WideAngle AI Advisor

導入・連携設定ガイド

2026 年 11 月 11 日

NTT ドコモビジネス株式会社

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

目次

1. はじめに ... 3

1.1. 本書の目的 ... 3

1.2. 用語の定義 ... 3

1.3. 実施する章の確認 ... 3

2. Microsoft Sentinel の環境情報確認 ... 4

2.1. 前提条件と事前準備 ... 4

2.2. Microsoft Sentinel 環境情報の確認 ... 4

3. AI Advisor 用アプリの作成 ... 5

3.1. 前提条件と事前準備 ... 5

3.2. アプリの登録 ... 5

3.3. アプリ認証用クライアントシークレットの作成 ... 8

3.4. AI Advisor アプリへのアクセス許可付与 ... 11

3.4.1. Microsoft Graph へのアクセス許可追加 ... 11

3.4.2. WindowsDefenderATP のアクセス許可を追加する ... 13

3.4.3. Log Analytics API のアクセス許可を追加する ... 15

3.4.4. 管理者の同意の付与 ... 16

4. AI Advisor 用アプリへの Microsoft Sentinel アクセス権限の付与 ... 18

4.1. 前提条件と事前準備 ... 18

4.2. Microsoft Sentinel ロールの割り当て ... 18

5. Microsoft Entra ID との連携設定 ... 22

5.1. 前提条件と事前準備 ... 22

5.2. エンタープライズアプリケーションの登録 ... 23

5.3. SAML によるシングルサインオンのセットアップ ... 25

5.4. 識別情報および証明書の取得 ... 27

5.5. サインインの確認 ... 29

5.6. サインイン時にエラーコード「AADSTS50105」が表示された場合の対応 ... 31

5.6.1. ユーザーの割り当てを不要にする ... 31

5.6.2. ユーザーまたはグループを割り当てる ... 32

改訂履歴 ... 35

記載されている会社名や製品名は、各社の商標または登録商標です。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

1. はじめに

1.1. 本書の目的

本書は、WideAngle AI Advisor(以下、AI Advisor)の導入および利用開始に必要な環境確認と各種連携設定について説明するものです。本書の記載内容は、予告なく変更する場合があります。

1.2. 用語の定義

本サービスで使用する用語は以下の通りです。

用語	定義
NTT ドコモビジネス	NTT ドコモビジネス株式会社の略称
Microsoft Sentinel	Microsoft が提供する、セキュリティに関するログの収集、監視、検知、分析などを行うクラウドサービス
マネージド SOAR	NTT ドコモビジネスが提供するセキュリティインシデント対応の自動化サービス
Microsoft Graph (API)	Microsoft 365 のユーザー、メール、ファイルなどのデータを取得・操作するための API
WindowsDefenderATP (API)	Microsoft Defender for Endpoint の端末・脅威情報を取得し、対応操作を自動化するための API
Log Analytics API	Log Analytics ワークスペースに保存されたログを検索･参照するための API
SAML 連携	Microsoft Entra ID を認証基盤として、SAML 規格により外部サービスへのシングルサインオン（SSO）を実現する連携方式

1.3. 実施する章の確認

本書に記載する手順は、ご利用になる機能によって実施対象が異なります。以下を確認し、対象となる章の手順を実施してください。

※複数の機能を利用する場合は、該当するすべての章を実施してください。

利用する機能	実施する章
Microsoft Sentinel との連携※1	第 2 章、第 3 章、第 4 章
Microsoft Entra ID による SAML 認証	第 5 章

※1 AI SOC(WideAngle マネージド SOAR 連携)を利用する場合も、Microsoft Sentinel との連携が必要となるため、第 2 章から第 4 章の手順を実施してください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

2. Microsoft Sentinel の環境情報確認

実施対象：Microsoft Sentinel との連携を利用するお客さま

本章では、AI Advisor から Microsoft Sentinel のログを参照するために、対象となる Microsoft Sentinel / Log Analytics Workspace の情報を確認します。

2.1. 前提条件と事前準備

- Azure Portal にサインインできるアカウントを使用できること。
- AI Advisor との連携対象となる Microsoft Sentinel / Log Analytics Workspace が用意されていること。
- 確認した情報を記入するための「WideAngle AI Advisor ヒアリングシート」が用意されていること。

2.2. Microsoft Sentinel 環境情報の確認

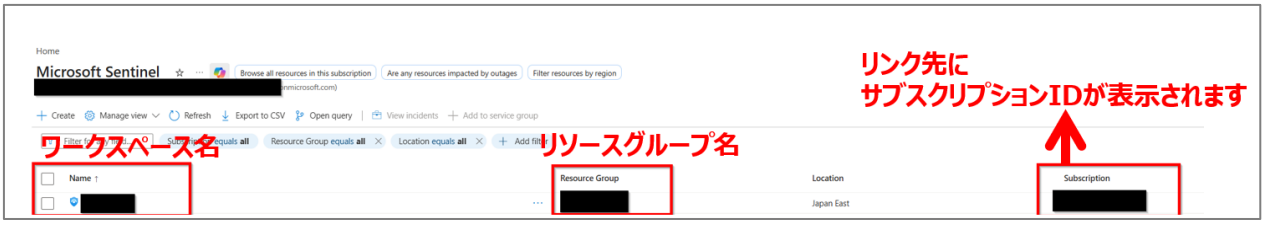
(1) Azure Portal の URL にアクセスしてログインします。

Azure Portal：https://portal.azure.com

(2) Azure Portal の検索バーから「Sentinel」を入力して検索します。

(3) Microsoft Sentinel を開き、以下の情報を確認し、「WideAngle AI Advisor ヒアリングシート」>「ヒアリングシート」 >「インシデントダッシュボード設定」に記入してください。

- サブスクリプション ID
- リソースグループ名
- ワークスペース名



※複数のワークスペースが表示される場合は、AI Advisor の連携対象となるワークスペースの情報を記入してください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. AI Advisor 用アプリの作成

実施対象：Microsoft Sentinel との連携を利用するお客さま

本章では、AI Advisor が Microsoft Sentinel などに保存されたインシデント情報やログを参照するために、Microsoft Entra ID に AI Advisor 用アプリを登録します。あわせて、アプリ認証に使用するクライアントシークレットを作成し、必要な API アクセス許可を付与します。

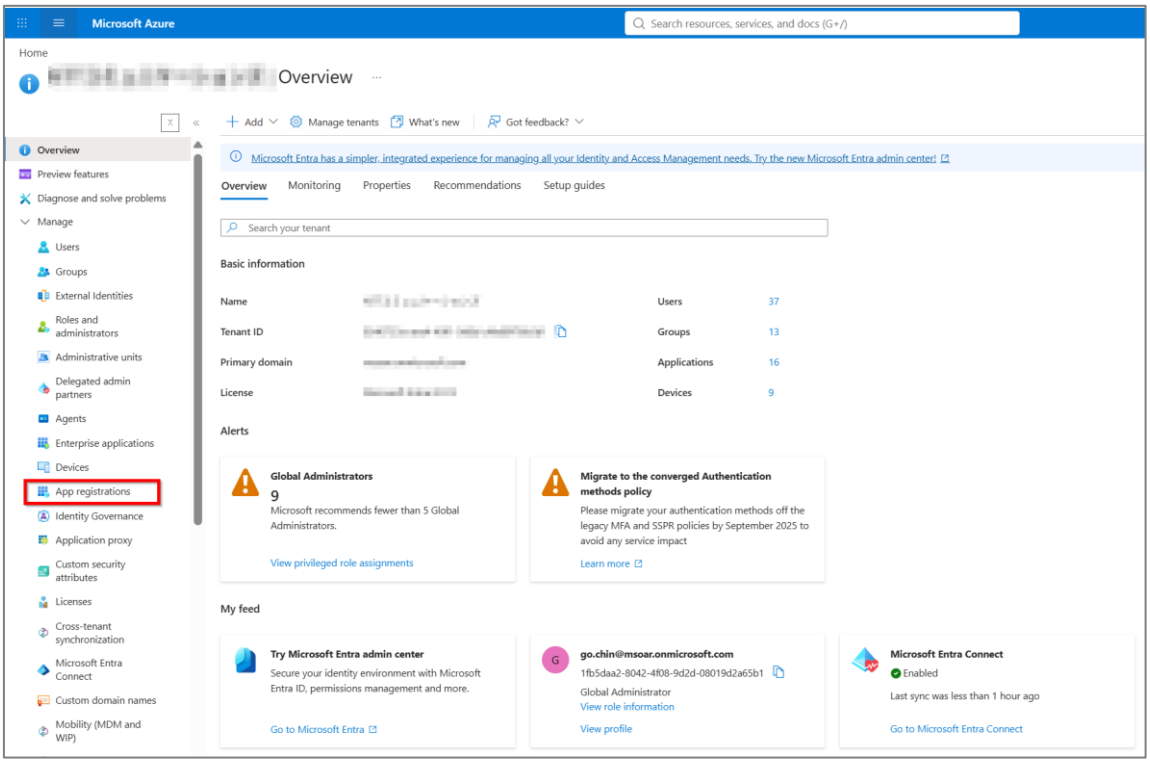
3.1. 前提条件と事前準備

- AI Advisor 用アプリを登録する Microsoft Entra ID テナントが特定されており、作業実施者が作業対象のテナントにサインインできること。
- 作業実施者が Microsoft Azure テナントにおいて、ユーザー登録/ロール割り当て権限のあるアカウントであること。
- 確認した情報を記入するための「WideAngle AI Advisor ヒアリングシート」が用意されていること。

3.2. アプリの登録

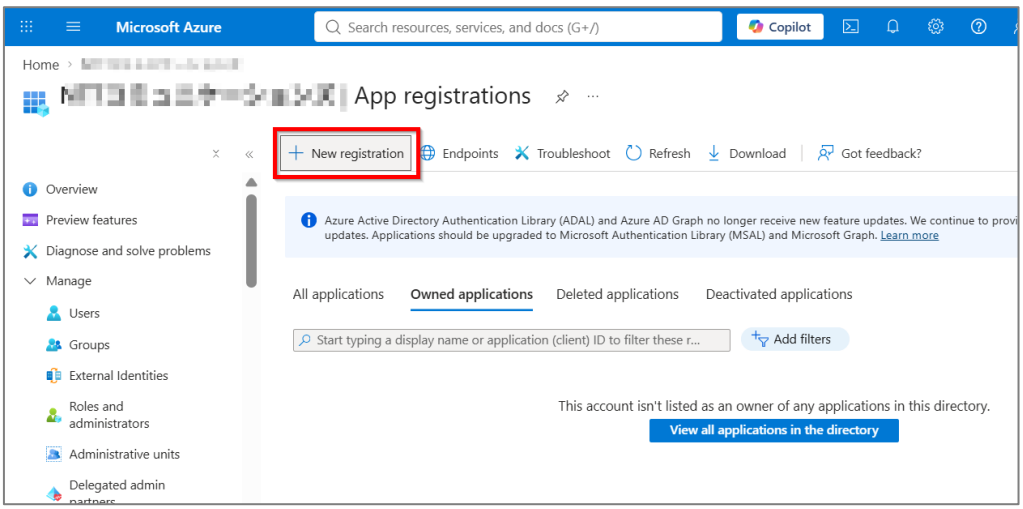
(1) Azure Portal で Microsoft Entra ID を開きます。

(2) 左メニューから 「App registrations」 を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

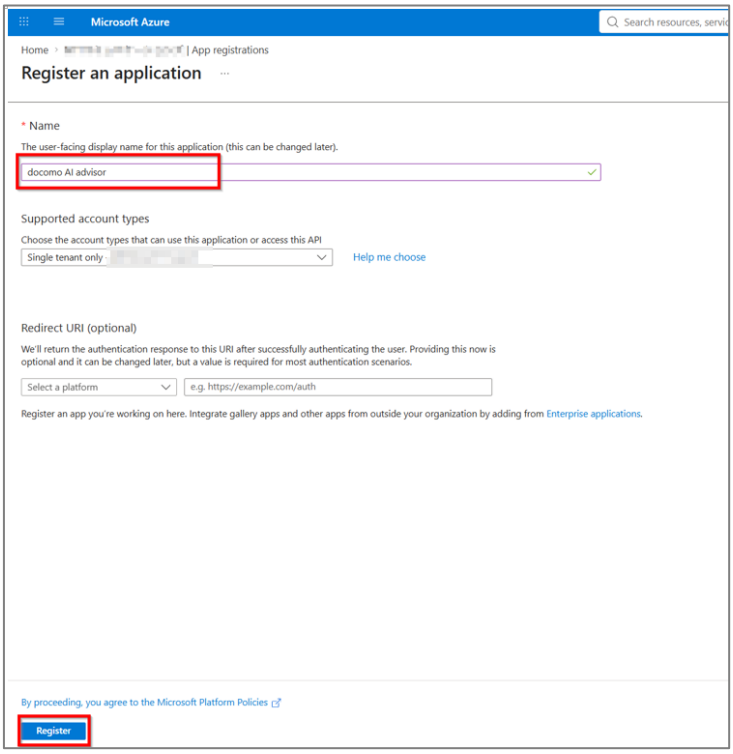
(3) 画面上部の「＋ New registration」を選択します。



(4) 「Name」にアプリ名を入力し、登録をクリックします。

※ アプリ名には、必ず「AI advisor」という文言を含めてください。

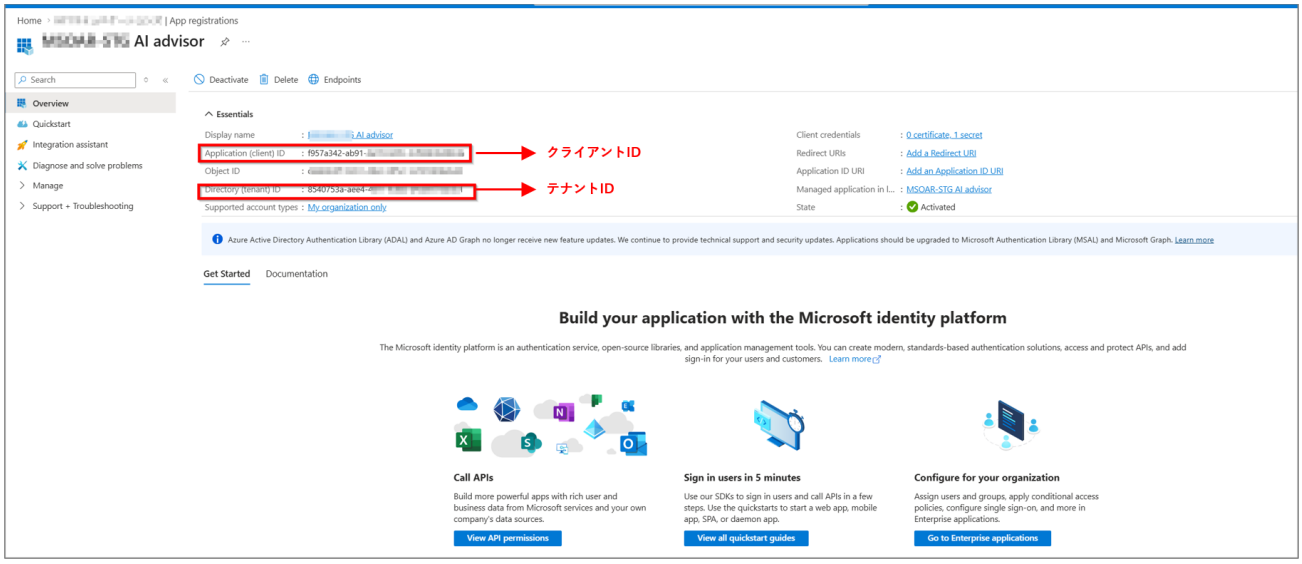
例：AI advisor、docomo AI advisor



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(5) 登録したアプリの「Overview」画面を開き、以下の情報を確認します。確認した情報は、「WideAngle AI Advisor ヒアリングシート」の「ヒアリングシート」シートにある「インシデントダッシュボード設定」欄に記入してください。

- テナント ID
- クライアント ID



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

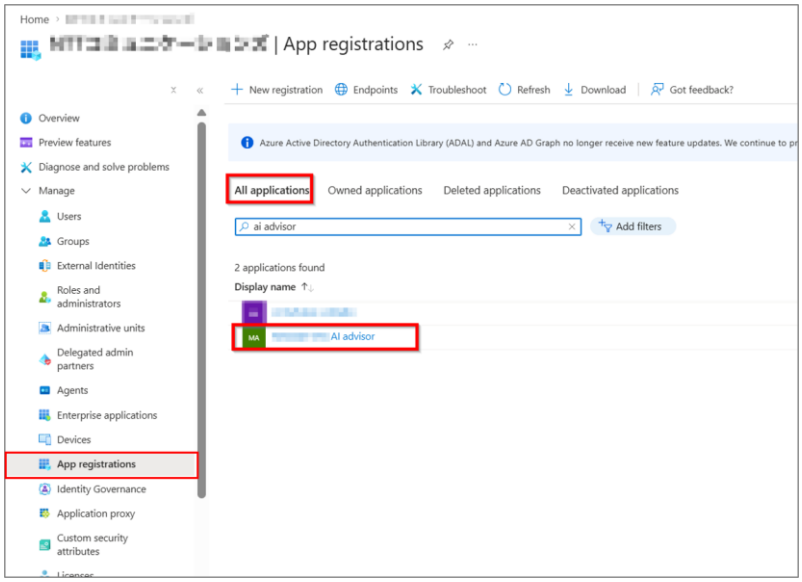
3.3. アプリ認証用クライアントシークレットの作成

第 3.2.章で登録した AI Advisor 用アプリに対して、認証情報(クライアントシークレット）を作成します。

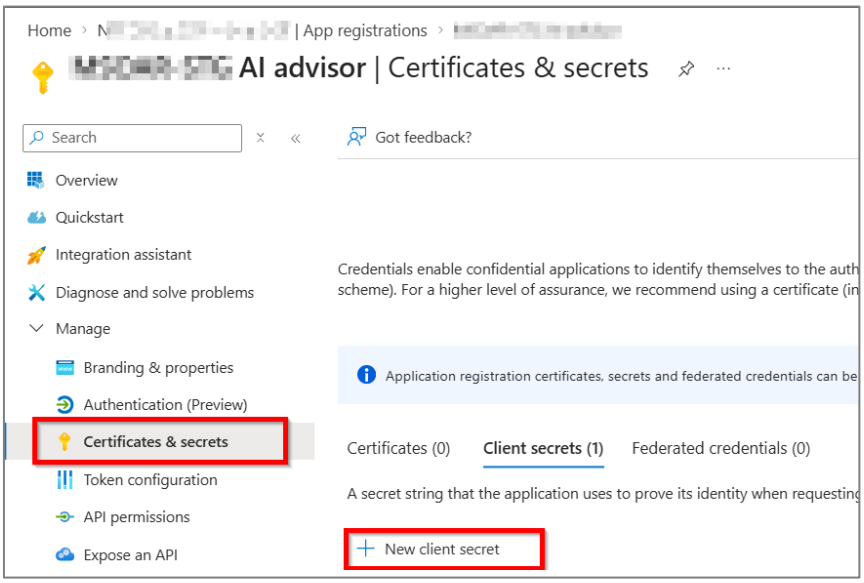
(1) Azure Portal で Microsoft Entra ID を開きます。

(2) 左メニューから 「App registrations」 を選択します。

(3) 「All applications」タブから第 3.2.章で登録したアプリを選択します。



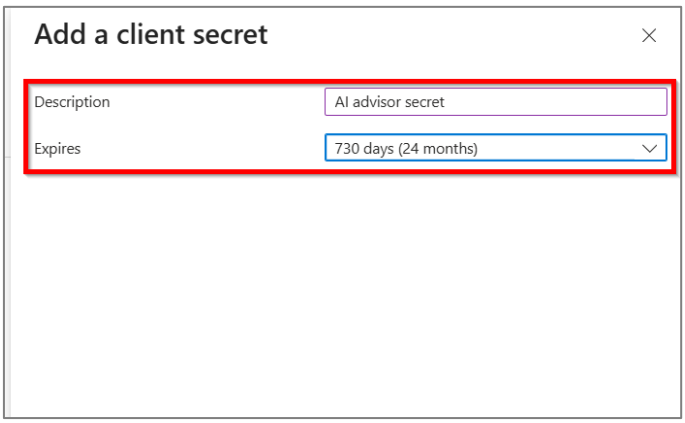
(4) 左メニューから「Certificates & secret」を選択し、「Client secrets」タブで、「＋New client secret」を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(5) 作成するクライアントシークレットの説明を「Description」に入力し、「Expires」で有効期限を選択します。

※有効期限は「730 日(24 か月)」を推奨します。

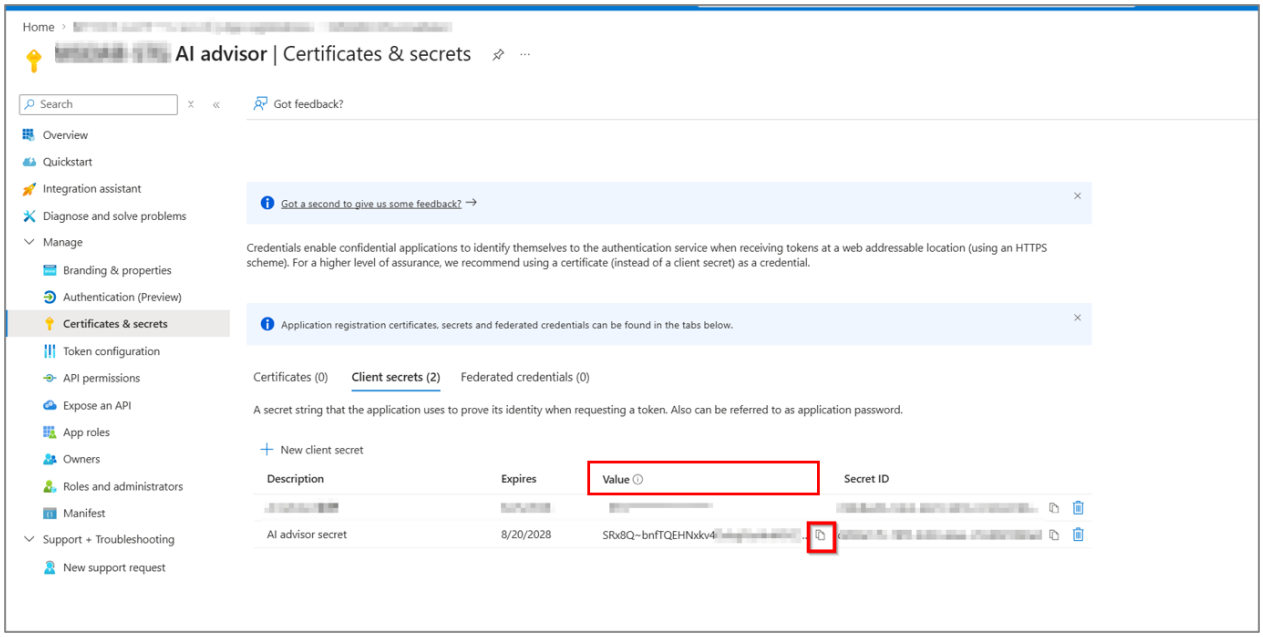


(6) 入力内容を確認後、「Add」を選択し、クライアントシークレットを作成します。

(7) 作成後に表示されるクライアントシークレット(シークレット値)を「WideAngle AI Advisor ヒアリングシート」の「ヒアリングシート」シートにある「インシデントダッシュボード設定」欄に記入してください。

※シークレット値は作成直後のみ表示され、画面を移動すると再表示できません。表示されたシークレット値を、この画面で必ずヒアリングシートに記入してください。

※ 控える対象は 「シークレット ID(Secret ID)」ではなく**「シークレット値(Value)」** です。



(8) クライアントシークレットの期限(Expires) を「WideAngle AI Advisor ヒアリングシート」の「ヒアリングシート」シートにある「インシデントダッシュボード設定」欄に記入してください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

クライアントシークレットの更新

クライアントシークレットには有効期限があります。有効期限を迎える前に、本章に記載する手順に従って、新しいクライアントシークレットを作成してください。

作成後、新しいクライアントシークレットのシークレット値および有効期限を、「WideAngle AI Advisor ヒアリングシート」>「ヒアリングシート」シート>「インシデントダッシュボード設定」欄に記入してください。

シークレット値および有効期限を更新したヒアリングシートは、弊社担当者がご案内する方法で提出してください。

現在使用しているヒアリングシートが不明な場合は、弊社担当者までお問い合わせください。

※新しいクライアントシークレットのシークレット値を弊社が受領後、原則 1 か月以内の営業時間外に、新しいクライアントシークレットへの切り替えを実施します。

切り替え作業中も、AI Advisor によるインシデント分析は継続して実施されます。また、WideAngle マネージド SOAR の自動対処にも影響はありません。

※弊社における新しいクライアントシークレットへの切り替えが完了するまで、現在使用しているクライアントシークレットは削除しないでください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.4. AI Advisor アプリへのアクセス許可付与

第 3.2.章で登録した AI Advisor 用アプリに、以下の API アクセス許可を追加します。追加対象となる API アクセス許可およびアクセス許可の種類は、以下のとおりです。
※以下の API アクセス許可は、AI Advisor の利用に必要です。お客さま環境における各製品の利用状況にかかわらず、すべて追加してください。

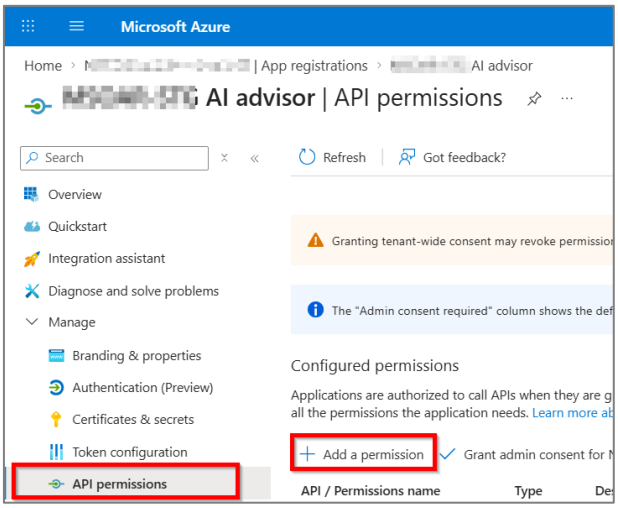
API	追加するアクセス許可	アクセス許可の種類	利用目的
Microsoft Graph	ThreatHunting.Read.All	アプリケーションのアクセス許可	AI Advisor がログを分析する際に、Sentinel 上のログだけでは情報が不足する場合、Defender XDR から追加のログ・証跡情報を取得するために使用します。
WindowsDefenderATP	AdvancedQuery.Read.All	アプリケーションのアクセス許可	AI Advisor がログを分析する際に、Sentinel 上のログだけでは端末に関する情報が不足する場合、Microsoft Defender for Endpoint から追加のログ・証跡情報を取得するために使用します。
Log Analytics API	Data.Read	アプリケーションのアクセス許可	Sentinel 上で利用するログは Log Analytics Workspace 上に保存されているため、AI Advisor が当該ログを参照するために使用します。

3.4.1. Microsoft Graph へのアクセス許可追加

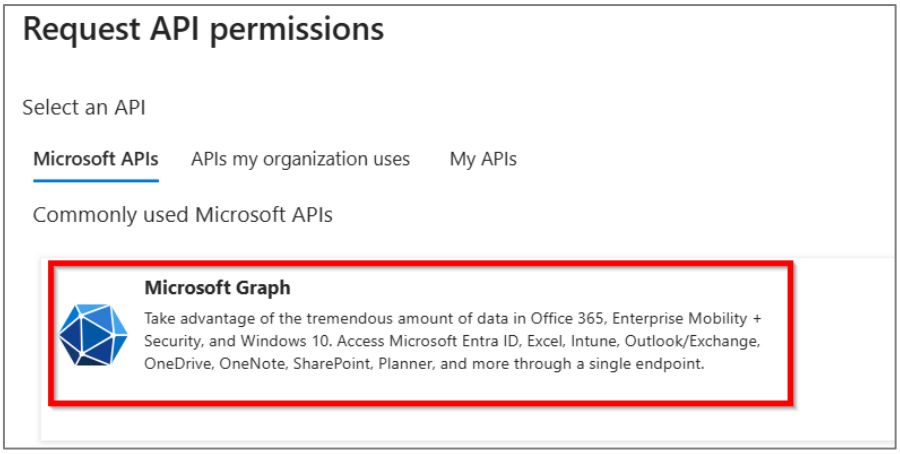
(1) Azure Portal で Microsoft Entra ID を開き、左メニューから「App registrations」を選択し、第 3.2.章で登録したアプリを選択します。
(2) 「All applications」タブから、第 3.2.章で登録したアプリを選択します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

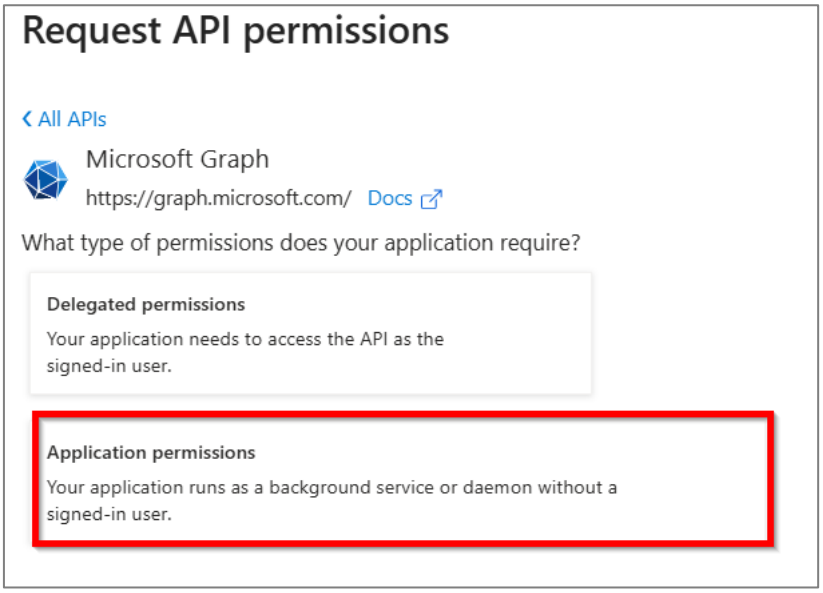
(3) 左メニューから 「API permissions」 を選択し、画面上部の 「＋ Add a permission」を選択します。



(4) 「Microsoft APIs」>「Microsoft Graph」 を選択します。



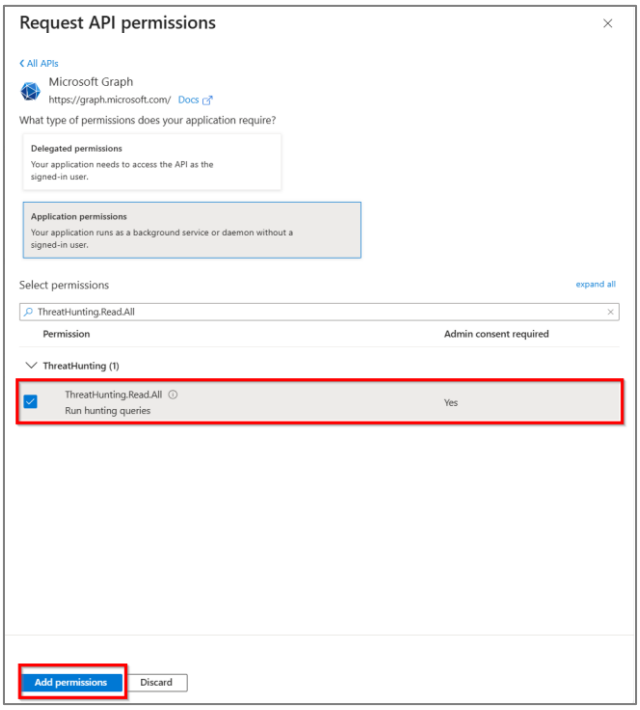
(5) 「Application permissions」 を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(6) 「ThreatHunting.Read.All」を検索し、チェックを入れます。

(7) 「Add permissions」 を選択します。

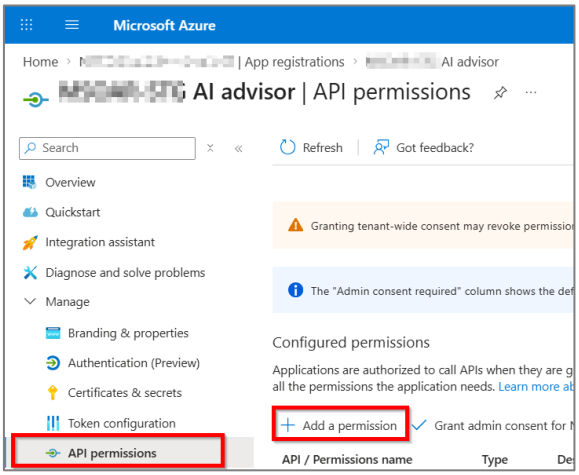


3.4.2. WindowsDefenderATP のアクセス許可を追加する

(1) Azure Portal で Microsoft Entra ID を開き、左メニューから「App registrations」 を選択し、第 3.2.章で登録したアプリを選択します。

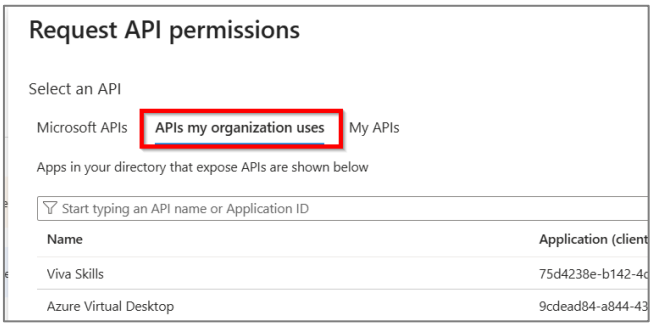
(2) 「All applications」タブから、第 3.2.章で登録したアプリを選択します。

(3) 左メニューから 「API permissions」 を選択し、画面上部の 「＋ Add a permission」を選択します。



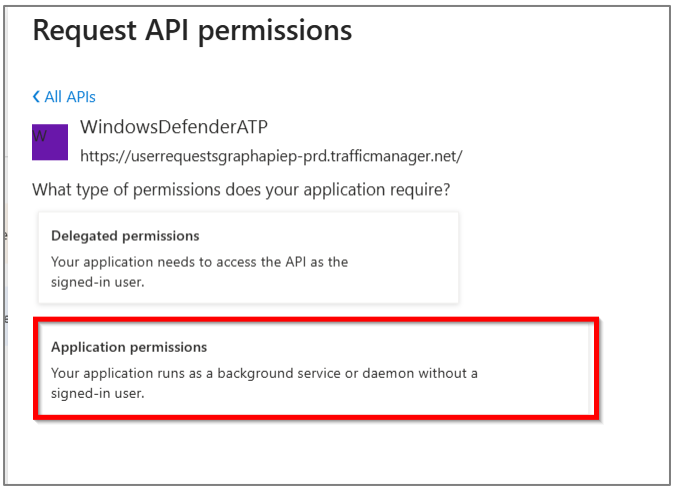
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(4) 「APIs my organization uses」 を選択します。



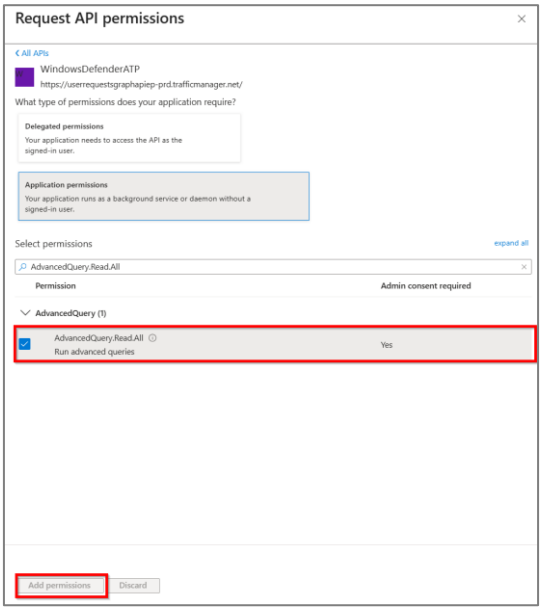
(5) 検索欄に「WindowsDefenderATP」と入力し、該当する API を選択します。

(6) 「Application permissions」 を選択します。



(7) 「AdvancedQuery.Read.All」を検索し、チェックを入れます。

(8) 「Add permissions」 を選択します。



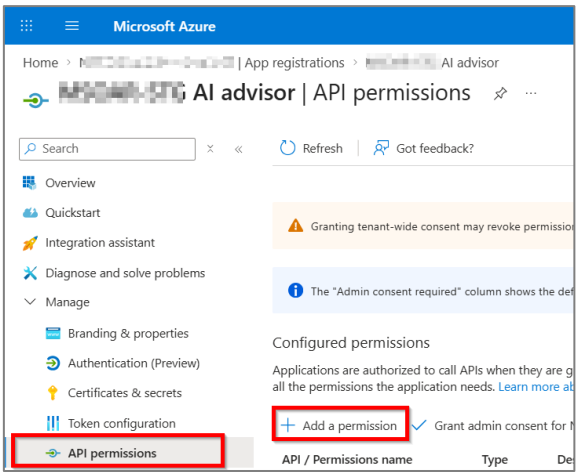
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.4.3. Log Analytics API のアクセス許可を追加する

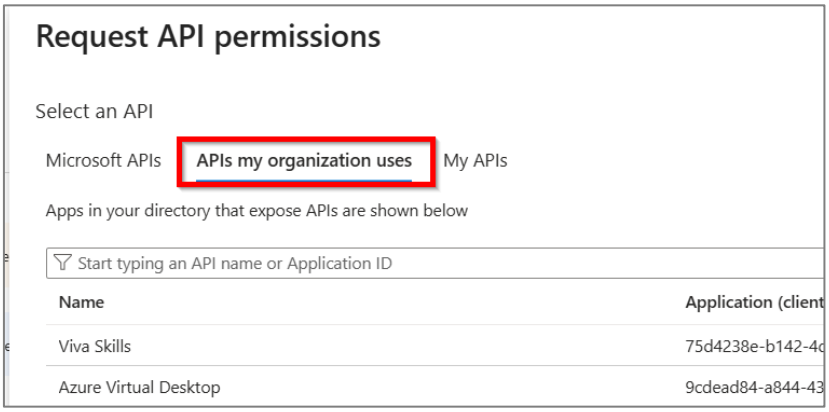
(1) Azure Portal で Microsoft Entra ID を開き、左メニューから「App registrations」 を選択し、第 3.2.章で登録したアプリを選択します。

(2) 「All applications」タブから、第 3.2.章で登録したアプリを選択します。

(3) 左メニューから 「API permissions」 を選択し、画面上部の 「＋ Add a permission」を選択します。



(4) 「APIs my organization uses」 を選択します。



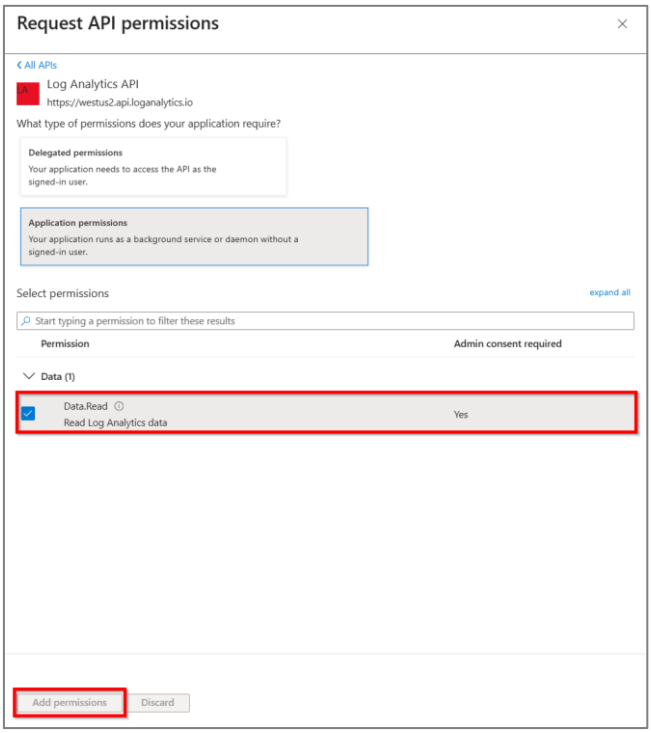
(5) 検索欄に「Log Analytics API」と入力し、該当する API を選択します。

(6) 「Application permissions」 を選択します。

(7) 「Data.Read」を検索し、チェックを入れます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(8) 「Add permissions」 を選択します。

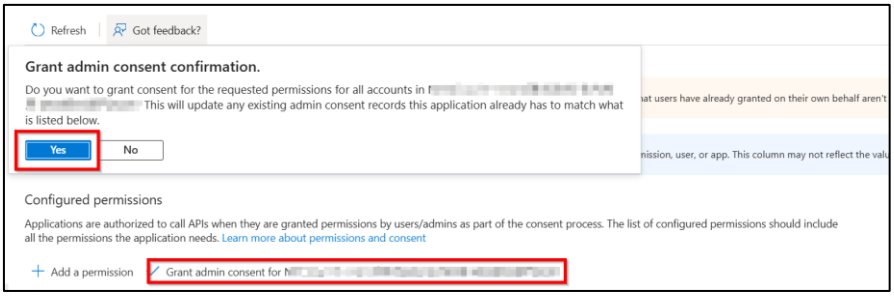


3.4.4. 管理者の同意の付与

第 3.4.1.章から第 3.4.3.章で API アクセス許可を追加した後、管理者の同意を付与します。

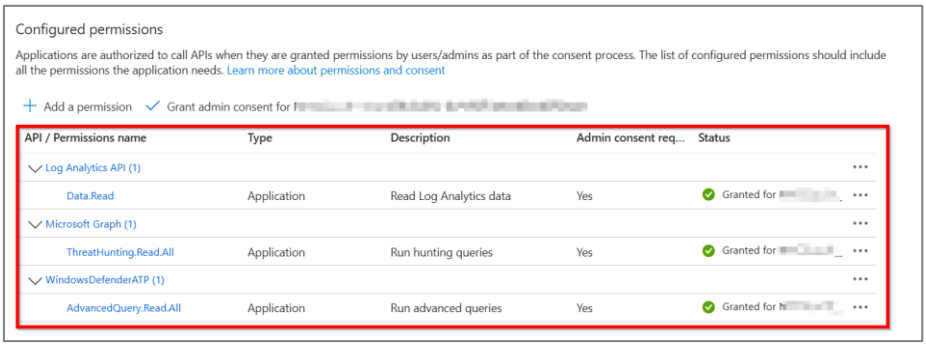
(1) 「API のアクセス許可」 画面上部の 「Grant admin consent for <テナント名> （管理者の同意を与えます)」 を選択します。

(2) 管理者の同意確認画面で 「Yes」 を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(3) 追加したアクセス許可の状態欄に、緑色のチェックが表示されていることを確認します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

4. AI Advisor 用アプリへの Microsoft Sentinel アクセス権限の付与

実施対象：Microsoft Sentinel との連携を利用するお客さま

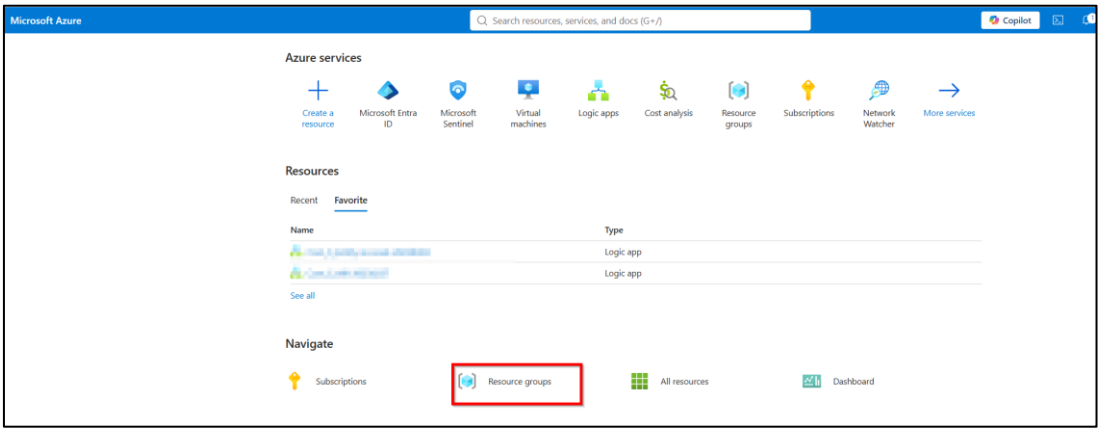
第 3.2.章で登録した AI Advisor 用アプリに Microsoft Sentinel へのアクセス権限を付与するため、連携対象のリソースグループに対して「Microsoft Sentinel Responder」ロールを割り当てます。

4.1. 前提条件と事前準備

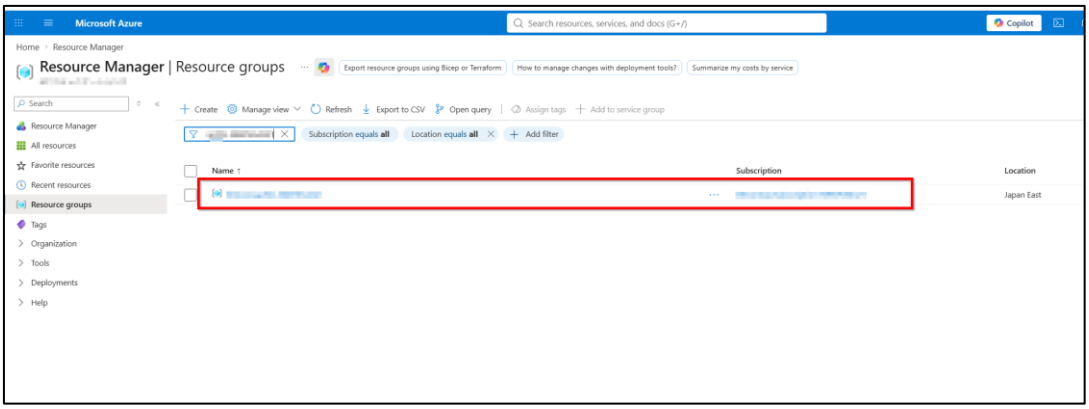
- 第 2.2.章の手順により、連携対象のリソースグループを確認していること。
- 第 3.2.章の手順により、AI Advisor 用アプリを登録していること。
- 作業実施者が、対象のリソースグループにロールを割り当てるために必要な権限を持っていること。

4.2. Microsoft Sentinel ロールの割り当て

(1) Azure Portal で 「Resource groups」 を開きます。

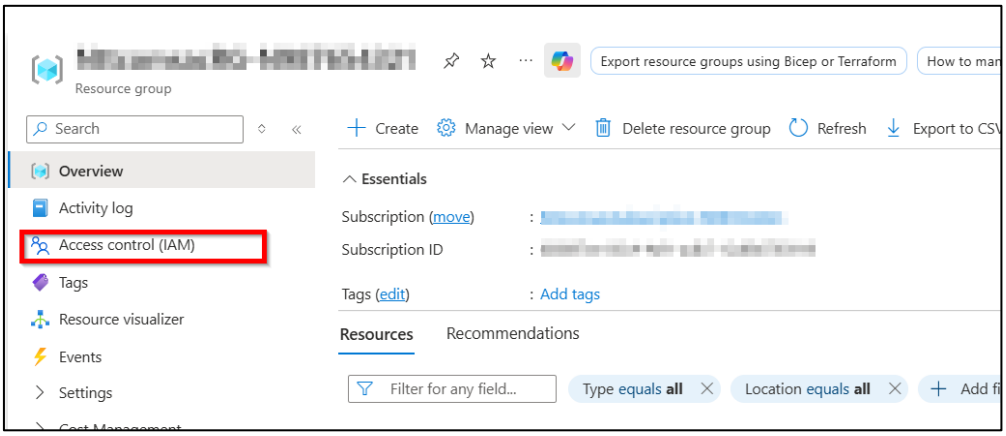


(2) 第 2.2.章で確認した、AI Advisor との連携対象となるリソースグループを選択します。

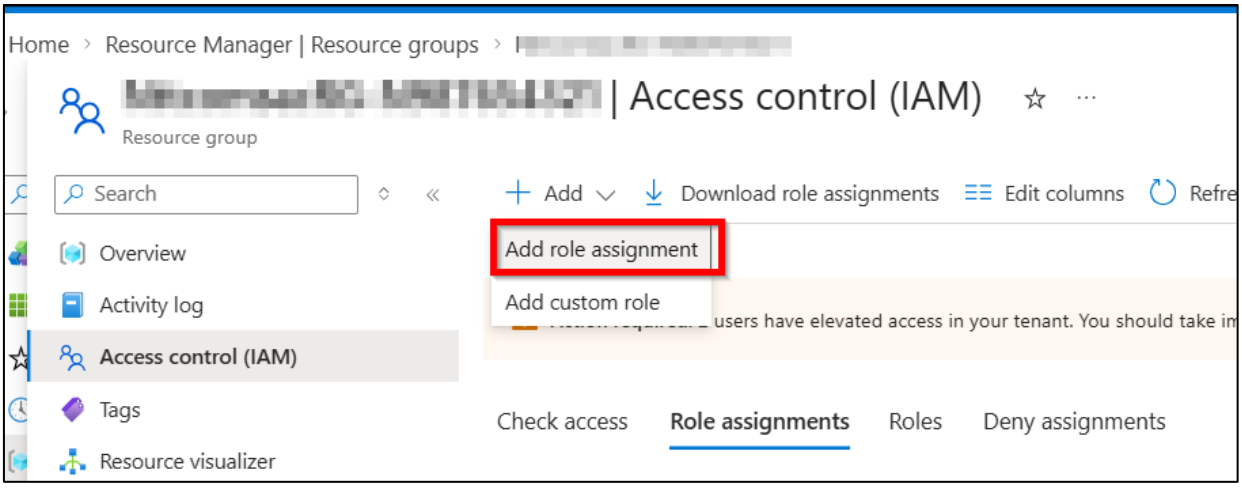


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

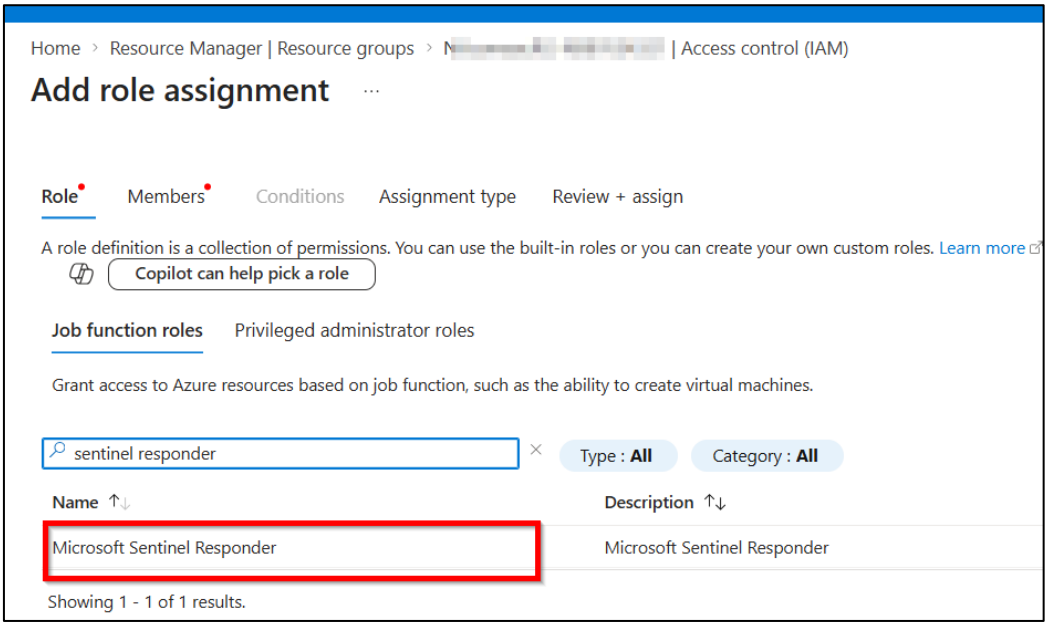
(3) 左メニューから「Access control(IAM)」を選択します。



(4) 画面上部の 「＋ Add」 を選択し、「Add role assignment」 を選択します。

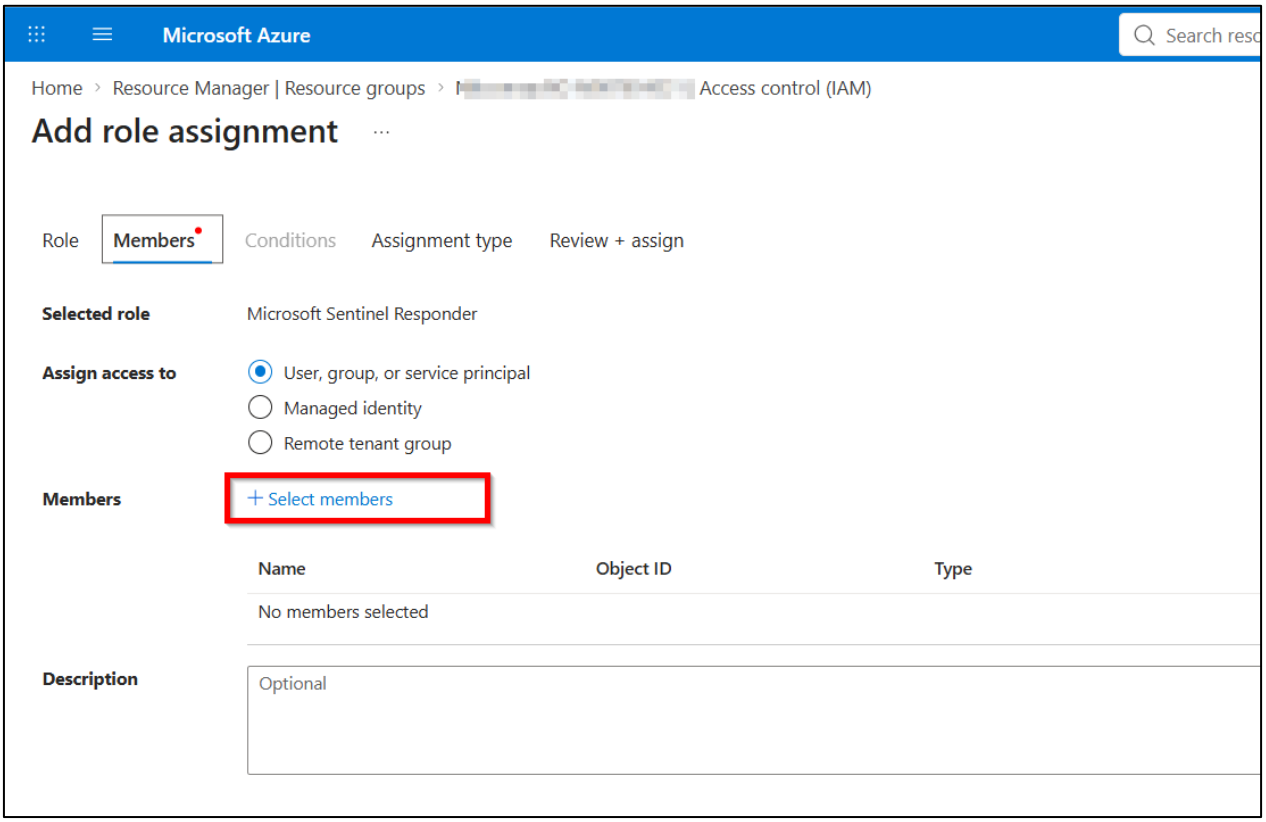


(5) ロールの検索欄に「Microsoft Sentinel Responder」と入力し、検索結果に表示された「Microsoft Sentinel Responder」を選択して、「Next」を選択します

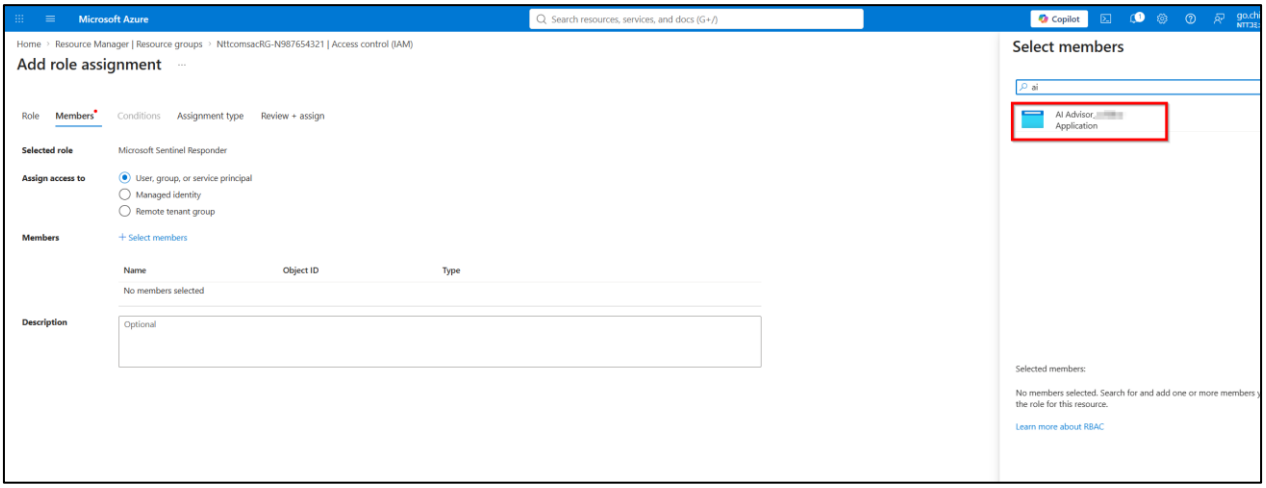


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(6) 「Members」画面で「＋ Select members」を選択します。



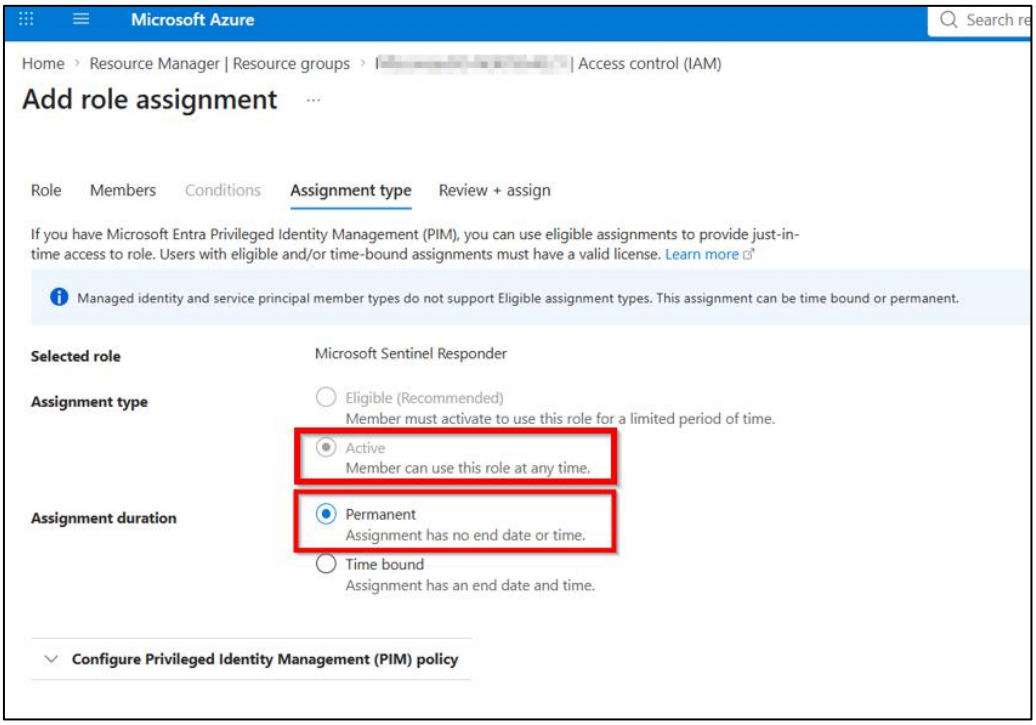
(7) 第 3.2 章で登録した AI Advisor 用アプリ名を検索し、対象のアプリを選択します。



(8) 「Next」 を選択し、内容を確認します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(9) 「Assignment type」では「Active」を選択し、「Assignment duration」では「Permanent」を選択します。



(10)「Review + assign」 を選択します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. Microsoft Entra ID との連携設定

実施対象：Microsoft Entra ID による SAML 認証を利用するお客さま

本章では、AI Advisor ポータルの認証方式として、Microsoft Entra ID を利用した SAML 連携を行うための設定手順について説明します。

5.1. 前提条件と事前準備

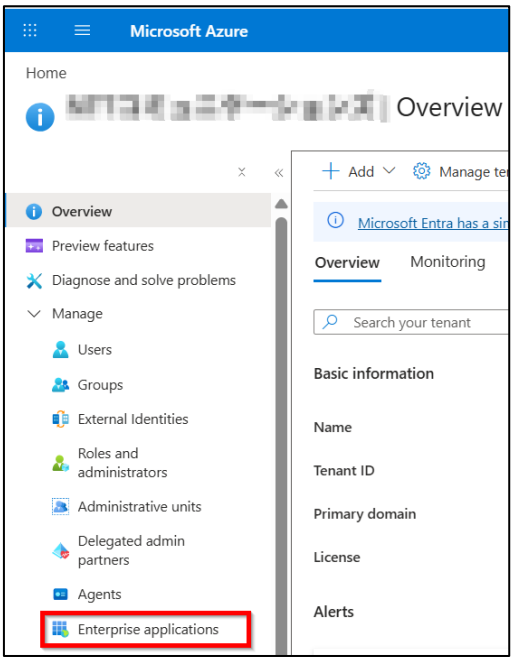
本章の手順を実施する前に、以下を確認してください。

- AI Advisor ポータルの認証方式として、Microsoft Entra ID による SAML 認証を利用すること。
- 作業対象の Microsoft Entra ID テナントが特定されていること。
- 作業実施者に、Microsoft Entra ID でエンタープライズアプリケーションの登録、SAML 設定、プロパティ変更、ならびにユーザーまたはグループの割り当てを行うために必要な権限が付与されていること。
- 弊社から SAML 連携に必要な「識別子（エンティティ ID）」および「応答 URL（Assertion Consumer Service URL）」を受領していること。
- 確認した情報を記入するための「WideAngle AI Advisor ヒアリングシート」が用意されていること。

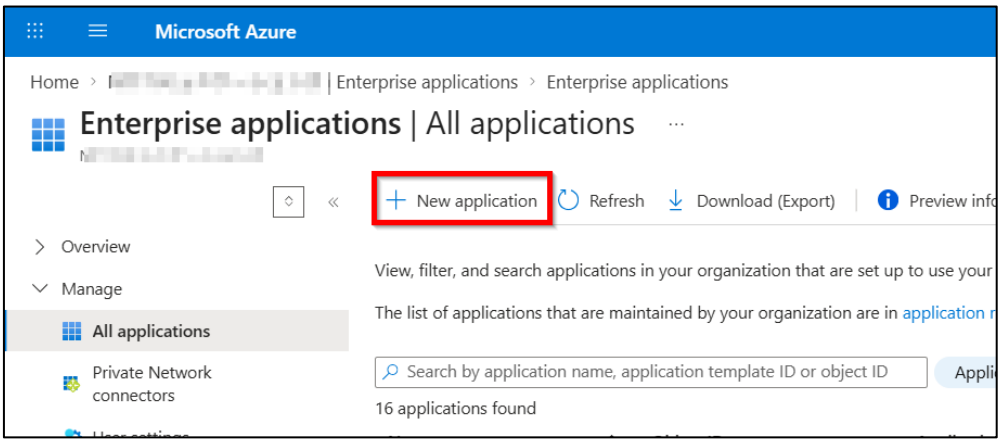
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5.2. エンタープライズアプリケーションの登録

(1) Azure Portal で Microsoft Entra ID を開き、左メニューから「Enterprise applications」を選択します。

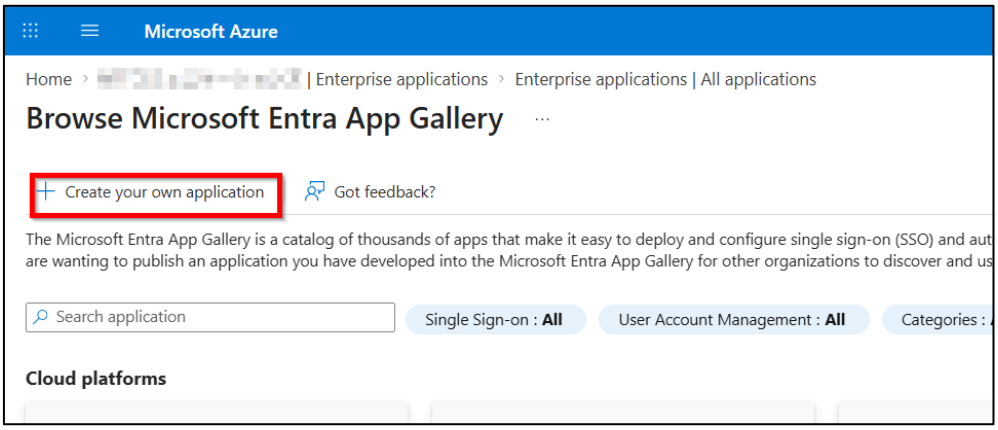


(2) 画面上部の「＋ New application」を選択します。



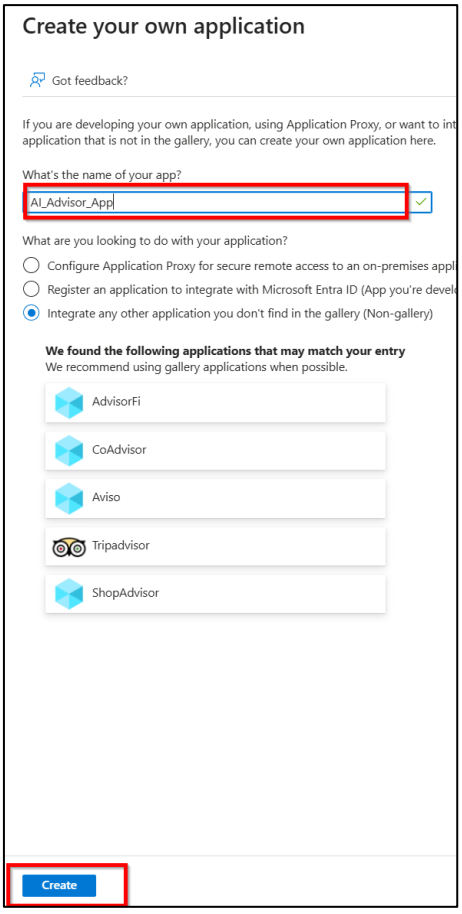
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(3) 「+ Create your own application」を選択します。



(4) 任意の名称を付与して登録します。AI Advisor 用のアプリケーションであることが分かる名前を入力し、画面の案内に従って登録します。

※本章で登録するエンタープライズアプリケーションは、AI Advisor ポータルへの SAML 認証に使用します。第 3 章で登録した、Microsoft Sentinel などとの API 連携に使用する AI Advisor 用アプリとは異なります。以降の手順では、本章で登録したエンタープライズアプリケーションを選択してください。

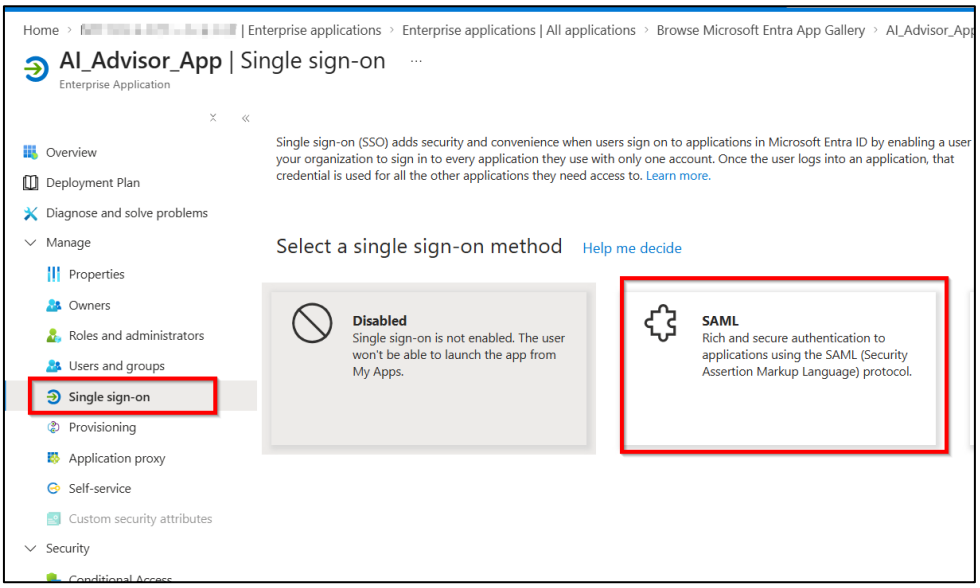


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5.3. SAML によるシングルサインオンのセットアップ

(1) 第 5.2.章で作成したエンタープライズアプリケーションを開き、「Manage」セクションから「Single sign-on」を選択します。

(2) 「Select a single sign-on method」画面が表示されたら、「SAML」を選択します。

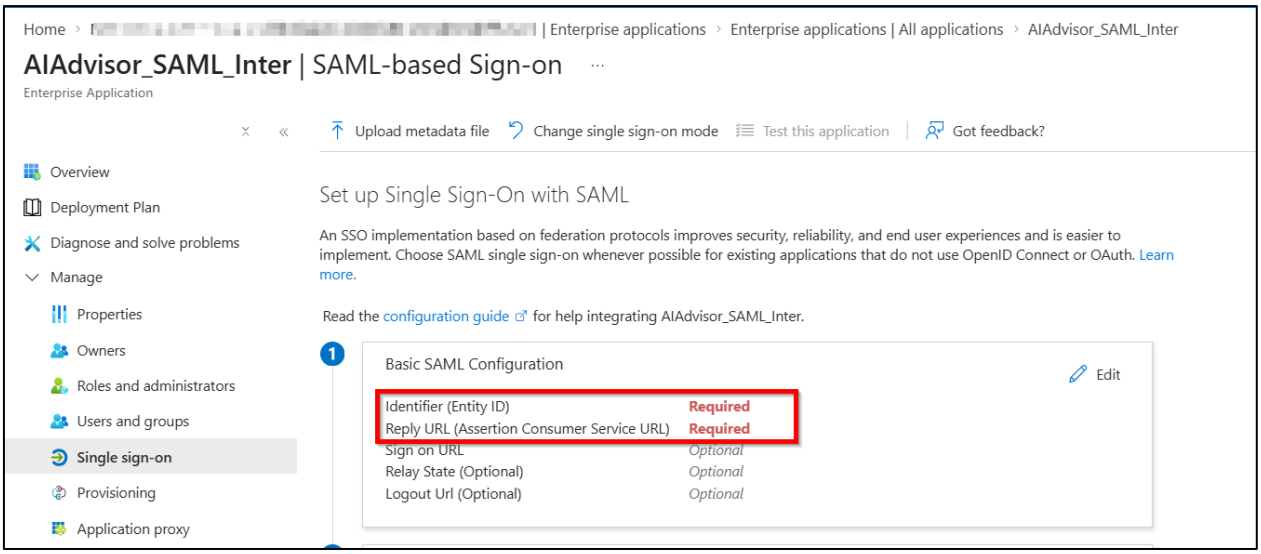


(3) 「SAML-based Sign-on」画面の「Basic SAML Configuration」で「Edit」を選択します。
弊社からご案内した以下の情報を入力してください。

・識別子（エンティティ ID）

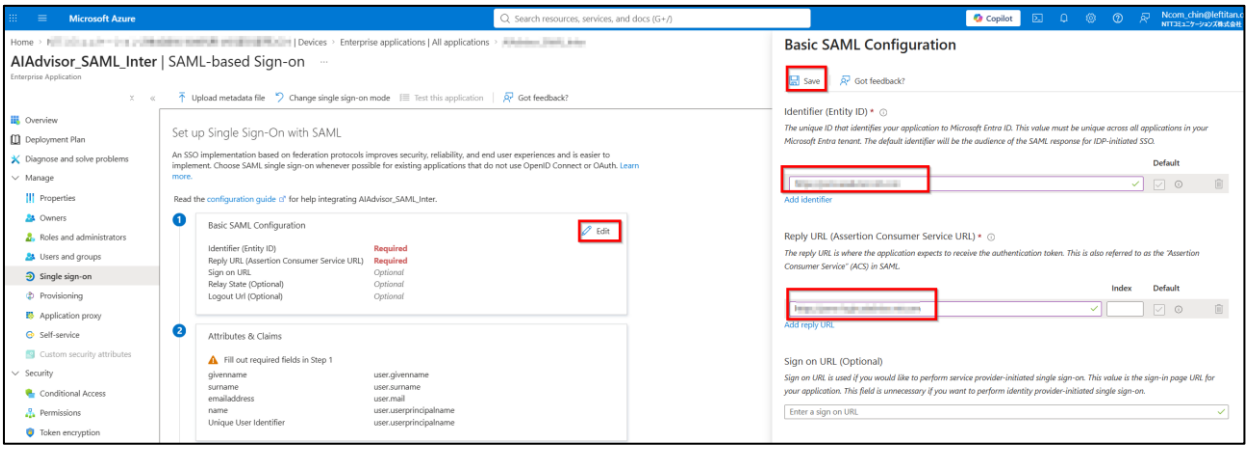
・応答 URL（Assertion Consumer Service URL）

※「識別子（エンティティ ID）」および「応答 URL（Assertion Consumer Service URL）」は弊社からご案内します。設定値はお客さまごとに異なるため、弊社からご案内した値を入力してください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(4) 入力内容を確認し、「Save」を選択します。



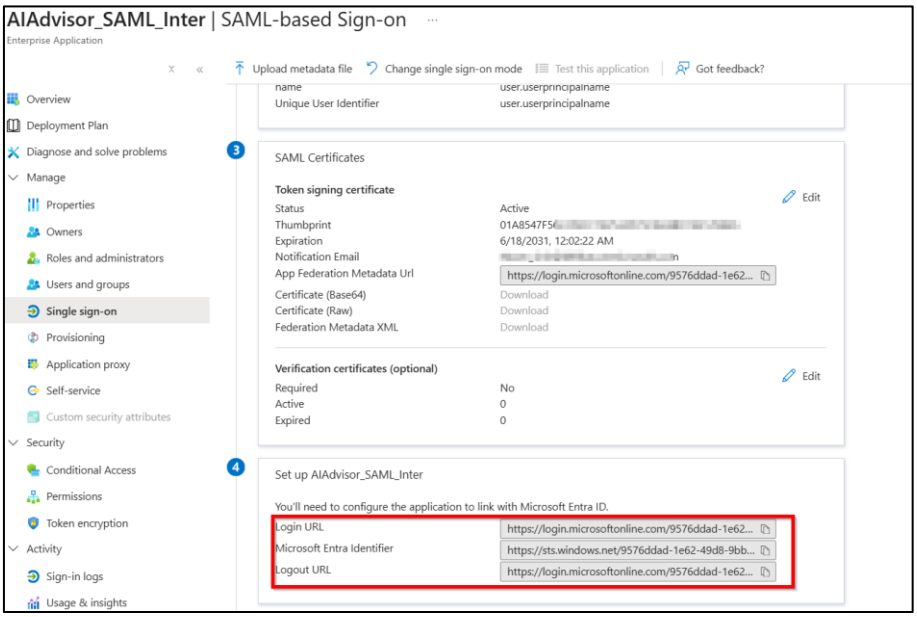
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5.4. 識別情報および証明書の取得

本章では、SAML 連携に必要な識別情報および証明書ファイルを取得します。

識別情報の確認と記入

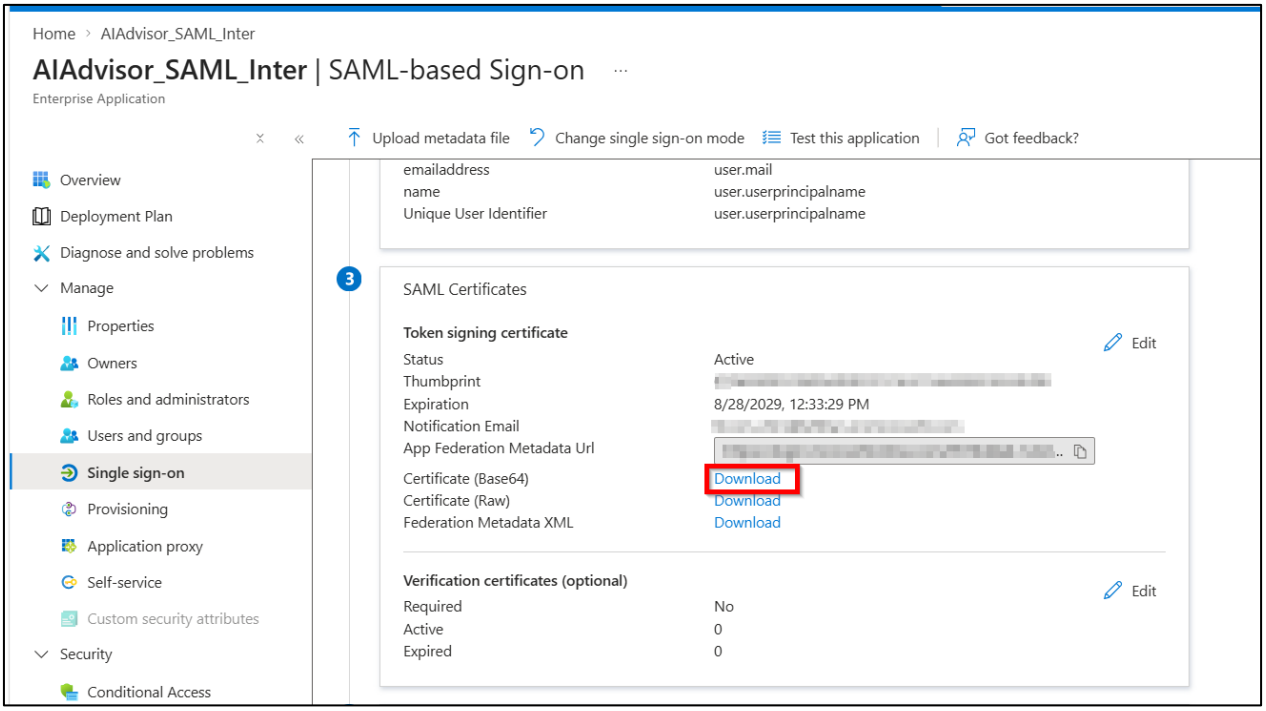
- 「Set up ＜アプリケーション名＞」セクションに表示される以下の情報を確認します。
  - Login URL
  - Microsoft Entra Identifier
  - Logout URL
- 確認した情報を「WideAngle AI Advisor ヒアリングシート」の「ヒアリングシート」シートにある「Microsoft Entra ID の SAML 設定情報」欄に記入します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

証明書ファイルの取得

- 「SAML Certificates」セクションの「Certificate（Base64）」で、「Download」を選択し、証明書ファイルをダウンロードします。
- ダウンロードした証明書ファイルを、弊社担当者からご案内する方法でご提出ください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

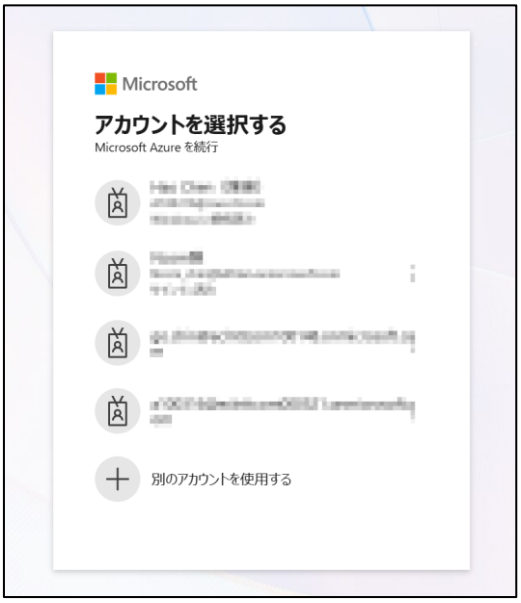
5.5. サインインの確認

弊社からご案内した AI Advisor ポータルの URL にアクセスします。

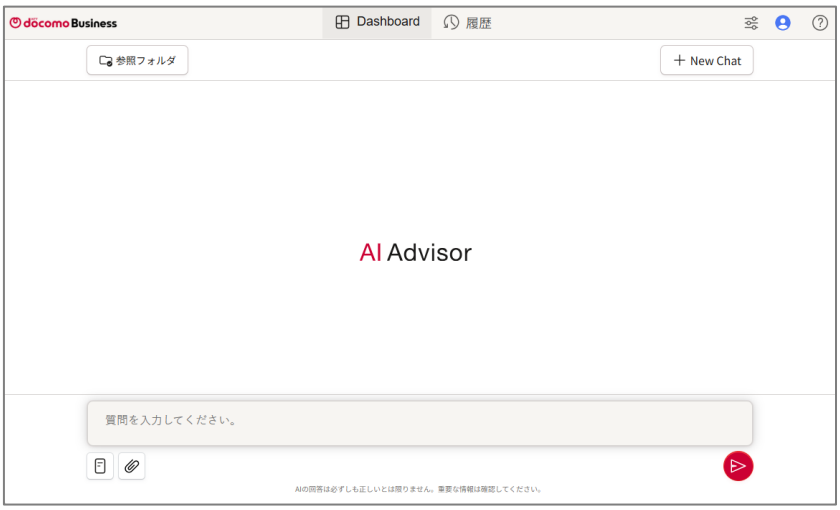
AI Advisor ポータル URL の例：https://xxxx.aiadvisor.ntt.com/

※実際にアクセスする URL はお客さまごとに異なります。弊社からご案内した URL にアクセスしてください。

Microsoft Entra ID のアカウント選択画面が表示された場合は、AI Advisor の利用対象となるアカウントを選択してサインインします。



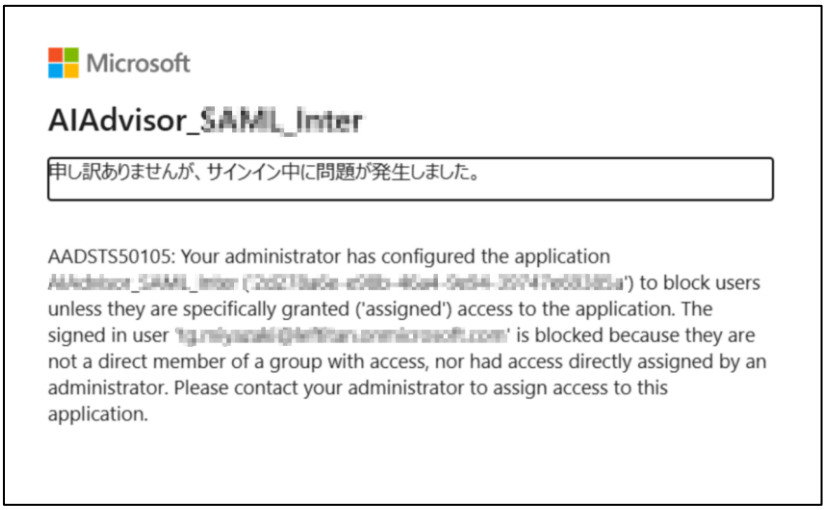
サインイン後、AI Advisor ポータルが表示されることを確認します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

※正常にサインインできない場合は、表示されたエラーコードを確認してください。

エラーコード「AADSTS50105」が表示された場合は、第 5.6.章を参照してください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5.6. サインイン時にエラーコード「AADSTS50105」が表示された場合の対応

AI Advisor ポータルへのサインイン時に、エラーコード「AADSTS50105」が表示された場合は、作成したエンタープライズアプリケーションにおいて、AI Advisor を利用するユーザーのサインインが許可されていない可能性があります。

AI Advisor ポータルへのユーザー追加のみで利用者を管理する場合は、「5.6.1 ユーザーの割り当てを不要にする」を実施してください。

Microsoft Entra ID 側でも AI Advisor を利用できるユーザーまたはグループを制限する場合は、「5.6.2 ユーザーまたはグループを割り当てる」を実施してください。

※対応方法は、お客さまのセキュリティポリシーおよび Microsoft Entra ID の運用方針に応じて選択してください。

5.6.1. ユーザーの割り当てを不要にする

AI Advisor ポータルへのユーザー追加のみで利用者を管理する場合は、エンタープライズアプリケーションへのユーザーの割り当てを不要にします。本設定により、Microsoft Entra ID のエンタープライズアプリケーションに利用者を個別に割り当てる必要がなくなります。AI Advisor の利用者は、AI Advisor ポータルへのユーザー追加によって管理します。

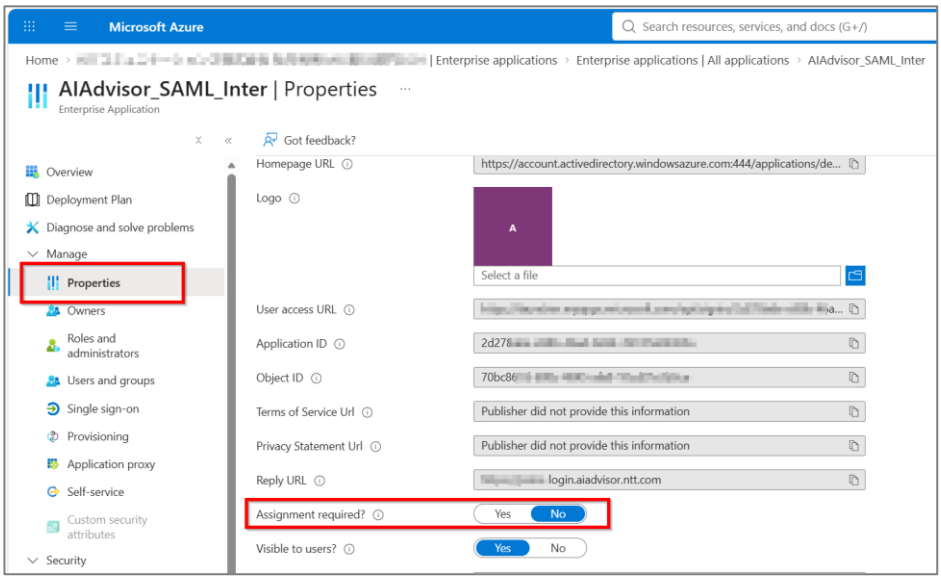
(1) Azure Portal で Microsoft Entra ID を開きます。

(2) 左メニューから「Enterprise applications」を選択します。

(3) 「All applications」から、第 5.2.章で作成したエンタープライズアプリケーションを選択します。

(4) 「Manage」セクションから「Properties」を選択します。

(5) 「Assignment required?」で「No」を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(6) 「Save」を選択し、設定を保存します。

(7) 再度 AI Advisor ポータルへアクセスし、正常にサインインできることを確認します。

5.6.2. ユーザーまたはグループを割り当てる

Microsoft Entra ID 側でも AI Advisor を利用できるユーザーまたはグループを制限する場合は、AI Advisor の利用を許可するユーザーまたはグループを、エンタープライズアプリケーションに割り当てます。

本設定を行う場合は、「Assignment required?」を「Yes」に設定したうえで、エンタープライズアプリケーションに対象のユーザーまたはグループを割り当てます。なお、AI Advisor を利用するには、エンタープライズアプリケーションへの割り当てに加えて、AI Advisor ポータルへのユーザー追加も必要です。

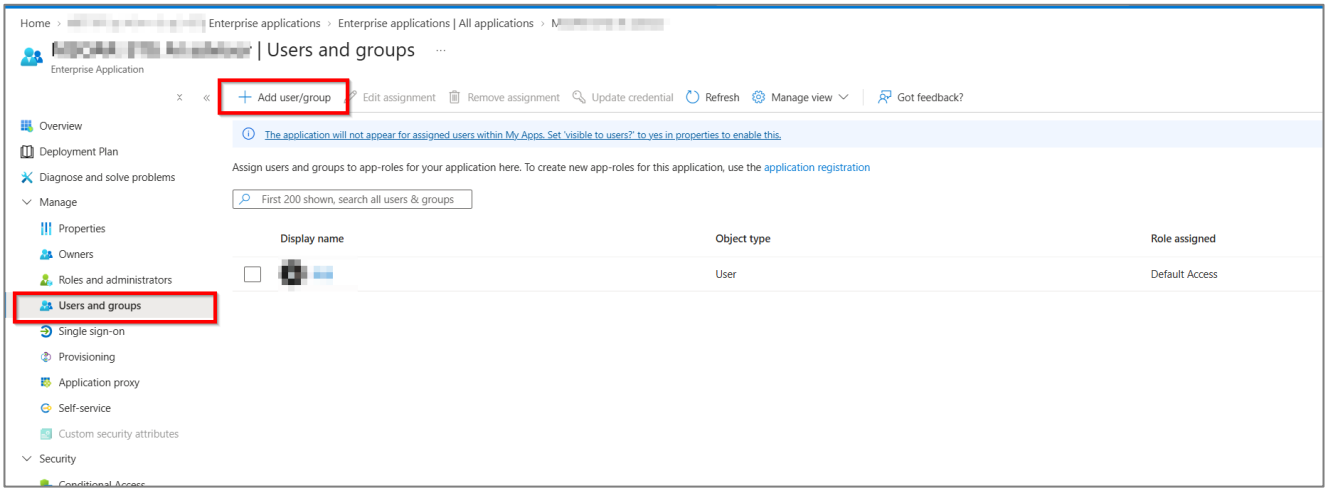
(1) Azure Portal で Microsoft Entra ID を開きます。

(2) 左メニューから「Enterprise applications」を選択します。

(3) 「All applications」から、第 5.2 章で作成したエンタープライズアプリケーションを選択します。

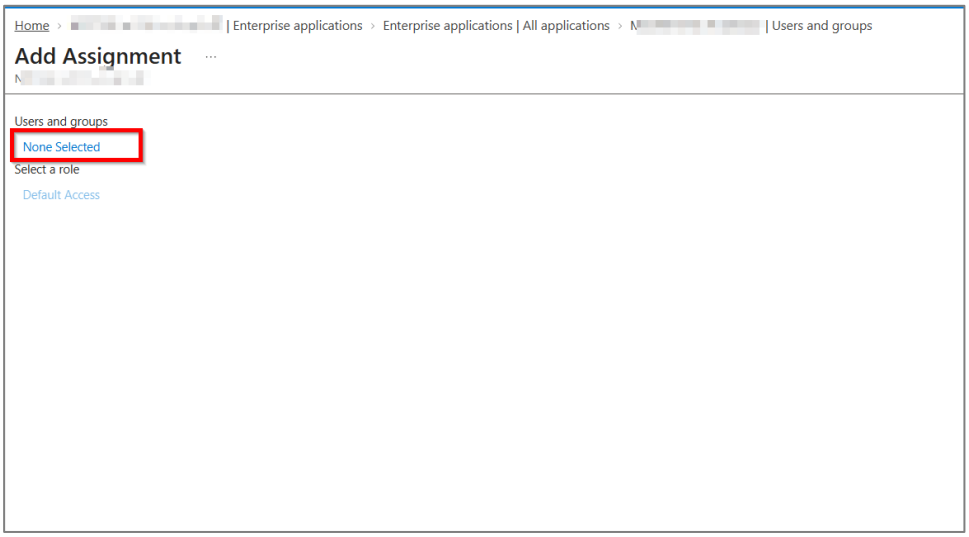
(4) 「Manage」セクションから「Users and groups」を選択します。

(5) 画面上部の「+ Add user/group」を選択します。

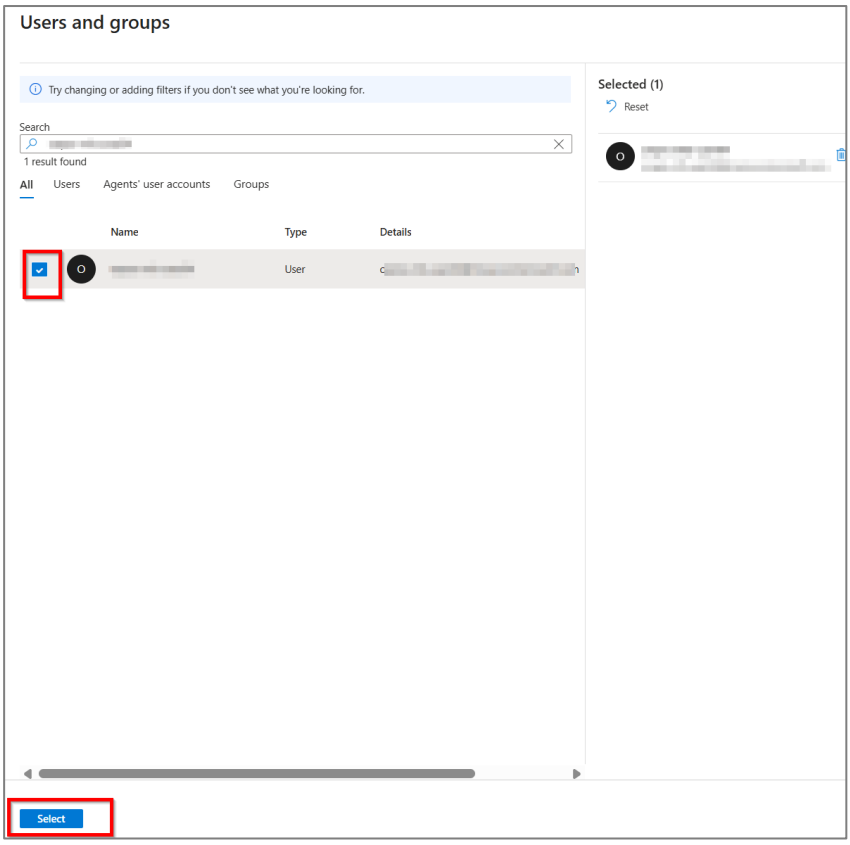


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(6) 「Users and groups」の「None Selected」を選択します。

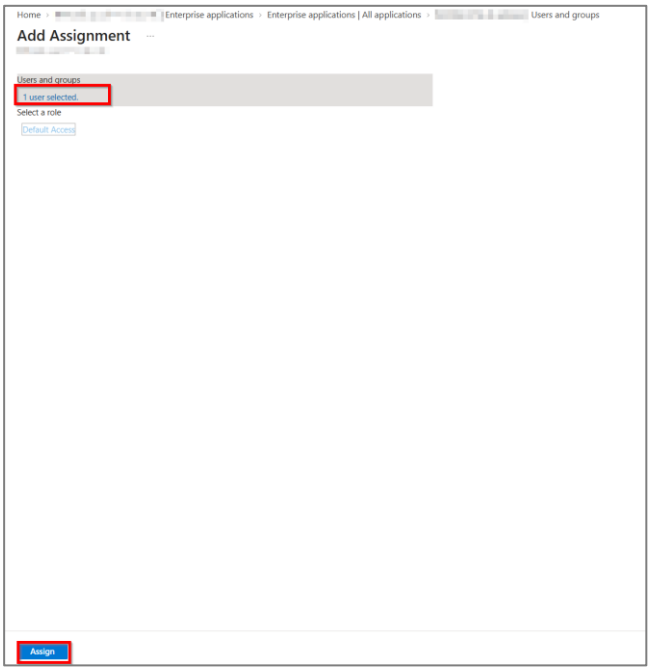


(7) AI Advisor の利用を許可するユーザーまたはグループを選択し、「Select」を選択します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

(8) 選択したユーザーまたはグループに誤りがないことを確認し、「Assign」を選択します。



(9) 再度 AI Advisor ポータルへアクセスし、割り当てたユーザーが正常にサインインできることを確認します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

改訂履歴

バージョン	主な変更	日付
1.00	初版発行	2026 年 11 月 1 日
1.01	クライアントシークレット更新時のサービス影響に関する記載を修正 3.3. アプリ認証用クライアントシークレットの作成	2026 年 11 月 11 日

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.