Azure ADを使用したSAML SSO経由のISE 3.1管理者ログインフローの設定

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](#)

- [ご利用条件](#)
- [SAML](#)
- [SAMLアサーション](#)

[高レベルフロー図](#)

[Azure ADとのSAML SSO統合の構成](#)

- [ステップ 1：ISEでのSAML IDプロバイダーの設定](#)
- [ステップ 2：Azure AD IdP設定の構成](#)
- [ステップ 3：Azure Active DirectoryからISEへのメタデータのアップロード](#)
- [ステップ 4：ISEでのSAMLグループの設定](#)
- [（オプション）手順5:RBACポリシーの設定](#)

[確認](#)

[トラブルシュート](#)

- [一般的な問題](#)
- [ISEのトラブルシューティング](#)
  - [SAMLログインとグループ要求名の不一致を含むログ](#)

はじめに

このドキュメントでは、Azure Active Directory(AD)などの外部IDプロバイダーとCisco ISE 3.1 SAML SSO統合を設定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。

1. Cisco ISE 3.1
2. SAML SSOの導入
3. Azure AD

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。

1. Cisco ISE 3.1
2. Azure AD

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

ご利用条件

Identity Provider (IdP):ユーザーIDとアクセス特権を検証し、要求されたリソース（サービスプロバイダー）に対してアサートする機関のAzure AD。

サービスプロバイダー(SP):ユーザがアクセスするホストされたリソースまたはサービス（ISEアプリケーションサーバ）。

SAML

Security Assertion Markup Language(SAML)は、SPに認証クレデンシャルを渡すためにIdPを許可するオープンスタンダードです。

SAMLトランザクションは、IDプロバイダーとサービスプロバイダー間の標準化された通信にExtensible Markup Language(XML)を使用します。

SAMLは、サービスを使用するためのユーザIDの認証と認可の間のリンクです。

SAMLアサーション

SAMLアサーションは、アイデンティティプロバイダーがサービスプロバイダーに送信するXMLドキュメントであり、ユーザ認証が含まれています。

SAMLアサーションには、認証、属性、および許可決定という3つの異なるタイプがあります。

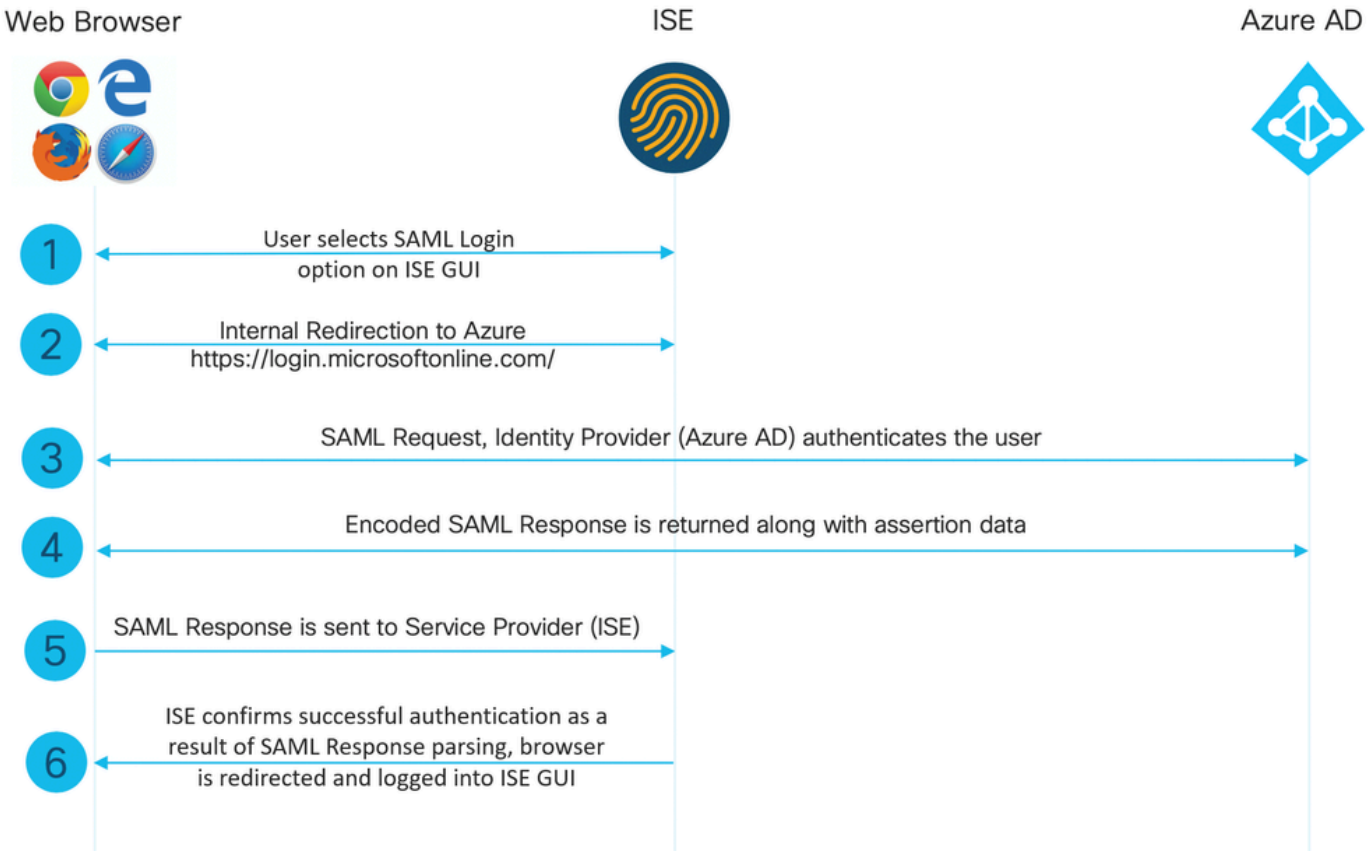
- 認証アサーションは、ユーザのIDを証明し、ユーザがログインした時間と使用した認証方法（例としてKerberos、2要素）を提供します
- アトリビューションアサーションは、ユーザに関する情報を提供する特定のデータであるSAML属性をサービスプロバイダーに渡します。
- ユーザーがサービスを使用する権限を持っているか、パスワードの失敗またはサービスに対する権限の欠如が原因で識別プロバイダが要求を拒否したかを示す、承認の決定アサーションが宣言されます。

高レベルフロー図

SAMLは、IDプロバイダーであるAzure ADとサービスプロバイダーであるISEの間でユーザー、ログイン、属性に関する情報を渡すことで機能します。

各ユーザがIDプロバイダーを使用してシングルサインオン(SSO)に一度ログインすると、ユーザがそれらのサービスにアクセスしようとしたときに、Azure ADプロバイダーからSAML属性がISEに渡されます。

ISEがAzure ADに許可と認証を要求する例を次の図に示します。



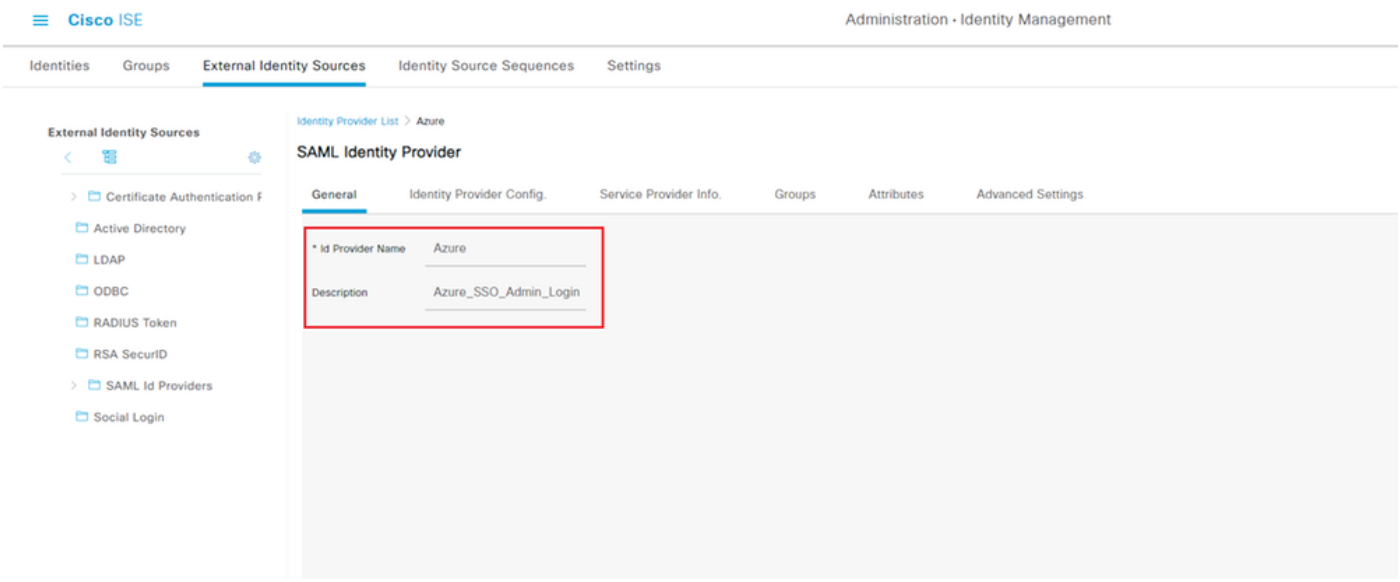
Azure ADとのSAML SSO統合の構成

ステップ 1：ISEでのSAML IDプロバイダーの設定

1. Azure ADを外部SAML IDソースとして構成します：

ISEで、Administration > Identity Management > External Identity Sources > SAML Id Providersの順に移動し、Addボタンをクリックします。

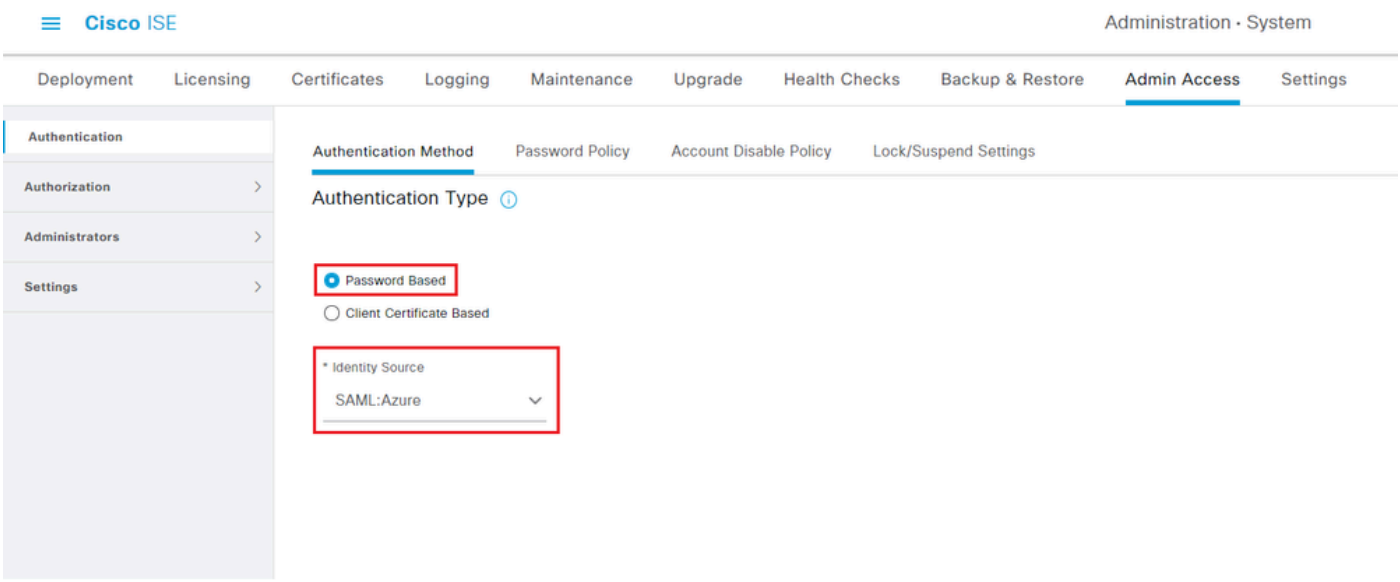
Id Provider Nameを入力し、Submitをクリックして保存します。Idプロバイダー名は、図に示すようにISEに対してのみ意味を持ちます。



2. ISE認証方式を設定します。

Administration >System > Admin Access > Authentication > Authentication Methodの順に選択し、Password Basedオプションボタンを選択します。

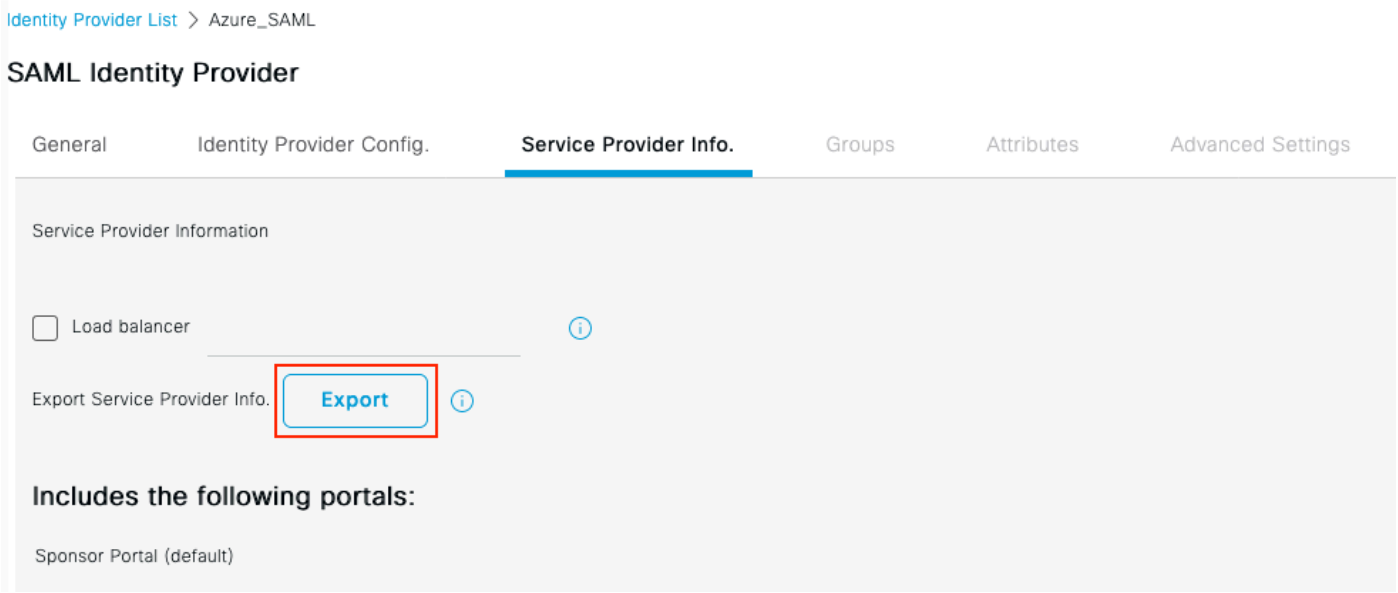
図に示すように、Identity Sourceドロップダウンリストから、先に作成した必要なIDプロバイダー名を選択します。



3. サービスプロバイダ情報のエクスポート：

Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]の順に移動します。

タブをService Provider Infoに切り替え、図に示すようにExportボタンをクリックします。



.xmlファイルをダウンロードして保存します。Location URLとentityIDの値をメモします。

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasi
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSig
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMS0xOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzFO38ciQqlm0sqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe79OR5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV8OmN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
2O6Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4HOvdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wkOBLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMcOaS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
```

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

</md:SPSSODescriptor>
</md:EntityDescriptor>
```

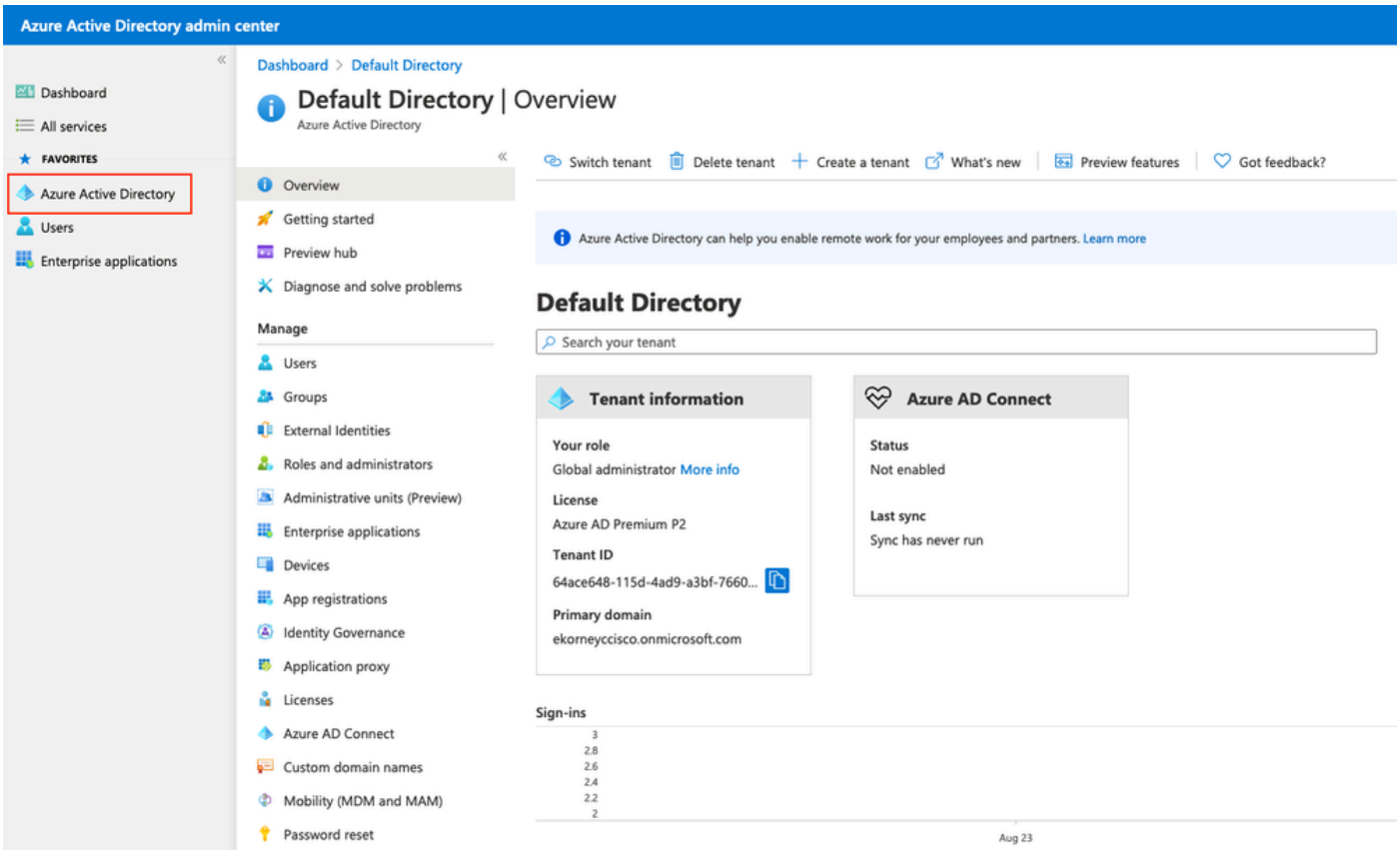
XMLファイルの対象の属性：

- entityID="http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2"
- AssertionConsumerService Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action"
- AssertionConsumerService Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action"

ステップ 2：Azure AD IdP設定の構成

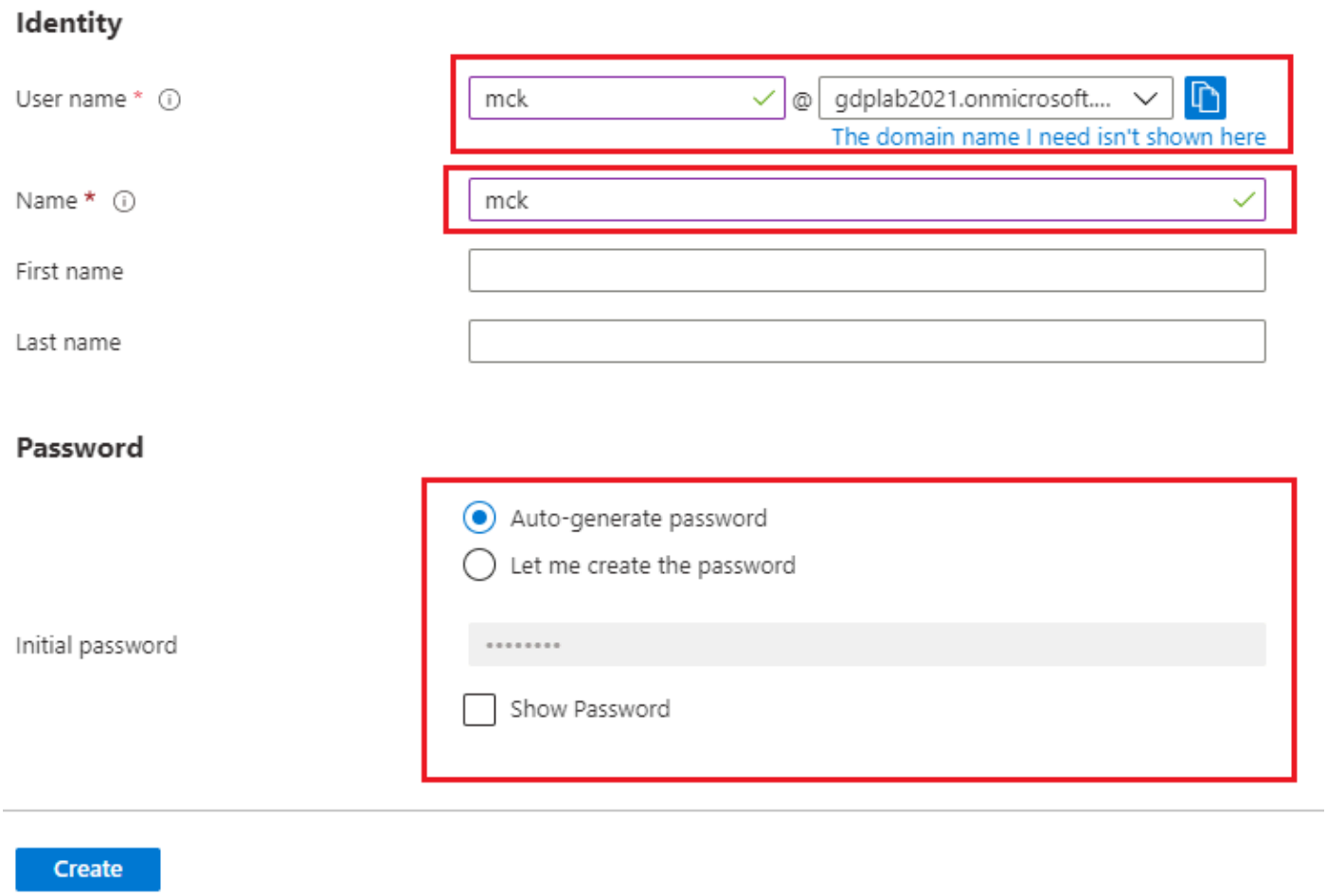
1. Azure ADユーザーを作成します：

Azure Active Directory管理センターダッシュボードにログインし、図に示すようにADを選択します。



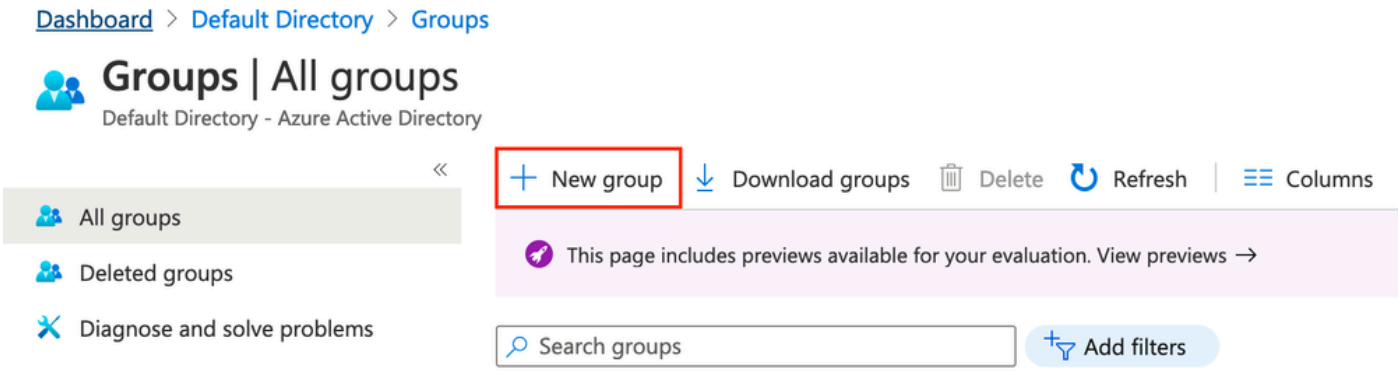
Usersを選択してNew Userをクリックし、必要に応じてUser name, Name およびInitial Password

を設定します。図に示すように、Createをクリックします。

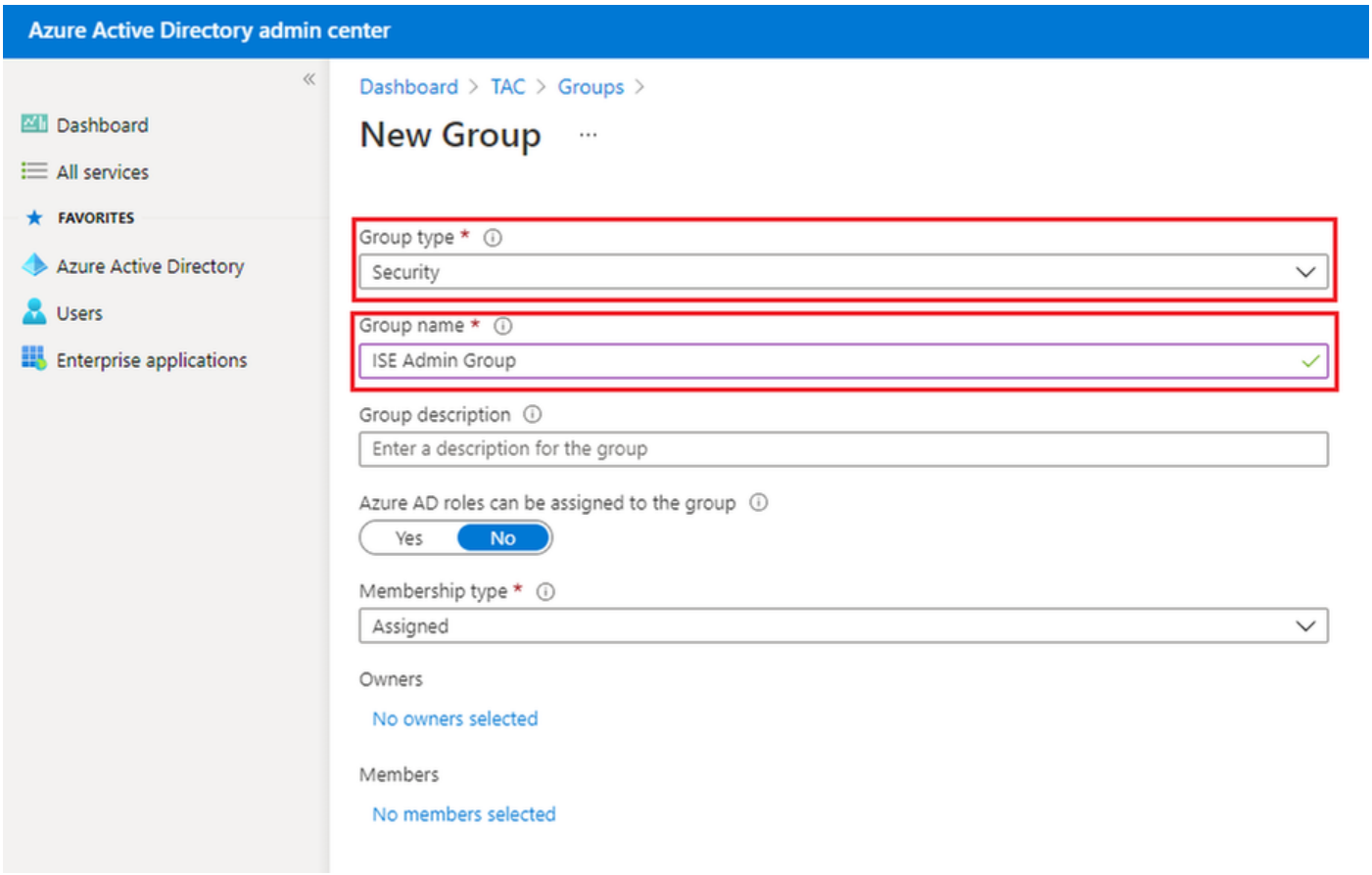


2. Azure ADグループを作成します：

Groupsを選択します。New Groupをクリックします。

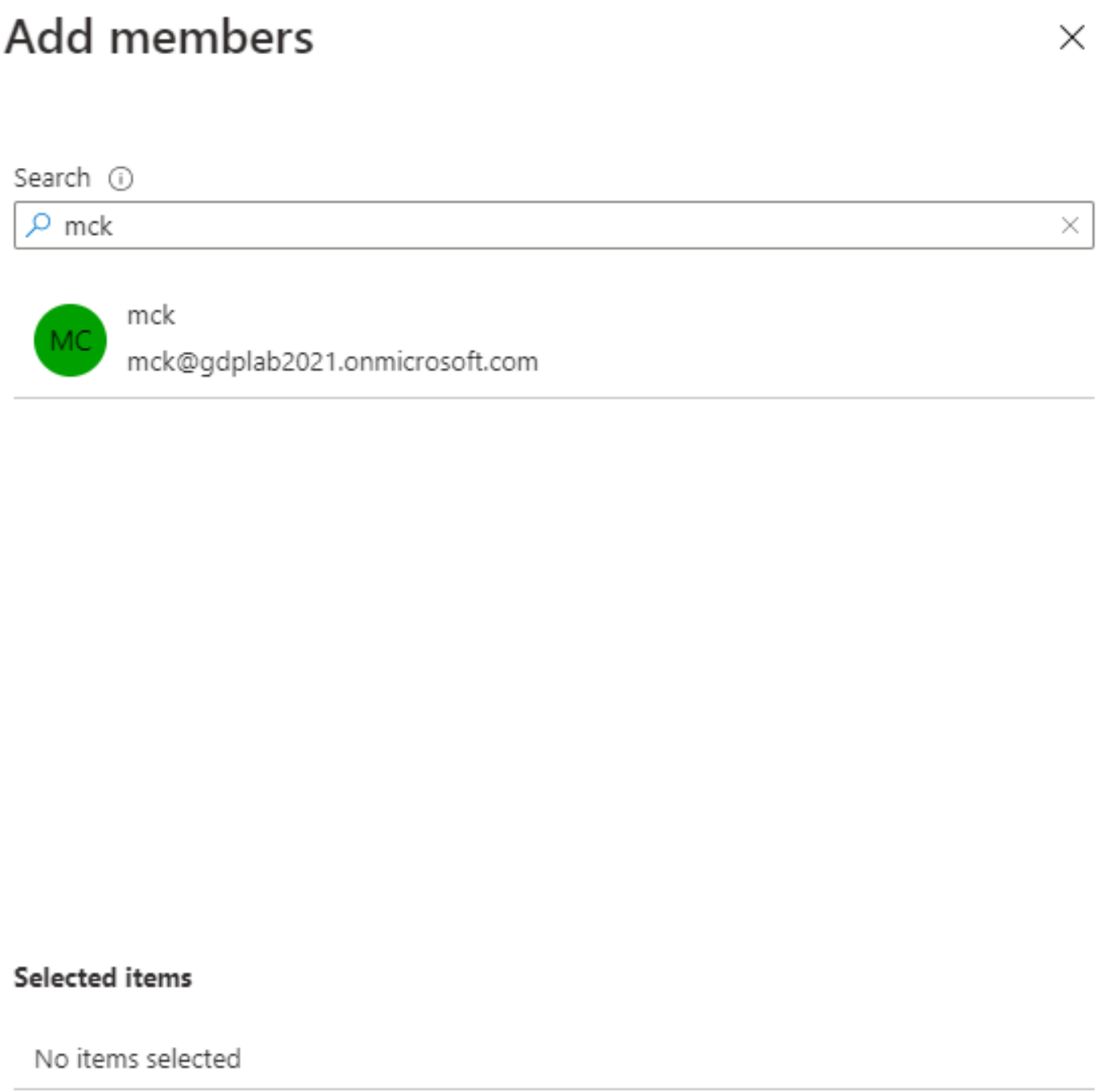


グループタイプはSecurityのままにしておきます。図に示すように、グループ名を設定します。

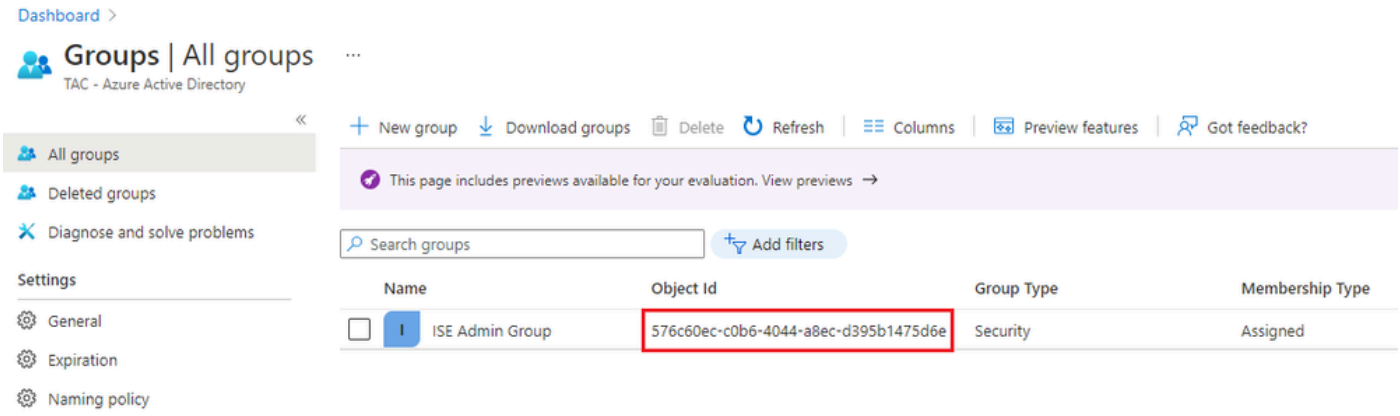


3. Azure ADユーザーをグループに割り当てます：

No members selectedをクリックします。ユーザを選択し、Selectをクリックします。Createをクリックし、ユーザが割り当てられたグループを作成します。

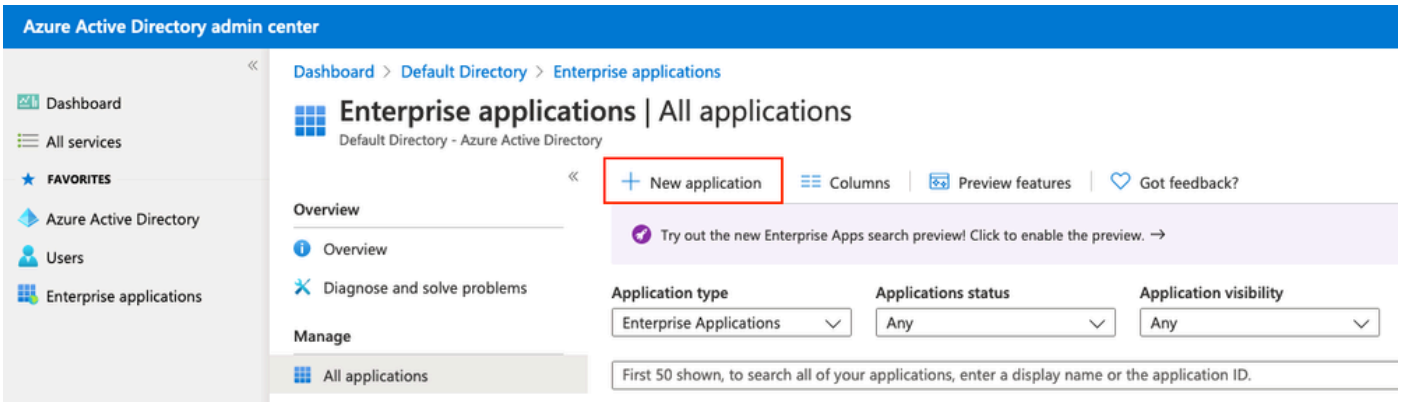


ISE管理グループの576c60ec-c0b6-4044-a8ec-d395b1475d6eというグループオブジェクトIDをメモします（次の図を参照）。

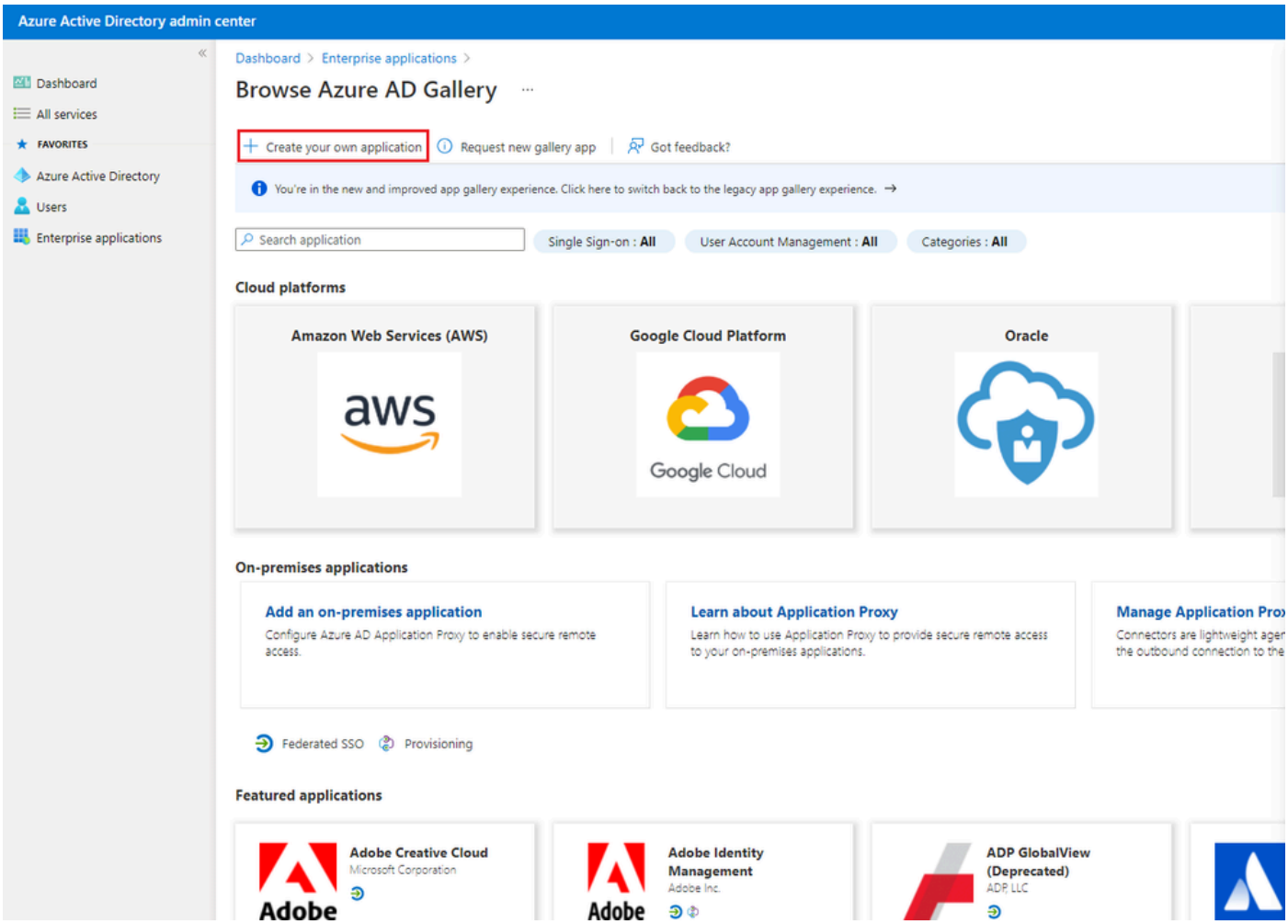


4. Azure AD Enterpriseアプリケーションを作成します：

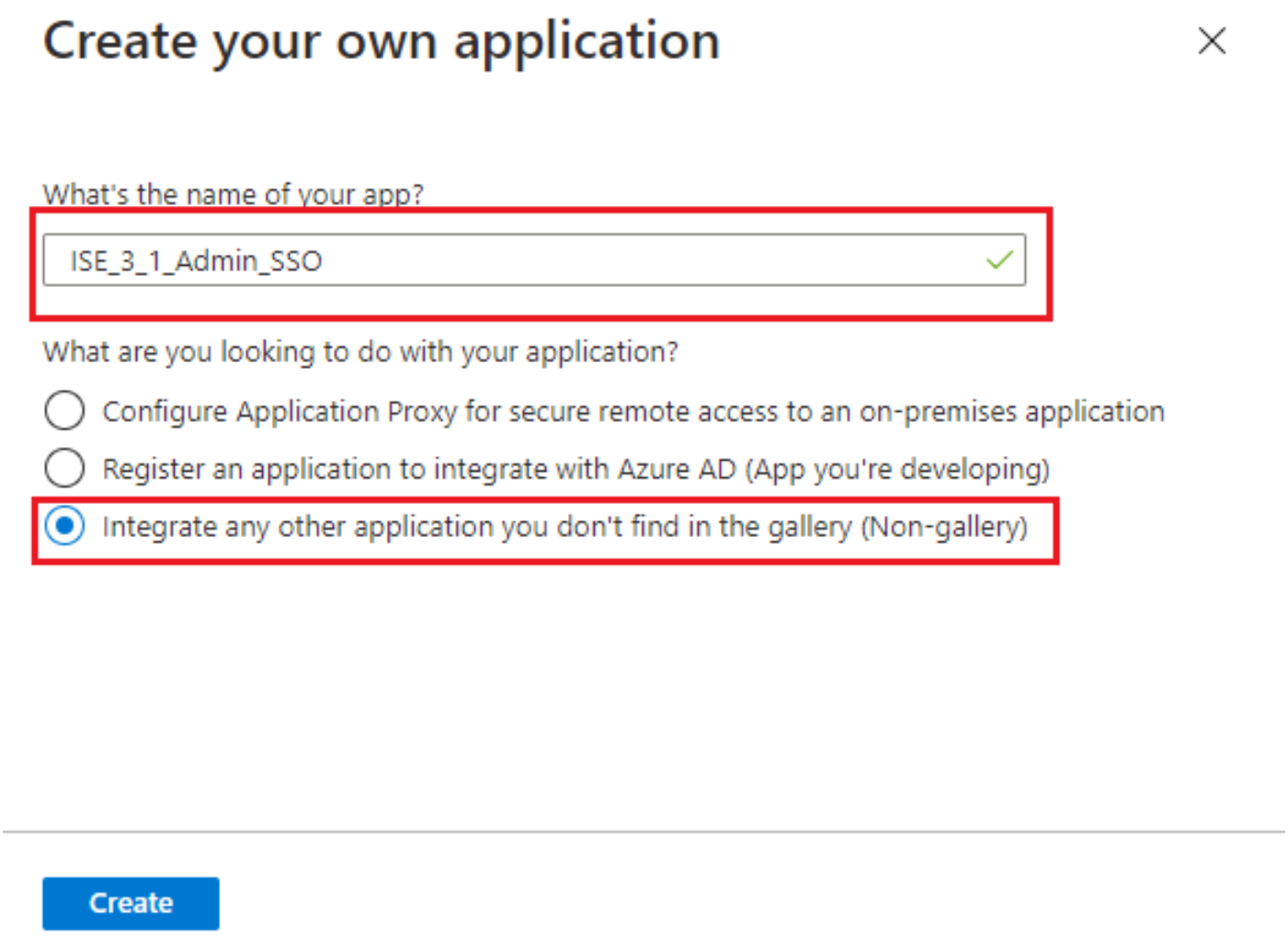
ADでEnterprise Applicationsを選択し、New applicationをクリックします。



Create your own applicationを選択します。

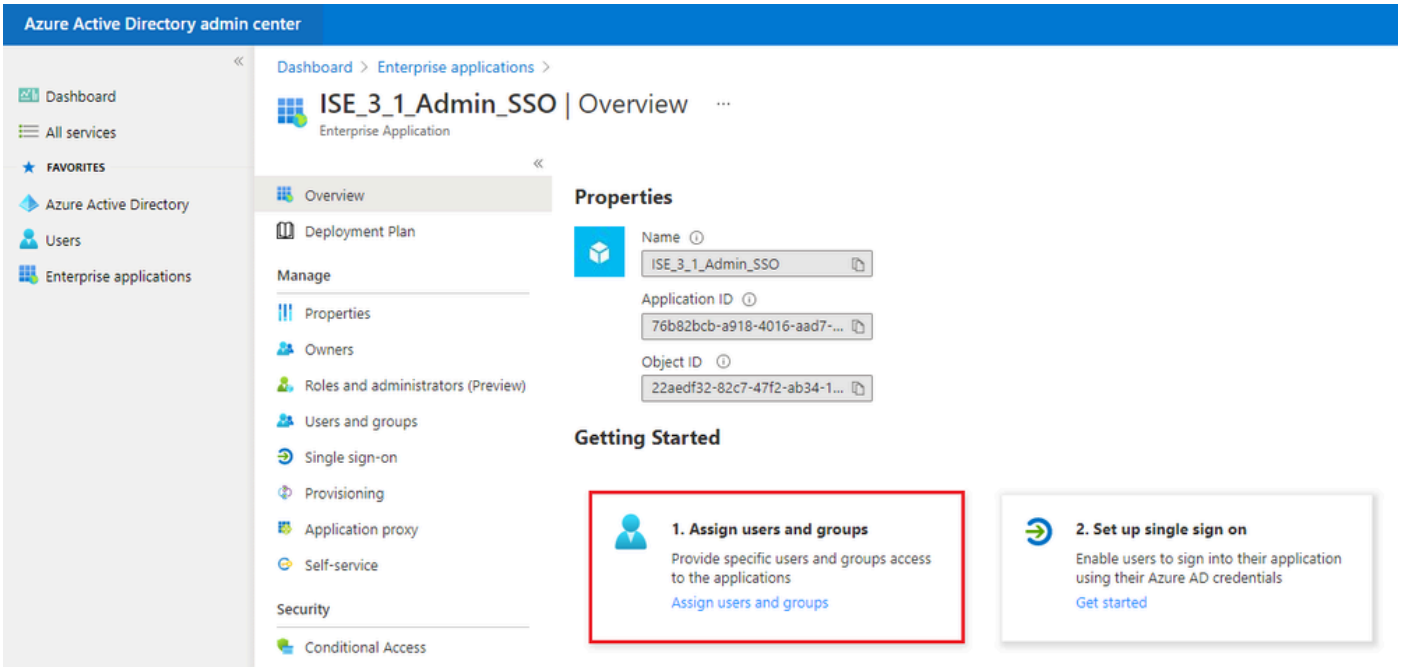


アプリケーションの名前を入力して、Integrate any other application you do not find in the gallery (Non-gallery)オプションボタンを選択し、図に示すようにCreateボタンをクリックします。

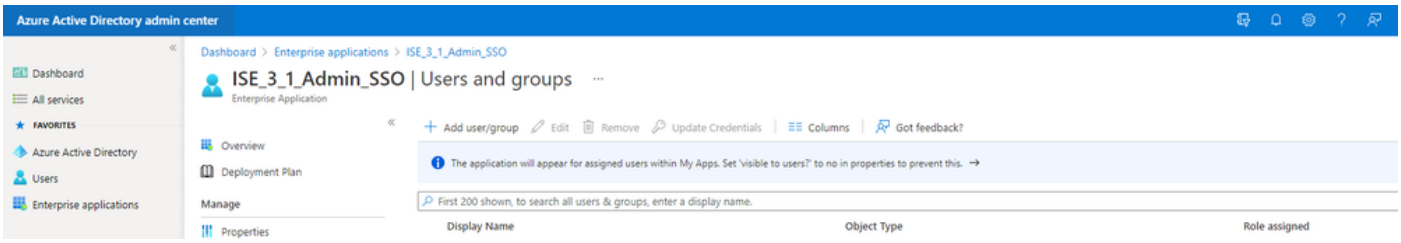


5. アプリケーションにグループを追加します。

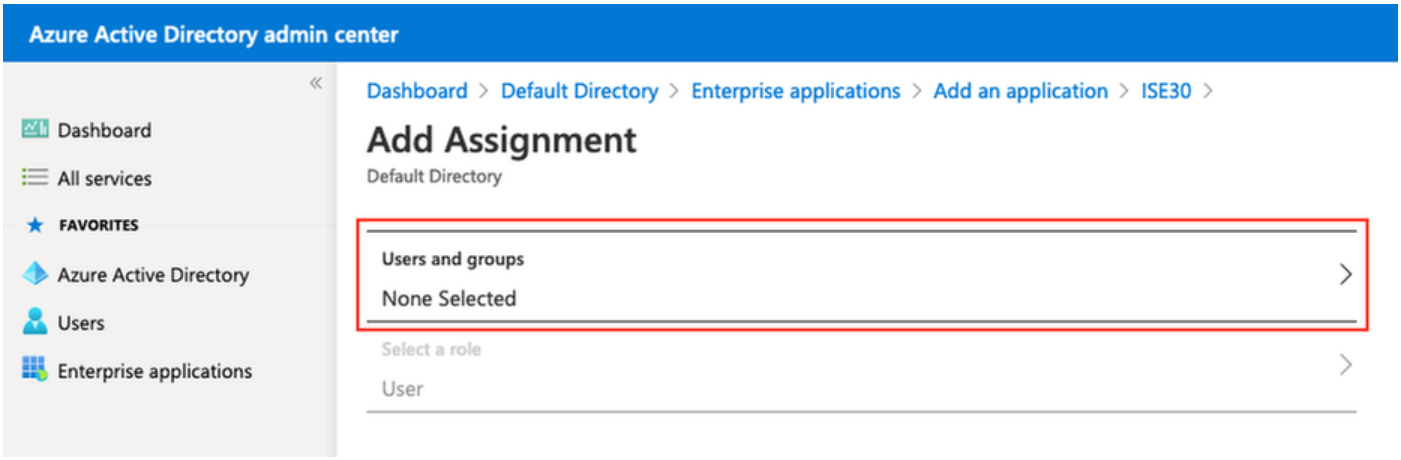
Assign users and groupsを選択します。



Add user/groupをクリックします。

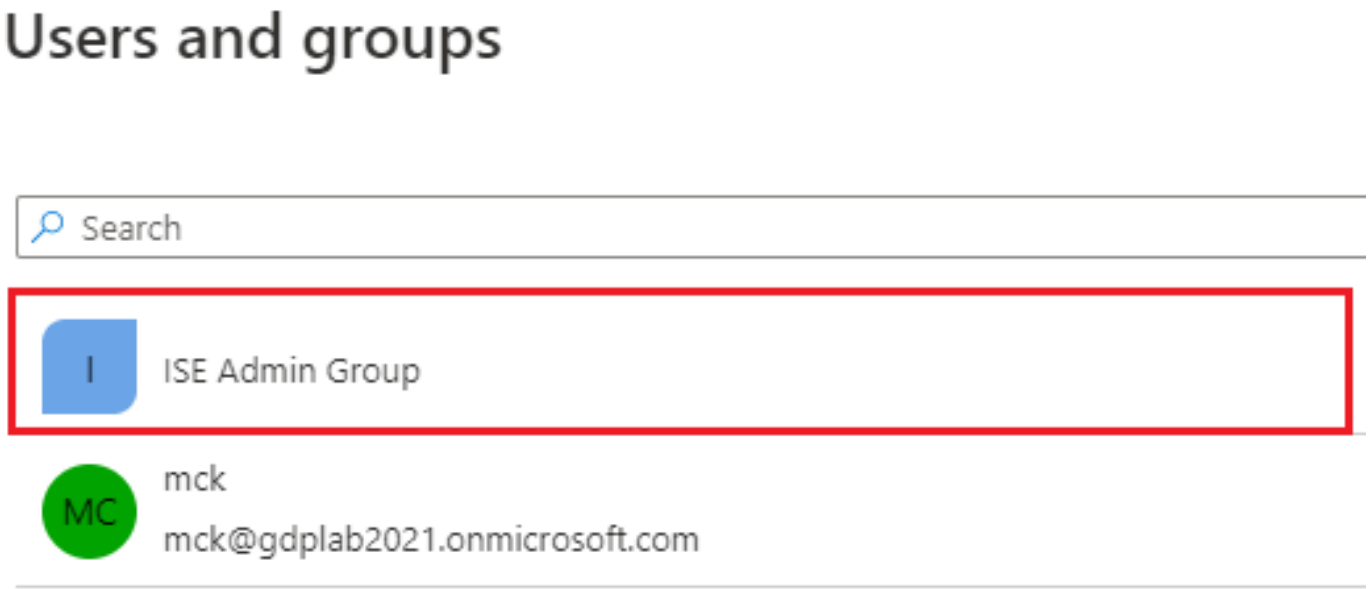


Users and groupsをクリックします。

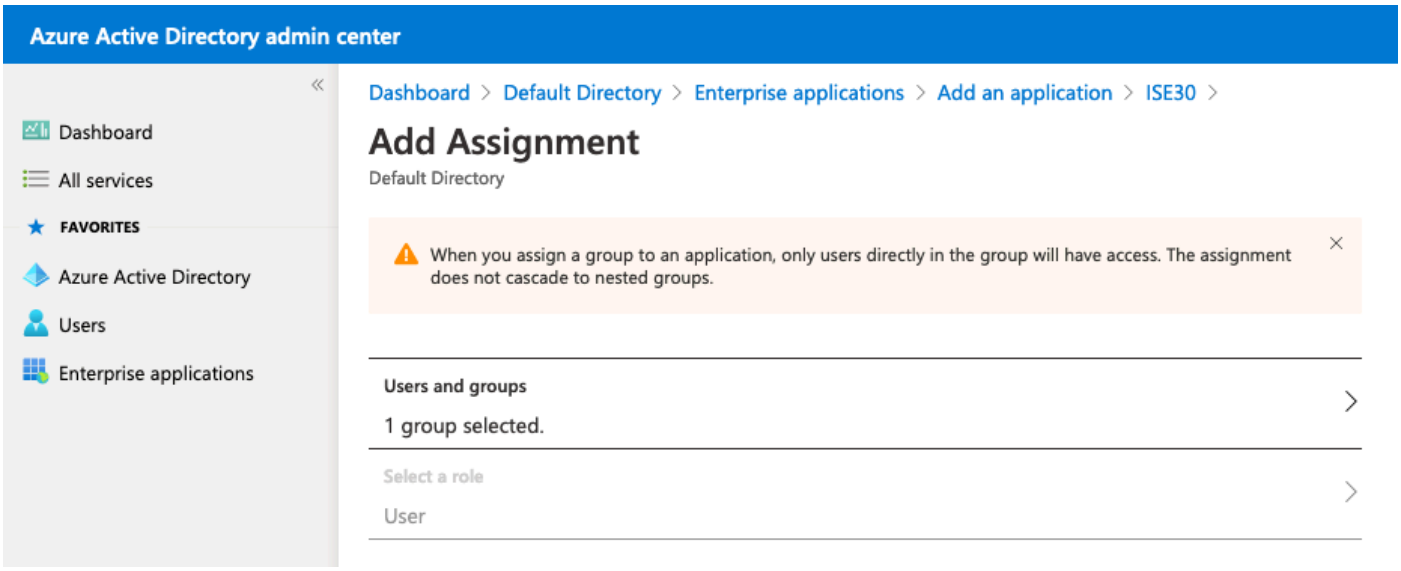


以前に設定したグループを選択し、Selectをクリックします。

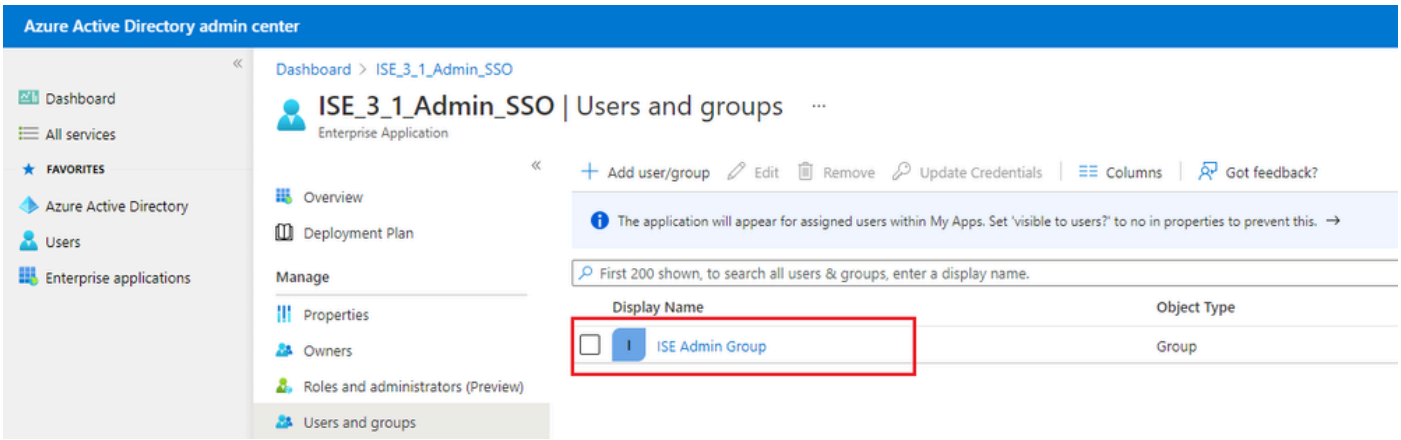
注： セットアップが完了すると、ここに記載したユーザとグループがISEにアクセスできるため、意図したとおりにアクセスできる適切なユーザまたはグループを選択します。



グループを選択したら、Assignをクリックする。

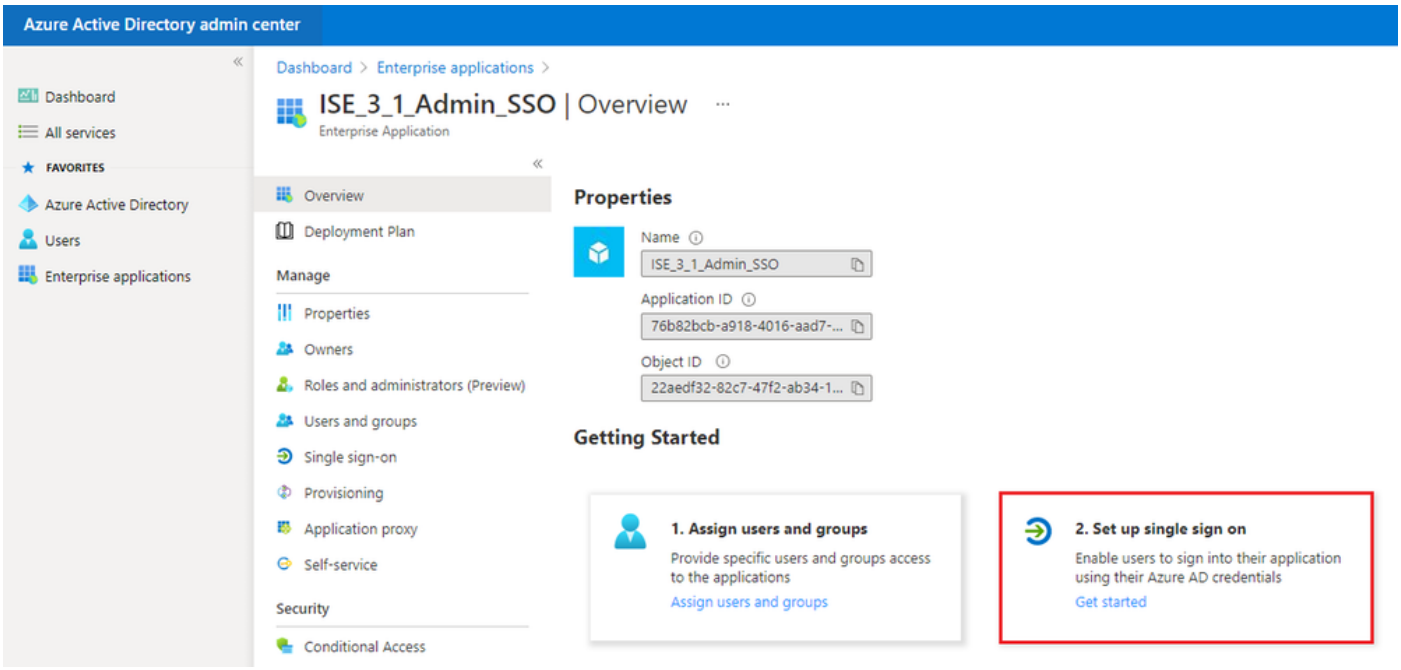


その結果、設定されたアプリケーションのUsers and groupsメニューに、選択されたグループが表示されます。

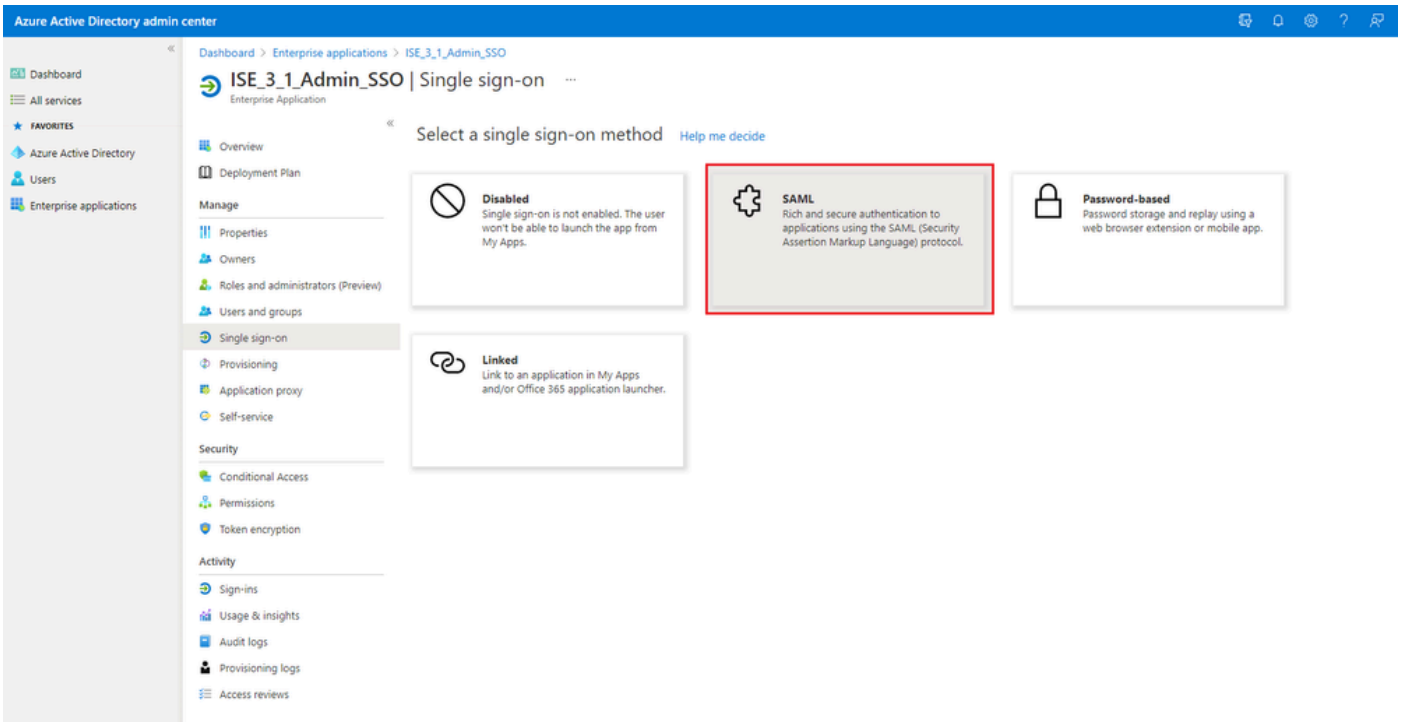


6. Azure AD Enterpriseアプリケーションを構成します：

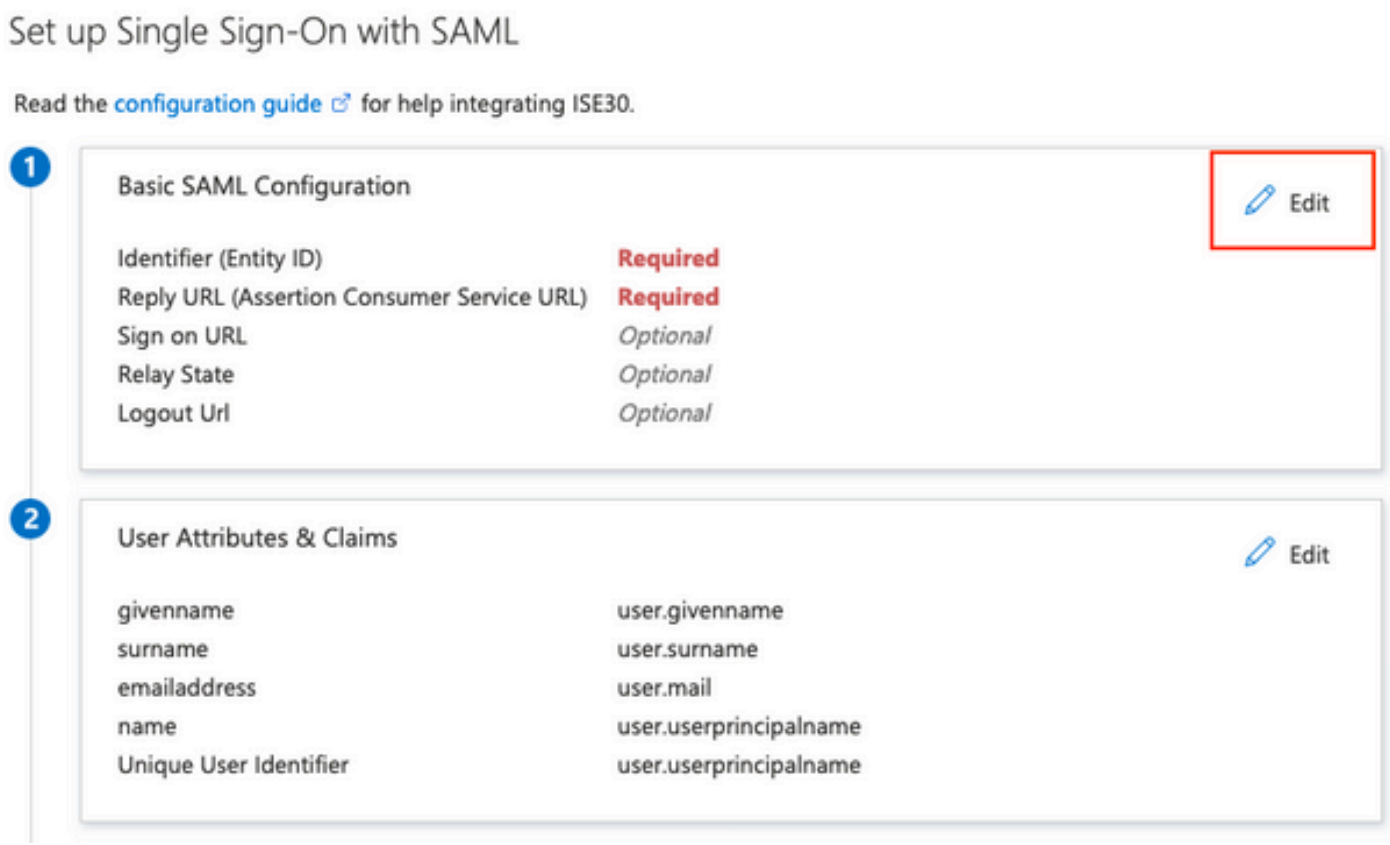
アプリケーションに戻り、シングルサインオンのセットアップをクリックします。



次の画面でSAMLを選択します。

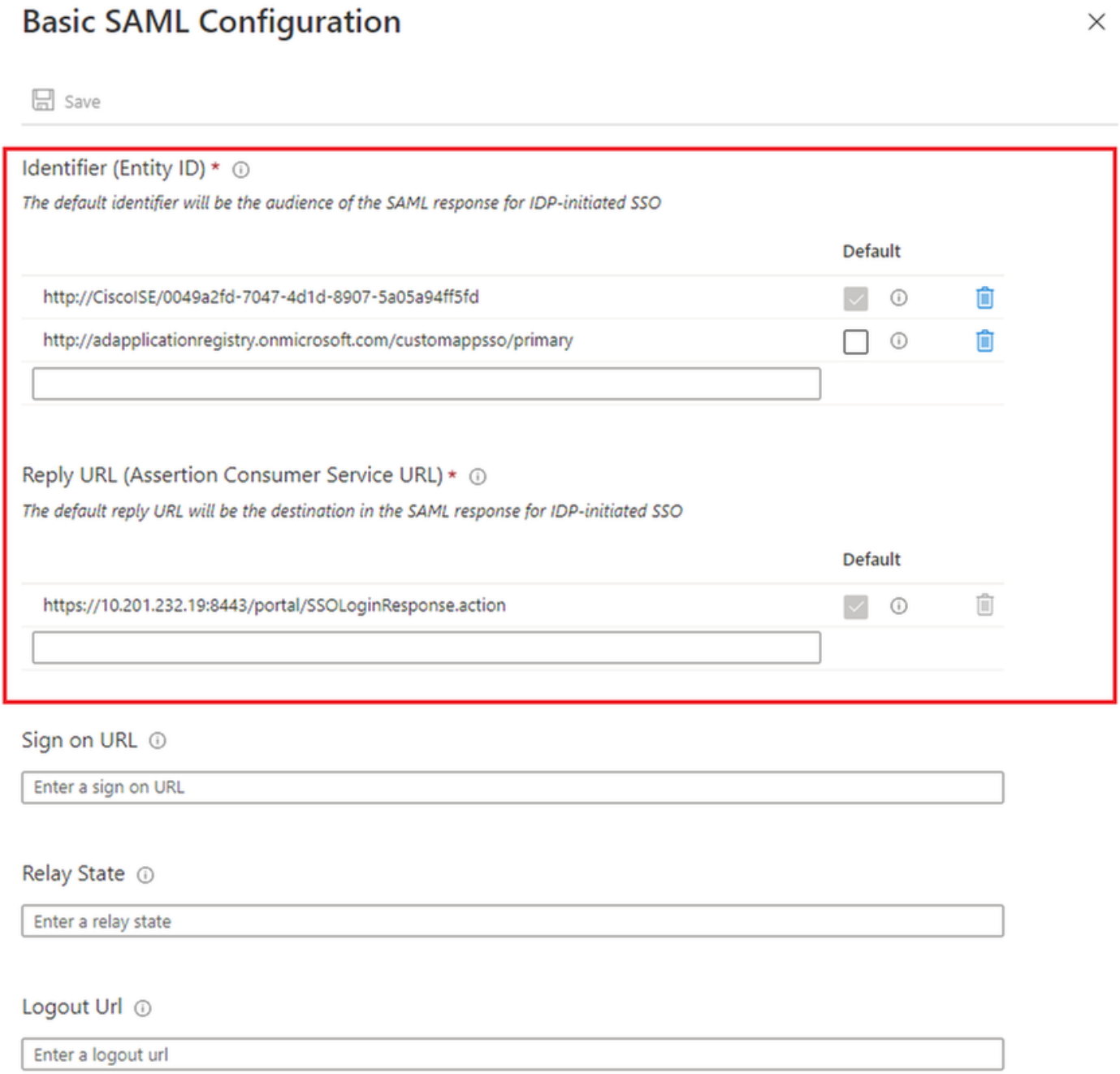


Basic SAML Configurationの横にあるEditをクリックします。



ID（エンティティID）に、サービスプロバイダー情報のエクスポート手順で取得したXMLファイルのentityIDの値を入力します。Reply URL(Assertion Consumer Service URL)に、AssertionConsumerServiceのLocationsの値を入力します。 [Save] をクリックします。

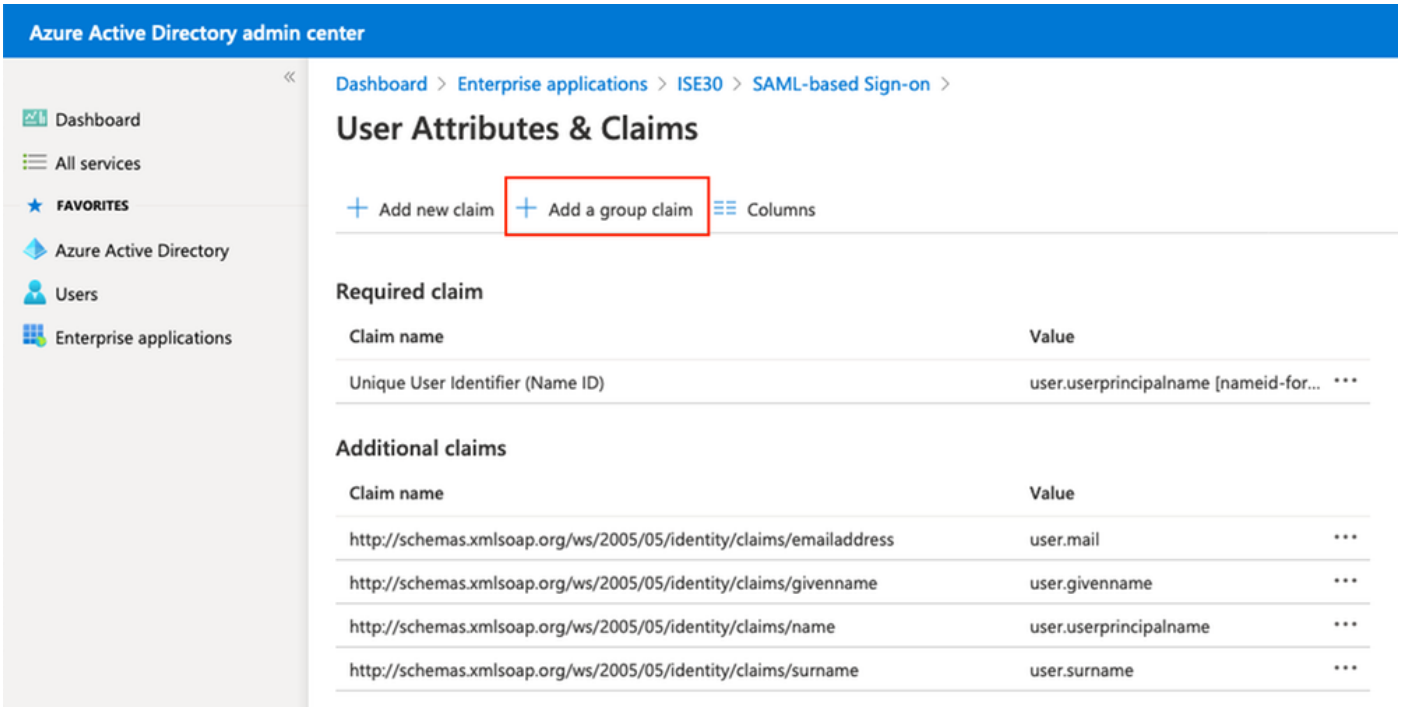
注： 応答URLはパスリストとして機能し、IdPページにリダイレクトされたときに特定のURLが送信元として機能できるようにします。



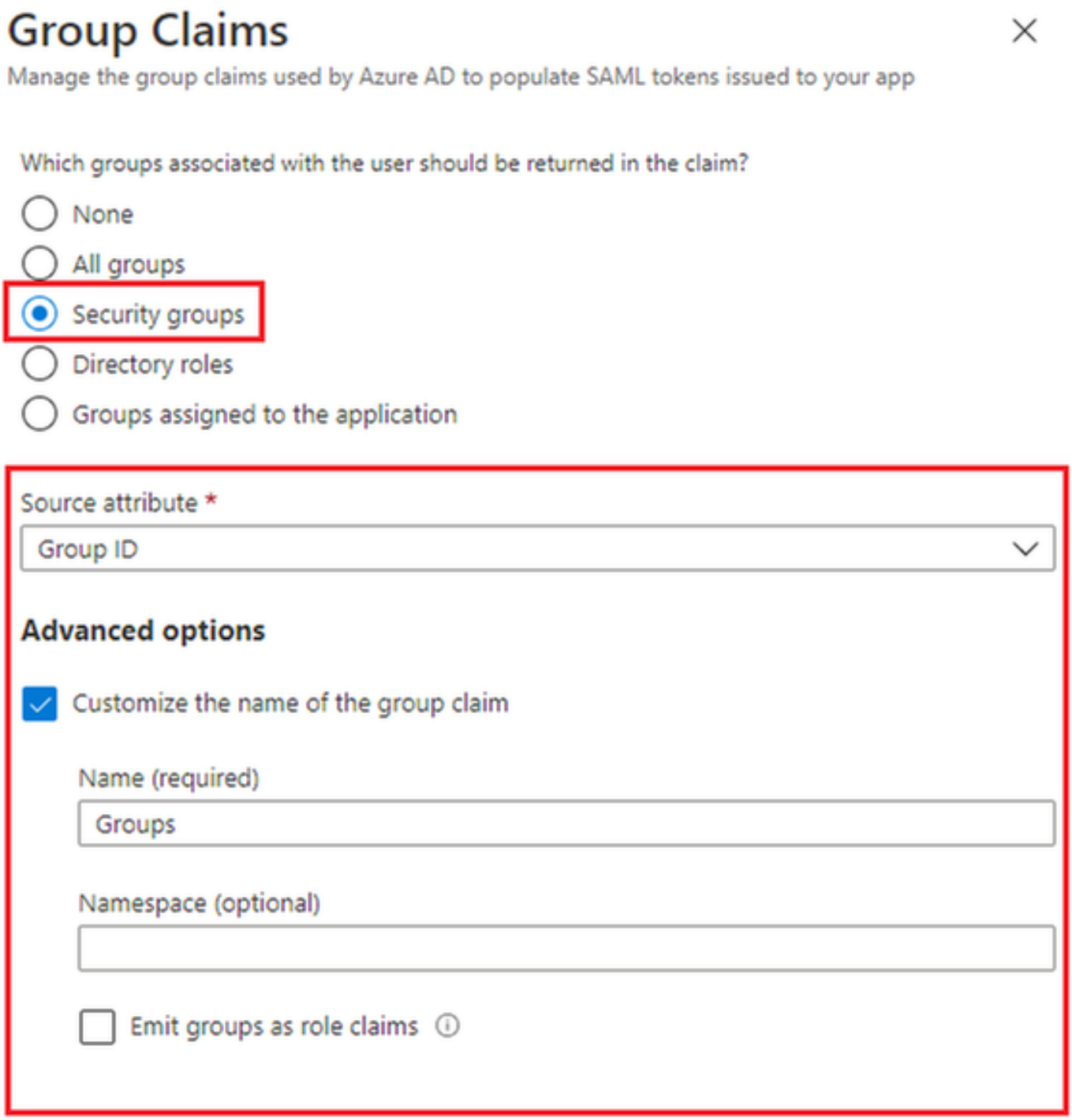
7. Active Directoryグループ属性を設定します。

以前に設定したグループ属性値を返すには、User Attributes & Claimsの横にあるEditをクリックします。

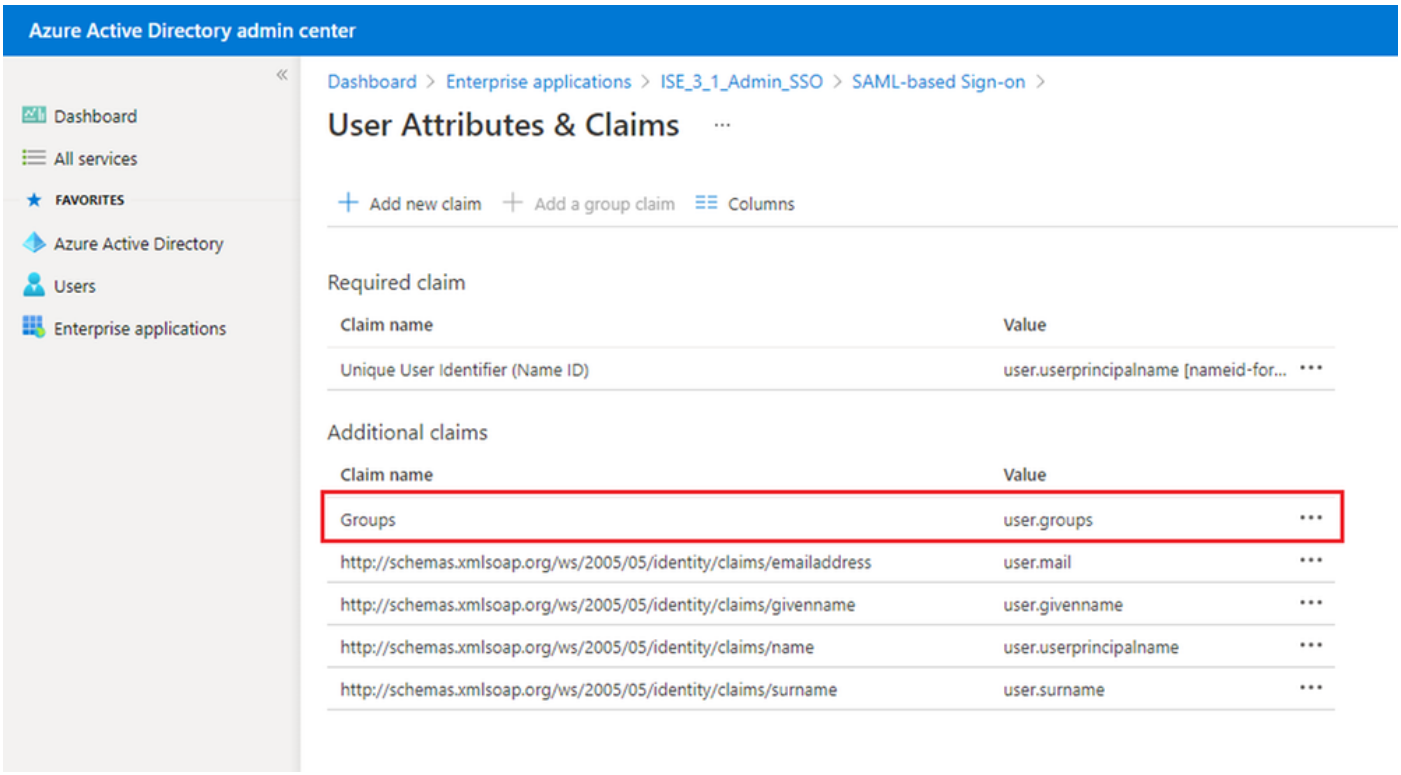
Add a group claimをクリックします。



Security groupsを選択し、Saveをクリックします。 Source attributeドロップダウンメニューで Group IDを選択します。このチェックボックスをオンにして、グループ要求の名前をカスタマイズし、名前をGroupsと入力します。

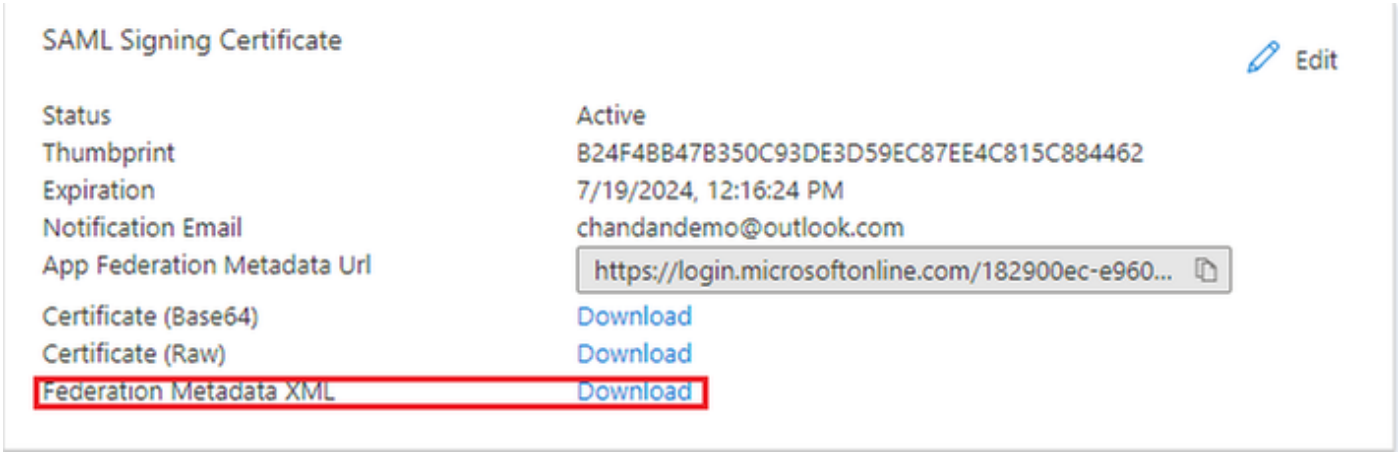


グループの請求名をメモします。この場合はGroupsです。



8. AzureフェデレーションメタデータXMLファイルをダウンロードします：

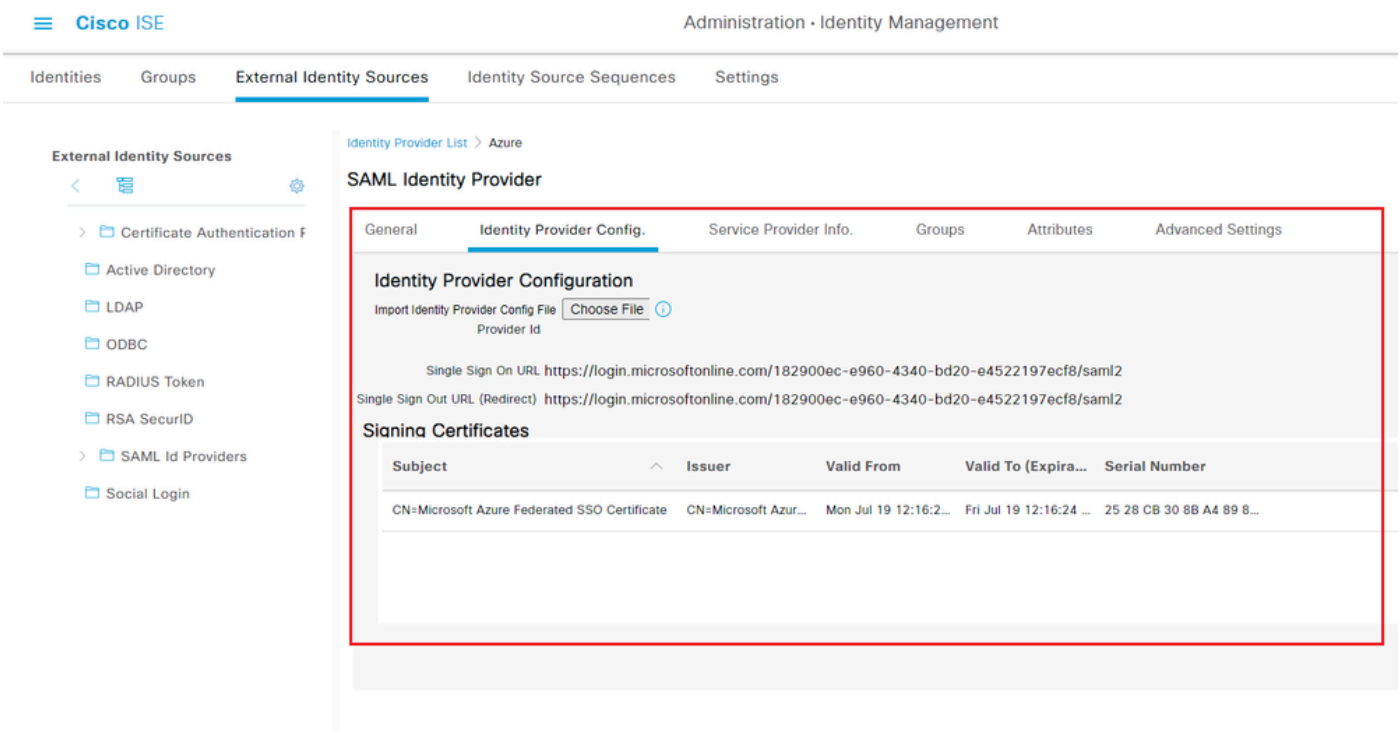
SAML署名証明書でフェデレーションメタデータXMLに対してダウンロードをクリックします。



ステップ 3：Azure Active DirectoryからISEへのメタデータのアップロード

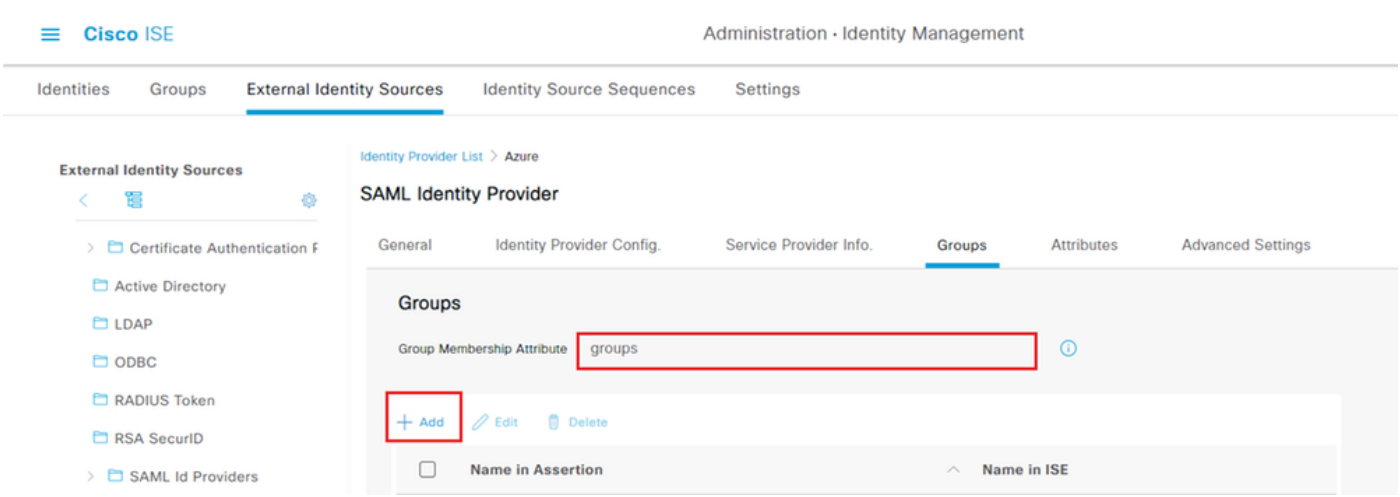
Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]に移動します。

タブをIdentity Provider Config.に切り替え、Browseをクリックします。Azure Federation Metadata XMLのダウンロードの手順でフェデレーションメタデータXMLファイルを選択し、保存をクリックします。



ステップ 4：ISEでのSAMLグループの設定

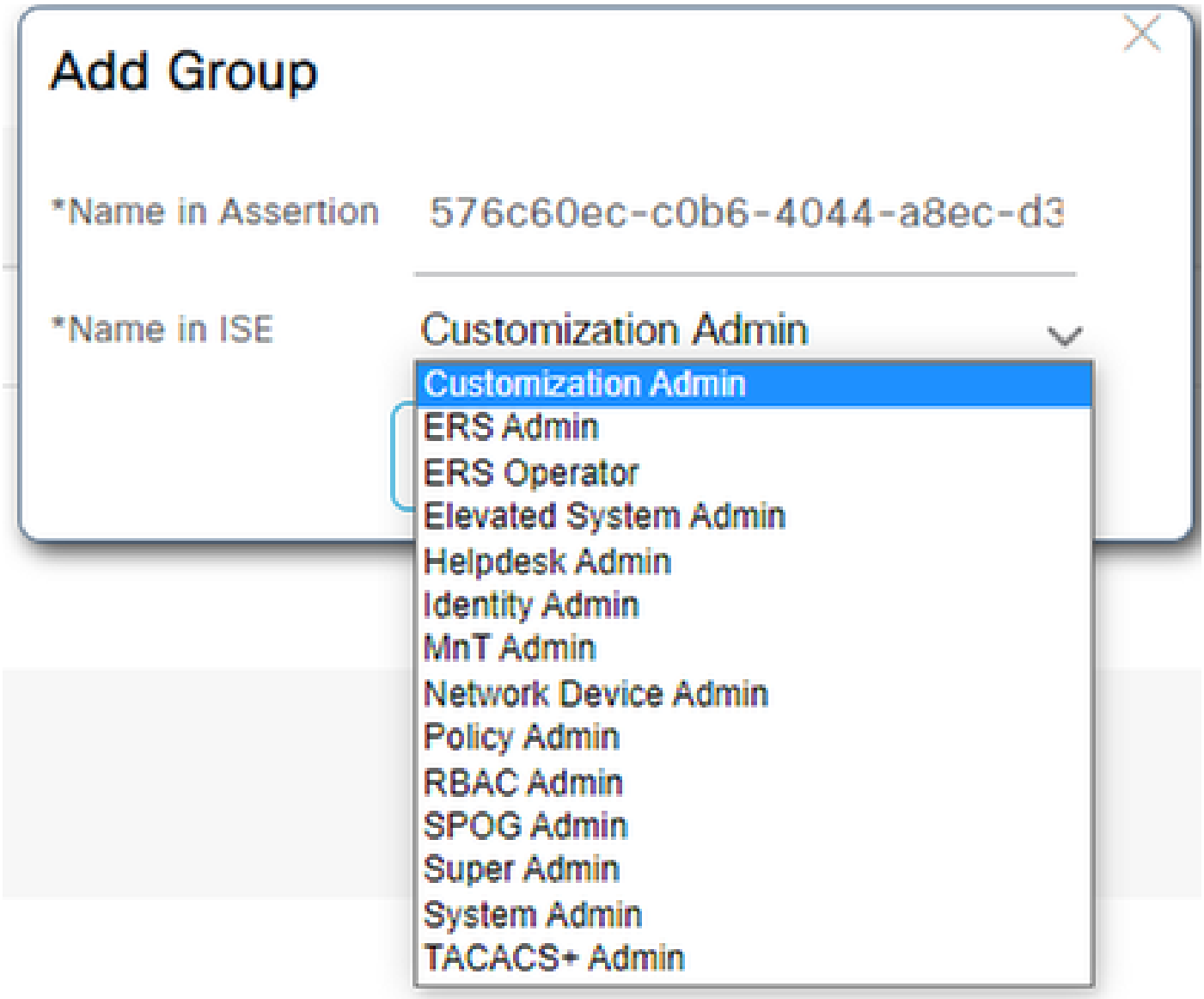
タブGroupsに切り替え、Configure Active Directory Group attributeのClaim nameの値をGroup Membership Attributeに貼り付けます。



[Add] をクリックします。Name in Assertionに、Assign Azure Active Directory User to the GroupでキャプチャしたISE Admin GroupのGroup Object IDの値を入力します。

ドロップダウンでISEの名前を設定し、ISEで適切なグループを選択します。この例で使用するグループはSuper Adminです。[OK] をクリックします。[Save] をクリックします。

これにより、AzureのグループとISEのグループ名の間にマッピングが作成されます。



（オプション）手順5:RBACポリシーの設定

前のステップから、ISEで設定できるユーザアクセスレベルにはさまざまなタイプがあります。

ロールベースアクセスコントロールポリシー(RBAC)を編集するには、Administration > System > Admin Access > Authorization > Permissions > RBAC Policiesの順に選択し、必要に応じて設定します。

この図は、設定例のリファレンスです。

RBAC Policies

Rule Name	Admin Groups	Permissions
Customization Admin Policy	If Customization Admin	then Customization Admin Menu ... Actions
Elevated System Admin Poli	If Elevated System Admin	then System Admin Menu Access... Actions
ERS Admin Policy	If ERS Admin	then Super Admin Data Access Actions
ERS Operator Policy	If ERS Operator	then Super Admin Data Access Actions
ERS Trustsec Policy	If ERS Trustsec	then Super Admin Data Access Actions
Helpdesk Admin Policy	If Helpdesk Admin	then Helpdesk Admin Menu Access Actions
Identity Admin Policy	If Identity Admin	then Identity Admin Menu Access... Actions
MnT Admin Policy	If MnT Admin	then MnT Admin Menu Access Actions
Network Device Policy	If Network Device Admin	then Network Device Menu Acce... Actions
Policy Admin Policy	If Policy Admin	then Policy Admin Menu Access ... Actions
RBAC Admin Policy	If RBAC Admin	then RBAC Admin Menu Access ... Actions
Read Only Admin Policy	If Read Only Admin	then Super Admin Menu Access ... Actions
SPOG Admin Policy	If SPOG Admin	then Super Admin Data Access Actions
Super Admin Policy	If Super Admin	then Super Admin Menu Access ... Actions
Super Admin_Azure	If Super Admin	then Super Admin Menu Access ... Actions
System Admin Policy	If System Admin	then System Admin Menu Access... Actions
TACACS+ Admin Policy	If TACACS+ Admin	then TACACS+ Admin Menu Acc... Actions

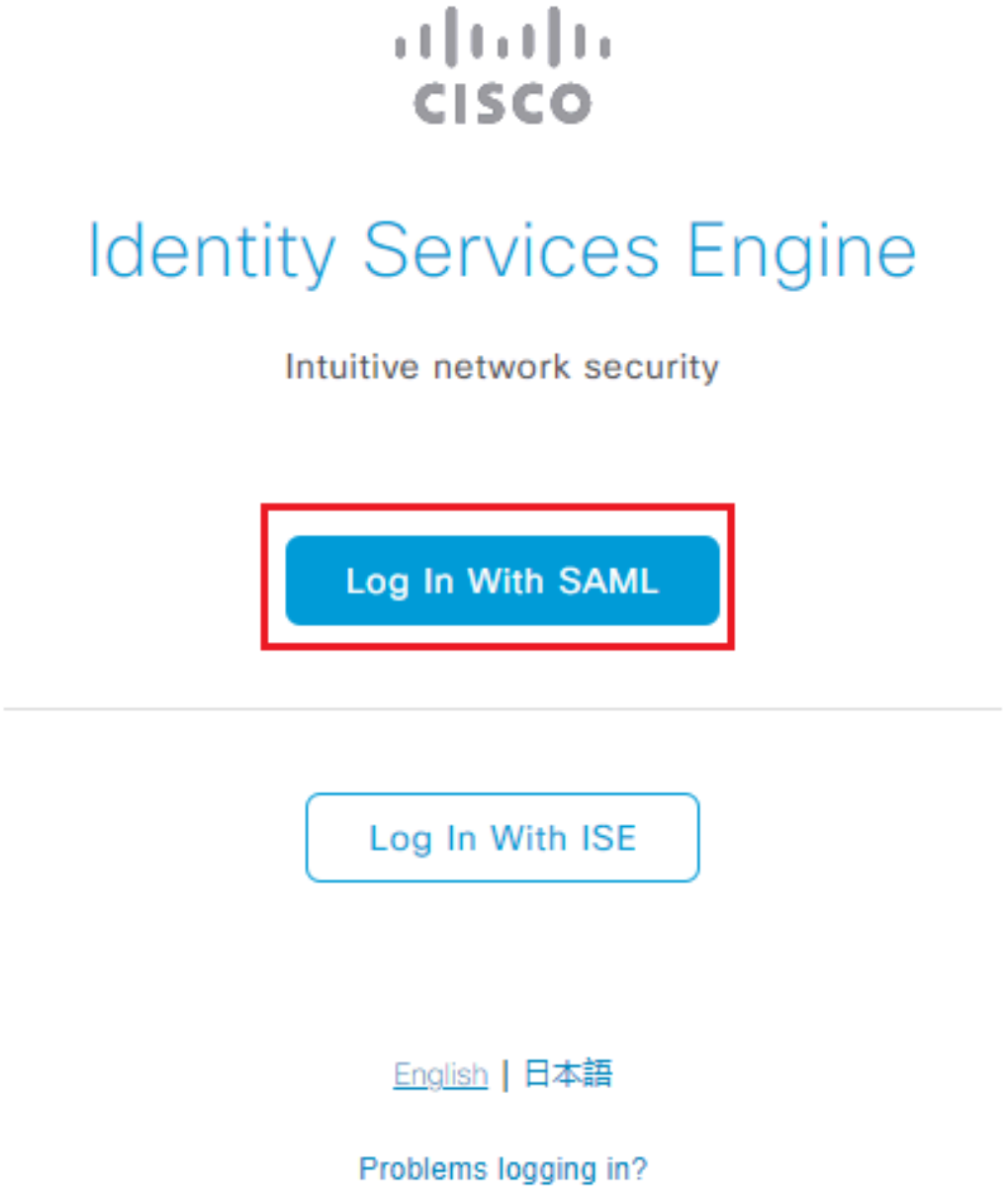
確認

設定が正しく動作していることを確認します。

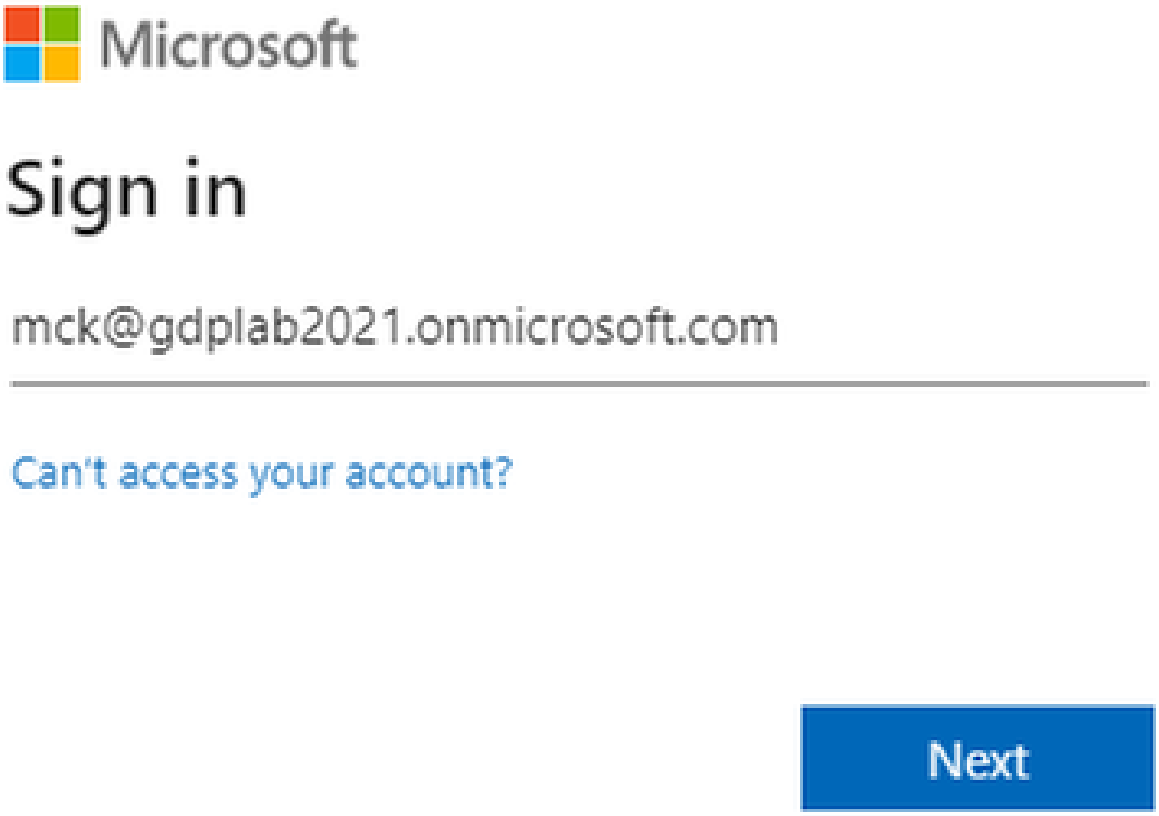
注：Azureテスト機能からのSAML SSOログインテストは機能しません。Azure SAML SSOが正しく動作するためには、ISEがSAML要求を開始する必要があります。

ISE GUIログインプロンプト画面を開きます。SAMLでログインする新しいオプションが表示されます。

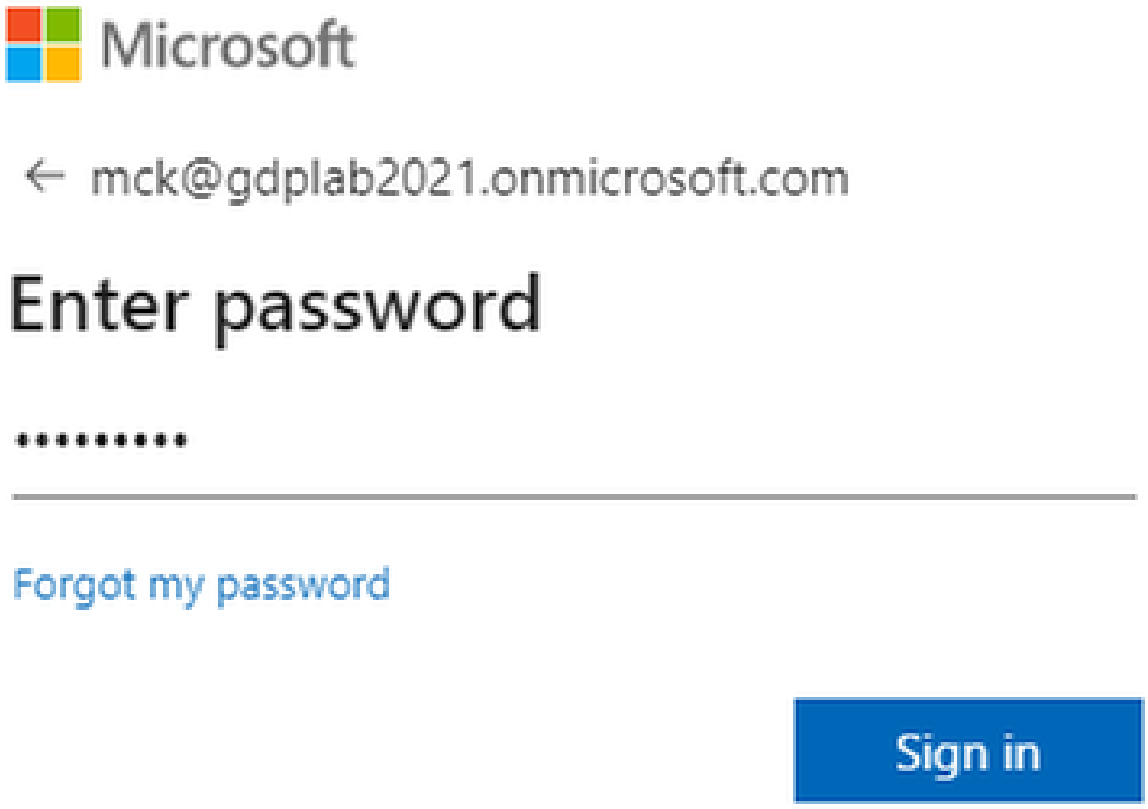
1. ISE GUIログインページにアクセスし、Log In with SAMLをクリックします。



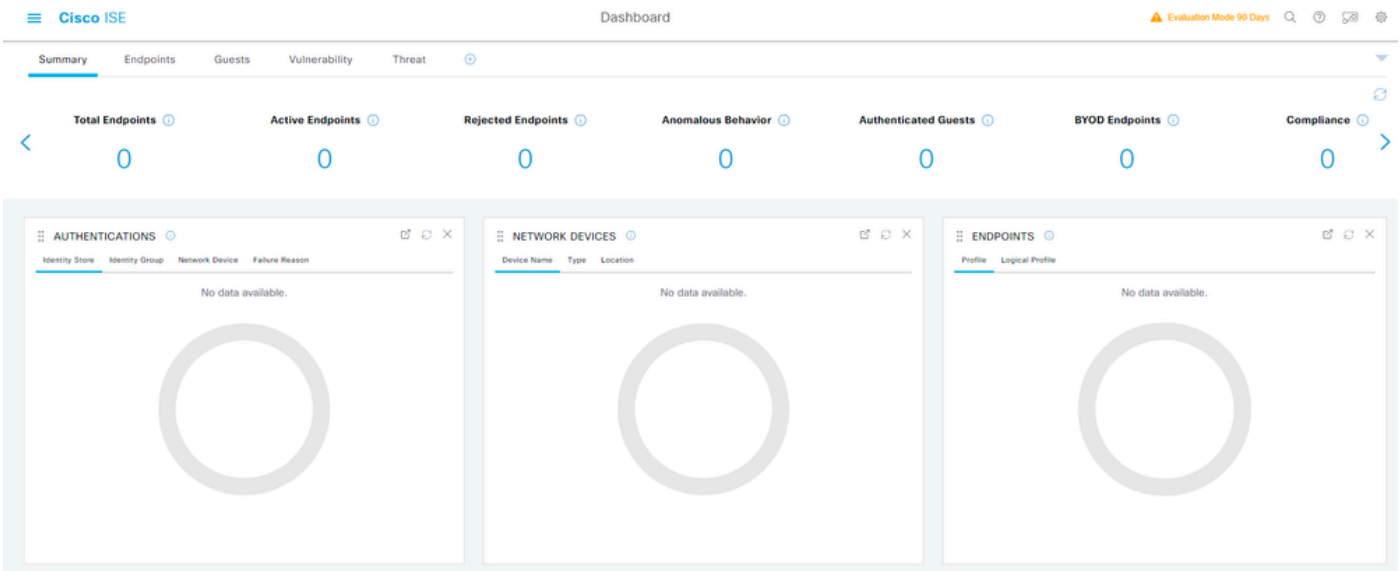
2. Microsoftログイン画面にリダイレクトされます。次に示すように、ISEにマッピングされたグループのアカウントのユーザ名クレデンシャルを入力し、図に示すように次へをクリックします。



3. ユーザのパスワードを入力し、サインインをクリックします。



4. これで、図に示すように、前に設定したISEグループに基づいて適切な権限が設定されたISEアプリケーションダッシュボードにリダイレクトされます。



トラブルシュート

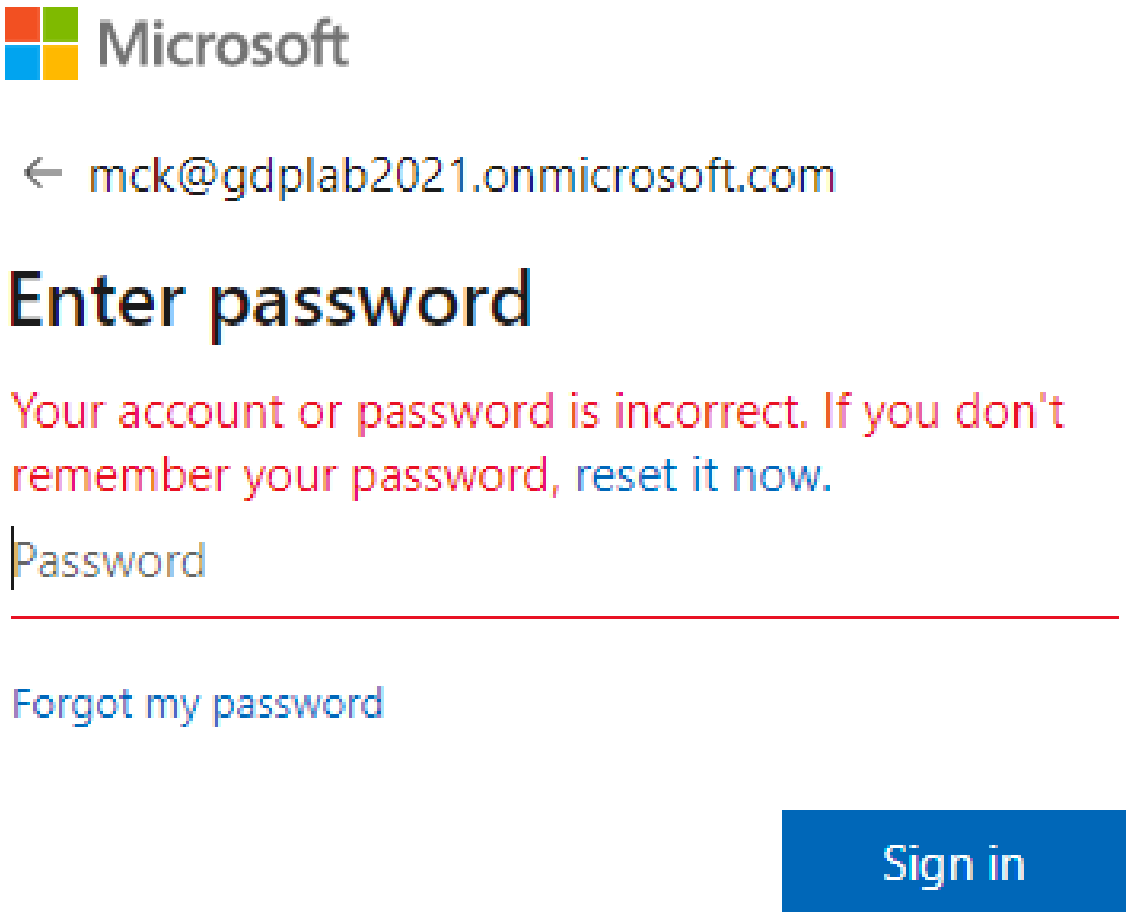
このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

一般的な問題

SAML認証は、ブラウザとAzure Active Directoryの間で処理されることを理解する必要があります。したがって、ISEエンゲージメントがまだ開始されていないIDプロバイダー(Azure)から認証関連のエラーを直接取得できます。

問題1：クレデンシャルを入力した後に「Your account or password is incorrect」エラーが表示される。ここでは、ユーザデータはまだISEで受信されておらず、この時点のプロセスは引き続きIdP(Azure)で実行されます。

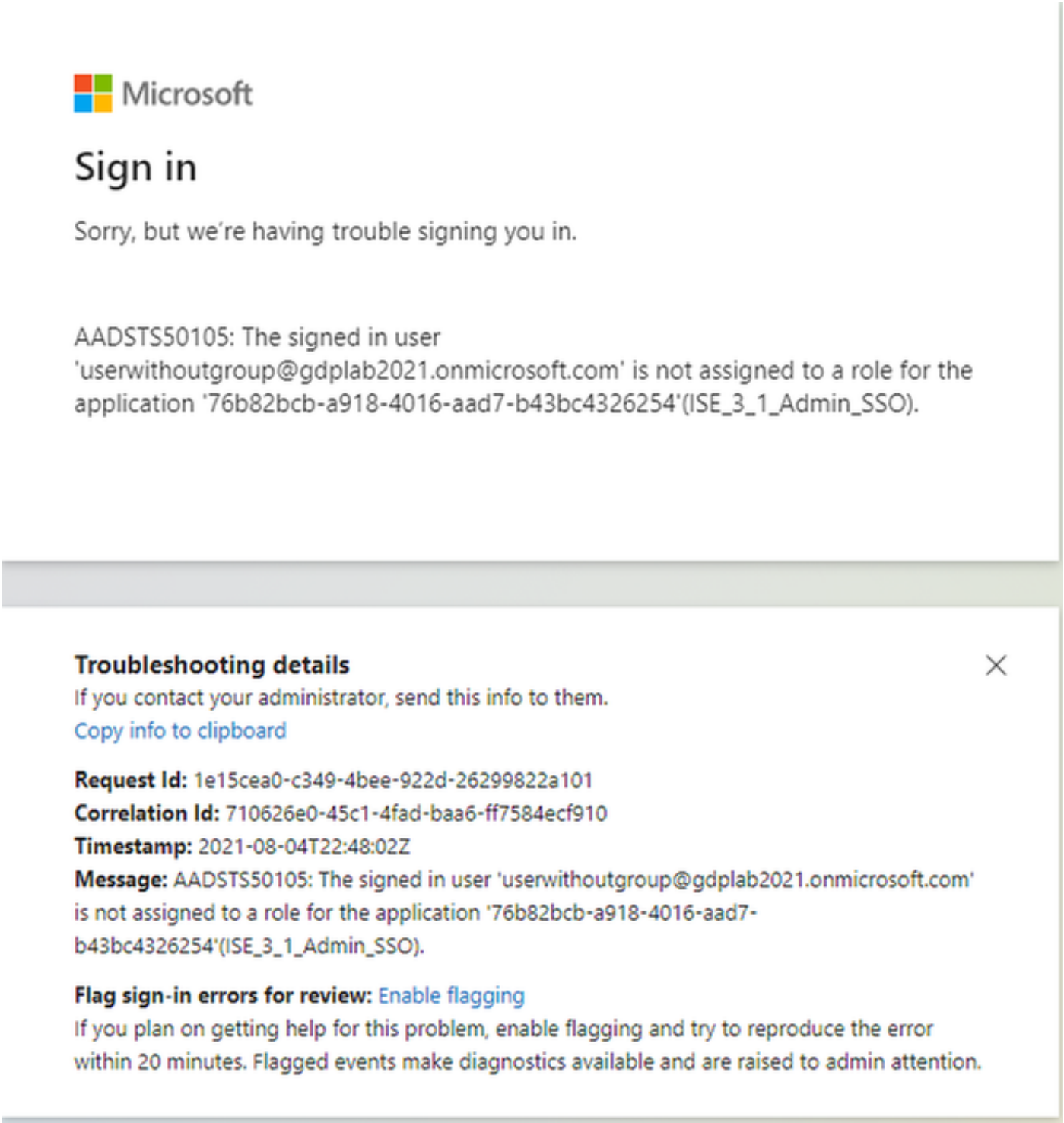
最も可能性の高い原因は、アカウント情報が正しくないか、パスワードが正しくないことです。修正するには：パスワードをリセットするか、図に示すように、そのアカウントの正しいパスワードを入力します。



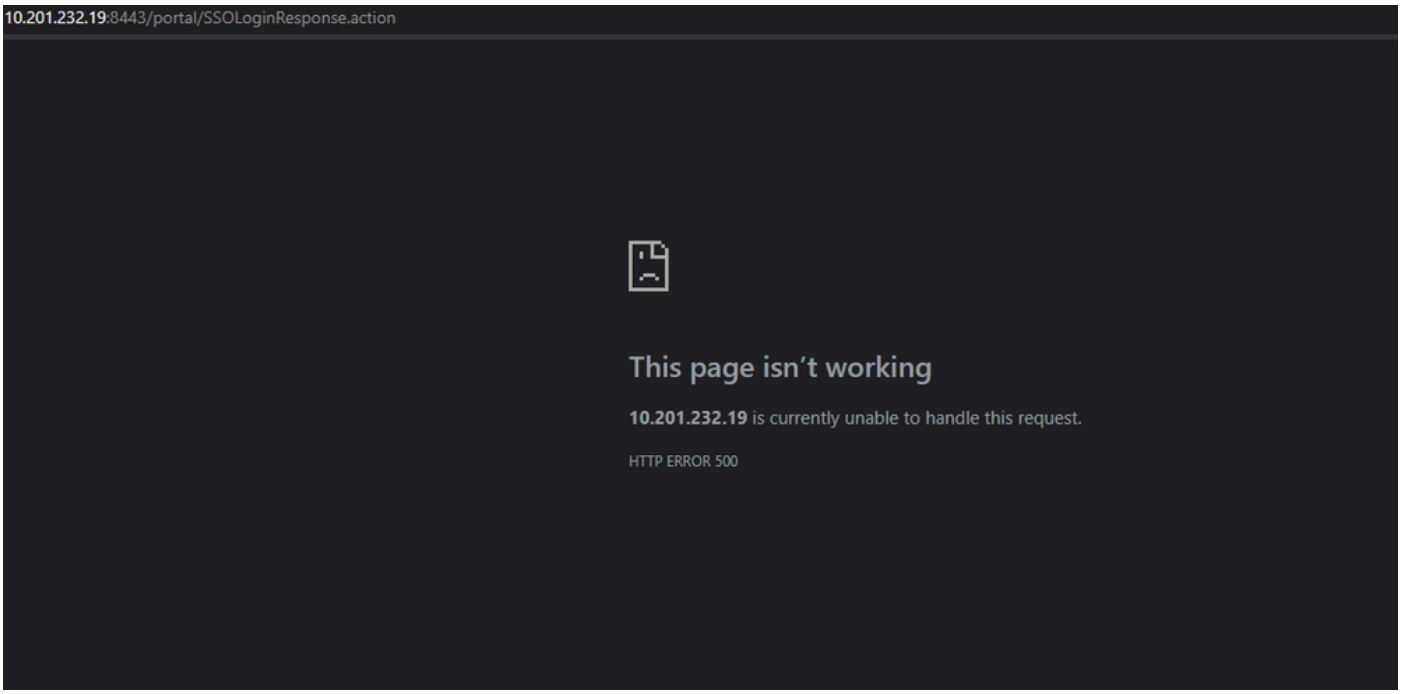
問題 2：このユーザは、SAML SSOへのアクセスが許可されているグループに属していません。前述のケースと同様に、ユーザデータはまだISEで受信されておらず、この時点のプロセスは引き続きIdP(Azure)で実行されます。

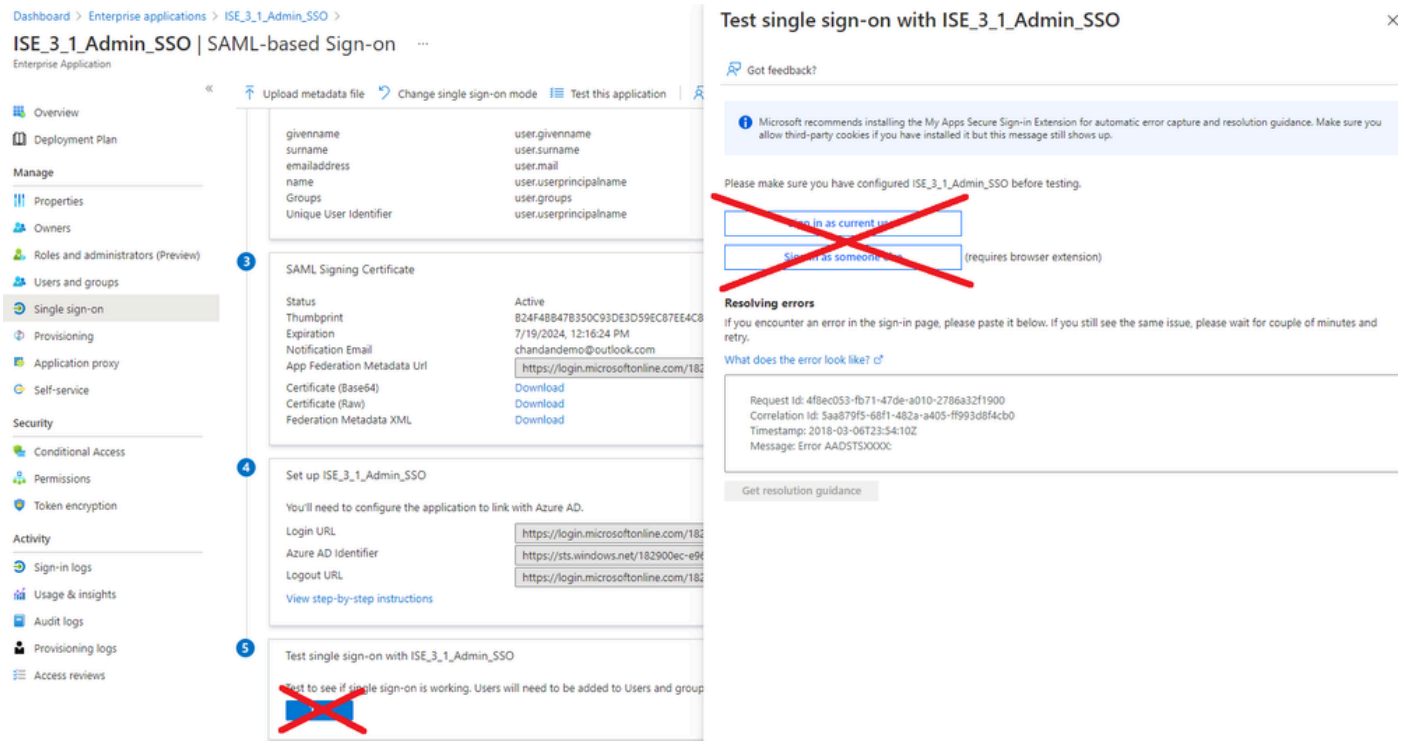
解決策:Add group to the Application設定手順が図のように正しく実行されていることを確認しま

す。



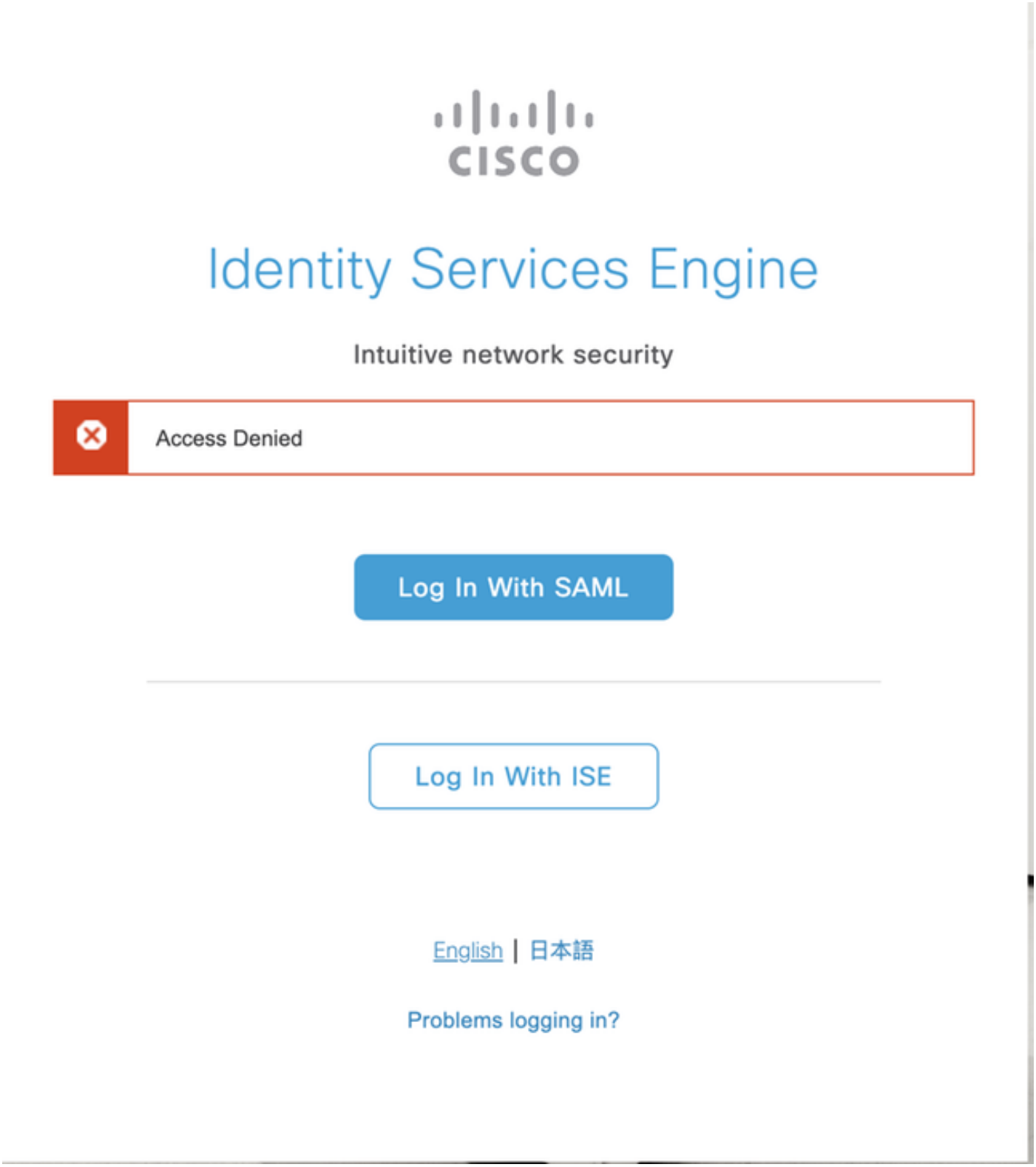
問題 3：ISEアプリケーションサーバがSAMLログイン要求を処理できません。この問題は、SAML要求がサービスプロバイダーのISEではなく、Identity Provider（IDプロバイダー）Azureから開始された場合に発生します。Azure ADからのSSOログインのテストは、ISEがアイデンティティプロバイダーが開始したSAML要求をサポートしていないため、機能しません。





問題 4：ログイン試行後に「Access Denied」エラーが表示される。このエラーは、Azureエンタープライズアプリケーションで以前に作成されたグループの要求名がISEで一致しない場合に発生します。

解決策：AzureとISEのSAML IDプロバイダーグループタブのグループ要求名が同じであることを確認してください。詳細については、このドキュメントの「Azure ADでのSAML SSOの設定」セクションのステップ2.7.および4.を参照してください。



ISEのトラブルシューティング

ここでのコンポーネントのログレベルは、ISEで変更する必要があります。Operations > Troubleshoot > Debug Wizard > Debug Log Configurationの順に移動します。

コンポーネント名	ログ レベル	ログファイル名

ポータル	デバッグ	ゲスト。ログ
opensaml	デバッグ	ise-psc.log
saml	デバッグ	ise-psc.log

SAMLログインとグループ要求名の不一致を含むログ

フロー実行時のクレーム名の不一致のトラブルシューティングシナリオを表示するデバッグのセット(ise-psc.log)。

注：太字の項目に注意してください。分かりやすくするために、ログは短くしてあります。

---

1. ユーザはISE管理ページからIdP URLにリダイレクトされます。

<#root>

```
2021-07-29 13:48:20,709 INFO   [admin-http-pool46][] api.services.persistance.dao.DistributionDAO -::::
2021-07-29 13:48:20,712 INFO   [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -::
```

forwardStr for: https://10.201.232.19/admin/LoginAction.do

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

IDP URL: https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2

```
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

SAML request - spUrlToReturnTo:https://10.201.232.19:8443/portal/SSOLoginResponse.action

```
2021-07-29 13:48:20,844 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
```

2. ブラウザからSAML応答を受信します。

<#root>

```
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,172 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

```
-:::- Decoded SAML relay state of: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a

2021-07-29 13:48:27,177 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode

-:::- Decoded SAML message

2021-07-29 13:48:27,182 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.dec
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decode
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: h
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de
2021-07-29 13:48:27,183 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.de

2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
```

3. 属性（アサーション）解析が開始されました。

<#root>

```
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA

2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA

[parseAttributes] Set on IdpResponse object  - attribute<http://schemas.xmlsoap.org/ws/2005/05/identity/


2021-07-29 13:48:27,184 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

4. グループ属性が576c60ec-c0b6-4044-a8ec-d395b1475d6eの値で受信され、署名が検証されます。

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
        IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
        SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
        Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOLoginResponse.action
        Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-89
        Client Address: 10.24.226.171
        Load Balancer: null
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,358 INFO   [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp
```

5. RBAC認証検証。

<#root>

```
************************Rbac Log Summary for user samlUser*************************
2021-07-29 13:48:27,360 INFO   [admin-http-pool50][] com.cisco.ise.util.RBACUtil -::::- Populating cach

2021-07-29 13:48:27,368 ERROR  [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::

java.lang.NullPointerException

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- In Login
```

```
2021-07-29 13:48:27,369 ERROR  [admin-http-pool50][] cpm.admin.infra.action.LoginAction -::::- Can't sav

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -::

2021-07-29 13:48:27,369 INFO   [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

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。