

Azure Active Directoryを使用したISE 3.0 REST IDの構成

内容

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[高レベルフローの概要](#)

[Azure ADの統合の構成](#)

[統合のためのISEの設定](#)

[さまざまな使用例のISEポリシーの例](#)

[確認](#)

[トラブルシューティング](#)

[REST認証サービスに関する問題](#)

[REST ID認証に関する問題](#)

[ログファイルの操作](#)

はじめに

このドキュメントでは、リソース所有者のパスワードクレデンシャルを使用してREST Identityサービスを通じて実装されるCisco ISE 3.0とAzure ADの統合について説明します。

背景説明

このドキュメントでは、リソース所有者パスワードクレデンシャル(ROPC)を使用して、Representational State Transfer(REST)ID(ID)サービスを介して実装されたMicrosoft(MS)Azure Active Directory(AD)とのIdentity Services Engine(ISE)3.0の統合を設定およびトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE
- MS Azure AD

- ROPCプロトコルの実装と制限事項の理解、[リンク](#)

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。

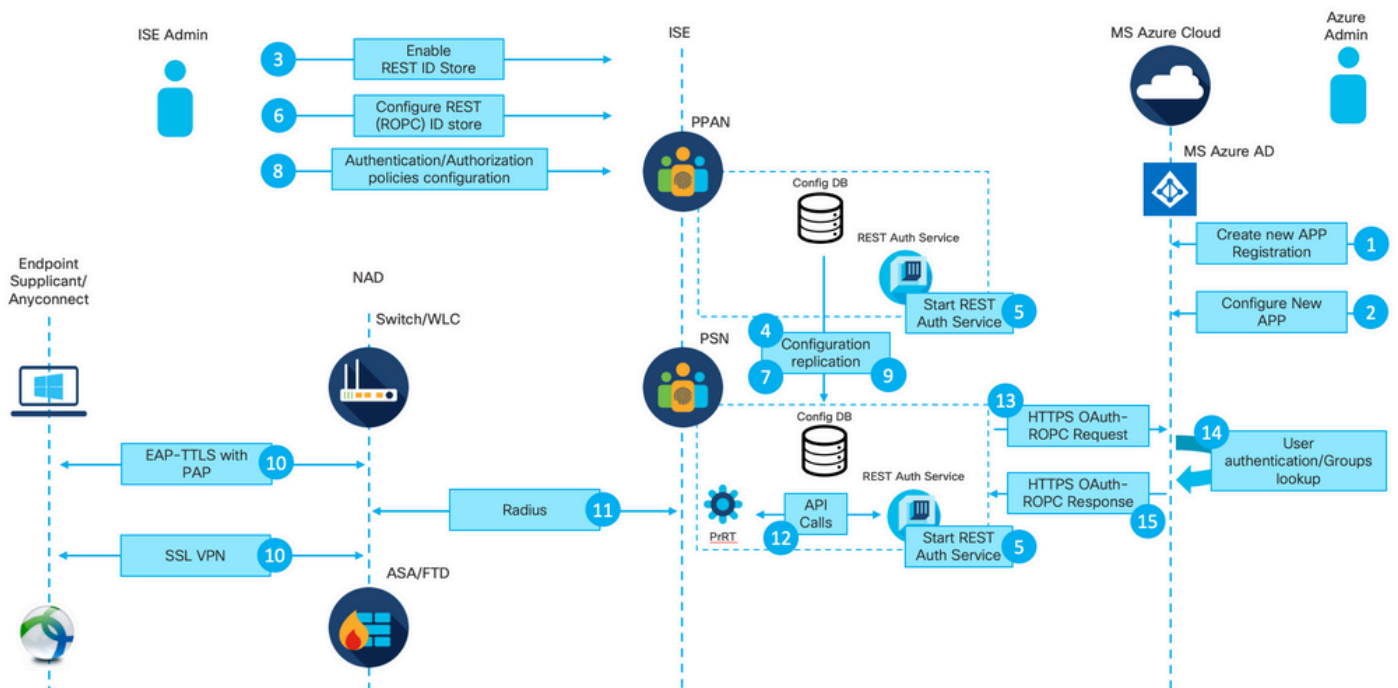
- Cisco ISE バージョン 3.0
- MS Azure AD
- WS-C3850-24P (ソフトウェア16.9.2)
- 9.10を使用したASA(1)
- Windows 10.0.18363

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。

設定

ISE REST ID機能は、ISE 3.0(REST Auth Service)で導入された新しいサービスに基づいています。このサービスは、ユーザー認証とグループ取得を実行するために、オープン認証(OAuth) ROPC交換を介してAzure ADと通信します。REST認証サービスはデフォルトで無効になっており、管理者が有効にすると、導入環境内のすべてのISEノードで実行されます。ユーザー認証時にクラウドとのREST Auth Service通信が発生するため、パスの遅延によって認証/認可フローに追加の遅延が発生します。この遅延はISEの制御外であり、REST認証の実装は、他のISEサービスへの影響を避けるために慎重に計画およびテストする必要があります。

高レベルフローの概要



1. Azureクラウド管理者が新しいアプリケーション (アプリ) 登録を作成します。このアプリの詳細は、後でAzure ADとの接続を確立するためにISEで使用されます。

2. Azureクラウド管理者は、次の項目でアプリを構成する必要があります：

- クライアントシークレットの作成
- ROPCの有効化
- グループ要求の追加
- アプリケーションプログラミングインターフェイス(API)権限の定義

3. ISE管理者がREST認証サービスを有効にします。他のアクションを実行する前に行う必要があります。

4.変更は構成データベースに書き込まれ、ISE環境全体でレプリケートされます。

5. REST認証サービスがすべてのノードで開始されます。

6. ISE管理者が、手順2の詳細を使用してREST IDストアを設定します。

7.変更は設定データベースに書き込まれ、ISE環境全体で複製されます。

8. ISE管理者が新しいIDストアシーケンスを作成するか、既存のIDストアシーケンスを変更して、認証/認可ポリシーを設定します。

9.変更は構成データベースに書き込まれ、ISE環境全体でレプリケートされます。

10.エンドポイントが認証を開始します。ROPCプロトコルの仕様に従って、暗号化されたHTTP接続を介してMicrosoft IDプラットフォームにクリアテキストでユーザパスワードを提供する必要があります。この事実により、現在ISEでサポートされている使用可能な認証オプションは次のものだけです。

- 内部方式としてパスワード認証プロトコル(PAP)を使用するExtensible Authentication Protocol-Tunneled Transport Layer Security(EAP-TTLS)

- PAPを使用したAnyConnect SSL VPN認証

11. Radius上のISEポリシーサービスノード(PSN)との交換。

12.プロセスランタイム(PrRT)は、内部APIを介して、ユーザの詳細(ユーザ名/パスワード)を含む要求をREST IDサービスに送信します。

13. REST IDサービスは、HyperText Transfer Protocol Secure (HTTPS)を介してOAuth ROPC要求をAzure ADに送信します。

14. Azure ADはユーザー認証を実行し、ユーザーグループを取得します。

15.認証/認可の結果がISEに返されます。

ポイント15の後、認証結果とフェッチされたグループがPrRTに返されます。これには、ポリシー評価フローが含まれ、最終的な認証/認可結果が割り当てられます。認可プロファイルからの属性を使用したアクセス承認(ACL)またはネットワークアクセスデバイス(NAD)に返されるアクセス拒否。

Azure ADの統合の構成

1.図に示すように、AppRegistration Serviceを見つけます。

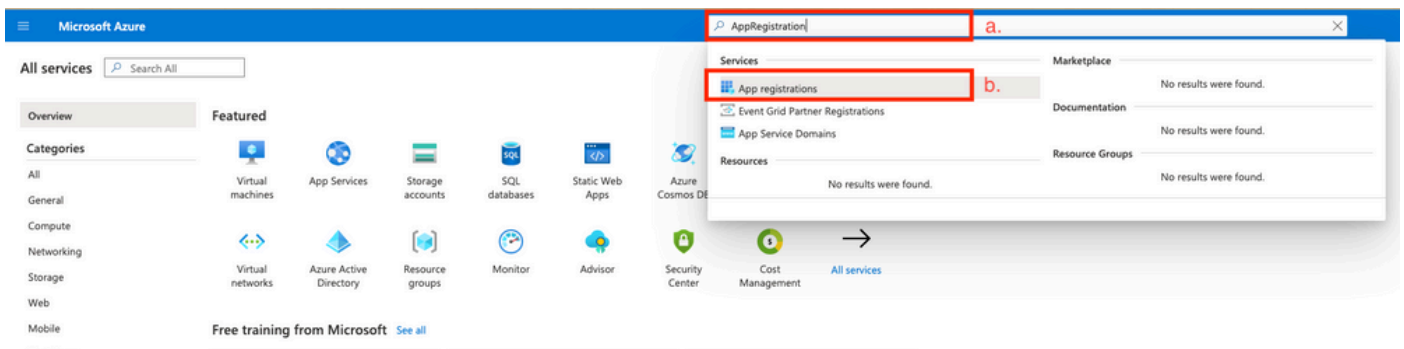


図 2 :


a.グローバル検索バーに「AppRegistration」と入力します。

b. App registration serviceをクリックします。

2.新しいアプリ登録を作成します。

All services >

App registrations

 New registration



Endpoints



Troubleshooting



Download (Preview)



Got feedback?



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will con

All applications

Owned applications



Start typing a name or Application ID to filter these results

図 3 :

3.新しいアプリを登録します。

Register an application

* Name

The user-facing display name for this application (this can be changed later).

 ✓

a.

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (DEMO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

b.

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

c.

```
ISE PROCESS NAME STATE PROCESS ID
-----
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled

REST Auth Service running 63052

SSE Connector disabled
```

2. 認証時にREST IDストアが使用されていることを確認します (詳細な認証レポートの「手順」セクションを確認してください) 。

15013 Selected Identity Source - Azure_AD

25103 Perform plain text password authentication in external REST ID store server - Azure_AD a.

25100 Connecting to external REST ID store server - Azure_AD b.

25101 Successfully connected to external REST ID store server - Azure_AD (🕒 Step latency=1660 ms) c.

25104 Plain text password authentication in external REST ID store server succeeded - Azure_AD d.

25107 REST ID store server respond with groups - Azure_AD e.

25110 User groups inserted to session cache - Azure_AD f.

22037 Authentication Passed

a. PSNは、選択されたREST IDストアを使用して平文認証を開始します。

b. Azureクラウドとの接続が確立されました。

c. 実際の認証ステップ - ここで示す遅延値に注意してください。Azure Cloudによるすべての認証で大幅な遅延が発生し、問題が生じた場合は、他のISEフローに影響が生じ、その結果、ISE展開全体が不安定になります。

d. 認証の成功の確認。

e. 回答として提示したグループデータの確認

f. ユーザーグループデータが入力されたセッションコンテキスト。ISEセッション管理プロセスの詳細については、この記事の[リンク](#)を参照してください。

3. Expect Authentication/Authorizationポリシーが選択されていることを確認します (詳細な認証レポートのこの調査の概要セクションに関して) 。

Overview

Event 5200 Authentication succeeded

Username bob

Endpoint Id ED:37:E1:08:57:15 ⊕

Endpoint Profile

Authentication Policy SPRT-Policy-Set >> Azure-AD

Authorization Policy SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

図 30.

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

REST認証サービスに関する問題

REST認証サービスに関する問題をトラブルシューティングするには、まずADE.logファイルを確認する必要があります。サポートバンドルの場所：/support/adeos/ade

REST認証サービスの検索キーワードはROPC-controlです。

次の例は、REST認証サービスの開始方法を示しています。

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

サービスの開始に失敗した場合や、予期せず停止した場合は、問題のあるタイムフレームを ADE.log で確認することから始めるのが常に理にかなっています。

REST ID 認証に関する問題

REST ID ストアを使用する際に認証に失敗した場合は、必ず詳細な認証レポートから開始する必要があります。[その他の属性] 領域に、Azure クラウドによって返されたエラーを含むセクション RestAuthErrorMsg が表示されます。

```
RestAuthErrorMsg      Error Key - invalid_client | Error Description -
                        AADSTS7000218: The request body must contain the
                        following parameter: 'client_assertion' or 'client_secret'. Trace
                        ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID:
                        519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp:
                        2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI
                        - https://login.microsoftonline.com/error?code=7000218
```

図 31.

ログファイルの操作

ISE 3.0 では、REST ID 機能の制御された導入により、そのデバッグはデフォルトで有効になっています。すべての REST ID 関連のログは、CLI で表示できる ROPC ファイルに保存されます。

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

パッチがインストールされた ISE 3.0 で、ファイル名が ropc.log ではなく rest-id-store.log であることに注意してください。前述の検索例は、フォルダ名が変更されていないため機能します。

または、これらのファイルを ISE サポートバンドルから抽出することもできます。

次に、さまざまな動作シナリオと非動作シナリオを示すいくつかのログ例を示します。

1. Azure Graph が ISE ノードによって信頼されていない場合の証明書エラーです。このエラーは、グループが REST ID ストア設定でロードされない場合に発生する可能性があります。

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
```

```
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appl
```

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

この問題は、Microsoft Graph API証明書がISEによって信頼されていないことを示しています。ISE 3.0.0.458では、信頼できるストアにDigiCertグローバルルートG2 CAがインストールされていません。これは、不具合に記載されています

- Cisco Bug ID [CSCcv80297](https://tools.cisco.com/bugcenter/bug/?bugID=CSCcv80297) : この問題に対処するには、DigiCert Global Root G2 CAをISE信頼ストアにインストールし、シスコサービスに対して信頼できるものとしてマークする必要があります。

証明書は、<https://www.digicert.com/kb/digicert-root-certificates.htm>からダウンロードできます。

2.アプリケーションシークレットが正しくありません。

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client s
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentity
```

3.アプリIDが正しくありません。

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4.ユーザーが見つかりません。

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
```

```
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5.ユーザーパスワードの期限切れ – 通常、Azure管理者によって定義されたパスワードをOffice365へのログイン時に変更する必要があるため、新しく作成されたユーザーに対して発生する可能性があります。

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCEFlow.authenticateUser(AzureROPCEFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCEFlow.doEntireFlow(AzureROPCEFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6. APIアクセス許可が正しくないため、グループを読み込めません。

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Stat
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7. ROPCがAzure側で許可されていない場合、認証が失敗します。

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCCResponseErrorException: {"error":"invalid_client","error_des
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCEFlow.authenticateUser(AzureROPCEFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCEFlow.doEntireFlow(AzureROPCEFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
```

```
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8.ユーザーがAzure側のどのグループにも属していないため、認証に失敗しました。

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9.ユーザ認証とグループ取得に成功します。

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filte
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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。