

Azure ADを使用したSAML SSO経由のフローでのISE 3.1管理者ログインの設定

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](#)

[アイデンティティプロバイダー\(IdP\):](#)

[サービスプロバイダー\(SP\):](#)

[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](#)

- [1. Azure ADを外部SAML IDソースとして構成](#)
- [2. ISE認証方式の設定](#)
- [3. サービスプロバイダー情報のエクスポート](#)

[ステップ 2 : Azure AD IdP設定の構成](#)

- [1. Azure ADユーザーの作成](#)
- [2. Azure ADグループの作成](#)
- [3. Azure ADユーザーをグループに割り当てる](#)
- [4. Azure ADエンタープライズアプリケーションの作成](#)
- [5. アプリケーションへのグループの追加](#)
- [6. Azure ADエンタープライズアプリケーションの構成](#)
- [7. Active Directoryグループ属性の設定](#)
- [8. AzureフェデレーションメタデータXMLファイルのダウンロード](#)

[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](#)

[\(オプション \) ステップ5:RBACポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[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に関するログ](#)

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:

アイデンティティプロバイダー(IdP):

要求されたリソース（サービスプロバイダー）に対してユーザーIDとアクセス特権を確認し、アサートするAzure ADの権限。

サービスプロバイダー(SP):

ユーザがアクセスするホステッド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に認証資格情報を渡すために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、ユーザー認証が含まれています。

SAMLアサーションには、認証、属性、認可の決定という3つの異なるタイプがあります。

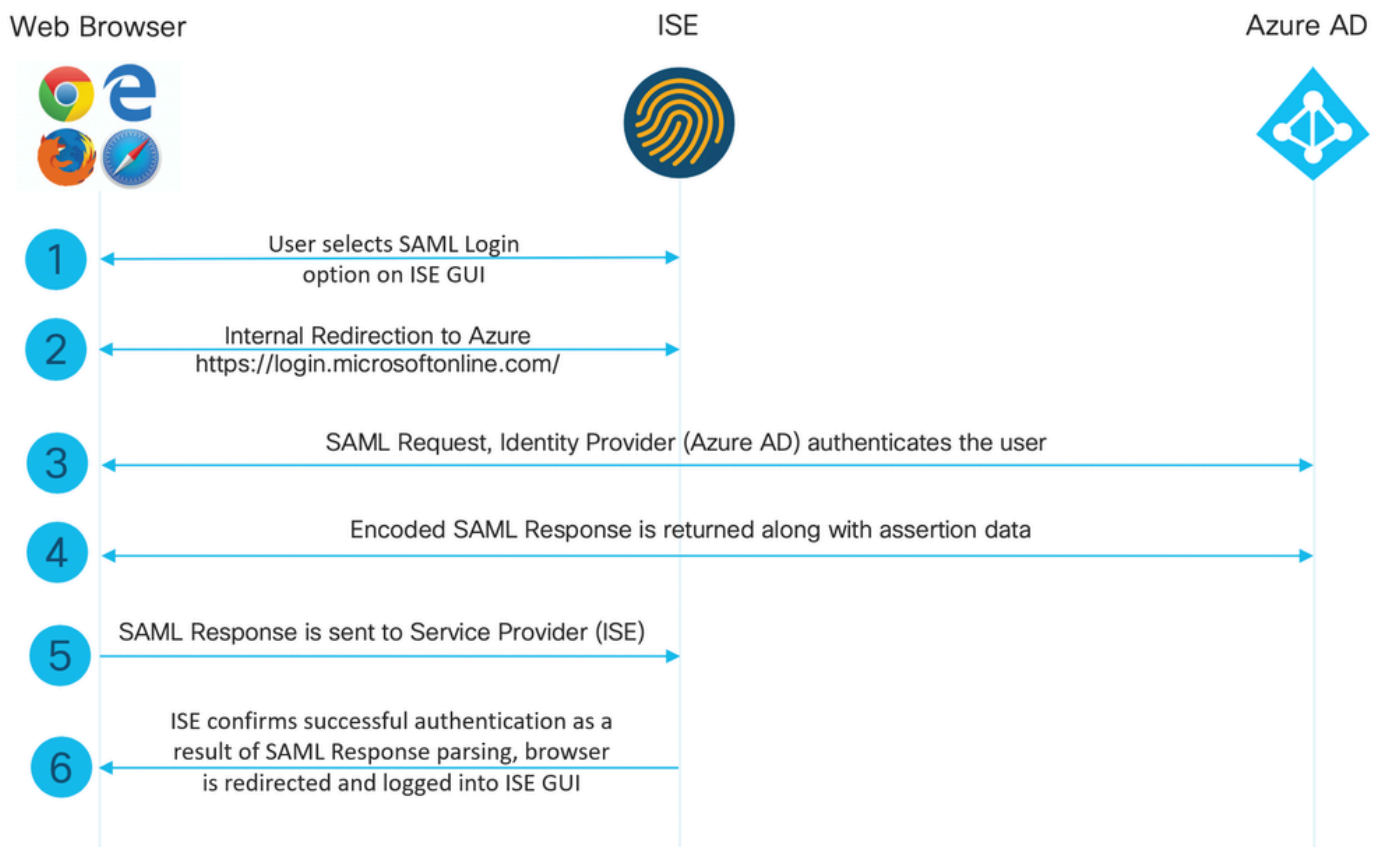
- 認証アサーションは、ユーザのIDを証明し、ユーザがログインした時間と使用した認証方法（例としてKerberos、2要素）を提供します
- アトリビューションアサーションは、SAML属性（ユーザに関する情報を提供する特定のデータ）をサービスプロバイダーに渡します。
- ユーザーがサービスを使用する権限を持っているか、パスワードの失敗またはサービスに対する権限の欠如が原因でIDプロバイダーが要求を拒否したかを示す認証の決定アサーションが宣言されます。

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、ユーザがこれらのサービスにアクセスしようとする時、Azure ADプロバイダーからSAML属性がISEに渡されます。

図に示すように、ISEはAzure ADに認可と認証を要求します。



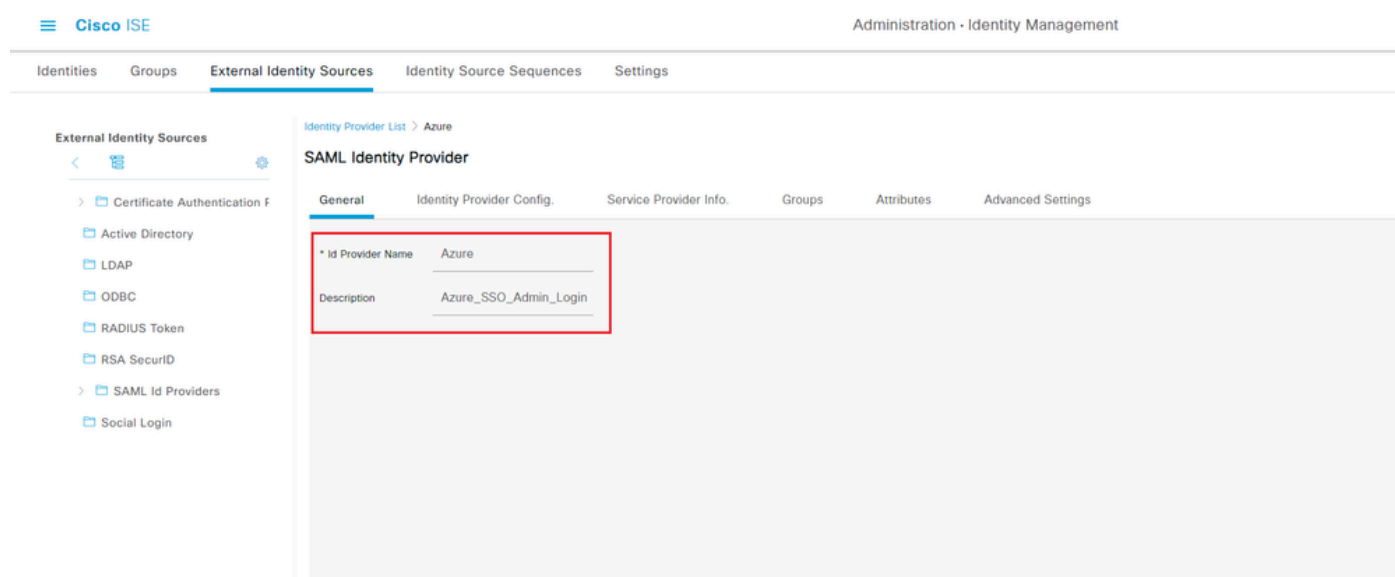
Azure ADとのSAML SSO統合の構成

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

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認証方式の設定

Administration > System > Admin Access > Authentication > Authentication Methodの順に移動し、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。

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings

Authentication Type ⓘ

Password Based

Client Certificate Based

* Identity Source

SAML:Azure ▼

3. サービスプロバイダー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。

Identity Provider List > Azure_SAML

SAML Identity Provider

General Identity Provider Config. **Service Provider Info.** Groups Attributes Advanced Settings

Service Provider Information

Load balancer ⓘ

Export Service Provider Info. **Export** ⓘ

Includes the following portals:

Sponsor Portal (default)

.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:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpTQU1MX21zZTMtMS0xOS5ja3VtYXJyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yMTA3MTkwMzI4MDBa
```

```
MCUxIzAhBgNVBAMTG1NBtUxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOAg8AMIICCgKCAgEAvi1a4+S0uP3j037yCOXnHAzADupfqcwcp1JQnFxbVfnDd0ixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDziyGKDDPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqrVrrYzUuAXDWUNUg9pSGzH0FkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g14WJWmizET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshkGSjgVn31XQ5vgDH1PvqNaYs/PwiCvmI/
wYKSTn9/hn7JM1Dq0R1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrC/1avr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwNGo7pQI8CAwEAAa9MHswIAYDVR0RBBkwF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oAdBgNVHSUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwqxvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIIdCf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUteif0bqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwvt6gfH0bE51uT4EYVuuHwMNGbZgqgb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJC0vUpdNmYC8cfAZuiv/e3wk0BLZM
TgV8FTVQSnra9LwHP/PgeNAPUcRPXSwake4rvjvMc0aS/iYdwZhiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTfjfoITTMdQXNHhg+w1P0KXS2GCZ29vAM52d8ZCq
Urz0VxNHKwKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/nChcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/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://Cisc0lSE/100d02da-9457-41e8-87d7-0965b0714db2>"

AssertionConsumerService

Location="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

AssertionConsumerService Location="[https://ise3-1-](https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action)

[19.onmicrosoft.com:8443/portal/SSOLoginResponse.action](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ユーザーの作成

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

択します。

The screenshot shows the Azure Active Directory admin center interface. The top navigation bar is blue with the text 'Azure Active Directory admin center'. Below it, the breadcrumb is 'Dashboard > Default Directory'. The main heading is 'Default Directory | Overview' with a sub-heading 'Azure Active Directory'. There are utility links: 'Switch tenant', 'Delete tenant', 'Create a tenant', 'What's new', 'Preview features', and 'Got feedback?'. A blue banner states: 'Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)'. The main content area is titled 'Default Directory' and has a search bar 'Search your tenant'. There are two main panels: 'Tenant information' and 'Azure AD Connect'. The 'Tenant information' panel shows: 'Your role: Global administrator [More info](#)', 'License: Azure AD Premium P2', 'Tenant ID: 64ace648-115d-4ad9-a3bf-7660...', and 'Primary domain: ekorneyccisco.onmicrosoft.com'. The 'Azure AD Connect' panel shows: 'Status: Not enabled' and 'Last sync: Sync has never run'. At the bottom, there is a 'Sign-ins' chart showing a bar graph with values 3, 2.8, 2.6, 2.4, 2.2, and 2. The date 'Aug 23' is shown in the bottom right corner.

Usersを選択してNew Userをクリックし、必要に応じてUser name, Name とInitial Password を設定します。図に示すように、Createをクリックします。

Identity

User name * ⓘ

mck ✓

@ gdplab2021.onmicrosoft... ▼



The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

.....

Show Password

Create

2. Azure ADグループの作成

Groupsを選択します。New Groupをクリックします。

[Dashboard](#) > [Default Directory](#) > [Groups](#)



Groups | All groups

Default Directory - Azure Active Directory

<<

+ New group

↓ Download groups

🗑 Delete

🔄 Refresh

☰ Columns

👤 All groups

👤 Deleted groups

🔧 Diagnose and solve problems

🔗 This page includes previews available for your evaluation. [View previews](#) →

🔍 Search groups

+ Add filters

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。

Dashboard > TAC > Groups >

New Group

Group type * ⓘ
Security

Group name * ⓘ
ISE Admin Group

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group ⓘ
Yes No

Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

3. Azure ADユーザーをグループに割り当てる

No members selectedをクリックします。ユーザを選択して、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。

Add members



Search ⓘ



mck

mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

次の図に示すように、ISE管理グループのグループオブジェクトID(GPO)をメモします。この画面では、576c60ec-c0b6-4044-a8ec-d395b1475d6eです。

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
 - General
 - Expiration
 - Naming policy

+ New group | Download groups | Delete | Refresh | Columns | Preview features | Got feedback?

This page includes previews available for your evaluation. View previews →

Search groups | Add filters

| Name | Object Id | Group Type | Membership Type |
|--|--------------------------------------|------------|-----------------|
| <input type="checkbox"/> I ISE Admin Group | 576c60ec-c0b6-4044-a8ec-d395b1475d6e | Security | Assigned |

4. Azure ADエンタープライズアプリケーションの作成

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

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

Enterprise applications | All applications

Default Directory - Azure Active Directory

+ New application | Columns | Preview features | Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application type: Enterprise Applications | Applications status: Any | Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Create your own applicationを選択します。

Azure Active Directory admin center

Dashboard > Enterprise applications >

Browse Azure AD Gallery

[+ Create your own application](#) | [Request new gallery app](#) | [Got feedback?](#)

i You're in the new and improved app gallery experience. [Click here to switch back to the legacy app gallery experience.](#) →

Search application

Single Sign-on : All | User Account Management : All | Categories : All

Cloud platforms

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle

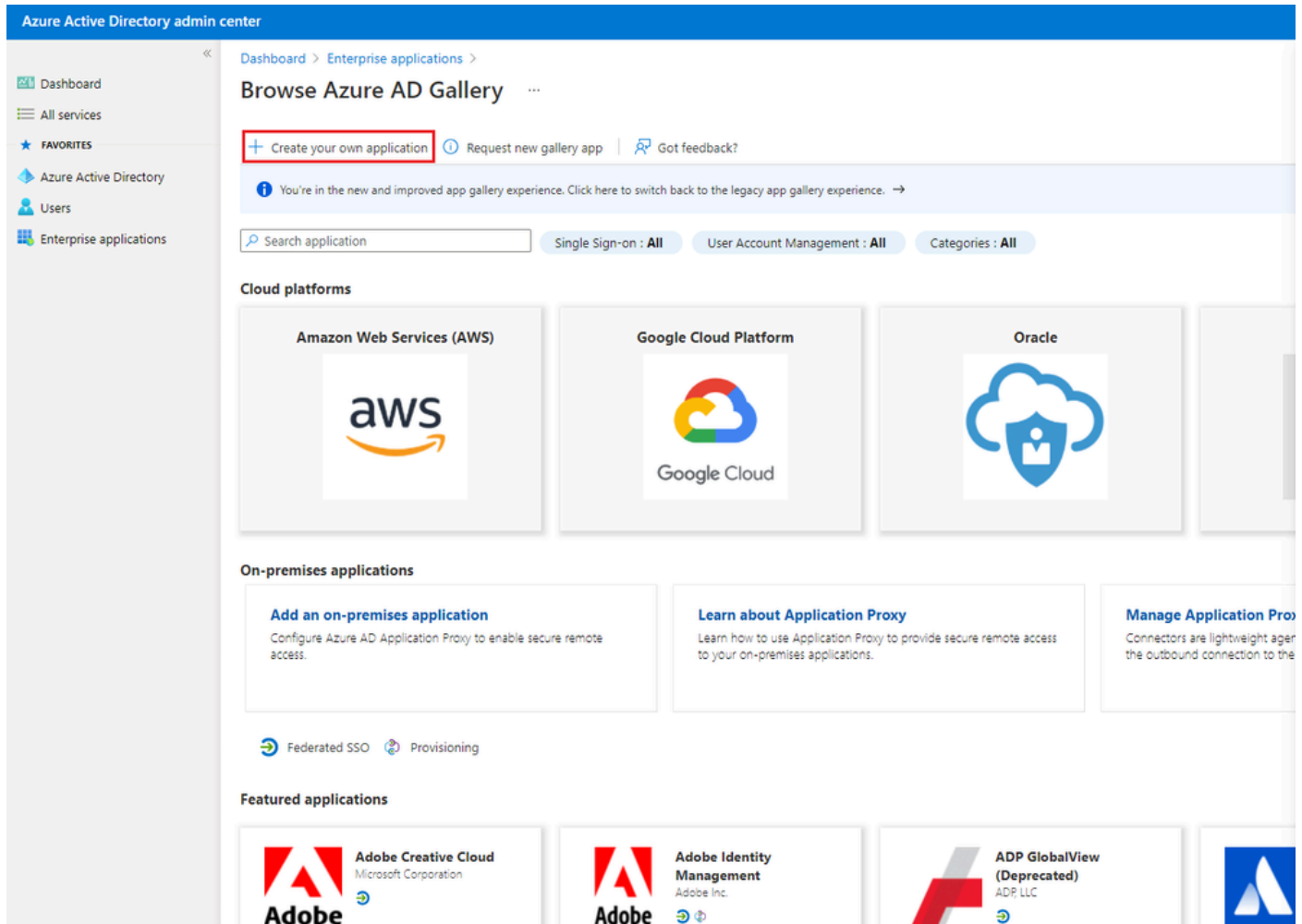
On-premises applications

- [Add an on-premises application](#)
Configure Azure AD Application Proxy to enable secure remote access.
- [Learn about Application Proxy](#)
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.
- [Manage Application Proxy](#)
Connectors are lightweight agents that manage the outbound connection to the on-premises application.

[Federated SSO](#) | [Provisioning](#)

Featured applications

- Adobe Creative Cloud
Microsoft Corporation
- Adobe Identity Management
Adobe Inc.
- ADP GlobalView (Deprecated)
ADP, LLC



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。

Create your own application



What's the name of your app?

ISE_3_1_Admin_SSO ✓

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

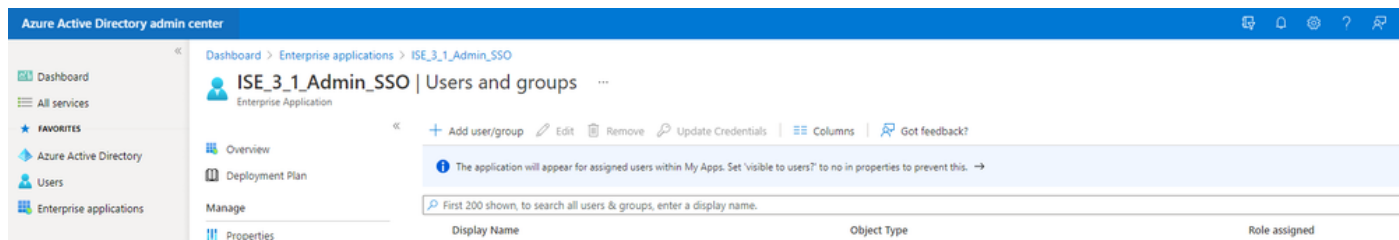
Create

5. アプリケーションへのグループの追加

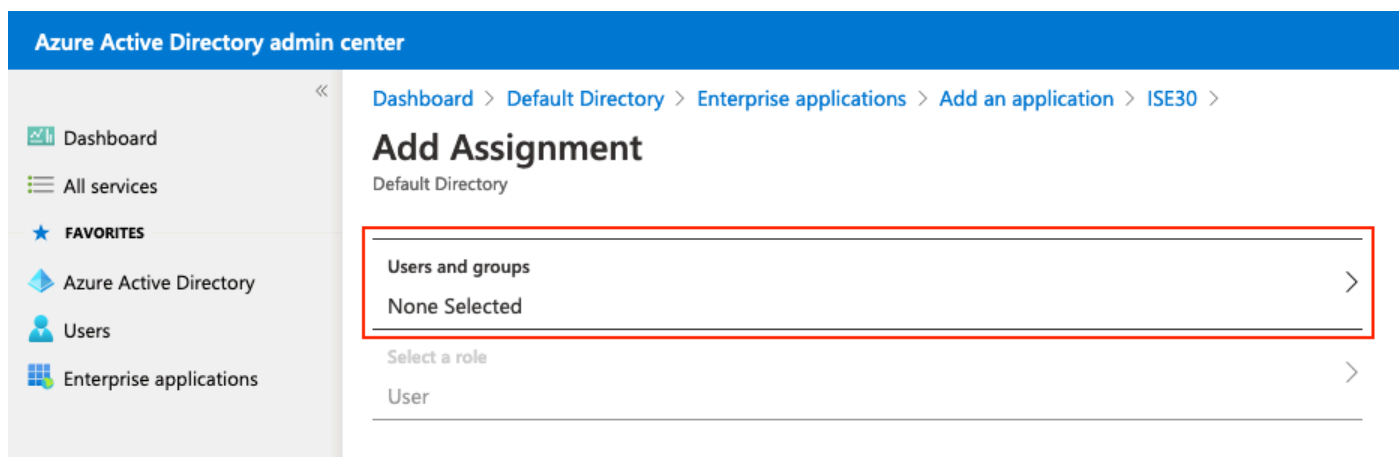
Assign users and groupsを選択します。

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area is titled 'ISE_3_1_Admin_SSO | Overview' and includes a 'Properties' section with fields for Name, Application ID, and Object ID. Below this is a 'Getting Started' section with two steps: '1. Assign users and groups' (highlighted with a red box) and '2. Set up single sign on'. The 'Assign users and groups' step includes a sub-step 'Assign users and groups' with a blue link.


Add user/groupをクリックします。



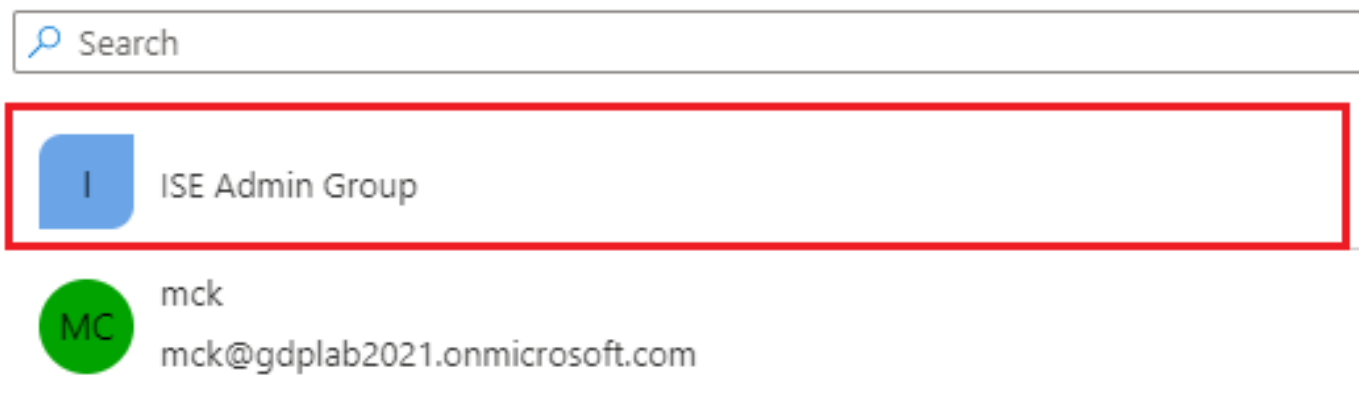
Users and groupsをクリックします。



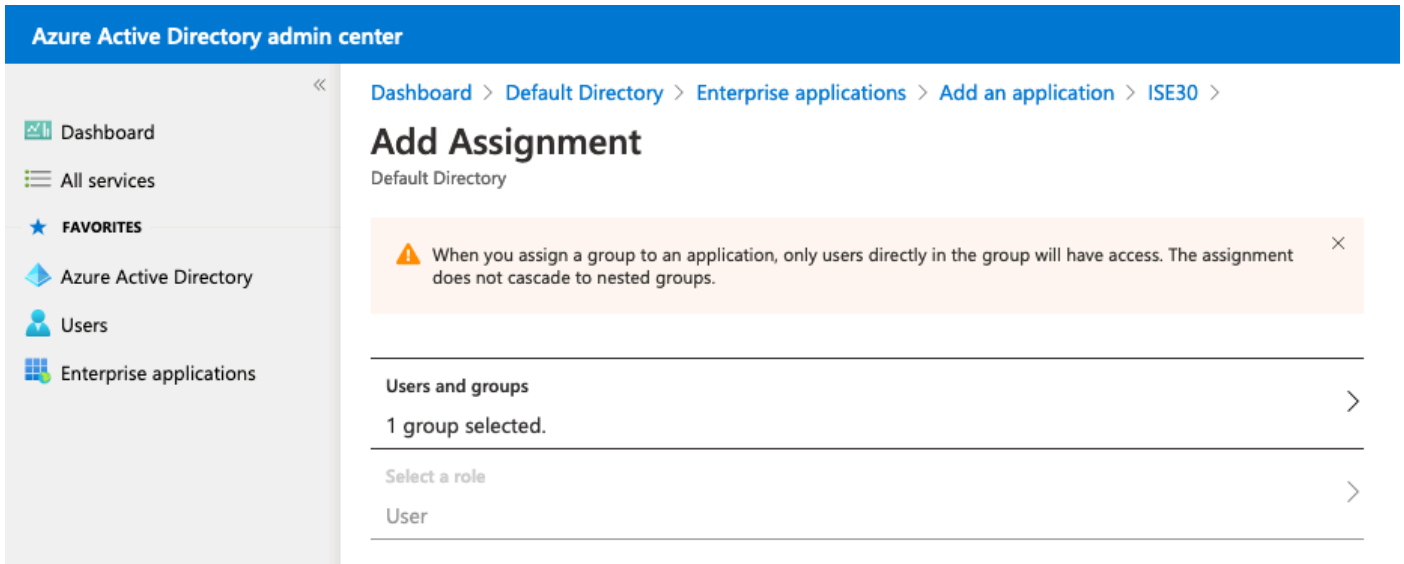
以前に設定したGroupを選択し、Selectをクリックします。

 注：セットアップ完了後にここに記載されているユーザとグループがISEにアクセスできるため、目的ど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。

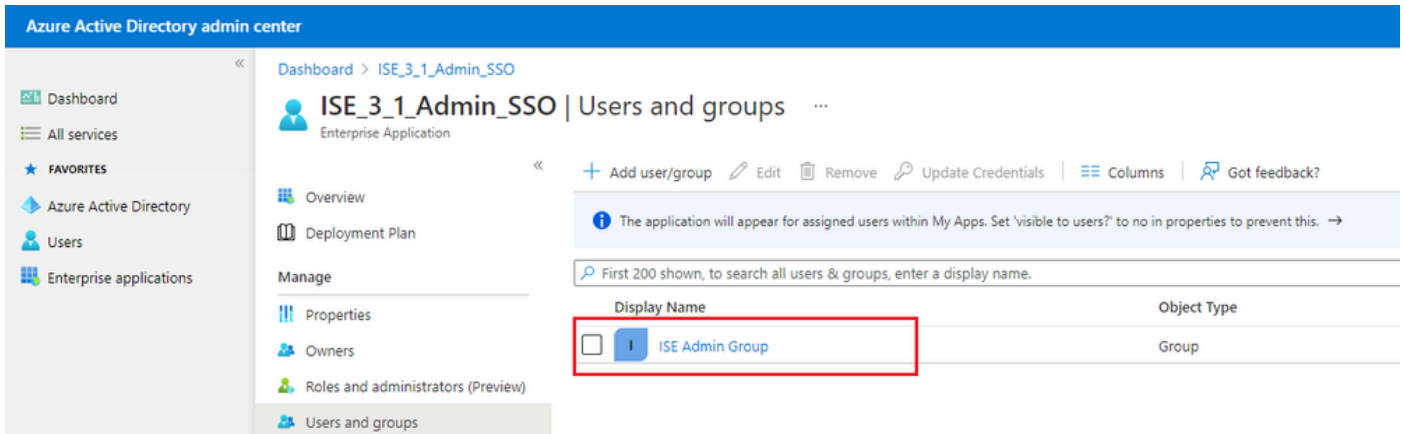
Users and groups



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エンタープライズアプリケーションの構成

アプリケーションに戻り、シングルサインオンの設定をクリックします。

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Properties

Name: ISE_3_1_Admin_SSO

Application ID: 76b82bcb-a918-4016-aad7-...

Object ID: 22aedf32-82c7-47f2-ab34-1...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

次の画面でSAMLを選択します。

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO

ISE_3_1_Admin_SSO | Single sign-on

Enterprise Application

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.


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

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating ISE30.

1


Basic SAML Configuration

 Edit

| | |
|--|-----------------|
| Identifier (Entity ID) | Required |
| Reply URL (Assertion Consumer Service URL) | Required |
| Sign on URL | <i>Optional</i> |
| Relay State | <i>Optional</i> |
| Logout Url | <i>Optional</i> |


2

User Attributes & Claims

 Edit

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

「サービスプロバイダー情報のエクスポート」の手順で取得したXMLファイルのentityIDの値を Identifier (エンティティID) に入力します。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。

Basic SAML Configuration



Save

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

ⓘ

ⓘ

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

ⓘ

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

7. Active Directoryグループ属性の設定

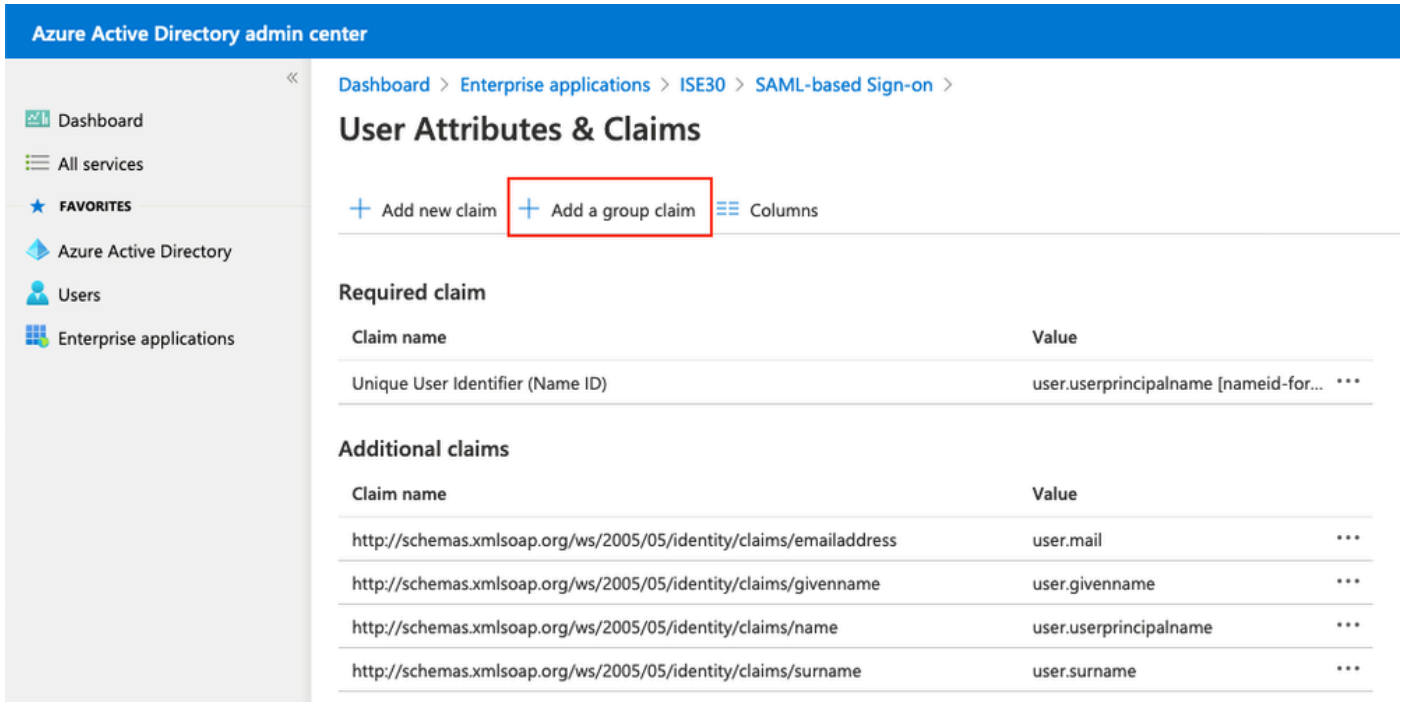
以前に設定したグループ属性値を返すには、User Attributes & Claimsの横にあるEditをクリックします。

User Attributes & Claims

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

 Edit

Add a group claimをクリックします。



Azure Active Directory admin center

Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

| Claim name | Value |
|----------------------------------|---|
| Unique User Identifier (Name ID) | user.userprincipalname [nameid-for... *** |

Additional claims

| Claim name | Value |
|--|----------------------------|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | user.mail *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | user.givenname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | user.userprincipalname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | user.surname *** |

Security groupsを選択して、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。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。

Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID



Advanced options

- Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

- Emit groups as role claims ⓘ

グループのクレーム名をメモします。この場合はGroupsです。

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

| Claim name | Value |
|----------------------------------|---|
| Unique User Identifier (Name ID) | user.userprincipalname [nameid-for... *** |

Additional claims

| Claim name | Value |
|--|----------------------------|
| Groups | user.groups *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | user.mail *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | user.givenname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | user.userprincipalname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | user.surname *** |

8. Azure フェデレーションメタデータXMLファイルのダウンロード

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。

SAML Signing Certificate Edit

| | |
|-----------------------------|---|
| Status | Active |
| Thumbprint | B24F48B47B350C93DE3D59EC87EE4C815C884462 |
| Expiration | 7/19/2024, 12:16:24 PM |
| Notification Email | chandandemo@outlook.com |
| App Federation Metadata Url | https://login.microsoftonline.com/182900ec-e960... |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

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。

External Identity Sources

- < 外部
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers
- Social Login

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups Attributes Advanced Settings

Identity Provider Configuration

Import Identity Provider Config File ⓘ

Provider Id

Single Sign On URL <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

Single Sign Out URL (Redirect) <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

Sianina Certificates

| Subject | Issuer | Valid From | Valid To (Expira... | Serial Number |
|--|----------------------|-----------------------|-------------------------|---------------------------|
| CN=Microsoft Azure Federated SSO Certificate | CN=Microsoft Azur... | Mon Jul 19 12:16:2... | Fri Jul 19 12:16:24 ... | 25 28 CB 30 8B A4 89 8... |

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。

External Identity Sources

- < 外部
- > Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- > SAML Id Providers

Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. **Groups** Attributes Advanced Settings

Groups

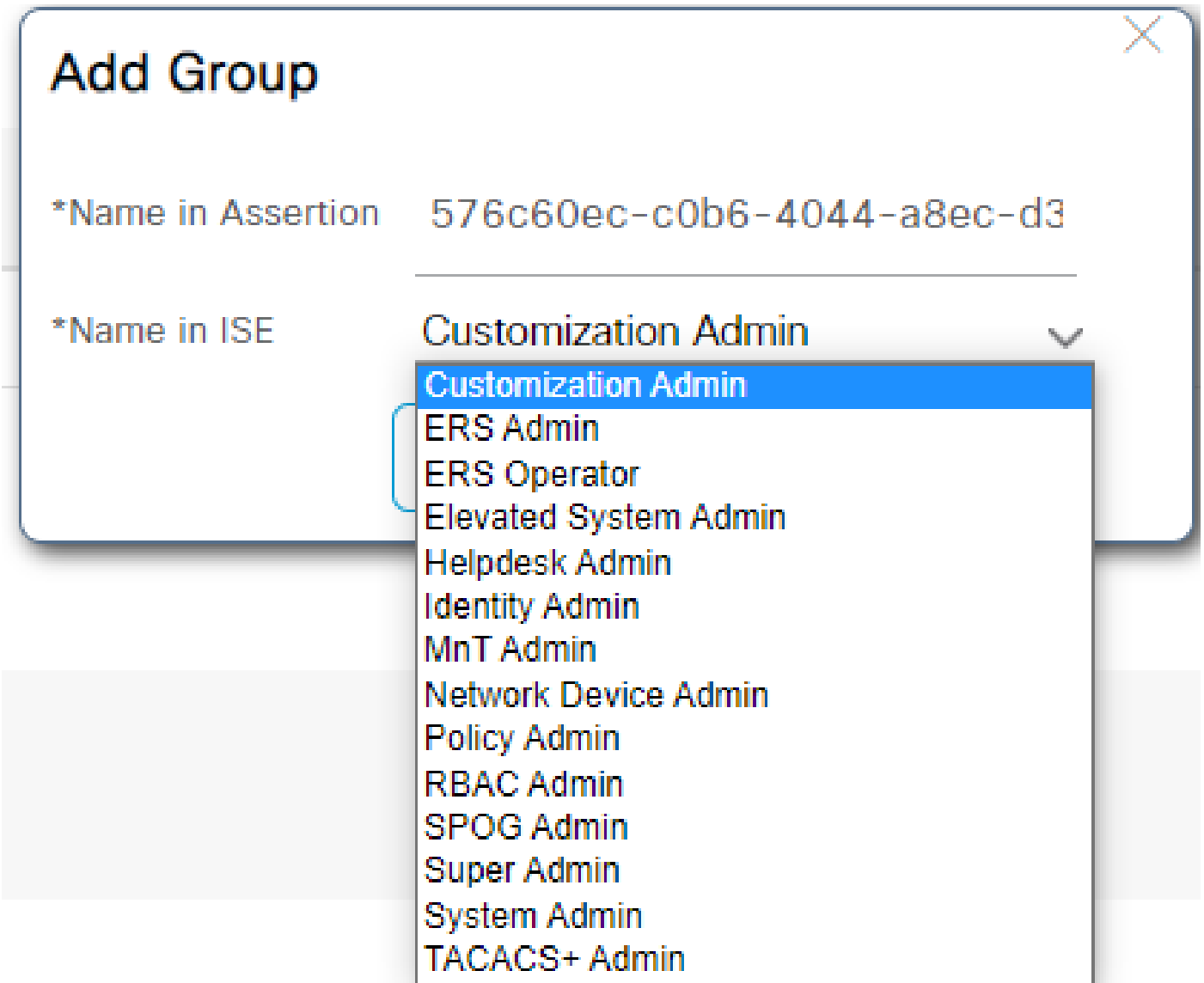
Group Membership Attribute ⓘ

Name in Assertion Name in ISE

[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。

ISEの名前をドロップダウンで設定し、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のグループ名の上にマッピングが作成されます。



(オプション) ステップ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の順に移動し、必要に応じて設定します。


次の図は、設定例のリファレンスです。

▼ RBAC Policies

| Rule Name | Admin Groups | Permissions |
|--|----------------------------|--|
| <input checked="" type="checkbox"/> Customization Admin Policy | If Customization Admin + | then Customization Admin Menu ... + Actions ▾ |
| <input checked="" type="checkbox"/> Elevated System Admin Poli | If Elevated System Admin + | then System Admin Menu Access... + Actions ▾ |
| <input checked="" type="checkbox"/> ERS Admin Policy | If ERS Admin + | then Super Admin Data Access + Actions ▾ |
| <input checked="" type="checkbox"/> ERS Operator Policy | If ERS Operator + | then Super Admin Data Access + Actions ▾ |
| <input checked="" type="checkbox"/> ERS Trustsec Policy | If ERS Trustsec + | then Super Admin Data Access + Actions ▾ |
| <input checked="" type="checkbox"/> Helpdesk Admin Policy | If Helpdesk Admin + | then Helpdesk Admin Menu Access + Actions ▾ |
| <input checked="" type="checkbox"/> Identity Admin Policy | If Identity Admin + | then Identity Admin Menu Access... + Actions ▾ |
| <input checked="" type="checkbox"/> MnT Admin Policy | If MnT Admin + | then MnT Admin Menu Access + Actions ▾ |
| <input checked="" type="checkbox"/> Network Device Policy | If Network Device Admin + | then Network Device Menu Acce... + Actions ▾ |
| <input checked="" type="checkbox"/> Policy Admin Policy | If Policy Admin + | then Policy Admin Menu Access ... + Actions ▾ |
| <input checked="" type="checkbox"/> RBAC Admin Policy | If RBAC Admin + | then RBAC Admin Menu Access ... + Actions ▾ |
| <input checked="" type="checkbox"/> Read Only Admin Policy | If Read Only Admin + | then Super Admin Menu Access ... + Actions ▾ |
| <input checked="" type="checkbox"/> SPOG Admin Policy | If SPOG Admin + | then Super Admin Data Access + Actions ▾ |
| <input checked="" type="checkbox"/> Super Admin Policy | If Super Admin + | then Super Admin Menu Access ... + Actions ▾ |
| <input checked="" type="checkbox"/> Super Admin_Azure | If Super Admin + | then Super Admin Menu Access ... + Actions ▾ |
| <input checked="" type="checkbox"/> System Admin Policy | If System Admin + | then System Admin Menu Access... + Actions ▾ |
| <input checked="" type="checkbox"/> 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。



Identity Services Engine

Intuitive network security

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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とパスワードを入力し、図に示すようにNextをクリックします。



Sign in

mck@gdplab2021.onmicrosoft.com

[Can't access your account?](#)

Next

3. ユーザのパスワードを入力し、Sign Inをクリックします。



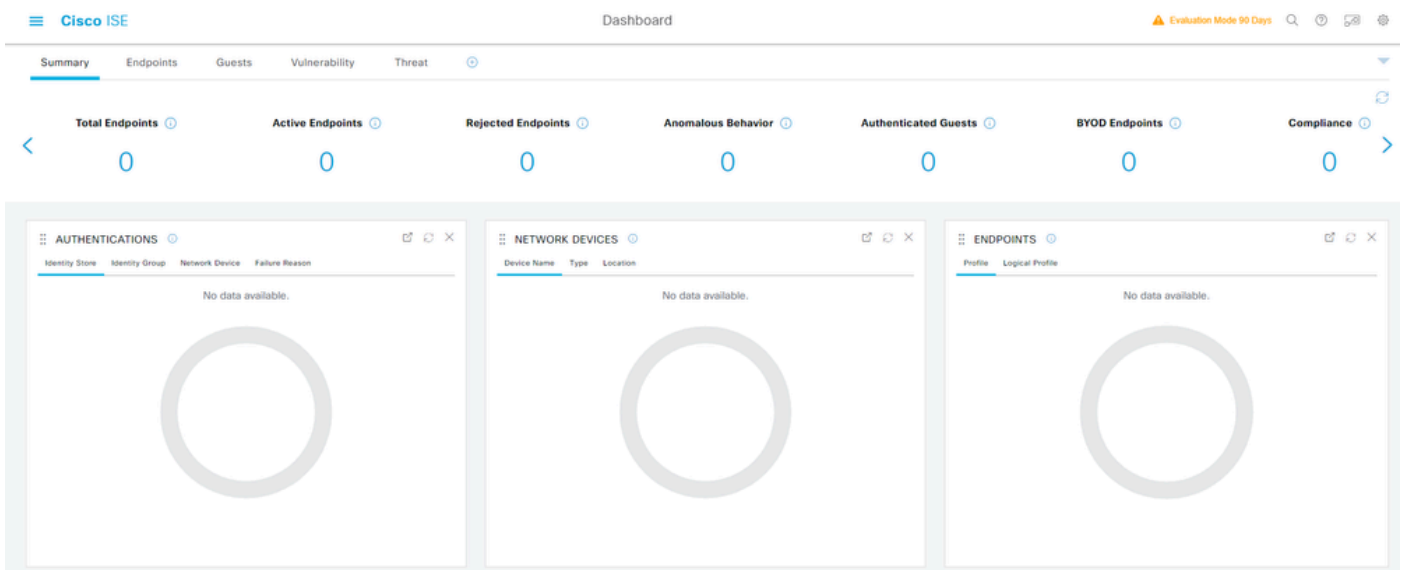
← mck@gdplab2021.onmicrosoft.com

Enter password

[Forgot my password](#)

Sign in

4. 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ことが重要です。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せん。

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、この時点でのプロセスはまだIdP(Azure)で維持されています。

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。



← mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, [reset it now.](#)

Password

[Forgot my password](#)

Sign in

問題2：ユーザは、SAML SSOへのアクセスが許可されるグループに属していません。前のケースと同様に、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)で処理されます。

これを修正するには、次の図に示すように、Add group to the Application設定手順が正しく実行さ

れていることを確認します。



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ×

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

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、アイデンティティプロバイダーのAzureから開始された場合に発生します。ISEはIdentity Providerが開始したSAML要求をサポートしていないため、Azure ADからのSSOログインのテストは機能しません。



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO >

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Upload metadata file Change single sign-on mode Test this application

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Groups | user.groups |
| Unique User Identifier | user.userprincipalname |

3

SAML Signing Certificate

| | |
|-----------------------------|---|
| Status | Active |
| Thumbprint | 824F48B478350C93DE3D59EC87EE4C8 |
| Expiration | 7/19/2024, 12:16:24 PM |
| Notification Email | chandandemo@outlook.com |
| App Federation Metadata Url | https://login.microsoftonline.com/182900ec-e99d-44b3-b951-44c84e11d749/... |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

4

Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

| | |
|---------------------|---|
| Login URL | https://login.microsoftonline.com/182900ec-e99d-44b3-b951-44c84e11d749/... |
| Azure AD Identifier | https://sts.windows.net/182900ec-e99d-44b3-b951-44c84e11d749/ |
| Logout URL | https://login.microsoftonline.com/182900ec-e99d-44b3-b951-44c84e11d749/... |

[View step-by-step instructions](#)

5

Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up.

Please make sure you have configured ISE_3_1_Admin_SSO before testing.

[Sign in as current user](#)

[Sign in as someone else](#) (requires browser extension)

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

```
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: Saa879f5-68f1-482a-a405-f993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXXX
```

[Get resolution guidance](#)

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。

これを修正するには、AzureとISEの[SAML IDプロバイダーグループ]タブのグループの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」セクションの手順2.7.および4.を参照してください。



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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に関するログ

フロー実行時に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を短縮しました。

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


-:::- 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.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.ws.message.decode

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: [https://schemas.xmlsoap.org/ws/2005/05/identity/](#)

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

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

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.SAML

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.SAML

4. グループ属性が値576c60ec-c0b6-4044-a8ec-d395b1475d6e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.sam].framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.impl.SAM
    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.sam].framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
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.sam].framework.validate
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.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.sam].framework.validate
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 samUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool50] [] com.cisco.ise.util.RBACUtil -:::- Populating cache
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 save

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。