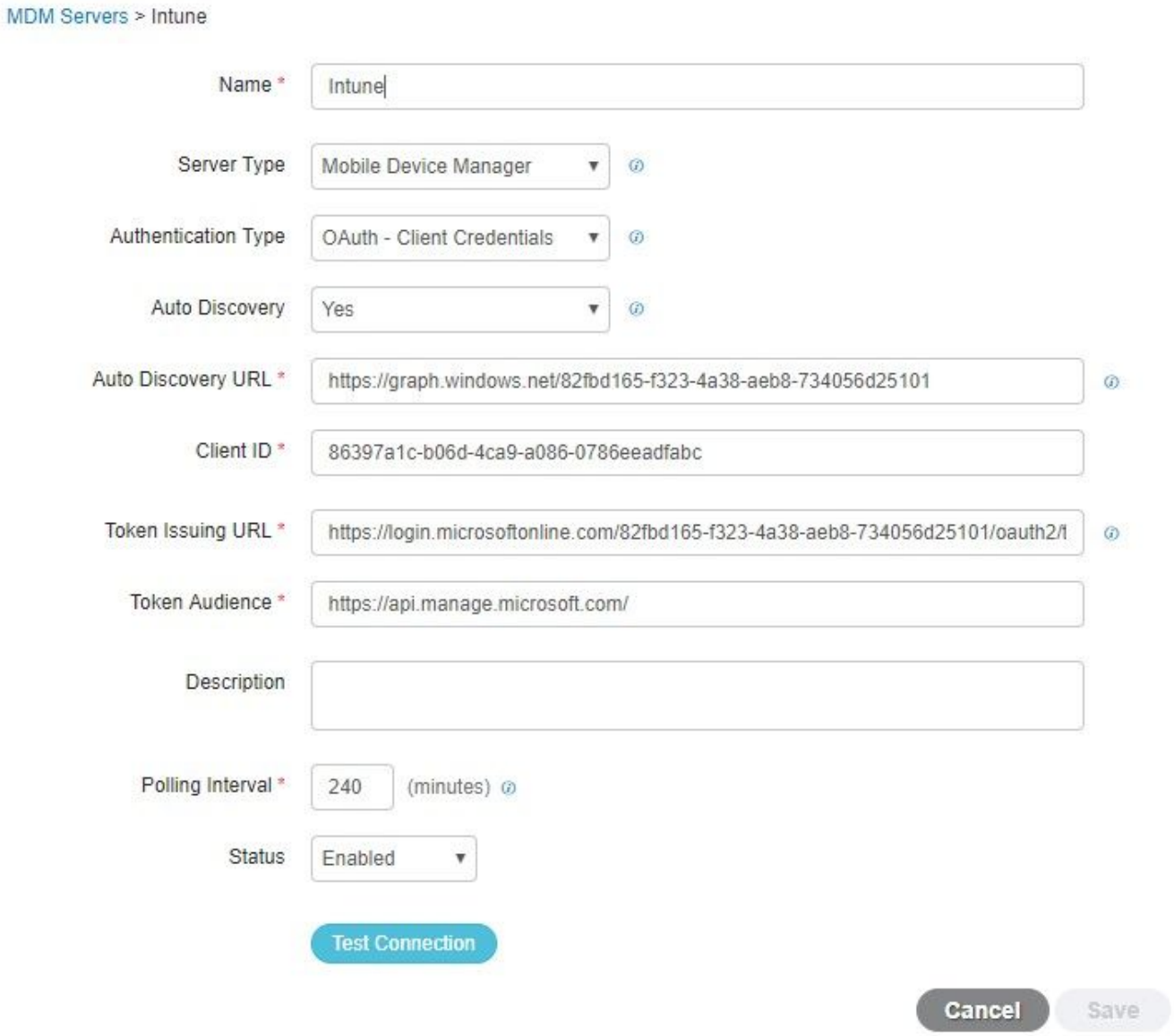

ステップ 4 : アップロード後は、Microsoft側によって最初のアップロード後にこれらの値が表示されないように強制されるため、下のフ value ィールドが keyCredentials 表示さ null れることに注意してください。

ISEにMDMサーバを追加するために必要な値は、 Microsoft Azure AD Graph API Endpoint および OAUTH 2.0 Token Endpointからコピーできます。

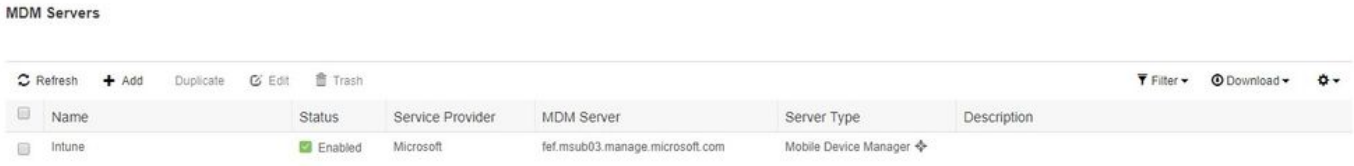


これらの値は、ISE GUIで入力する必要があります。新しいサーバAdministration > Network Resources > External MDM に移動し、追加します。

ISE	Intune
自動検出URL	[エンドポイント] > [Microsoft Azure AD Graph APIエンドポイント]
クライアント ID	{Registered-App-Name} >アプリケーションID
トークン発行URL	「エンドポイント」>「OAuth 2.0トークンエンドポイント」

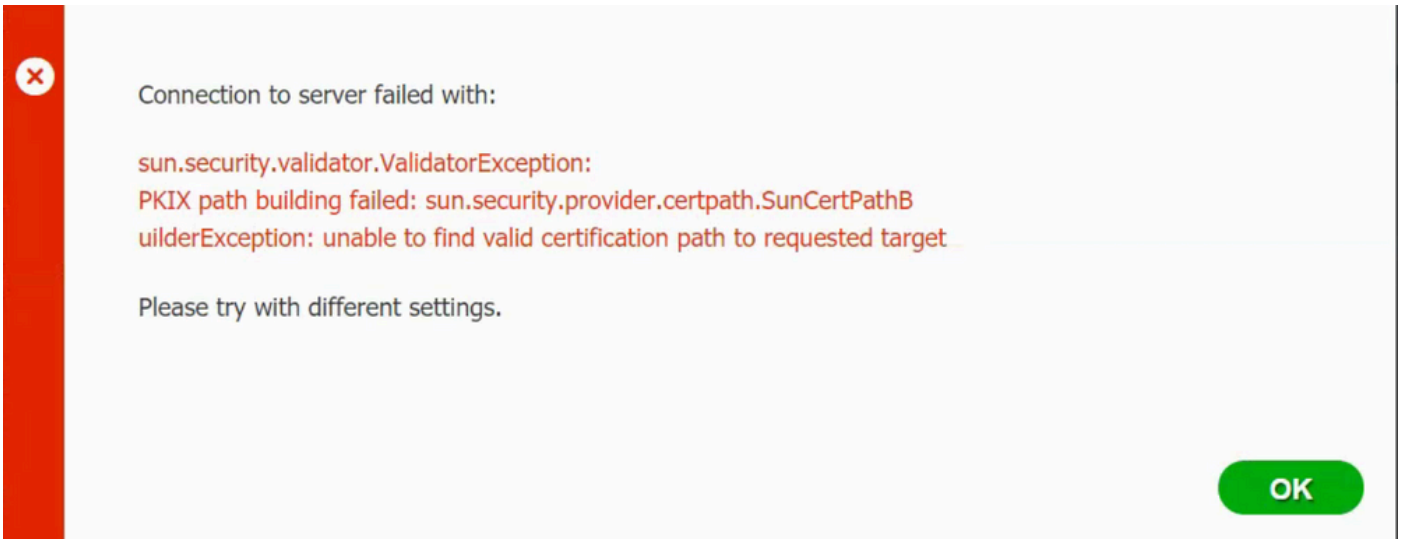


設定が完了すると、ステータスがenabledと表示されます。



確認とトラブルシューティング

sun.security.validator.ValidatorExceptionに基づく「Connection to the server failed」



ステップ 1：次のログを含むサポートバンドルをTRACEレベルで収集します。

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

ステップ 2：次 ise-psc.log のログを確認します。

- 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

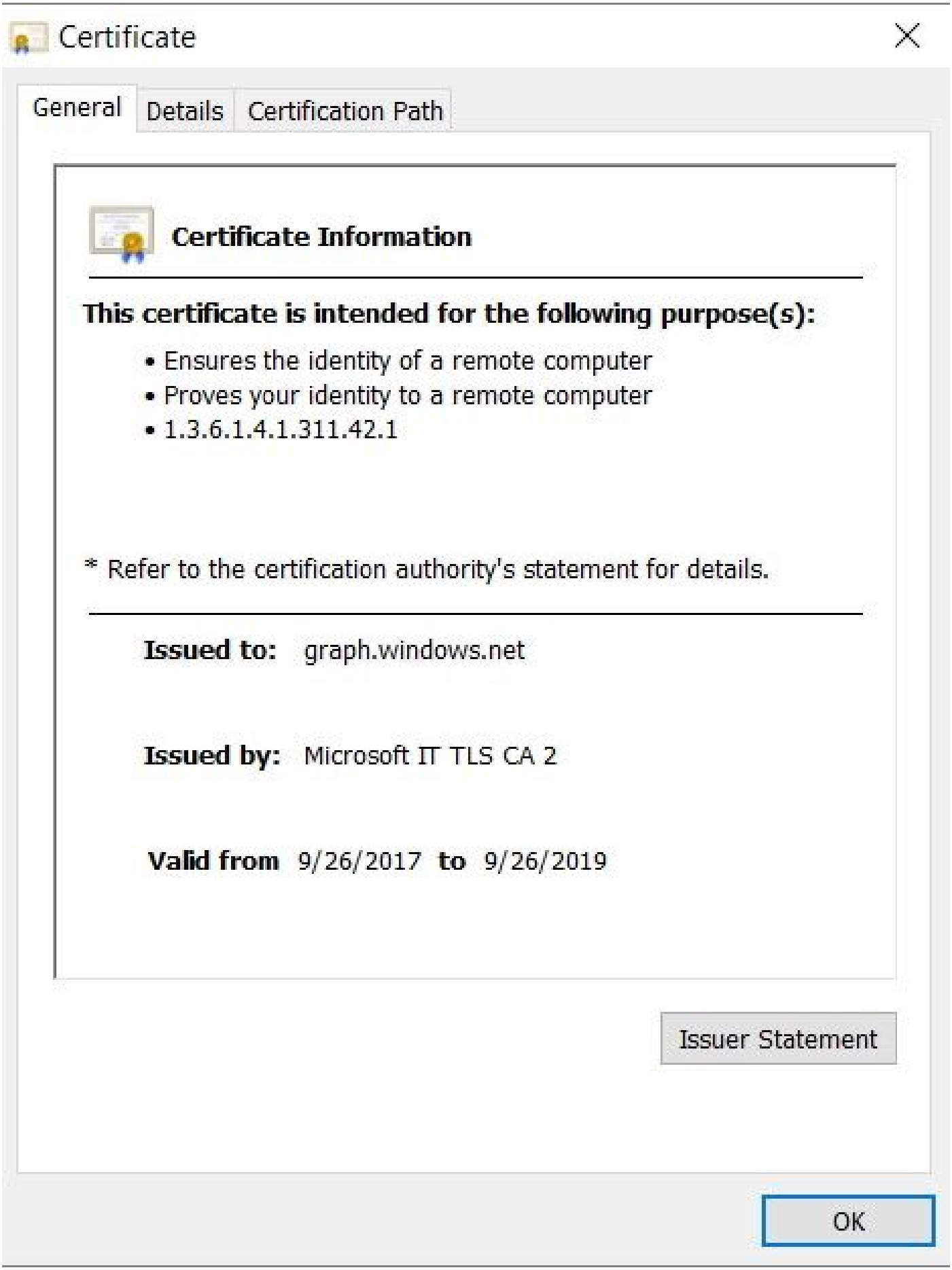
- 2016-10-17 12:45:52,794 ERROR [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- Unable to acquire access token from Azure

- 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

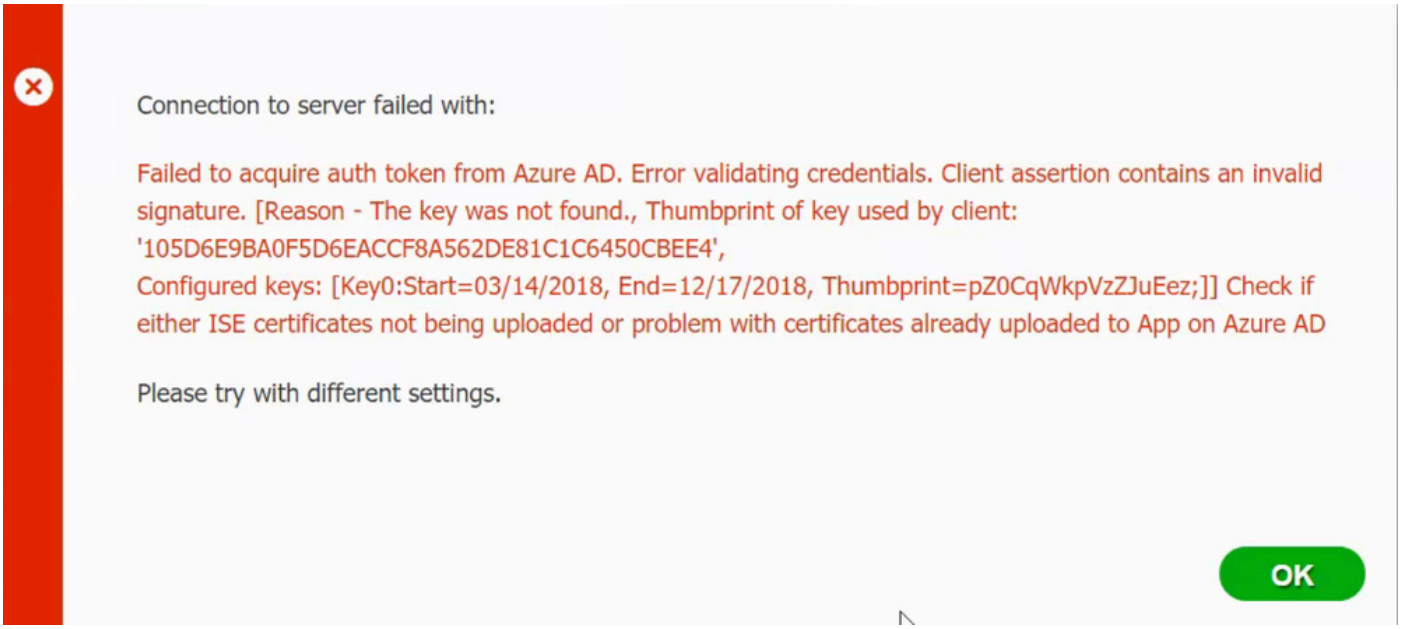
これは、このページに表示されている証graph.microsoft.com 明書をインポートする必要があることを示します。

ステップ 3：アイlockerコンをクリックし、証明書の詳細を確認します。



ステップ 4：これをBASE64形式のファイルに保存し、ISE信頼ストアにインポートします。完全な証明書チェーンをインポートしたことを確認します。その後、MDMサーバへの接続を再度テストします。

Azure ADから認証トークンを取得できませんでした



通常、このエラーは、マニフェストファJSON イルに誤ったISE証明書チェーンが含まれている場合に発生します。マニフェストファイルをAzureにアップロードする前に、少なくとも次の構成が存在するかどうかを確認してください：

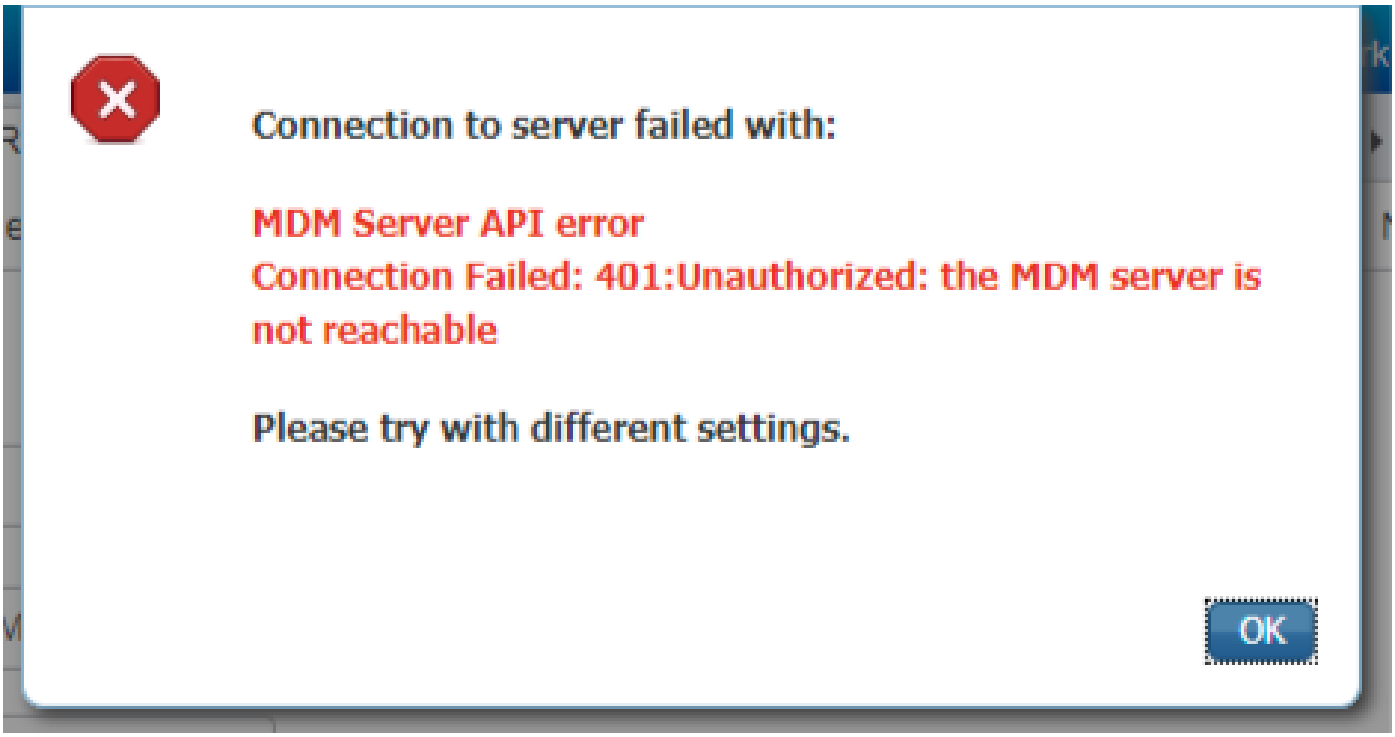
"keyCredentials": [{ “customKeyIdentifier“: “$base64Thumbprint_from_powerShell_for_PPAN”, “keyId“: “$keyid_from_above_PPAN“, "type": "Asym

前の例は、PANとSANがあるシナリオに基づいています。PowerShellからスクリプトを再度実行し、適切なBASE64値をインポートします。マニフェストファイルをアップロードしてください。エラーが発生することはありません。

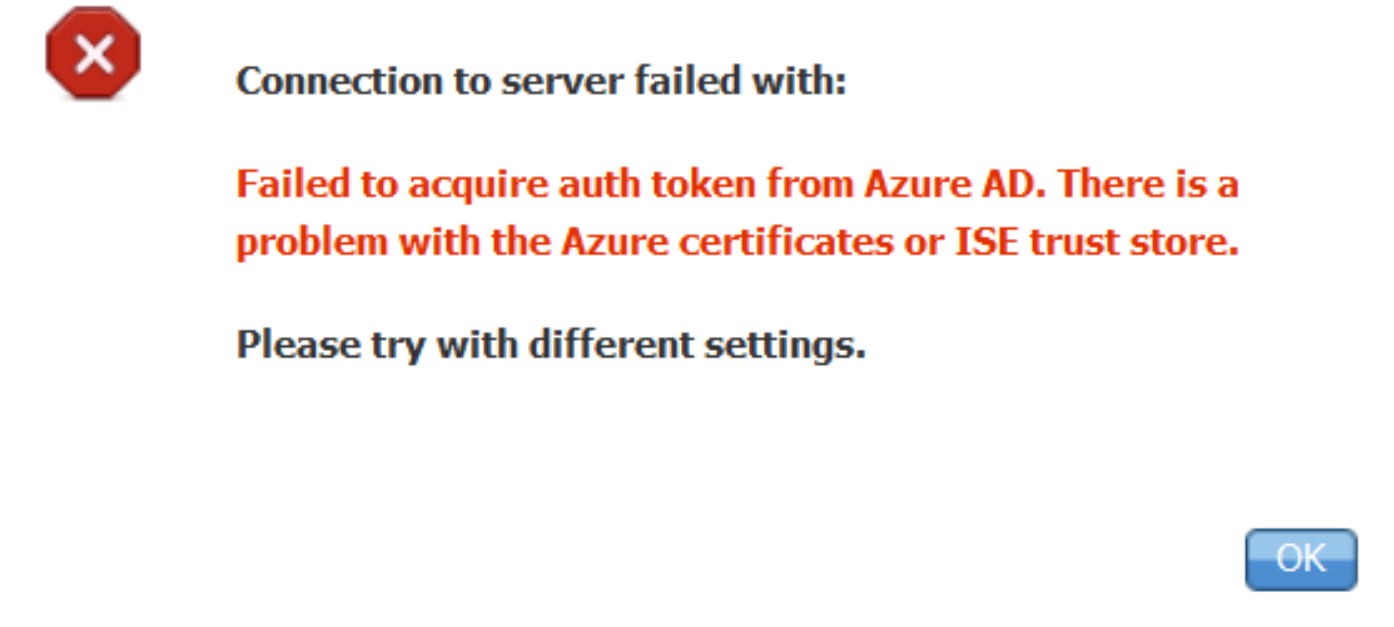
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import(“mycer.cer”) $bin = $cer.GetRawCertData() $base64Va

「設定」の項の手順で説明されているよう $base64Thumbprint, $base64Value に、 $keyid の値を必ず適用してください。

Azure ADから認証トークンを取得できませんでした



多くの場合、このエラーは、でAzureアプリに適切なアクセス許可が与えられていない場合に発生し portal.azure.comます。アプリに正しい属性が設定されていることを確認し、変更のたびにクリックGrant Permissionsすることを確認します。



このメッセージは、ISEがトークン発行URLへのアクセスを試行し、ISEが返さない証明書が返された場合に発生します。完全なCAチェーンがISE信頼ストアにあることを確認します。正しい証明書がISEの信頼できるストアにインストールされた後も問題が解決しない場合は、パケットキャプチャを実行し、何が送信されているかを確認するために接続をテストします。

関連情報

- クライアントクレデンシャルを使用したサービス間コール

    - Azure – 認証と承認

- Azure - Quickstart: Microsoft Identity Platformへのアプリケーションの登録
- Azure Active Directoryアプリマニフェスト
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。