

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

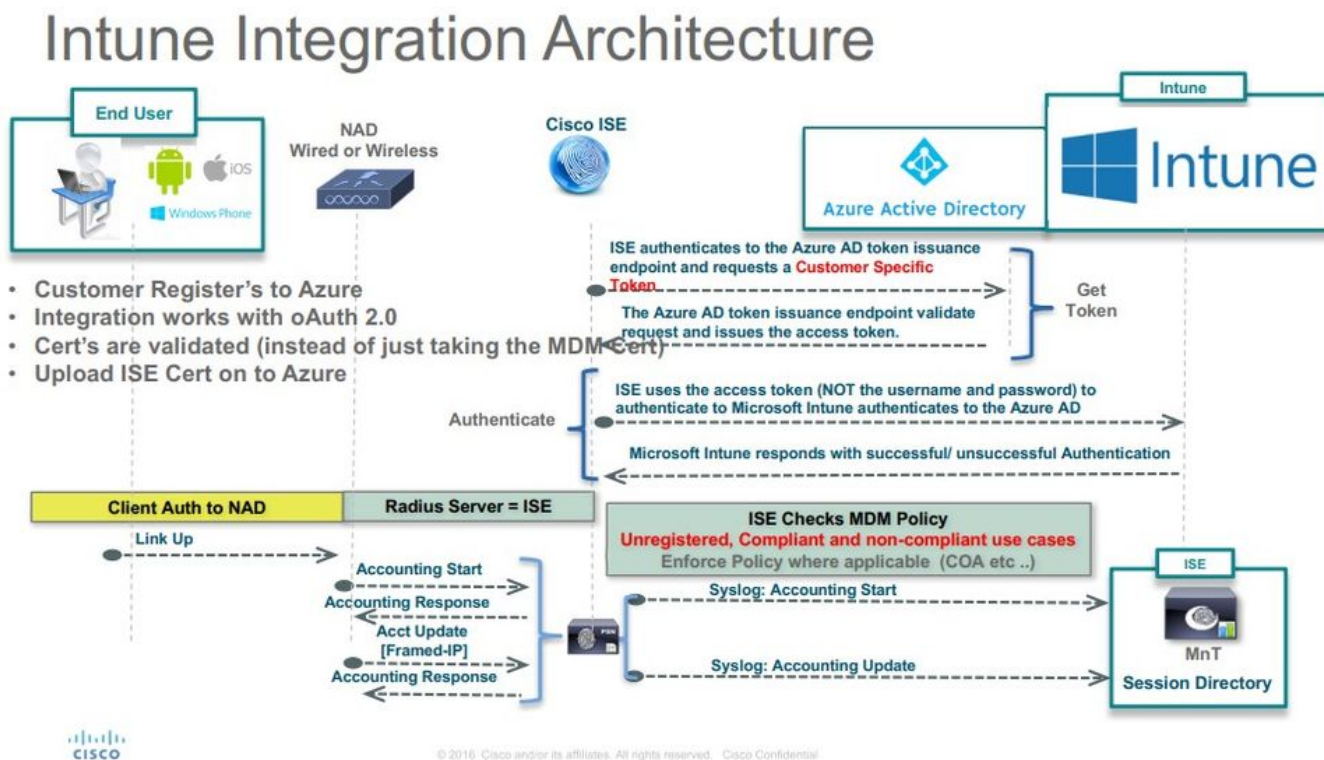
す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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ウインドウで、 Certification Path タブをクリックします。次に例を示します。

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

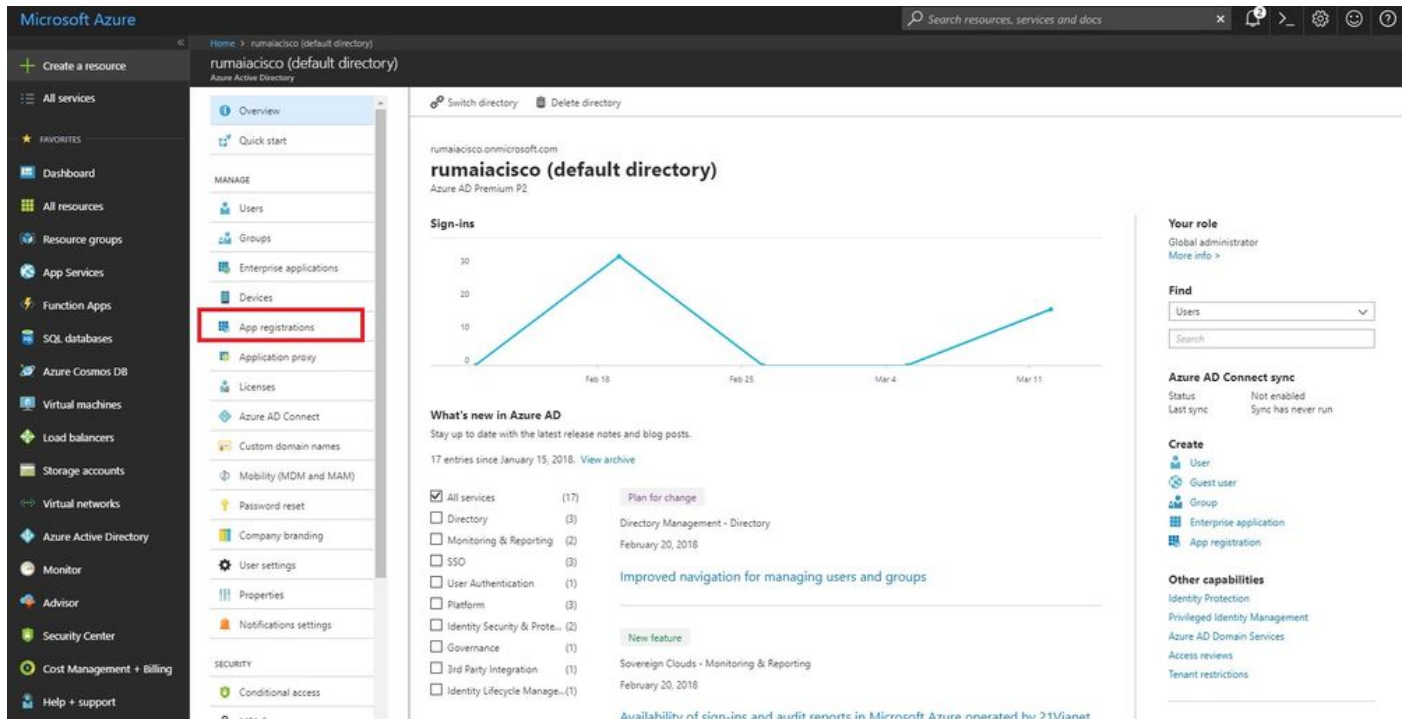
OK

きます。

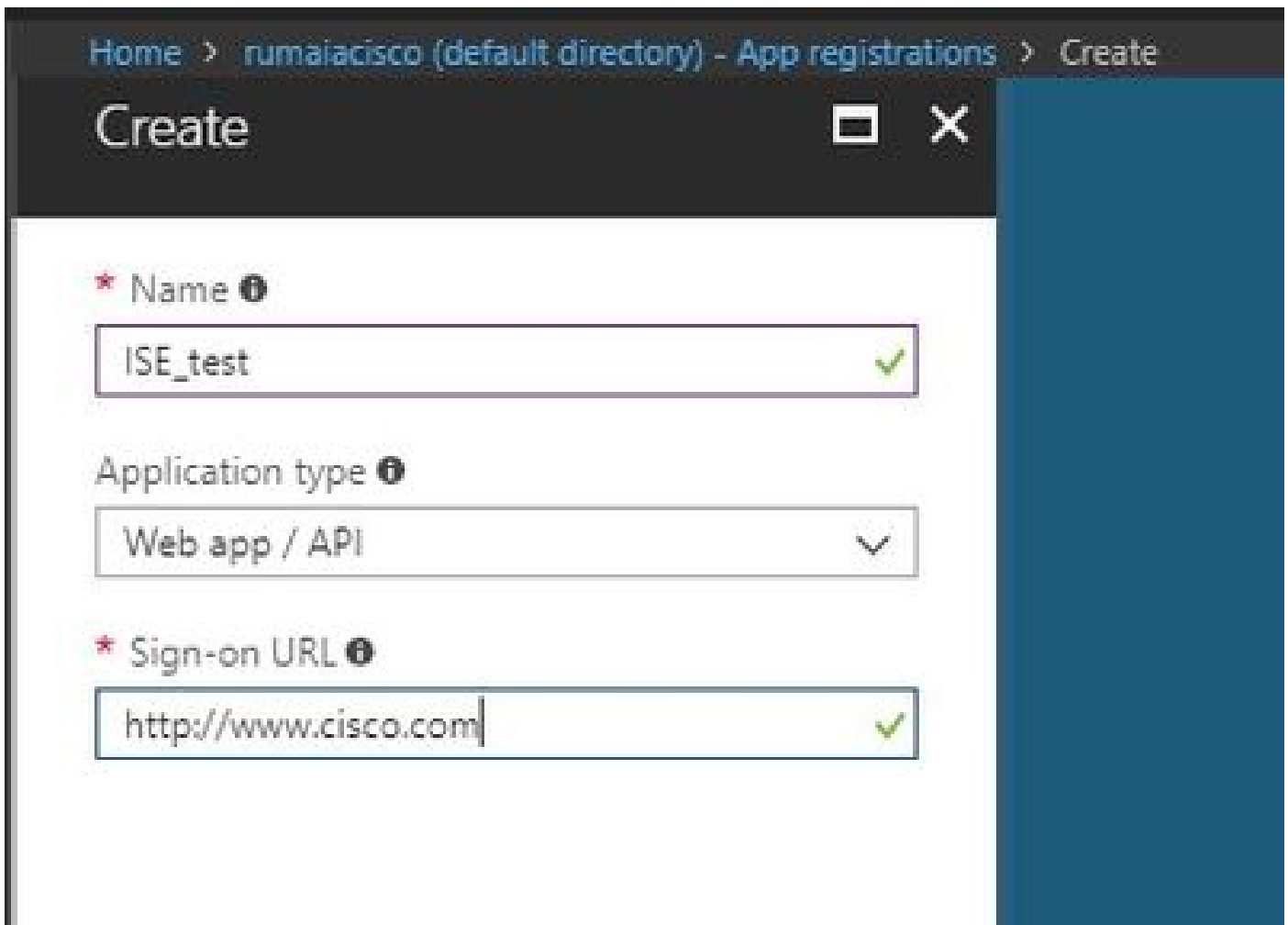
ステップ 5 : ISEで、保存したルート証明書に移動Administration > System > Certificates > Trusted Certificates, し、インポートします。証明書にわかりやすい名前 (Azure MDMなど) を付けます。中間CA証明書についても、この手順を繰り返します。

ISEをAzureポータルアプリケーションとして展開する

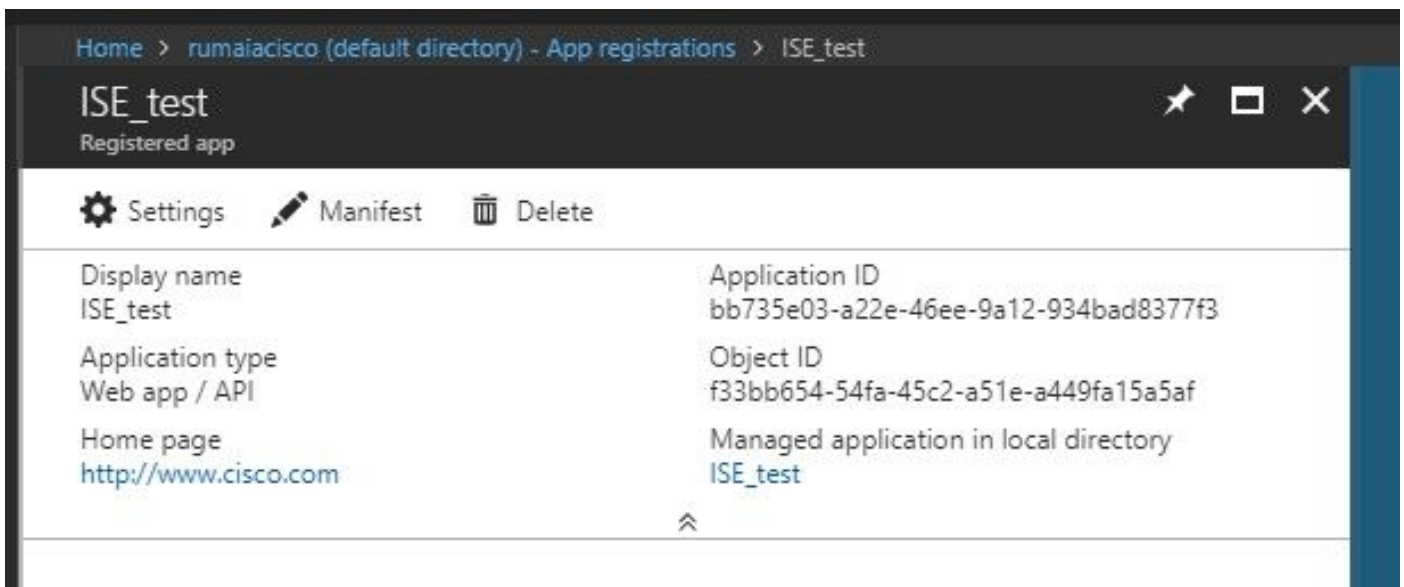
ステップ 1 : に移動し Azure Active Directory、 App registrations.



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をクリックします。



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。

+ 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

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。

Home > rumaiacisco (default directory) - App registrations > ISE > Edit manifest

ISE
Registered app

Settings Manifest Delete

Display name: ISE
Application ID: 86397a1c-b06d-4ca9-a086-0786eeadfabc
Application type: Object ID: 220a1c0e-e3d1-4eda-8739-e733019bd0fd
Web app / API: Managed application in local directory
Home page: http://www.cisco.com

Edit manifest

Save Discard Edit Upload Download

```

1 {
2   "appId": "86397a1c-b06d-4ca9-a086-0786eeadfabc",
3   "appRoles": [],
4   "availableToOtherTenants": false,
5   "displayName": "ISE",
6   "errorUrl": null,
7   "groupMembershipClaims": null,
8   "optionalClaims": null,
9   "acceptMappedClaims": null,

```

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。

Administration > Certificates > System Certificates

System Certificates ▲ For disaster recovery it is recommended to export certificate and private key pa

Cisco ISE Edit Generate Self Signed Certificate Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To
ise-1			
<input checked="" type="checkbox"/> 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

Client Machine

```

-----BEGIN CERTIFICATE-----
MIIE9jCCAT6gAwIBAgIQPzfz/HZnjSVKrlAgAYF/scjANBgkqhkiG9w0
MTUwNmYyVQDDCCBxJG0aM2pY2FOZSST2XJ2aWNLcyBmRmRwb2ludCST
LSBpc2UtaePw0xNjAzMDMxODQ4MTIwP0xODAzMDMxODQ4MTIwP0xODAz
BAMeG1s290xLarlbW8ubG9jYWVwggEiMA0GCSqGSIb3DQEBAQUAA4IBD
AcIBAQXfuoGvBgPqA9vqO/nwJ251t698oGBRlyN21ThkrStcpGf+Gw
fQ1M1QmHgqybsKEXLQzrEEqK+2/SK//D/R6kYab0F1gfc64t1RbHB
S/tQzLrLkMkbtP+IVWz20G2f0tq92eEMN2vB89Lk4100+rde3Hqf
28g9+r6582Lz/NOKQ3b2Pw1B8Xk1wKhYLAcVn1BqB0nEDN3tDe
MowSylDUz2f81INT8diV4cviFQBeNnEuz548M1uorXPvR32NtQie
xocl/EtqHn2vCe0DUJYVQ2ReIvAgMBAAGjggEYMIIBFDAsB9NVHRE
gRE2Ni01NS00MCOzMy0YMi0xdtAgBgkrBgEEAQkVAUEHQQBcHhHcm
ZmljYXRlR1R1bXBwYXRlR1R1R1R1R1R1R1R1R1R1R1R1R1R1R1R1R1
oToKMTA+MS0wKwYDQDDCCBxJG0aM2pY2FOZSST2XJ2aWNLcyBmRm
aWNLcyBmRmRwb2ludCSTLSBpc2UtaePw0xNjAzMDMxODQ4MTIwP0
0pm7w08BMA4GA1UdEwEB/wQEAwIF4DAGBgNVHSAkZm90Zm90Zm90Z
KwYBBQUHwIwDAYVR0TAgQ/BAIwADANBgkqhkiG9w0BAQoFARoCCG
341hLMDjrtm90rjQw0P+k+EqIvYI2Au5ACL2EgDedrcLp4MeP1q
Htuuj+AQX063KD2UhlLR7RAM5Pa6UZY50qa8a37HJGHP75Wa814a
jDeFb+6RVyjsBEMAmns+rWGV0NBjgLEJgJWv7h00Cq+oQmzLh
ukkyJfseW1LzEBSkNRis7jgt00jYQLiUe2pe3prvkQm2+/Jwcu
DYoRqteVqanJaNgS1fBC2ta5ayVrcTDeujkbD1lJG3zWVmt6N1
TnD7w3BfeThhuQWQy2a88/UKRhw/9c1Prc0P2+LshfFvKXjgmy
dQ+6qCANJFJcYusKJJD+xZrv3pgkVwDB14INOKtFv7vSpIDe1P
q/y+heUQTvKvYgF2QdMNC1ciEapp3B8eSvFKSE2PMSTAc24xMD
gL254nTJ0Fo6eZqf10Un690nk529BtFenJ+UT/goFUE8oJHP18Q
WgMgl18N8R1Lr6eZqf10Un690nk529BtFenJ+UT/goFUE8oJHP18
DjqtR8gV6xuvYozGktEfoMD2e-----
-----END CERTIFICATE-----

```

Delete this line

Delete this line

Things to do with the ISE System Cert

- Delete the -----BEGIN CERTIFICATE-----
- Delete the -----END CERTIFICATE-----
- All the text should be in single line ...

MIIE9jCCAT6gAwIBAgIQPzfz/HZnjSVKrlAgAYF/scjANBgkqhkiG9w0

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。

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

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。

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

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 | "identifierUri": [
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": "AsymmetricX509Cert" }
```

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が。

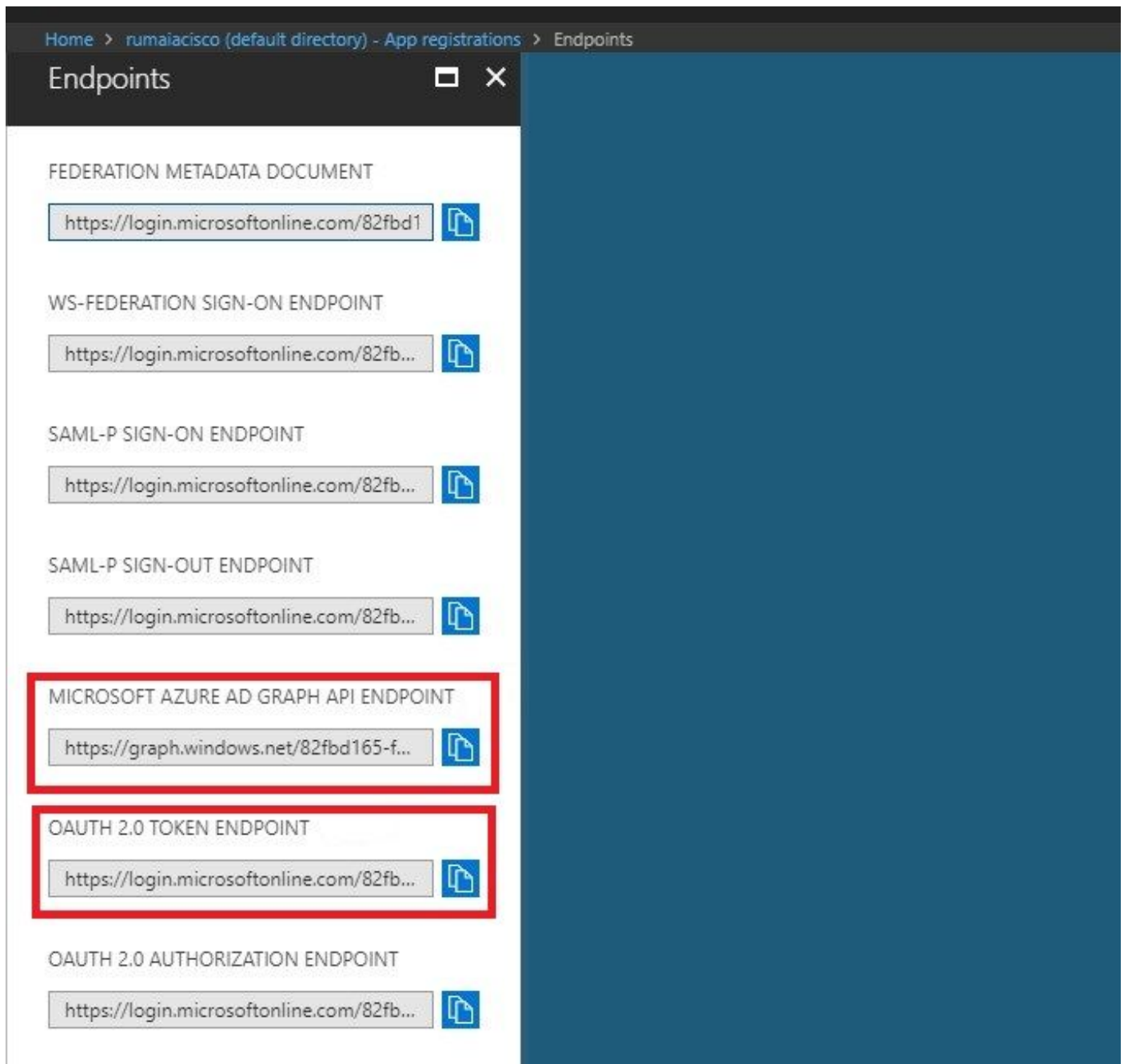
```

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   },

```

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 value フィールドが 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」

Name *

Server Type ⓘ

Authentication Type ⓘ

Auto Discovery ⓘ

Auto Discovery URL * ⓘ

Client ID *

Token Issuing URL * ⓘ

Token Audience *

Description

Polling Interval * (minutes) ⓘ

Status

設定が完了すると、ステータスがenabledと表示されます。

MDM Servers

<input type="checkbox"/>	Name	Status	Service Provider	MDM Server	Server Type	Description
<input type="checkbox"/>	Intune	■ Enabled	Microsoft	fef.ms03.manage.microsoft.com	Mobile Device Manager ↕	

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」



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

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 -::::- 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

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。



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>
```

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。

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

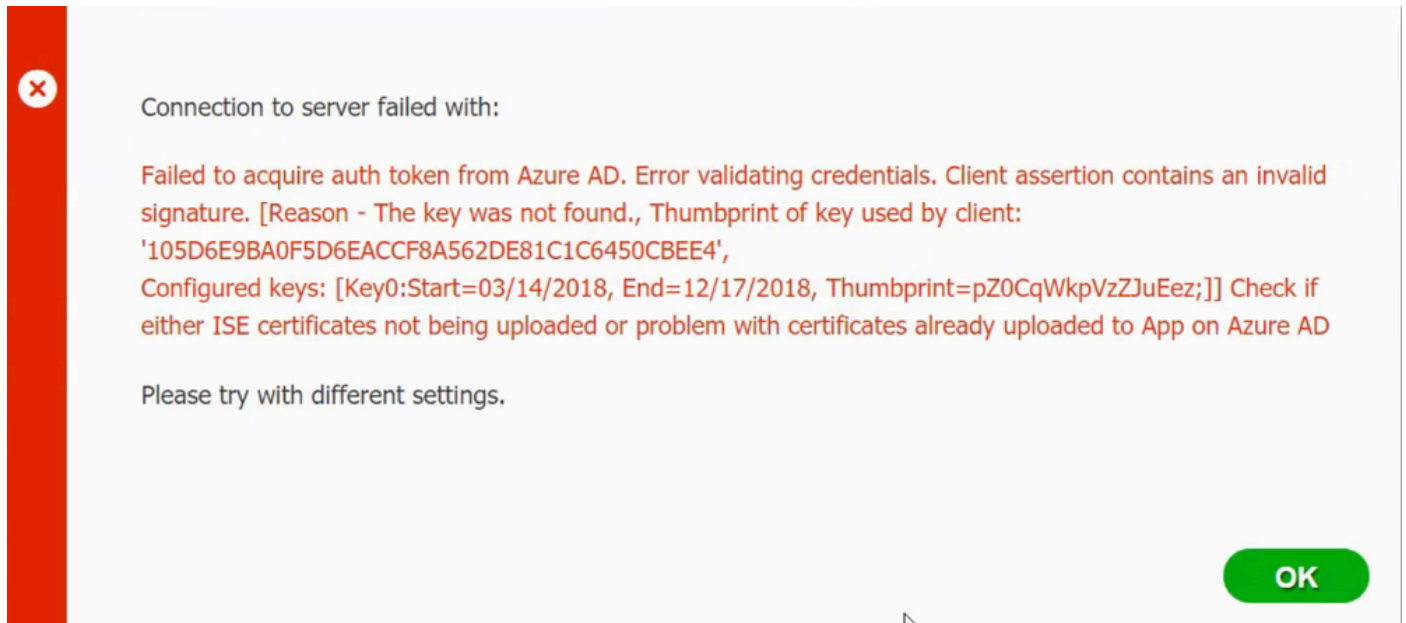
Valid from 9/26/2017 **to** 9/26/2019

Issuer Statement

OK

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、マニフェストファイルJSON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：

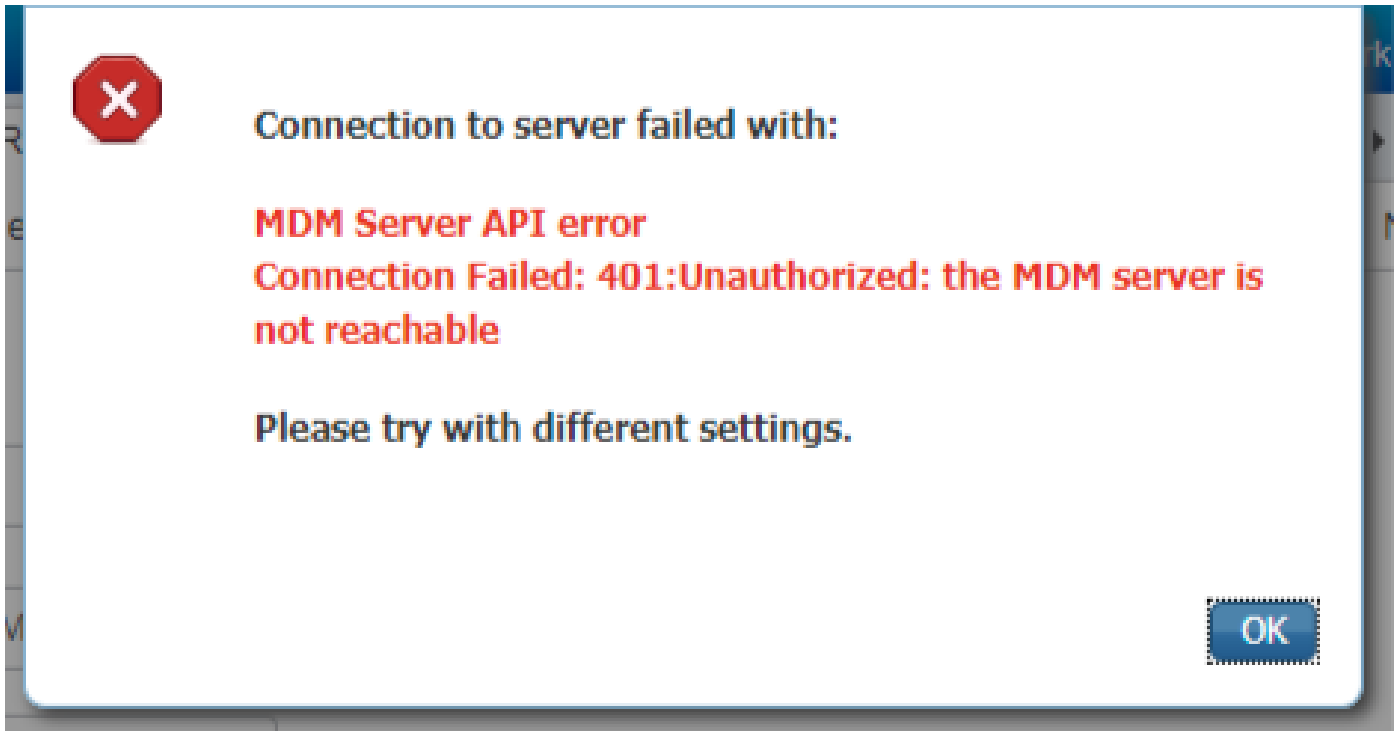
```
"keyCredentials": [ { "customKeyIdentifier": "$base64Thumbprint_from_powerShell_for_PPAN", "keyId": "$keyid_from_above_PPAN", "type": "Asym"
```

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。

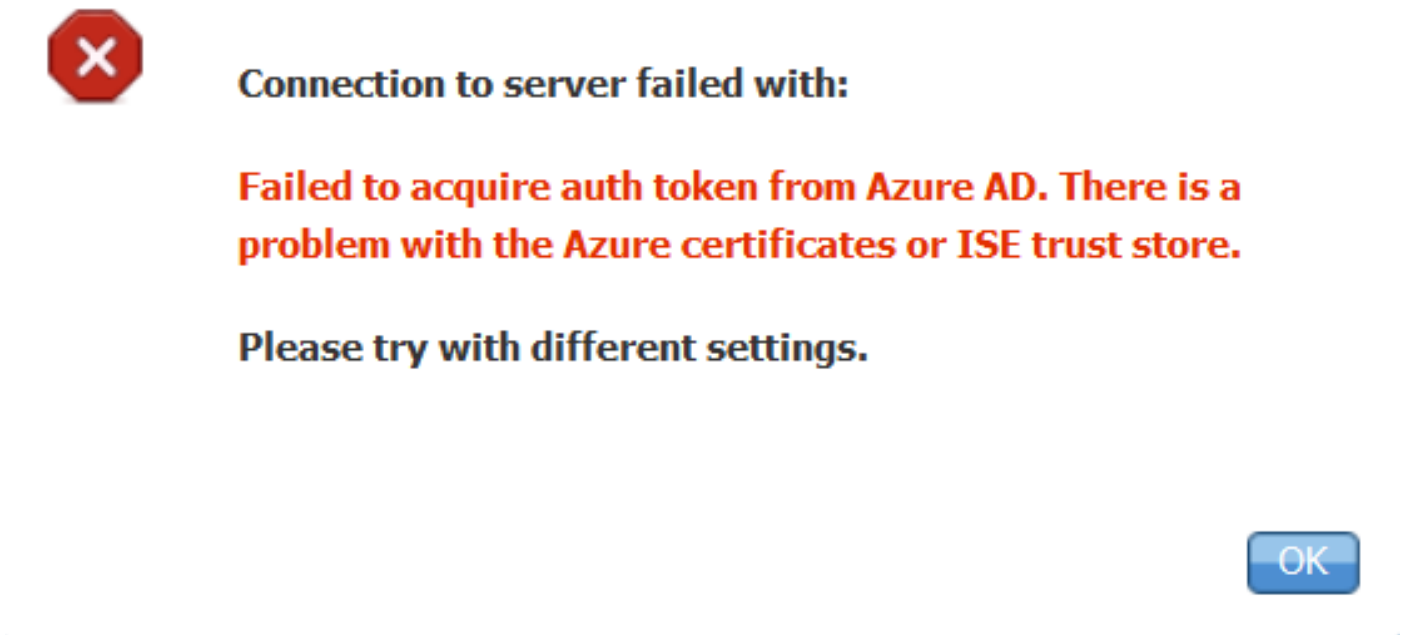
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $cer.Import("mycer.cer") $bin = $cer.GetRawCertData() $base64V
```

「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。