

# 次世代 Meeting Insights



## お知らせ

この文書に含まれる情報は、発行時点では正確かつ信頼できるものと考えられます。ただし、製品の継続的な改良および改訂により、AudioCodes は公開日以降の公開資料の正確性を保証することはできず、誤りや省略について責任を負うこともできません。この文書の更新版は<https://www.audiocodes.com/library/technical-documents>からダウンロードできます。

この文書は予告なく変更されることがあります。

公開日: MMMM-dd-yyyy

## セキュリティの脆弱性

すべてのセキュリティ脆弱性は、[vulnerability@audiocodes.com](mailto:vulnerability@audiocodes.com)に報告されます。

## カスタマー サポート

顧客向けの技術サポートおよびサービスは、AudioCodes または認定された AudioCodes サービスパートナーによって提供されます。AudioCodes 製品のテクニカルサポートの購入方法や連絡先の詳細については、当社のウェブサイト <https://www.audiocodes.com/services-support/maintenance-and-support>を参照してください。

## ドキュメントのフィードバック

AudioCodes は、高品質のドキュメントの作成に継続的に努めています。このドキュメントに関するご意見（ご提案や誤り）がございましたら、弊社 Web サイト <https://online.audiocodes.com/documentation-feedback>のドキュメント フィードバックフォームにご記入ください。

## AudioCodesで最新情報を入手



## 目次

<b>1 導入</b>	<b>1</b>
対象読者	1
<b>2 導入前の要件</b>	<b>2</b>
<b>3 サインイン</b>	<b>3</b>
<b>4 Meeting Insights の設定</b>	<b>5</b>
Microsoft Entra ID でユーザー グループを定義する	5
Microsoft 365 に接続する	7
顧客の Azure エンタープライズ アプリケーションにおける権限	24
Microsoft Entra ID Meeting Insights Web アプリケーション	24
Microsoft Entra ID Meeting Insights アプリケーション	24
Microsoft Entra ID Meeting Insights ボット アプリケーション	25
Microsoft Entra ID Meeting Insights Teams アプリケーション	25
Microsoft Entra ID Meeting Insights モバイル アプリケーション	25
Microsoft Entra ID 通知ボット アプリケーション (オプション)	26
進行中の会議に Meeting Insights を追加できるようにする – スクリプトを実行する必要があります (オプション)	26
ユーザーへの Meeting Insights ライセンスの割り当て	26
管理者モードとユーザーモードの切り替え	28
ユーザー インターフェースの言語の変更	29
<b>5 Meeting Insights アプリのテスト</b>	<b>30</b>
<b>6 誰がどのアクションを実行する権限を持っているかを決定する</b>	<b>34</b>
<b>7 チームのライブ イベント やウェビナーの録画</b>	<b>37</b>
<b>8 システム設定の構成</b>	<b>38</b>
ツール	38
Teams クライアントに Meeting Insights を追加する	38
TAC 経由で組織の Teams ストアにアプリを追加する	41
Outlook アドインの設定	45
ストレージ	50
AudioCodes Azure Blob アカウントでホストされるストレージ	52
顧客の Azure BLOB アカウントでホストされるストレージ	53
Azure Blob Storage アカウントの定義	54
BYOS で Meeting Insights を構成する	56
顧客の Amazon S3 アカウントでホストされるストレージ	58
Amazon S3 バケットを作成	59
AWS ベースの BYOS 用に Meeting Insights を構成する	60
ストレージの接続状態と容量の監視	67
BYOS エンティティの削除	69
タグ	69
デバイス	71

<b>9 ユーザー設定の構成</b>	<b>72</b>
ユーザープロフィール	72
AIの自動起動の有効化	77
テンプレートベースのAIを活用したサマリーの有効化	80
ユーザープロフィールごとの会議録画の種類	81
ユーザーが外部のTeams会議を録画できるようにする	82
ユーザーがZoom会議を録画できるようにする	84
ユーザーがGoogle Meet会議を録画できるようにする	86
管理者プロフィール	87
ライセンスありのユーザー	87
ライセンスなしのユーザー	89
会議の保持ポリシー	91
Microsoft録画通知	95
ユーザー設定	102
メール通知	102
公開時間の設定	103
<b>10 AI設定</b>	<b>106</b>
AIを活用した文字起こしの有効化と構成	106
AIを活用したInsightsの設定	107
声紋の表示とリセット	108
AIを活用したカスタムテンプレートの表示と命名	109
AIを活用したライブラリテンプレートの表示と命名	110
<b>11 監視</b>	<b>112</b>
監査証跡	112
システムアクティビティログ	114
<b>12 統合</b>	<b>116</b>
Meeting InsightsとMicrosoft Plannerの統合	116
Meeting InsightsとZohoの統合	119
Meeting Insightsとmonday.comの統合	121
Meeting InsightsとSalesforceの統合	127
Salesforceの設定と必要な情報の取得	128
Salesforceで接続アプリを作成する	128
SalesforceドメインURLの取得	132
Salesforce接続アプリのクライアントIDとシークレットの取得	132
Salesforceオブジェクトフィールド(API)名の取得	134
Salesforce統合のためのMeeting Insightsの設定	134
サードパーティの会議アプリ向けのMeeting Insightsボット名と通知のカスタマイズ	137
<b>13 スケジュールされた会議へのMIAの自動招待の設定</b>	<b>140</b>
メール対応セキュリティグループを追加する	140
自動招待ルールを設定する	144
ルールをテストする	150

Teams 会議のロビーの管理 .....	151
<b>14Power BI Analytics 使用状況レポートの作成 .....</b>	<b>152</b>
Meeting Insights で Power BI 統合を有効にする .....	152
インストール   Power BI Analytics の構成 .....	153
レポートを使用して製品の使用状況統計を確認する .....	159
Power BI 統合を無効にする .....	163
<b>15実用的な要約メールの有効化 .....</b>	<b>164</b>
<b>16Meeting Insights データセキュリティについて .....</b>	<b>167</b>

# 1 導入

AudioCodes Meeting Insights は、ユーザーが会議で生成されたコンテンツ(音声とビデオ)を録画し、Microsoft Teams 会議の議事録を自動的に作成できるようにする AI を活用したエンタープライズソリューションです。

Meeting Insights は、オンライン会議のあらゆる側面を録画、転記、整理します。すべての会議、ウェビナー、電話会議を一元管理する企業プラットフォームを提供し、組織全体で簡単に共有できるようになります。これにより、会議コンテンツへの個人のアクセスから会社全体のアプローチへと焦点が移り、情報に基づいた意思決定に役立ちます。

会議中、Meeting Insights の音声アシスタント「MIA」は、すべてのメモ、アクション項目、決定事項、サマリーを録画し、会議の特定の領域をワンクリックで強調表示して、会議後に簡単に見つけられるようにします。Meeting Insights では定期的な録画オプションが提供されており、会議中にいつでも録画を一時停止したり再開したりできます。

会議の録画が終了したら、Meeting Insights の機能豊富で柔軟な Web ベースの管理ツールを使用して、会議の録画を管理および編集できます。これには、会議の録画を公開して共有し、すべての参加者、およびオプションで組織内のすべての連絡先または特定の連絡先が、出席していない(または招待されていない)場合でも会議の録画を表示できるようにすること、およびスライドプレゼンテーションを編集すること(スライドの追加、置換、または削除)が含まれます。

Meeting Insights の詳細については、AudioCodes の[Web サイト](#)を参照してください。



現在、Meeting Insights では、Teams 内の **PowerPoint Live** の共有コンテンツは録画されません。

## 対象読者

このガイドは、企業 | 組織の管理者を対象としています。

## 2 導入前の要件

Meeting Insights を導入する前に、お客様は以下を提供する必要があります。

- 顧客のドメイン名。
- 導入状況に関する顧客連絡先のメール
- Meeting Insights への最初のアクセス (ログイン) に必要な Microsoft Entra ID ユーザー プリンシパル名 (UPN)。



- 最初のログインには任意のユーザー アカウントを使用できます。ただし、組織の **Microsoft によるアプリケーションの委任権限** ポリシー (以下にリストされています) に従って、Meeting Insights アプリケーションへのアクセスに同意するために組織の管理者からの承認を要求するように求められる場合があります。
  - ✓ **ユーザーの同意を許可しない:** 組織の管理者の同意が必要です。
  - ✓ **検証済みの発行元からのアプリに対して、選択した権限についてユーザーの同意を許可する:** ユーザーは同意できます (Meeting Insights は Microsoft によって検証された発行元であるため)。
  - ✓ **アプリのユーザー同意を許可する:** ユーザーは同意できます。
- オンボーディングプロセス中 (**Microsoft 365 に接続する** を参照)、Microsoft 365 の複数の権限 (同意) を付与する必要があり、これは**グローバル管理者**または**クラウドアプリケーション管理者**の同意の種類に応じて、役割が決まります。これらの管理者ユーザーは**排他的に**権限を付与します。各権限が付与されると、Meeting Insights セッションは自動的に Meeting Insights にログインしたユーザー アカウントに戻ります。

- 録音を保存するのに適した地域。Microsoft Azure Cloud で地域が利用できない場合は、デフォルトの地域が使用されます。

## 3 サインイン

このセクションでは、に指示されている通り、Meeting Insights に管理者としてサインインする方法について説明します。管理者は、通常のユーザーが実行できない管理タスクを実行できます。最大 5 人の管理者が許可されます。



- 顧客アプリケーションが作成されると、初期管理者が追加されます。
- アプリのサインイン準備が完了すると、デフォルトの管理者にメールが届きます。
- 管理者には、完全な Meeting Insights アクセス権があります。
  - ✓ 管理者はシステム構成と会議へのフルアクセス権を持ちます。
  - ✓ 管理者は会議の所有者に代わって、会議の所有者の権限の範囲内で操作できます。たとえば、会議の所有者が外部共有の権限を持っている場合、管理者は会議を外部で共有できます。

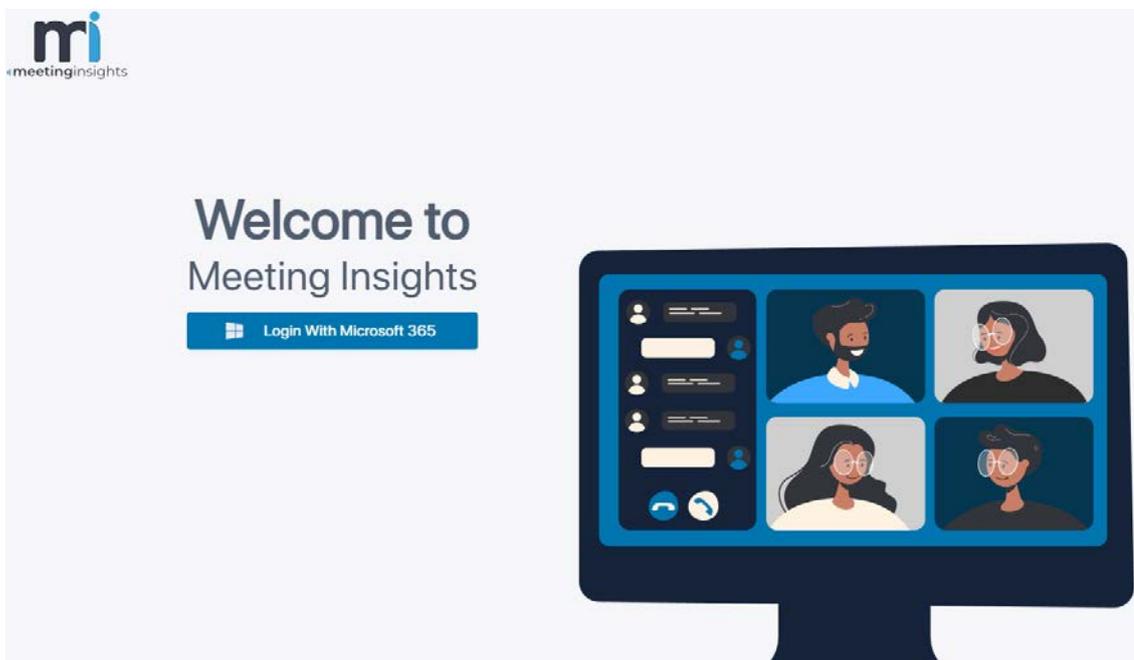
### ➤ 管理者としてサインインするには:

1. AudioCodes からのメール内のリンク (URL) を使用して、Meeting Insights アプリにアクセスします。



地域に応じて、Meeting Insights への URL は次のいずれかになります。

- <https://emea.meetinginsights.com/mi/login>
- <https://americas.meetinginsights.com/mi/login>
- <https://au.meetinginsights.com/mi/login>



2. **Login With Microsoft 365** をクリック。Microsoft 365 アカウントでサインインするように求められます。
3. Meeting Insights 管理者の UPN を使用してサインインします。



- 最初のログインには任意のユーザーアカウントを使用できます。ただし、組織の [Microsoft によるアプリケーションの委任権限](#) ポリシー (以下にリストされています) に従って、Meeting Insights アプリケーションへのアクセスに同意するために組織の管理者からの承認を要求するように求められる場合があります。
  - ✓ **ユーザーの同意を許可しない:** 組織の管理者の同意が必要です。
  - ✓ **検証済みの発行元からのアプリに対して、選択した権限についてユーザーの同意を許可する:** ユーザーは同意できます (Meeting Insights は Microsoft によって検証された発行元であるため)。
  - ✓ **アプリのユーザー同意を許可する:** ユーザーは同意できます。
- オンボーディングプロセス中 ([Microsoft 365 に接続する](#)を参照)、Microsoft 365 の複数の権限 (同意) を付与する必要があり、これは **グローバル管理者** または **クラウドアプリケーション管理者** の同意の種類に応じて、役割が決まります。これらの管理者ユーザーは **排他的に** 権限を付与します。各権限が付与されると、Meeting Insights セッションは自動的に Meeting Insights にログインしたユーザーアカウントに戻ります。

4. [こちら](#)に指示されている通り、Meeting Insights を組織の Microsoft 365 に接続します。

## 4 Meeting Insights の設定

ここで説明する3つの手順に従って、Meeting Insights を設定します。

➤ アプリを設定するには:

1. [Microsoft Entra ID でユーザー グループを定義する](#)で指示されている通りに、Meeting Insights ユーザー用の Microsoft Entra ID グループを構成します。
2. [Microsoft 365 に接続する](#)に示されているように、Microsoft 365 に接続します。
3. [ユーザーへの Meeting Insights ライセンスの割り当て](#)に示されているように、ユーザーグループに Meeting Insights ライセンスを割り当てます。



Meeting Insights の設定をしたら、[Meeting Insights アプリのテスト](#)に示されているように設定をテストします。

### Microsoft Entra ID でユーザー グループを定義する

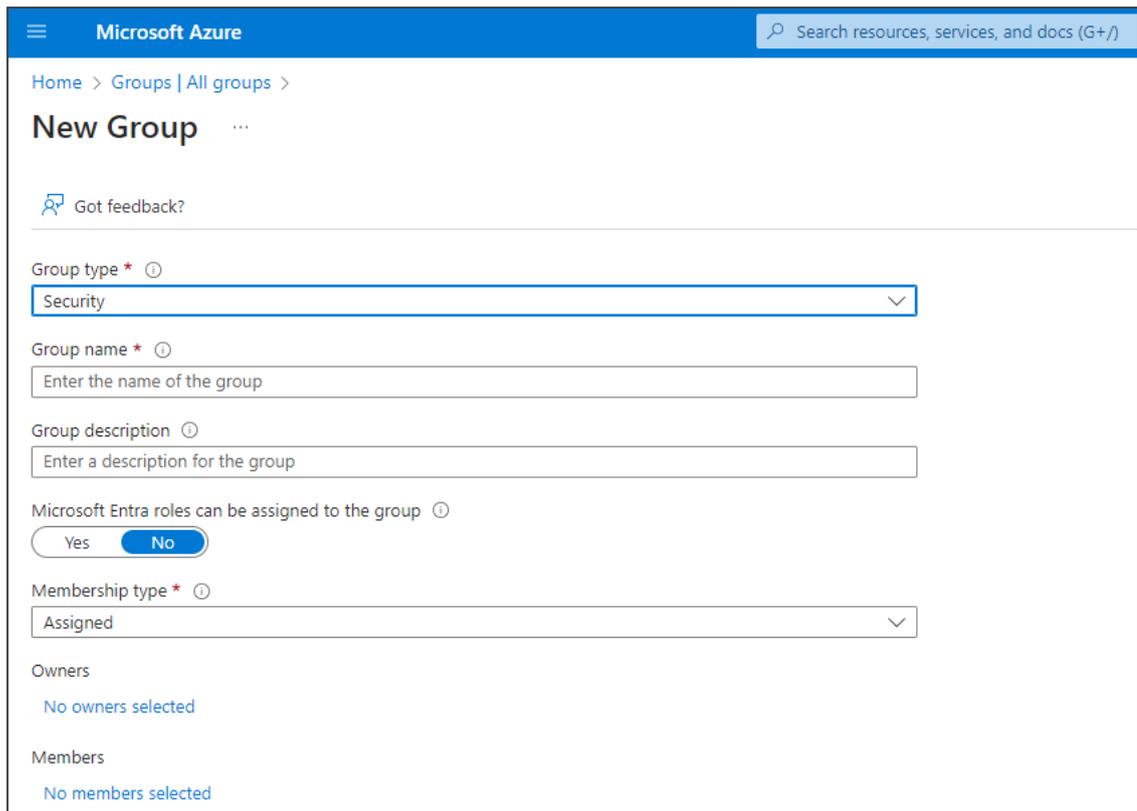
ライセンスを割り当てる前に、エンタープライズ管理者は、Meeting Insights を使用するユーザーのために、Microsoft Entra ID でユーザー グループを定義する必要があります。



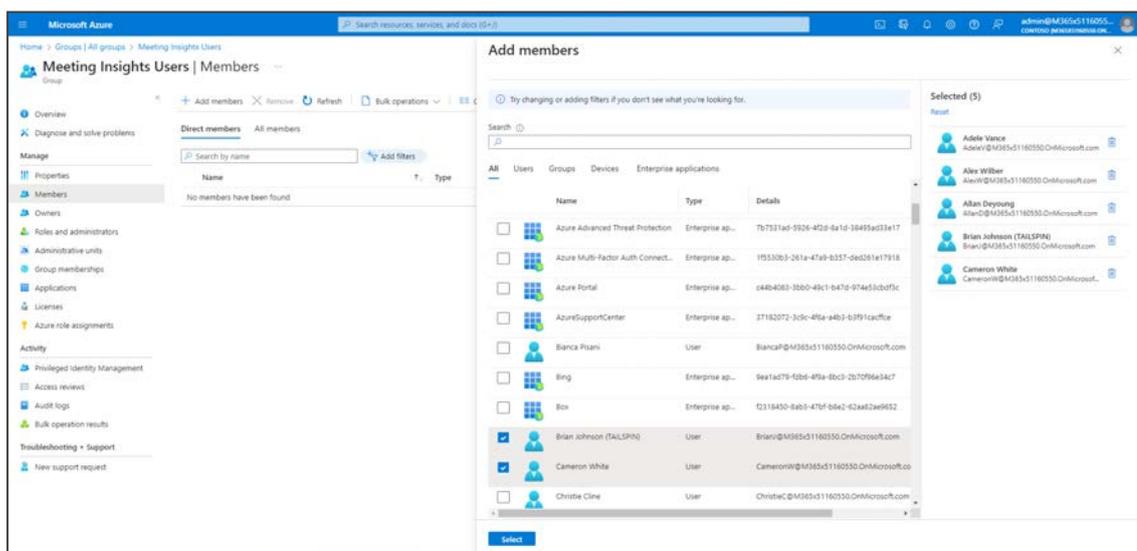
後で Microsoft Entra ID グループを変更する場合は、「ライセンス管理」ページにアクセスします([ユーザーへの Meeting Insights ライセンスの割り当て](#)参照)。次に、**Sync and Apply**をクリックして、変更を Meeting Insights に反映させます。

➤ Microsoft Entra ID でユーザー グループを定義するには:

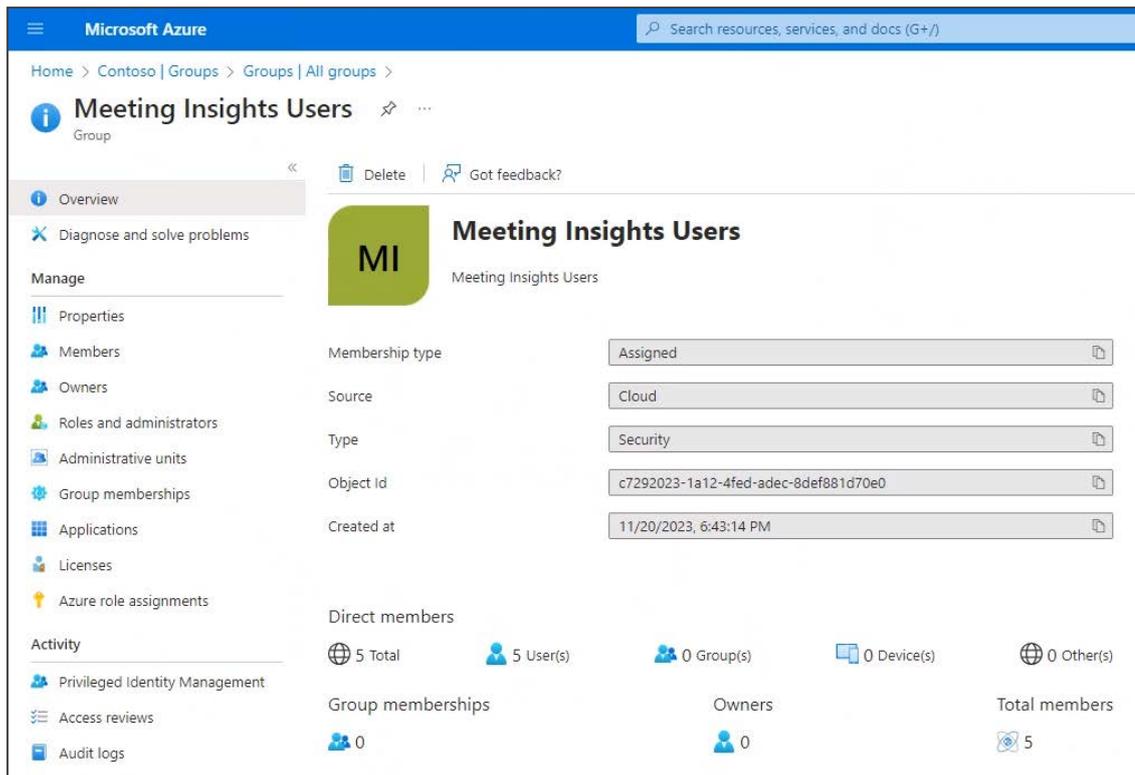
1. [こちら](#)から Microsoft Azure ポータルにサインインして、管理者の資格情報を使用してアクセスします。
2. **Entra ID > Groups > All groups**に進み、**New group** をクリックします。



3. [必須]「Group type」ドロップダウンから **Security** を選択します。
4. [強く推奨] グループ名を **Meeting Insights Users** と定義します。
5. グループに所有者を割り当てます。グループの所有者には、グループを管理するための固有の権限があることに注意してください。メンバーの追加や削除、グループ設定の変更、グループ名の変更、グループの説明の更新を行うことができます。
6. グループにメンバー (ユーザーまたはグループ) を割り当てます。



7. Microsoft Azure ポータルでグループの詳細を表示します。



## Microsoft 365 に接続する

このセクションでは、組織の Microsoft 365 環境内の Meeting Insights アプリにさまざまなアクセス許可 (同意) を付与することを含む、Microsoft 365 (M365) に接続する方法について説明します。

これらの権限は、同意の種類に応じて、グローバル管理者またはクラウド アプリケーション管理者のロールを持つユーザーのみが付与できます。次の表では、各同意タイプと、同意を付与できる必要なユーザー ロールについて説明します。

各同意の種類をクリックすると、必要なユーザー ロールで Microsoft 365 ユーザー アカウントにサインインするためのプロンプトが表示されます。したがって、必要な管理者ユーザー ロールを持たないユーザー アカウントで Meeting Insights にログインしている場合は、必要なロールを持つユーザーが一時的にサインインして各同意を付与できることを確認する必要があります。この管理者アカウントは排他的に権限を付与します。各権限が付与されると、Meeting Insights セッションは、Meeting Insights にログインした最初のユーザー アカウント (つまり、あなた) に自動的に戻ります。

同意	必要なユーザー ロール	説明
M365 Login	グローバル管理者またはクラウド アプリケーション管理	アプリケーションに、Microsoft 365 資格情報を使用してユーザーを認証する権限を付与します。アプリケーションは、認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。

同意	必要なユーザーロール	説明
	者	
Read Microsoft Entra ID Groups and Users	グローバル管理者またはクラウドアプリケーション管理者	アプリケーションに Microsoft Entra ID グループおよびユーザーを読み取る権限を付与します。これにより、該当グループのユーザーが録画機能およびアプリケーションへアクセスできるようになります。
Allow Meeting Insights to Join Meetings	グローバル管理者またはクラウドアプリケーション管理者	通話情報とメディアを録画するために、テナントの Teams 会議に参加する権限をアプリケーションに付与します。
Mobile App M365 Login	グローバル管理者またはクラウドアプリケーション管理者	モバイルアプリケーションに、Microsoft 365 資格情報を使用してユーザーを認証する権限を付与します。モバイルアプリケーションは、認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。
Publish Meeting Insights Teams Client App in your Teams Store	グローバル管理者	アクセスして進行中の会議に追加できるように、アプリケーションをユーザーの Teams クライアントに追加します。アプリを Teams ストアに公開します。ストアでは、特定のグループやユーザーにアプリケーションをインストールしたり自動的にピン留めするポリシーを設定できます
Allow Meeting Insights to be Added to Ongoing Meetings	<ul style="list-style-type: none"> <li>■ スクリプト ファイルをダウンロード:任意のユーザーロール</li> <li>■ ダウンロードしたスクリ</li> </ul>	Meeting Insights Teams クライアント アプリケーションに、オンライン会議グローバルアプリケーション アクセスを通じて進行中の会議に参加するための権限を付与します。

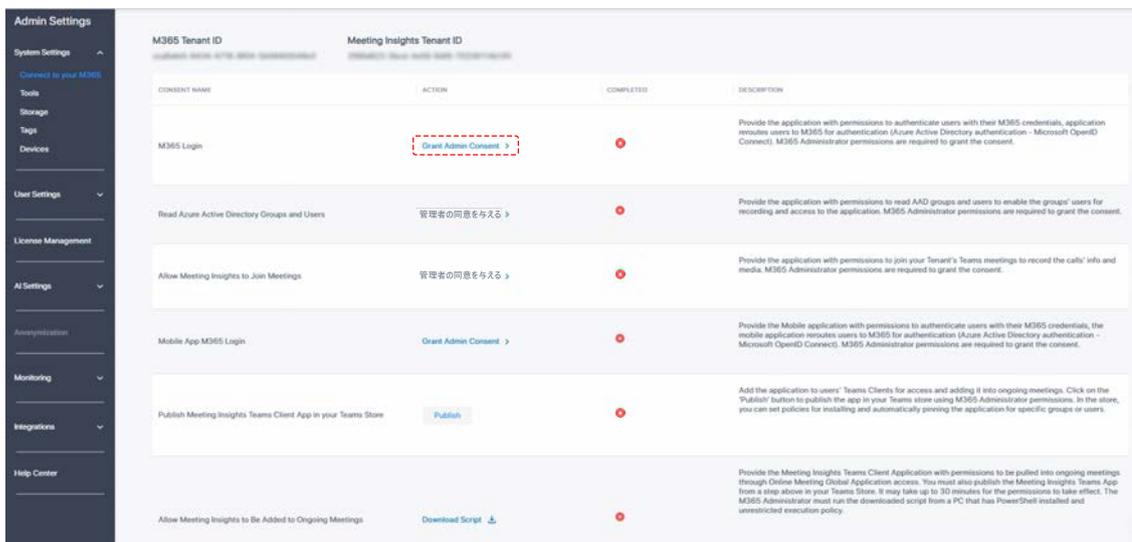
同意	必要なユーザーロール	説明
	プロファイルを実行します: グローバル管理者	



- このセクションで説明する権限の付与は、Meeting Insights アプリケーションにのみ適用されます。他のアプリケーションに影響を与えません。
- オプションとして、管理者は、Teams クライアントに Meeting Insights を追加することで説明するように、権限を付与することなく、アプリを Teams ストアに手動で追加できます。

➤ Microsoft 365 に接続する:

1. Meeting Insights にサインイン後、「M365 に接続」ページが表示されます (Admin Settings > System Settings > Connect to your M365)。「Completed」列には、 すべての同意のアイコンが表示され、いずれの同意タイプも付与されていないことが示されます。



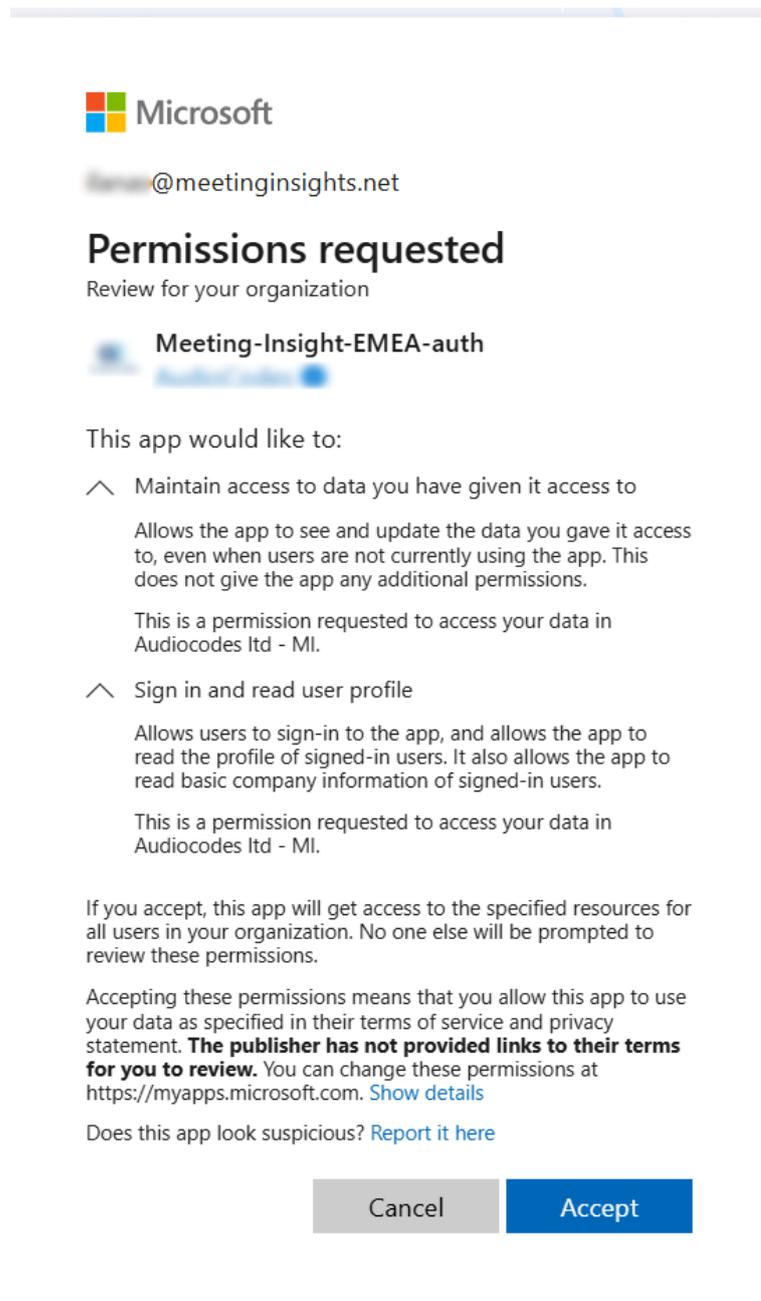
2. (必須) 「M365 Login」同意:(許可の詳細については[Microsoft Entra ID Meeting Insights Web アプリケーション](#)を参照してください)

この同意により、Meeting Insights アプリに、Microsoft 365 資格情報を使用してユーザーを認証する権限が付与されます。同意が承認されると、アプリは認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。



- 他の同意に進む前に、**まず**この同意を与える必要があります。
- 同意を与えるには Microsoft 365 **グローバル管理者**権限が必要です。

- a. 「M365 Login」の横にある **Grant Admin Consent** をクリックすると、Microsoft 365 アカウントにログインするように求められます。
- b. Microsoft 365 グローバル管理者アカウントにログインすると、次の権限ダイアログボックスが表示されます。



- c. **Accept** をクリックすると、「Completed」列に  アイコンが表示され、「M365 Login」の同意が正常に付与されたことが示されます。



後で同意を取り消した場合でも、アイコンは緑色のままになります。

### 3. (必須)「Read Microsoft Entra ID Groups and Users」同意:(権限の詳細は[Microsoft Entra ID Meeting Insights アプリケーション](#)を参照してください)

この同意により、Meeting Insights アプリに Microsoft Entra ID グループとユーザーを読み取る権限と、グループのユーザーがアプリにアクセスして録画する権限が付与されます。



- この同意は、上記のステップ2で説明されているように、「M365 ログイン」の同意を正常に許可した後にのみ許可できます。
- 同意を与えるには Microsoft 365 **グローバル管理者**権限が必要です。

CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent</a>	●	Provide the application with permissions to authenticate users with their M365 credentials, application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	<a href="#">Grant Admin Consent</a>	●	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	<a href="#">管理者の同意を与える</a>	●	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Mobile App M365 Login	<a href="#">Grant Admin Consent</a>	●	Provide the Mobile application with permissions to authenticate users with their M365 credentials, the mobile application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	<a href="#">Publish</a>	●	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the "Publish" button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	<a href="#">Download Script</a>	●	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Desktop Application access. You must also publish the Meeting Insights Teams App from a store above to your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

- 「Read Microsoft Entra ID Groups and Users」の横にある **Grant Admin Consent** をクリックすると、Microsoft 365 アカウントにログインするように求められます。
- Microsoft 365 **グローバル管理者**アカウントにログインすると、次の権限ダイアログボックスが表示されます。



██████████@meetinginsights.net

## Permissions requested

Review for your organization

### Meeting-Insight-EMEA-Meetings

This app would like to:

- ∧ Read all users' full profiles  
Allows the app to read user profiles without a signed in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ∧ Read all group memberships  
Allows the app to read memberships and basic group properties for all groups without a signed-in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ∧ Create tabs in Microsoft Teams.  
Allows the app to create tabs in any team in Microsoft Teams, without a signed-in user. This does not grant the ability to read, modify or delete tabs after they are created, or give access to the content inside the tabs.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ∧ Manage Teams apps for all chats  
Allows the app to read, install, upgrade, and uninstall Teams apps in any chat, without a signed-in user. Does not give the ability to read application-specific settings.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ∧ Allow the Teams app to manage all tabs for all chats  
Allows a Teams app to read, install, upgrade, and uninstall all tabs for any chat, without a signed-in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ∧ Sign in and read user profile  
Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.  
This is a permission requested to access your data in Audiocodes ltd - MI.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

- c. **Accept** をクリックすると、「Completed」列に🟢アイコンが表示され、「Read Microsoft Entra ID Groups and Users」同意が正常に付与されたことが示されます。
4. (必須) 「Allow Meeting Insights to Join Meetings」同意:( 権限の詳細は[Microsoft Entra ID Meeting Insights ポットアプリケーション](#)を参照してください)

この同意により、Meeting Insights アプリに、テナントの Teams 会議に参加して通話の情報とメディアを録画する権限が付与されます。



- 前の手順で説明したように、「M365 Login」および「Read Microsoft Entra ID Groups and Users」の同意を正常に付与した後にのみ、この同意を付与できます。
- 同意を与えるには Microsoft 365 **グローバル管理者**権限が必要です。

Admin Settings		M365 Tenant ID	Meeting Insights Tenant ID			
		CONSENT NAME	ACTION	COMPLETED	DESCRIPTION	
		M365 Login	<a href="#">Grant Admin Consent &gt;</a>	🟢	Provide the application with permissions to authenticate users with their M365 credentials, application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.	
		Read Azure Active Directory Groups and Users	<a href="#">Grant Admin Consent &gt;</a>	🟢	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.	
		Allow Meeting Insights to Join Meetings	<a href="#">Grant Admin Consent &gt;</a>	🔴	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.	
		Mobile App M365 Login	<a href="#">Grant Admin Consent &gt;</a>	🔴	Provide the Mobile application with permissions to authenticate users with their M365 credentials, the mobile application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.	
		Publish Meeting Insights Teams Client App in your Teams Store	<a href="#">Publish</a>	🔴	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.	
		Allow Meeting Insights to Be Added to Ongoing Meetings	<a href="#">Download Script</a> ↓	🔴	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Dialer Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.	

- a. 「Allow Meeting Insights to Join Meetings」の同意の横にある **Grant Admin Consent** をクリックすると、Microsoft 365 アカウントにログインするように求められます。
- b. Microsoft 365 **グローバル管理者**アカウントにログインすると、次の権限ダイアログボックスが表示されます。



██████████@meetinginsights.net

## Permissions requested (1 of 2 apps)

Review for your organization



This app would like to:

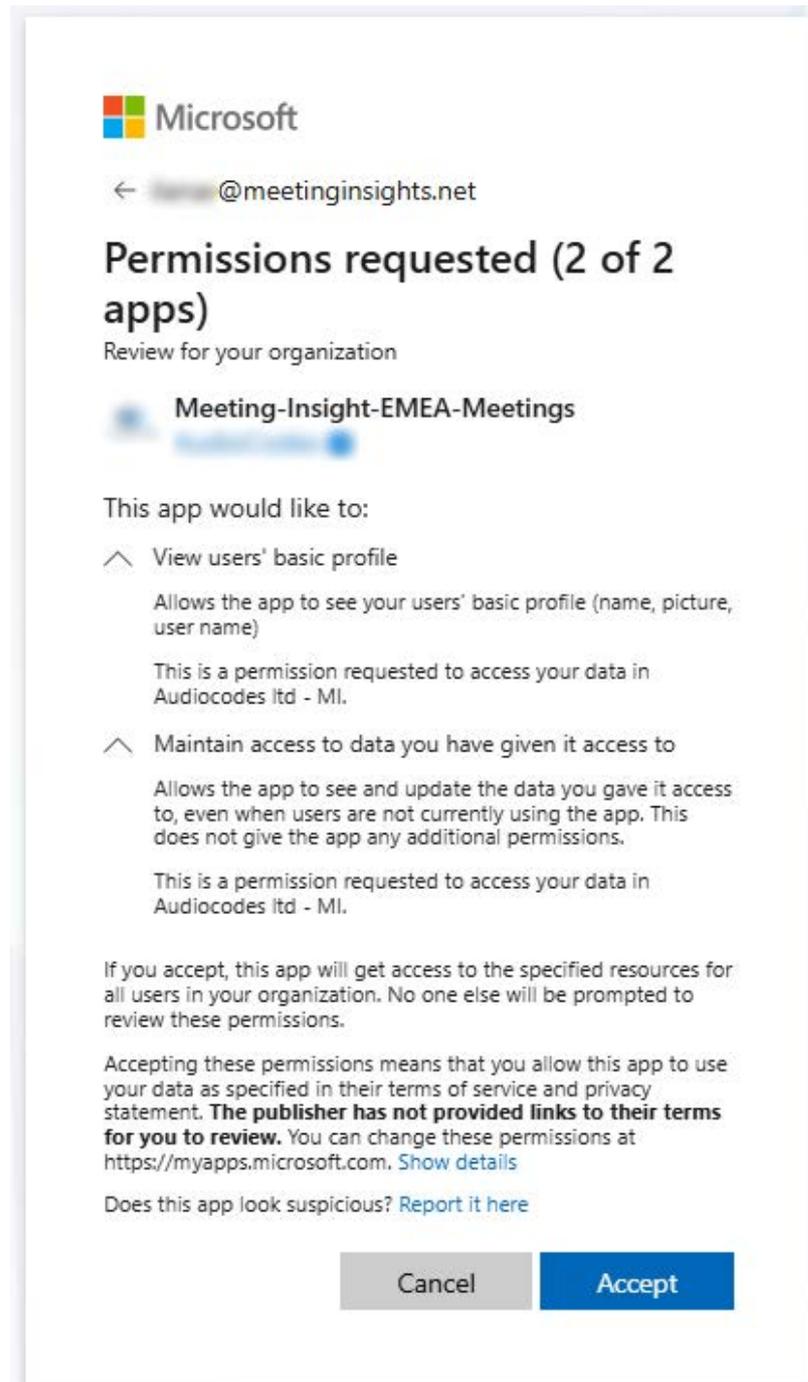
- ⌵ Daemon Role (Meeting-Insight-EMEA-Meetings)  
Daemon Role  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Bot Role (Meeting-Insight-EMEA-Meetings)  
Bot Role  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Access media streams in a call as an app  
Allows the app to get direct access to media streams in a call, without a signed-in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Join group calls and meetings as an app  
Allows the app to join group calls and scheduled meetings in your organization, without a signed-in user. The app will be joined with the privileges of a directory user to meetings in your organization.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Read online meeting details  
Allows the app to read online meeting details in your organization, without a signed-in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Read names and members of all chat threads  
Read names and members of all one-to-one and group chats in Microsoft Teams, without a signed-in user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ⌵ Sign in and read user profile  
Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.  
This is a permission requested to access your data in Audiocodes ltd - MI.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

- c. **Next** をクリックすると、2 番目の権限ダイアログボックスが表示されます。



- d. **Accept** をクリックすると、「Completed」列に🟢アイコンが表示され、「Allow Meeting Insights to Join Meetings」同意が正常に付与されたことが示されます。

5. (オプション) 「Mobile App M365 Login」同意:

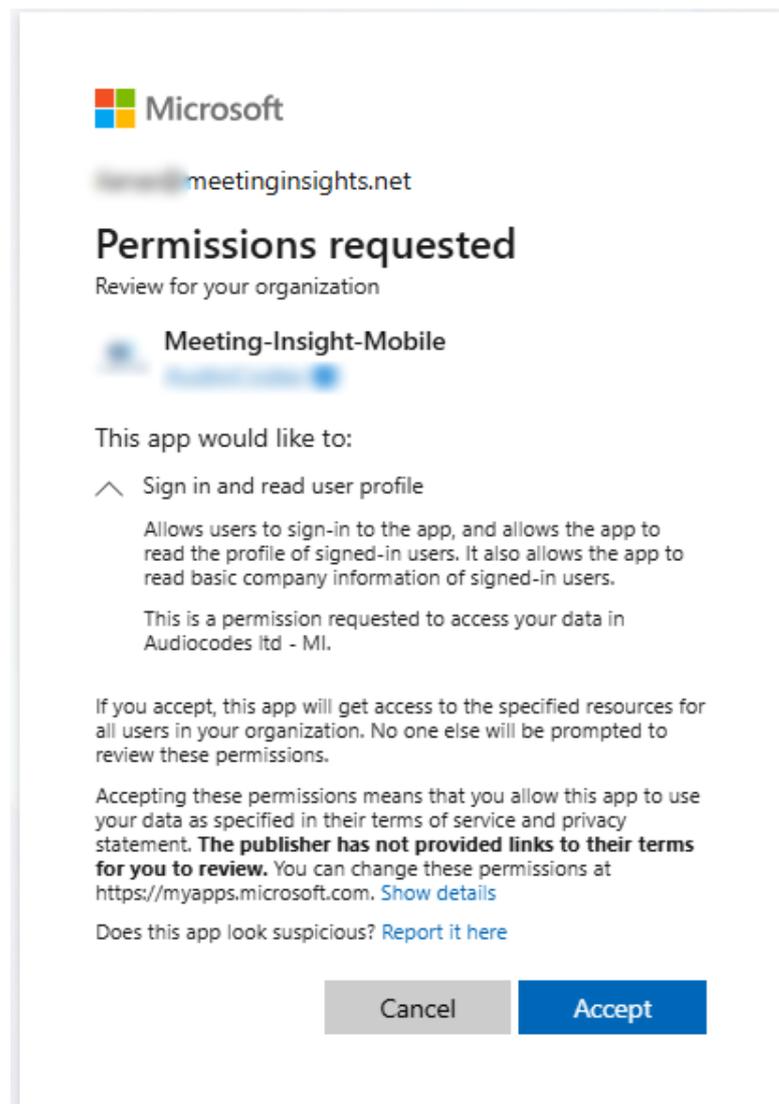
この同意により、Meeting Insights モバイルアプリに、Microsoft 365 資格情報を使用する権限が付与されます。ユーザーを認証します。同意が承認されると、アプリは認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。



- この同意は、前の手順で説明したように、「M365 Login」、「Read Microsoft Entra ID Groups and Users」、および「Allow Meeting Insights to Join Meetings」の同意を正常に付与した後にのみ付与できます。
- この同意を付与するには Microsoft 365 **グローバル管理者**の権限が必要です。

Admin Settings		M365 Tenant ID	Meeting Insights Tenant ID
		XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>	●	Provide the application with permissions to authenticate users with their M365 credentials, application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	<a href="#">Grant Admin Consent &gt;</a>	●	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	<a href="#">Grant Admin Consent &gt;</a>	●	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Mobile App M365 Login	<a href="#">Grant Admin Consent &gt;</a>	●	Provide the Mobile application with permissions to authenticate users with their M365 credentials, the mobile application routes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	<a href="#">Publish</a>	●	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	<a href="#">Download Script</a>	●	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

- 「Mobile App M365 Login」の横にある **Grant Admin Consent** をクリックすると、Microsoft 365 アカウントにログインするように求められます。
- Microsoft 365 **グローバル管理者** アカウントにログインすると、次の権限ダイアログボックスが表示されます。



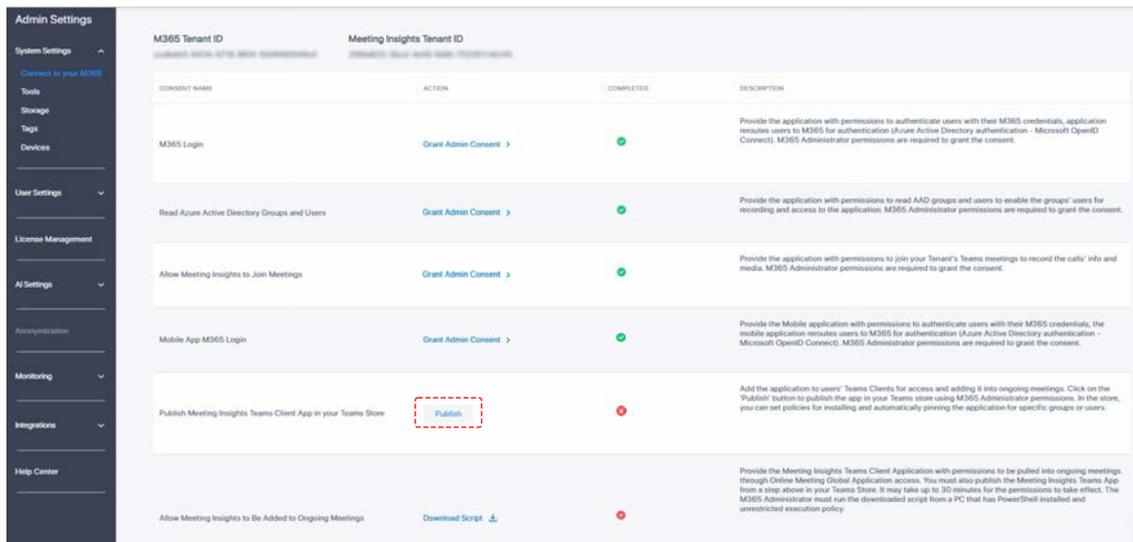
- c. **Accept** をクリックすると、「Completed」列に  アイコンが表示され、「Mobile App M365 Login」への同意が正常に付与されたことが示されます。

6. 「Publish Meeting Insights Teams Client App in your Teams Store」同意：( 権限の詳細は [Microsoft Entra ID Meeting Insights Teams アプリケーション](#) を参照してください)

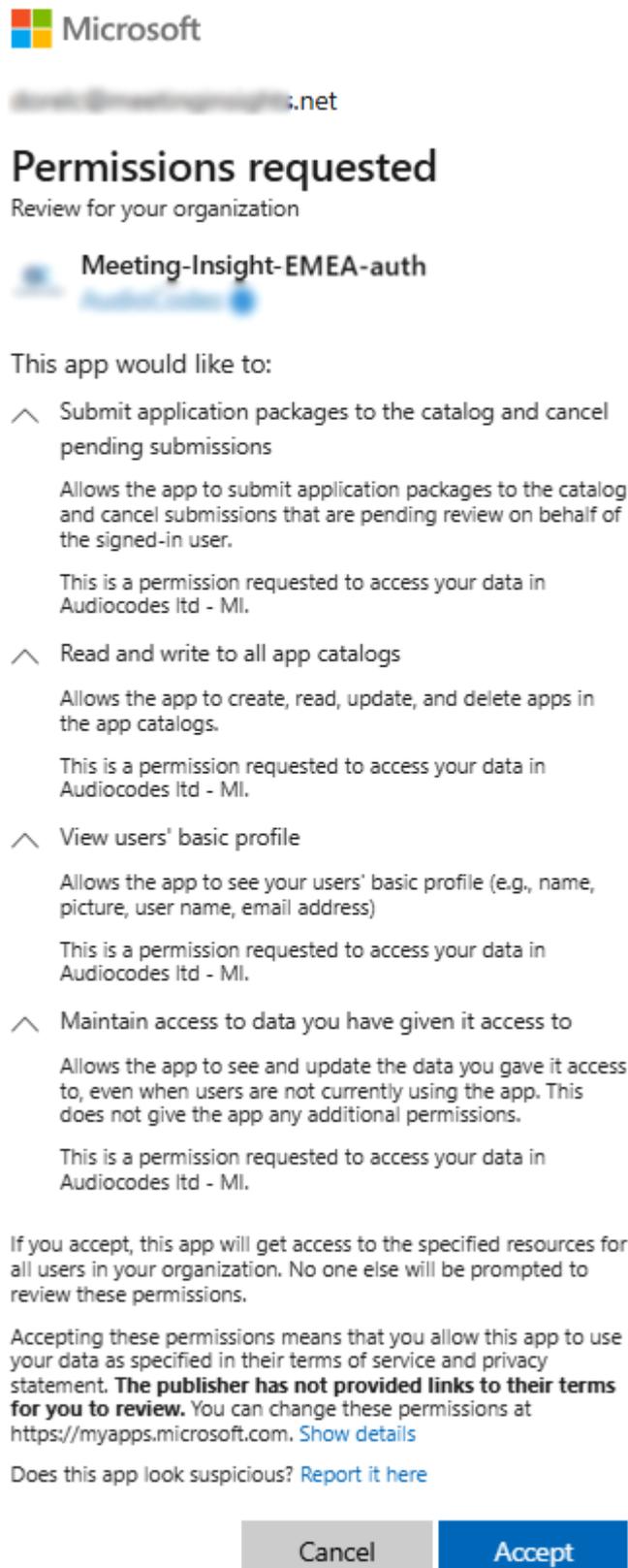
この同意により、Meeting Insights アプリが Teams ストアとユーザーの Teams クライアントに追加され、アクセスして進行中の会議に追加できるようになります。



- この同意を付与するには Microsoft 365 **グローバル管理者**の権限が必要です。
- Teams ストアでは、特定のグループやユーザーにアプリケーションをインストールしたり自動的にピン留めするポリシーを設定できます
- または、[こちら](#)に示されているように、「ツール」ページを使用してアプリを公開することもできます。



- a. 「Publish Meeting Insights Teams Client App in your Teams Store」の横にある **Publish** をクリックすると、Microsoft 365 アカウントにログインするように求められます。
- b. Microsoft 365 グローバル管理者アカウントにログインすると、次の権限ダイアログボックスが表示されます。



The screenshot shows a Microsoft permissions dialog box. At the top is the Microsoft logo and the text "Microsoft". Below that is the email address "xxxx@meetinginsights.net". The main heading is "Permissions requested" with the subtitle "Review for your organization". The app name "Meeting-Insight-EMEA-auth" is displayed with a blurred icon. The section "This app would like to:" lists four permissions, each with a description and a note that the data is accessed in "Audiocodes ltd - MI". The permissions are: "Submit application packages to the catalog and cancel pending submissions", "Read and write to all app catalogs", "View users' basic profile", and "Maintain access to data you have given it access to". Below the list, there is a warning: "If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions." A note states: "Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)". At the bottom, there is a question: "Does this app look suspicious? [Report it here](#)". At the very bottom are two buttons: "Cancel" and "Accept".

- c. **Accept** をクリックすると、「Completed」列に  アイコンが表示され、「Publish Meeting Insights Teams Client App in your Teams Store」の同意が正常に付与されたことが示さ

れます。さらに、「Application published in your Teams store successfully」という通知メッセージが表示されます。

- d. [推奨] [こちら](#)に示されているように、Meeting Insights ユーザー向けにアプリケーションをインストールしてピン留めします。

## 7. 「Allow Meeting Insights to be Added to Ongoing Meetings」同意:( 権限の詳細は進行中の会議に Meeting Insights を追加できるようにする – スクリプトを実行する必要がありま (オプション) を参照してください)

この同意により、Meeting Insights Teams クライアント アプリに、オンライン会議グローバルアプリケーションアクセスを通じて進行中の会議に参加するための権限が付与されます。このステージでは、PowerShell スクリプト ファイルを実行して、同じ同意済みアプリIDに接続するアクセス ポリシーを作成し、ユーザーが Mia を Teams 会議にアドホックに参加できるようにします。

The screenshot shows the 'Admin Settings' page with a table of consent requests. The table has columns for 'CONSENT NAME', 'ACTION', 'COMPLETED', and 'DESCRIPTION'. The row 'Allow Meeting Insights to be Added to Ongoing Meetings' has a 'Download Script' button highlighted with a red dashed box. The 'COMPLETED' column for this row shows a red dot, indicating it is not yet completed.

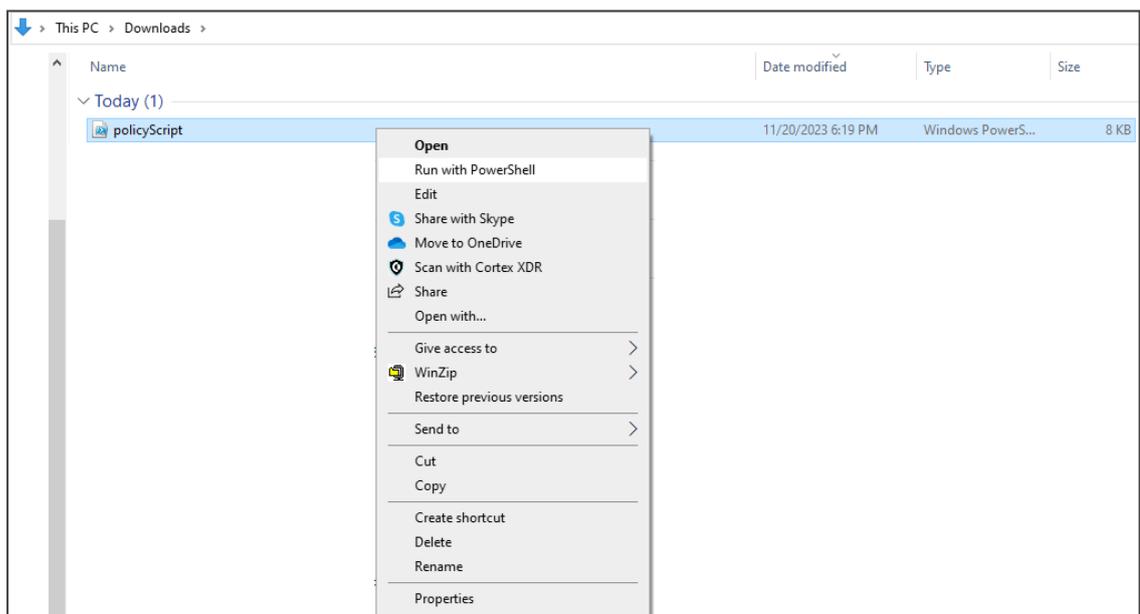
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent</a>	●	Provide the application with permissions to authenticate users with their M365 credentials, application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	<a href="#">Grant Admin Consent</a>	●	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	<a href="#">Grant Admin Consent</a>	●	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Mobile App M365 Login	<a href="#">Grant Admin Consent</a>	●	Provide the Mobile application with permissions to authenticate users with their M365 credentials, the mobile application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	<a href="#">Publish</a>	●	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to be Added to Ongoing Meetings	<a href="#">Download Script</a>	●	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

- a. 「Allow Meeting Insights to be Added to Ongoing Meetings」同意の横にある **Download Script** をクリックします。「policyScript」ファイルがPCにダウンロードされます。
- b. ダウンロードしたスクリプト ファイルはオペレーティングシステムによってブロックされている可能性があるため、実行前にブロックを解除してください。ブロックを解除するには、ファイルを右クリックし、**Properties** を選択します。Windows 11 を使用している場合は、まず **Show more options** をクリックして、コンテキスト メニューに **Properties** オプションを表示します。**General** タブを選択し、「Security」セクションの **Unblock** オプションをオンにします。

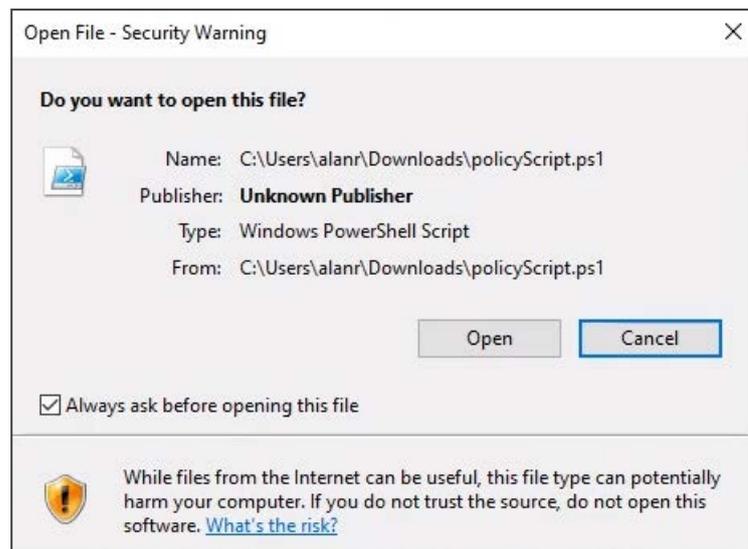


- ダウンロードしたスクリプトを実行するには、コンピューターに PowerShell がインストールされており、Microsoft 365 グローバル管理者の権限を持っている必要があります。
- デフォルトでは、スクリプトは「Bypass」実行ポリシーで実行されます。
- スクリプトは次の PowerShell コマンドレットを実行します。
  - ✓ `Start-Process`: ローカルコンピューター上でプロセスを開始します。
  - ✓ `Invoke-RestMethod`: 単純な HTTP/S リクエストを実行して、Meeting Insights でトークンを検証します。
  - ✓ `Install-Module MicrosoftTeams`: Microsoft Teams モジュールをインストールします。
  - ✓ `Import-Module MicrosoftTeams`: Microsoft Teams モジュールをインポートします。
  - ✓ `Connect-MicrosoftTeams`: Microsoft Teams に接続します。
  - ✓ `Get-CsApplicationAccessPolicy`: テナントで使用するために構成されたアプリケーション アクセス ポリシーを取得します。
  - ✓ `Set-CsApplicationAccessPolicy`: アプリケーション アクセス ポリシーを作成します。

c. ファイルを右クリックし、**Run with PowerShell** を選択します。

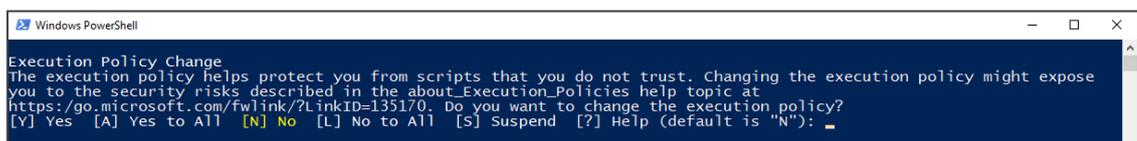


次のダイアログ ボックスが表示されます。

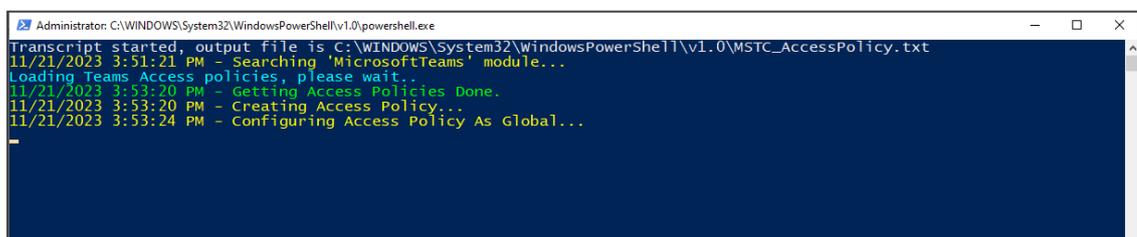


- d. **Open** をクリックすると、PowerShell が開きます。前述したように、PowerShell コマンドは次のように実行されます。

```
-----
Start-Process (PowerShell の実行を開始します)
Invoke-RestMethod (Meeting Insights システムへの接続を確認します)
Install-Module MicrosoftTeams & Import-Module MicrosoftTeams (Teams モジュールをインストールします)
Connect-MicrosoftTeams (Teams テナントに接続します)
Get-CsApplicationAccessPolicy (ボット ID が既に存在するかどうかを確認します)
Set-CsApplicationAccessPolicy( ボット IDをポリシーに追加します)
-----
```



- e. [注：実行ポリシーを初めて変更した後は、この画面が常に表示されるとは限りません。] **A (Yes to All)** と入力し、Enter キーを押します。



- f. 以下のプロンプトが表示されたら (常に表示されるとは限りません)、**Y (Yes)** と入力し、Enter キーを押します。

```
Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\Users\alanr\Downloads\MSTC_AccessPolicy.txt
11/21/2023 3:07:24 PM - Searching 'MicrosoftTeams' module...
11/21/2023 3:07:30 PM - 'MicrosoftTeams' module not found, installing module...

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\alanr\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): -
```

g. 続行するには Enter キーを押してください:

```
Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\WINDOWS\System32\WindowsPowerShell\v1.0\MSTC_AccessPolicy.txt
11/29/2023 11:54:15 AM - Searching 'MicrosoftTeams' module...
Loading Teams Access policies, please wait..
11/29/2023 11:55:31 AM - Getting Access Policies Done.
11/29/2023 11:55:31 AM - Creating Access Policy...
11/29/2023 11:55:36 AM - Configuring Access Policy As Global...
11/29/2023 11:55:40 AM - Access Policy As Global Has Been Configured.
{
  "time": "2023-11-29T11:54:15.292+02:00",
  "primaryBotAppId": "9477c4e8-d26e-433d-8258-289e7d2af586",
  "statusCode": 1,
  "message": "Failure",
  "extendedInfo": [
    {
      "stepName": "Access Policy Creation",
      "stepMessage": "\\\"MI-NG-AccessPolicy\" not found"
    }
  ]
}
Press Enter to continue...: -
```



上記を実行すると Meeting Insights ボット (「Mia」) のみに Teams の会議に参加する権限が付与されます。さらに、Meeting Insights ライセンスを持つユーザーのみが、Meeting Insights ボットを追加して会議に参加できます。

オンライン会議グローバルアプリケーションアクセスを通じて進行中の会議に参加するためのアクセス許可を、Meeting Insights Teams クライアント アプリに正常に付与しました。権限が有効になるまでに最大 30 分かかる場合があります。M365 管理者は、PowerShell がインストールされ、無制限の実行ポリシーが設定されている PC からダウンロードしたスクリプトを実行する必要があります。

CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>	<span style="color: green;">●</span>	Provide the application with permissions to authenticate users with their M365 credentials, application requires users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	<a href="#">Grant Admin Consent &gt;</a>	<span style="color: green;">●</span>	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	<a href="#">Grant Admin Consent &gt;</a>	<span style="color: green;">●</span>	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Mobile App M365 Login	<a href="#">Grant Admin Consent &gt;</a>	<span style="color: green;">●</span>	Provide the Mobile application with permissions to authenticate users with their M365 credentials, the mobile application routes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	<a href="#">Publish</a>	<span style="color: green;">●</span>	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	<a href="#">Download Script ↓</a>	<span style="color: green;">●</span>	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

Microsoft 365 の接続に成功しました。

Next: [こちら](#)に示されているように Meeting Insights ユーザーにライセンスを割り当てます。



「自動編集可能」機能は、この権限を持つユーザーが会議に参加した場合にのみ会議で有効になります。ユーザーが参加していない場合、自動的に編集することはできません。

## 顧客の Azure エンタープライズ アプリケーションにおける権限

このセクションでは、[Microsoft 365 に接続する](#)に指示されている通り、Microsoft 365 の接続と同意のプロセス中に顧客の Microsoft Entra ID エンタープライズ アプリケーションで作成される Meeting Insights アプリケーションに適用される Microsoft Graph のアクセス許可について説明します。。

### Microsoft Entra ID Meeting Insights Web アプリケーション

Microsoft 365 資格情報を使用してユーザーを認証するためのアプリケーション権限を付与し、アプリケーションは認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。

同意を与えるには、Microsoft 365 管理者の権限が必要です。

権限の説明:

1. Microsoft Graph メール - ユーザーのメールアドレスを表示する (委任)
2. Microsoft Graph オフライン アクセス - アクセスを許可したデータへのアクセスを維持します (委任)
3. Microsoft Graph openid - ユーザーのサインイン (委任)
4. Microsoft Graph プロフィール - ユーザーの基本プロフィールを表示する (委任)
5. Microsoft Graph User.Read - サインインしてユーザープロフィールを読み取る (委任)

MSFT Planner との統合については、管理者が有効にしている場合 (オプション):

6. Microsoft Graph Tasks.ReadWrite - ユーザーのタスクとタスクリストの作成、読み取り、更新、削除 (委任)

### Microsoft Entra ID Meeting Insights アプリケーション

アプリケーションに Microsoft Entra ID グループとユーザーの読み取り権限を付与し、グループのユーザーがアプリケーションを録画したりアクセスしたりできるようにしますアプリケーションを有効にして、会議に Meeting Insights Teams アプリを追加します。

同意を与えるには、Microsoft 365 管理者の権限が必要です。

1. Microsoft Graph User.Read.All - すべてのユーザーの完全なプロフィールを読み取る (アプリケーション)
2. Microsoft Graph TeamsTab.ReadWriteForChat.All - Teams アプリがすべてのチャットのすべてのタブを管理できるようにします (アプリケーション)
3. Microsoft Graph TeamsTab.Create - Microsoft Teams でタブを作成する (アプリケーション)

4. Microsoft Graph TeamsAppInstallation.ReadWriteForChat.All - すべてのチャットの Teams アプリを管理します (アプリケーション)
5. Microsoft Graph GroupMember.Read.All - すべてのグループメンバーシップを読み取る (アプリケーション)

### Microsoft Entra ID Meeting Insights ボットアプリケーション

通話情報とメディアを録画し、会議の参加者を読み取るために、テナントの Teams 会議に参加する権限をアプリケーションに付与します (チャット権限)。

同意を与えるには、Microsoft 365 管理者の権限が必要です。

1. **Microsoft Graph Calls.JoinGroupCall.All:** アプリとしてグループ通話や会議に参加する (アプリケーション)
2. **Microsoft Graph OnlineMeetings.Read.All:** オンライン会議の詳細を読み取る (アプリケーション)
3. **Microsoft Graph Chat.ReadBasic.All:** すべてのチャット スレッドの名前とメンバーを読み取ります (アプリケーション)
4. **Microsoft Graph Calls.AccessMedia.All:** アプリ (アプリケーション) として通話中のメディアストリームにアクセスする  
内部通信アプリケーション ロールの権限:
  5. **BotRole:** ボットロール (アプリケーション)
  6. **DaemonRole:** デーモンロール (アプリケーション)

### Microsoft Entra ID Meeting Insights Teams アプリケーション

組織の Teams ストアで Meeting Insights Teams アプリを追加および更新する権限をアプリケーションに付与します。

1. Microsoft Graph AppCatalog.Submit - アプリケーション パッケージをカタログに送信し、保留中の送信をキャンセルします (委任)
2. Microsoft Graph AppCatalog.ReadWrite.All - すべてのアプリカタログの読み取りと書き込み (委任)
3. Microsoft Graph openid - ユーザーのサインイン (委任)
4. Microsoft Graph メール - ユーザーのメールアドレスを表示する (委任)
5. Microsoft Graph プロフィール - ユーザーの基本プロフィールを表示する (委任)

### Microsoft Entra ID Meeting Insights モバイルアプリケーション

Microsoft 365 資格情報を使用してユーザーを認証するためのアプリケーション権限を付与し、アプリケーションは認証のためにユーザーを Microsoft 365 にリダイレクトします (Microsoft Entra ID 認証 - Microsoft OpenID Connect)。

同意を与えるには、Microsoft 365 管理者の権限が必要です。

権限の説明:

1. Microsoft Graph User.Read - サインインしてユーザープロフィールを読み取る (委任)

### Microsoft Entra ID 通知ボット アプリケーション (オプション)

Meeting Insights によって録画されたときに、テナントの Teams 会議で Microsoft Teams 録画通知をトリガーするための権限をアプリケーションに付与します。

同意を与えるには、Microsoft 365 管理者の権限が必要です。

1. Microsoft Graph Calls.JoinGroupCall.All: アプリとしてグループ通話や会議に参加する (アプリケーション)
2. Microsoft Graph OnlineMeetings.Read.All: オンライン会議の詳細を読み取る (アプリケーション)
3. Microsoft Graph Calls.AccessMedia.All: アプリ (アプリケーション) として通話中のメディアストリームにアクセスする  
内部通信アプリケーション ロールの権限。
4. BotRole: ボット ロール (アプリケーション)
5. DaemonRole: デーモンロール (アプリケーション)

### 進行中の会議に Meeting Insights を追加できるようにする – スクリプトを実行する 必要があります (オプション)

Meeting Insights Teams クライアント アプリケーションに、オンライン会議グローバルアプリケーションアクセスを通じて進行中の会議に参加するための権限を付与します。

Microsoft 365 管理者は、PowerShell がインストールされ、無制限の実行ポリシーが設定されている PC からダウンロードしたスクリプトを実行する必要があります。

- オンライン会議グローバルアプリケーションアクセス

## ユーザーへの Meeting Insights ライセンスの割り当て

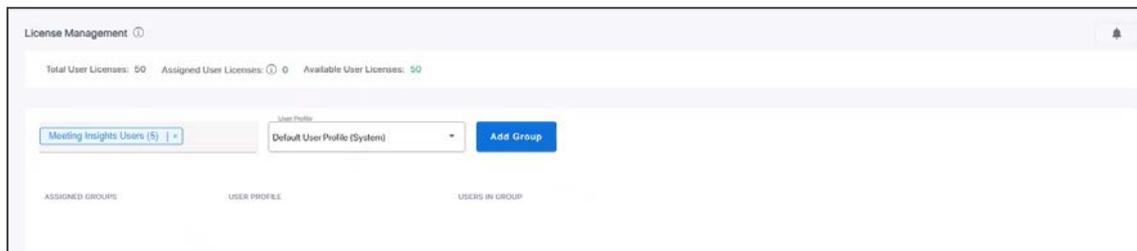
Meeting Insights の「ライセンス管理」ページを使用すると、エンタープライズ管理者は、組織の Microsoft Entra ID で管理されているユーザー グループに Meeting Insights ライセンスを割り当てることができます。

ライセンスはユーザーごとに割り当てられます。ライセンスがグループに割り当てられると、そのグループ内のユーザーごとに1つのライセンスが消費され、組織が購入したライセンスの合計数から差し引かれます。

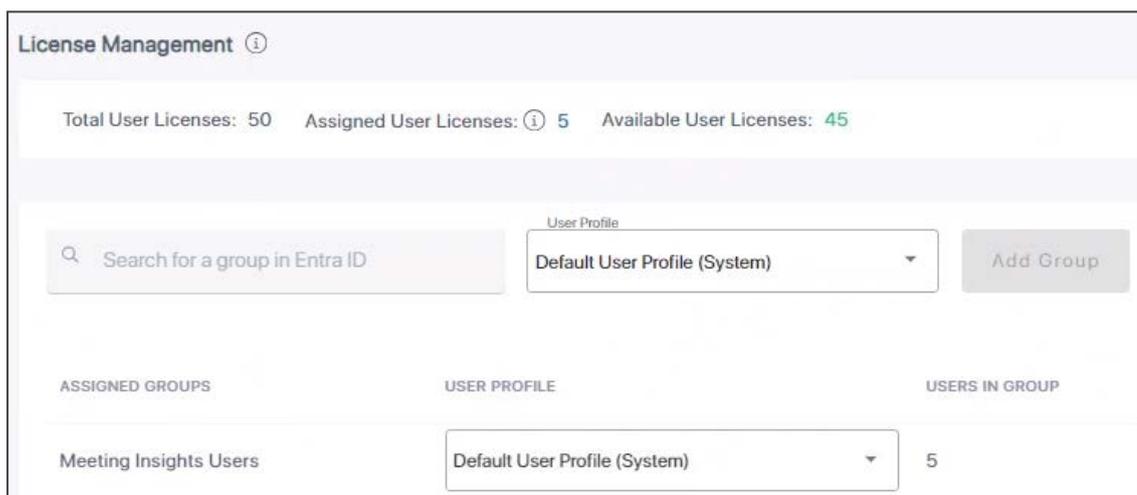
Entra ID からグループを選択するときは、そのグループをユーザープロフィールに関連付ける必要もあります。ユーザープロフィールはユーザープロフィールで定義され、これらのユーザーに対して Meeting Insights がどのように構成されるかを決定します。

➤ グループにライセンスを割り当てるには:

1. 「Admin Settings」メニュー ペインで **License Management** をクリックすると、「ライセンス管理」ページが表示されます。
2. 「Search for a group in Entra ID」フィールドに、Microsoft Entra ID で定義したグループの名前の最初の文字を入力します( [Microsoft Entra ID でユーザーグループを定義する参照](#) )。次にそれを選択します( 例 : **Meeting Insights Users (5)** ):

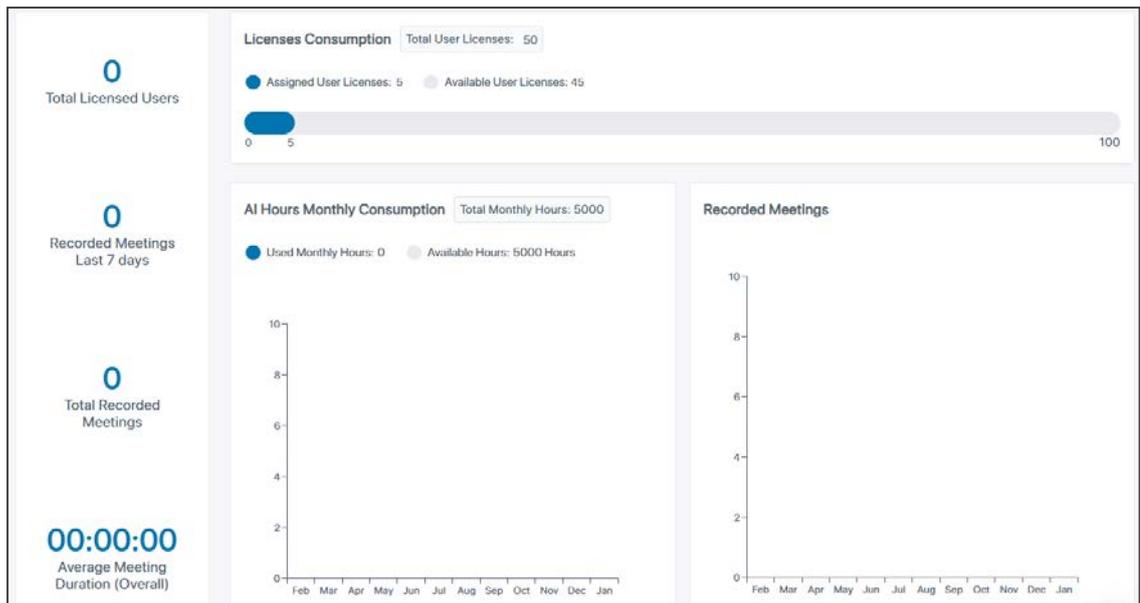


3. 「User Profile」フィールドはデフォルト ( **Default User Profile (System)** ) のままにしておきます。これにより、ユーザーは Meeting Insight にアクセスし、会議を録画できるようになります。[ユーザープロフィールの詳細情報は[こちら](#)を参照してください]。
4. **Add Group** をクリックし、**Sync and Apply** をクリックすると、Meeting Insights ライセンスがグループに割り当てられ、グループ内のユーザーはアプリを使用できるようになります。



5. 「ライセンス管理」ページの一番上に表示されるライセンスの割り当てを確認します。上の図の例では、次のようになります。
  - 合計ユーザーライセンス数: 50
  - 割り当てられたユーザーライセンス: 5
  - 利用可能なユーザーライセンス: 45
6. [オプション] この情報と使用状況を「ダッシュボード (ライセンス消費)」ページで表示します。

以下の例では、5人の Meeting Insights ユーザーのグループにライセンスが割り当てられ、過去7日間に録画された会議は0件、合計で開催された会議は0件です。



## 管理者モードとユーザーモードの切り替え

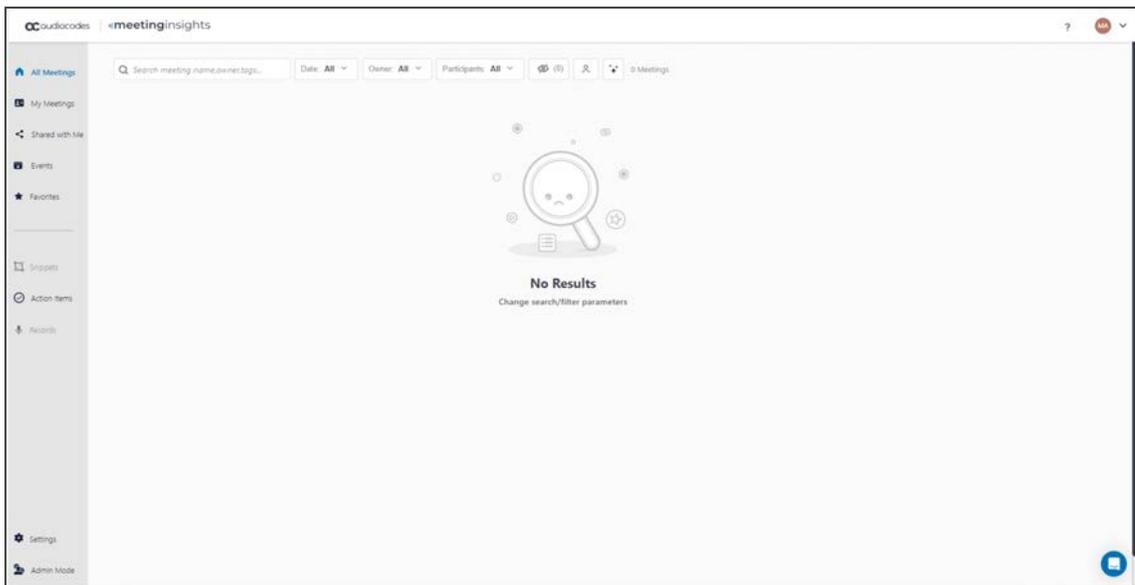
管理者はオプションで管理者モードとユーザーモードを切り替えることができます。



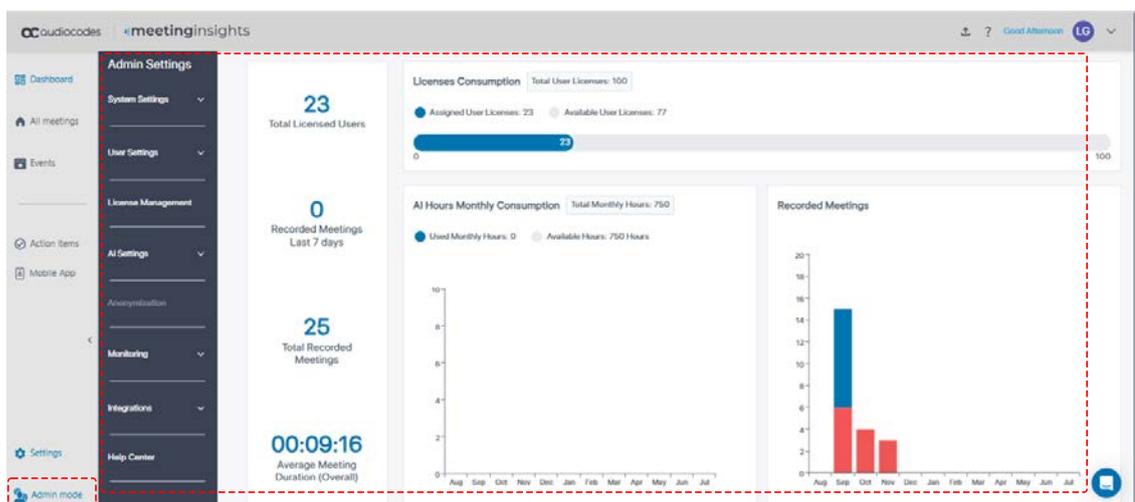
- ページの左下隅にある **Admin mode** は、管理者としてサインインしていることを示します。「Admin Settings」ナビゲーションペインにも、管理者としてサインインしたことが示されます。
- デフォルトの管理者はシステムにログインしているユーザーである必要があります(関連情報については[こちら](#)をご覧ください)。

### ➤ 管理者モードとユーザーモードを切り替えるには:

- **ユーザーモードにアクセスするには:** ウィンドウの左下隅で、 **Admin mode** をクリックします。管理者モードが終了し、ユーザーモードにアクセスします。デフォルトでは、User Settings ペインが表示されます(通常は、左側のナビゲーションメニューの **Settings** メニューをクリックすると開きます)。下の図は、展開後に会議が表示されないことを示しています。



- **管理者モードにアクセスするには:** ウィンドウの左下隅で、 **Admin mode** をクリックします。ユーザーモードが終了し、管理者モードにアクセスして、Admin Settings メニューページと「ダッシュボード」ページを表示します。



## ユーザー インターフェースの言語の変更

Meeting Insights ユーザー インターフェイス (UI) の表示言語を変更できます。言語を変更すると、通知メール、アクティビティログファイル、ダウンロードされたファイルなど、Meeting Insights の他の領域にも影響します。

言語の変更は、[ユーザー マニュアル](#)に定義されている通り、Meeting Insights のエンド ユーザー インターフェイスを通じて行われます。



現在、ユーザー インターフェイスでは次の言語がサポートされています。

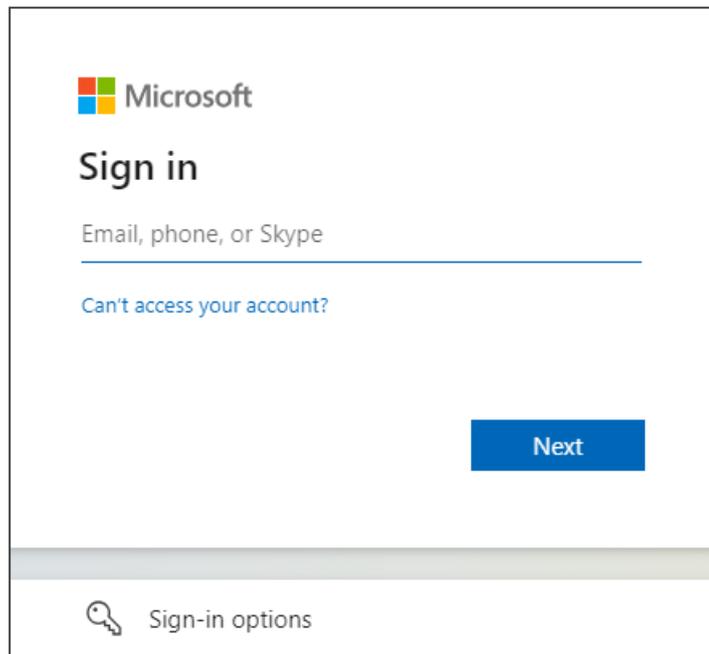
- 英語
- 日本語

## 5 Meeting Insights アプリのテスト

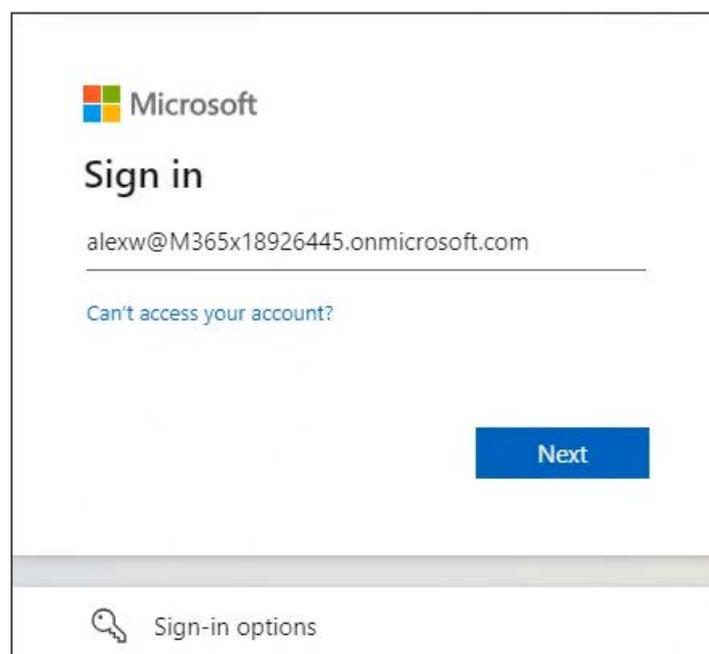
Meeting Insights を設定した後、Meeting Insights グループ内のユーザーの1人を使用してアプリをテストするのが最適な方法です。

➤ アプリをテストするには:

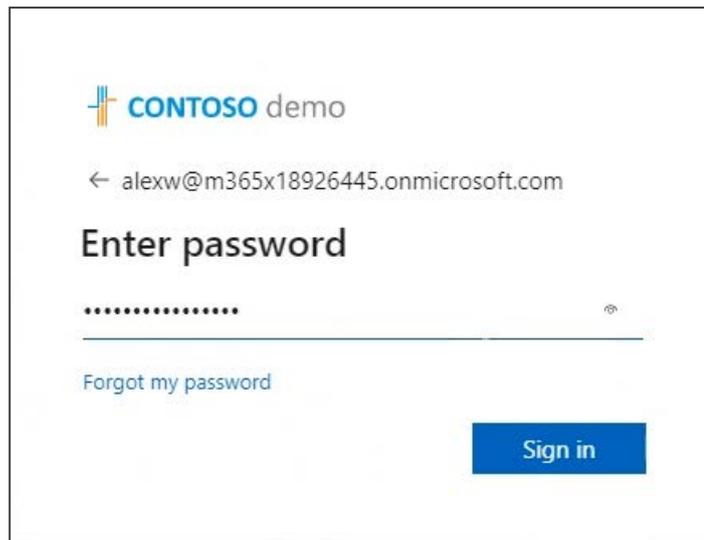
1. Teams Web アプリのリンクをクリックします。



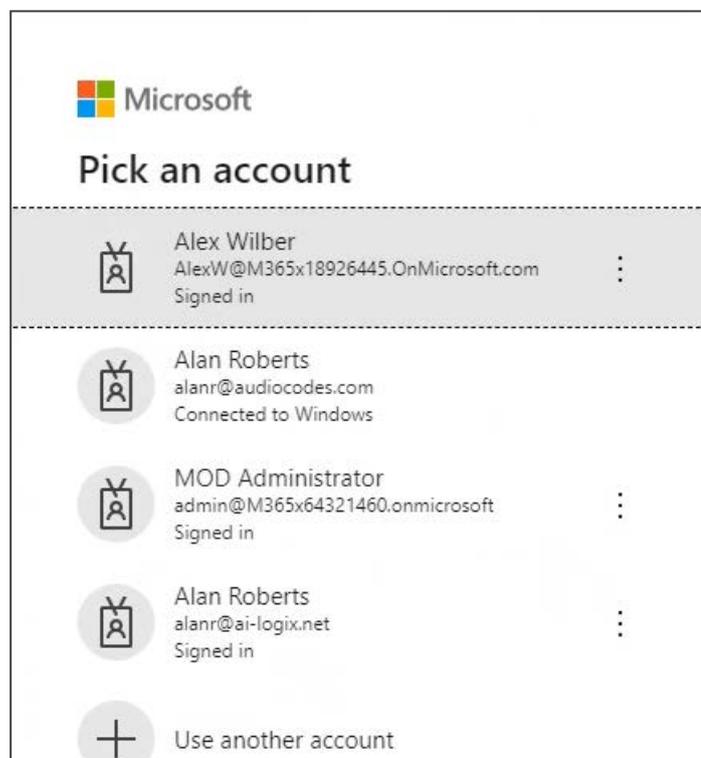
2. ユーザーの Teams クライアント のユーザー名を入力します。



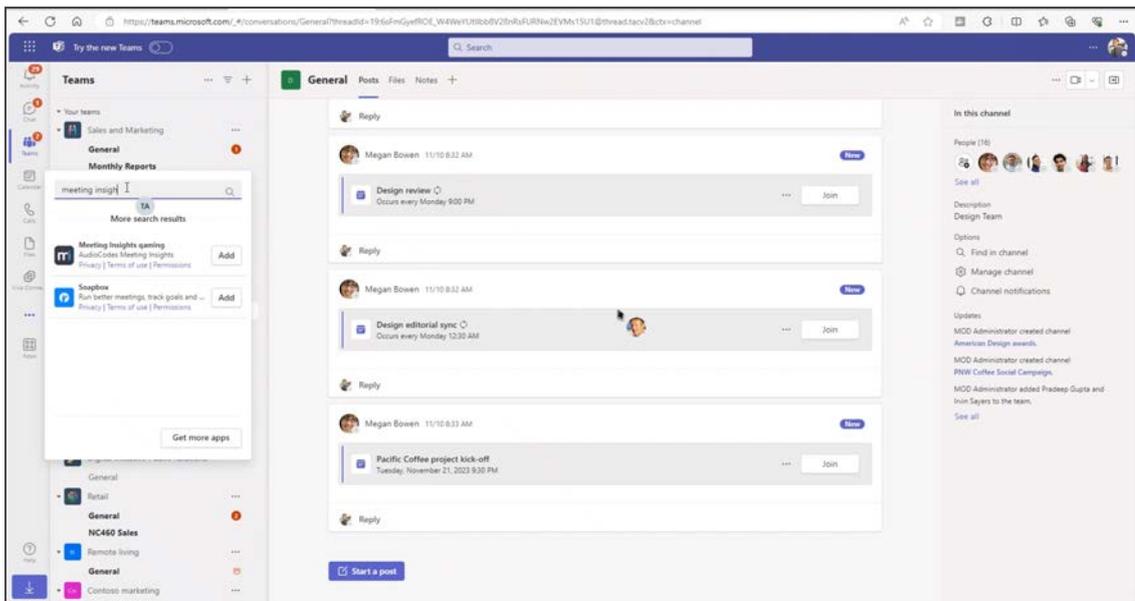
3. Next をクリックします。



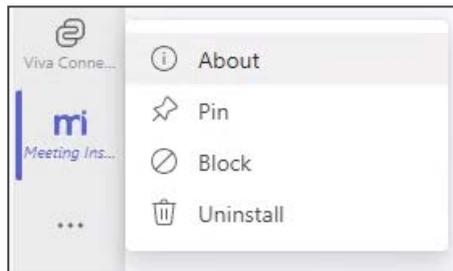
4. ユーザーの Teams クライアント パスワードを入力し、**Sign in** をクリックします。



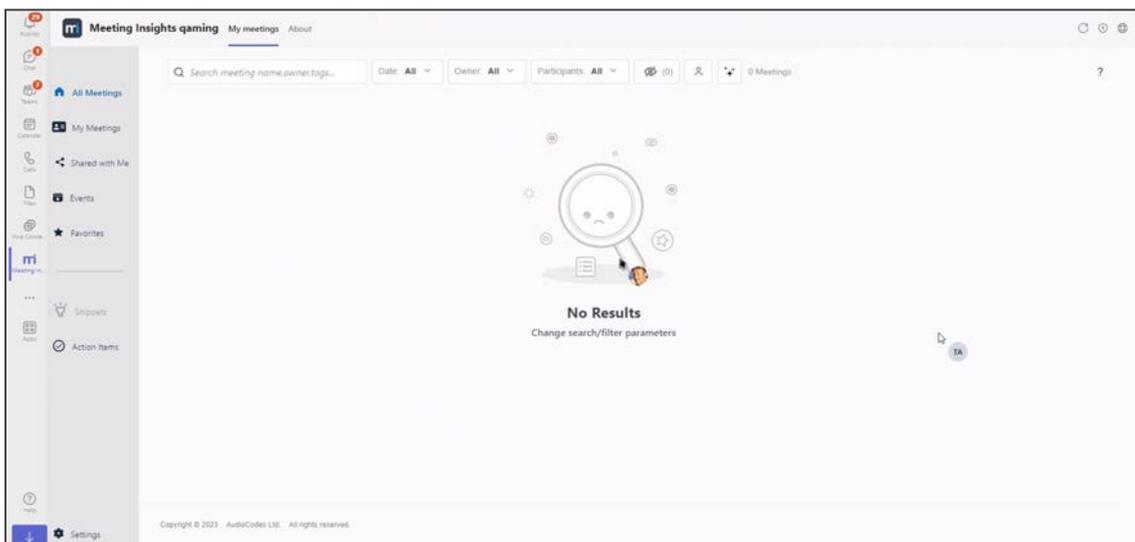
5. ユーザーのアカウントをクリックします。



6. Teams Web アプリで、左側のメニューバーの... オプションをクリックします。「Search for apps」フィールドに「Meeting Insights」と入力します。
7. Meeting Insights アプリを選択し、その横にある Add ボタンをクリックします。Meeting Insights が Teams クライアントに追加されます。
8. 左側のメニューバーに新しく追加された Meeting Insights アイコンを右クリックします。

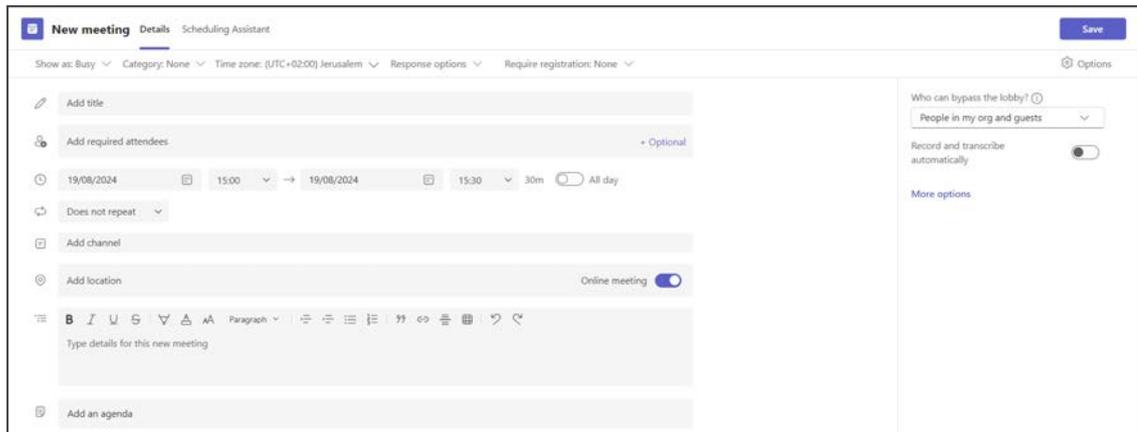


9. ポップアップから Pin を選択します。



ユーザーはこれまで Meeting Insights を使用したことがないので、会議の録画は表示されません。

10. Teams の **Calendar** アイコンをクリックし、カレンダーで **New meeting** をクリックします。



11. MIA( Meeting Insights Assistant) が参加できるよう、会議の開始時刻の少なくとも5分前に会議をスケジュールしてください。Meeting Insights Assistant( MIA) のメールアドレス (xx.mia@meetinginsights.com) を使用して、招待者リストに追加しますMeeting Insights は会議の2分前に参加します。

12. **Start Meeting** をクリックします。新しいユーザーが会議を開始して録画できることを正常にテストしました。会議ウィンドウの上部に Meeting Insights アプリのアイコンが表示されており、MIA が参加者の1人であることを確認します。



- 上記の手順では、MIA が参加するスケジュールされた会議をテストする方法について説明しています。
- 会議がスケジュールされていなかった場合は、+ **Apps** に移動して **Meeting Insights** を選択します。MIA が参加していることと、画面の上部に **Meeting Insights** タブがあることを確認します。
- 会議の終了時に、「List View」に移動して録画を再生します。Meeting Insights が会議を処理するには時間がかかりますが、ビデオ録画はほぼすぐに表示でき、オーディオは再生できることに注意してください。

## 6 誰がどのアクションを実行する権限を持っているかを決定する

次の表は、Meeting Insights でどのユーザーがどのようなアクションを実行する権限を持っているかを示しています。

	アクション	管理者	所有者	委任者	自動編集を許可	参加者
ハイライト	追加	X	√	√	√	√
	編集	X	自分の	自分の	自分の	自分の
	削除	X	自分の	自分の	自分の	自分の
	表示	√	自分の	自分の	自分の	自分の
ブックマーク	追加	X	√	√	√	√
	編集	X	自分の	自分の	自分の	自分の
	削除	X	自分の	自分の	自分の	自分の
	表示	√	自分の	自分の	自分の	自分の
スニペット	追加	X	√	√	√	√
	編集	X	自分の	自分の	自分の	自分の
	削除	X	自分の	自分の	自分の	自分の
	表示	√	自分の	自分の	自分の	自分の

	アクション	管理者	所有者	委任者	自動編集を許可	参加者
スニペット共有	制限付き	X	√	√	√	√
	共有可能	X	√	√	√	X
	組織	X	√	√	√	X
メモプライベート	追加	X	√	√	√	√
	編集	X	自分の	自分の	自分の	自分の
	削除	X	自分の	自分の	自分の	自分の
	表示	X	自分の	自分の	自分の	自分の
メモ公開	追加	X	√	√	√	√
	編集	X	√	√	√	自分の
	削除	√	√	√	√	自分の
	表示	√	√	√	√	√
リキャップ	追加	√	√	√	√	X
	編集	√	√	√	√	X
	削除	√	√	√	√	X
	表示	√	√	√	√	√
	AIトリガー	√	√	√	√	誰でもトリガーできる場合、管理者によって有効化されます

	アクション	管理者	所有者	委任者	自動編集を許可	参加者
文字起こし	編集	√	√	√	√	X
	削除	√	√	√	√	X
	表示	√	√	√	√	√
	トリガー	√	√	√	√	誰でもトリガーできる場合、管理者によって有効化されます
削除	-	√	√	√	√	X
ダウンロード	-	√	√	√	√	X
会議情報	編集	√	√	√	√	X
	表示	√	√	√	√	√
外部共有	所有者と相手側の両方に共有の許可がある場合のみ (これは外部共有の機密性のためです)。	√	√	√	√	X
内部共有	-	√	√	√	√	X
サードパーティ統合 (例: Zoho)	トリガー	√	√	√	√	X

## 7 チームのライブ イベント やウェビナーの録画

➤ Teams ライブ イベント またはウェビナーを録画するには:

- 招待状に Meeting Insights Assistant (MIA) の電子メールアドレスを追加するか、招待状を MIA に転送してください。



MIA をプレゼンター | プロデューサーとして追加できません。

## 8 システム設定の構成

通常のユーザーは管理タスクを実行できません。エンタープライズ管理者のみ可能です。管理者としてログイン後、「Admin Settings」が表示されます。

### ツール

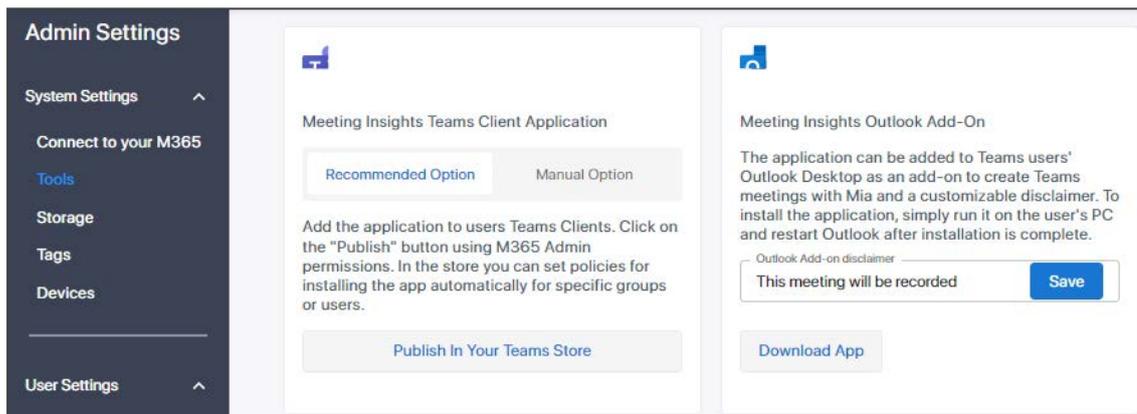
AudioCodes では、インストール追加として次の2つの補助アプリが提供されています。

- Teams クライアント内からポータルにアクセスするために AudioCodes によって提供される Meeting Insights Teams アドオン。
- AudioCodes が提供する Meeting Insights Outlook アドオンを使用すると、録画された会議のスケジュール設定が容易になります | MIA を使用した会議。

「ツール」ページを使用すると、管理者は Meeting Insights アプリを Teams クライアントや Outlook に追加できます。

#### ➤ アプリを Teams クライアント | Outlook に追加するには:

1. 「System Settings」メニューで、Tools オプションをクリックします。



2. (オプション) ユーザーの次の場所に Meeting Insights アプリを追加します。

- Teams クライアント - [こちら](#)に進む
- Outlook - [こちら](#)に進む

### Teams クライアントに Meeting Insights を追加する

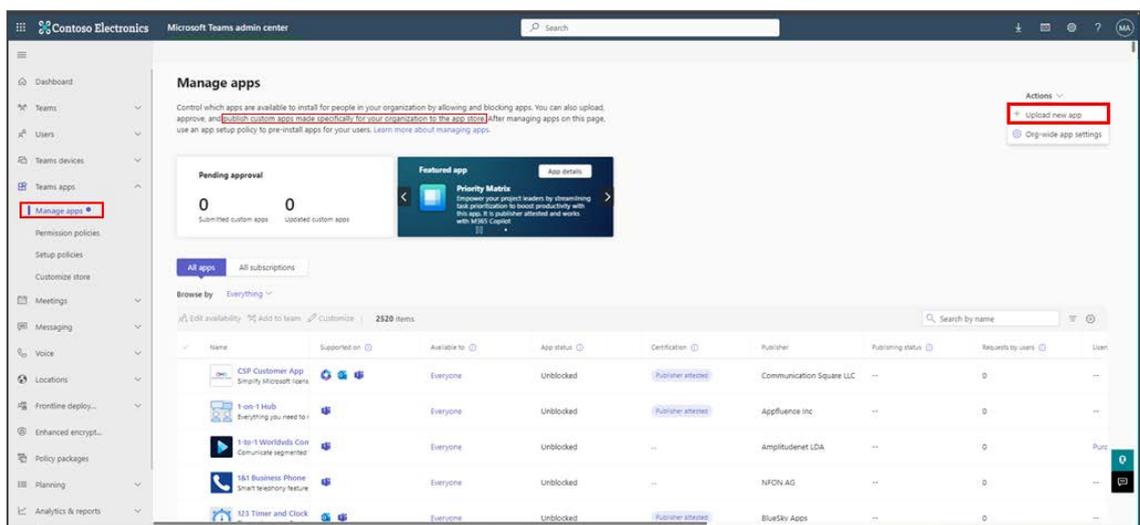
「ツール」ページを使用すると、管理者は Teams ユーザーの Teams クライアントに Meeting Insights アプリを追加できます。



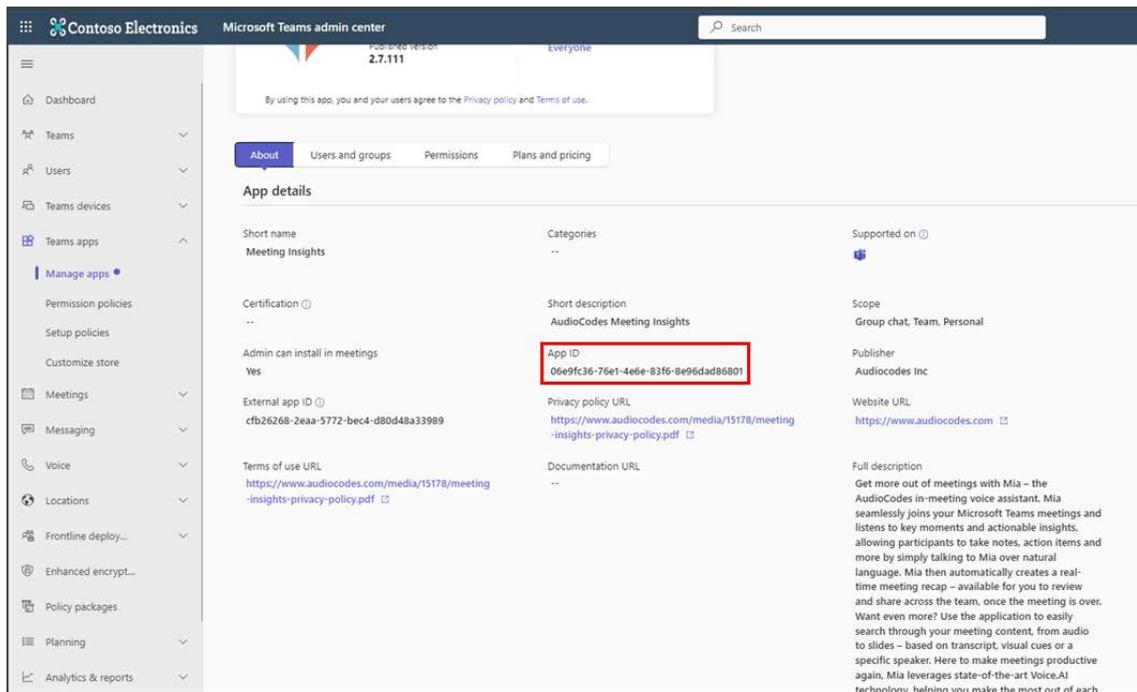
- この手順は通常、[こちら](#)に示されているように「M365に接続」ページの初期セットアップ中に実行されます(最後のステップ)。
- オプションとして、管理者は、以下で説明するように、権限を付与することなく、アプリを Teams ストアに手動で追加できます。

➤ Meeting Insights アプリを追加するには:

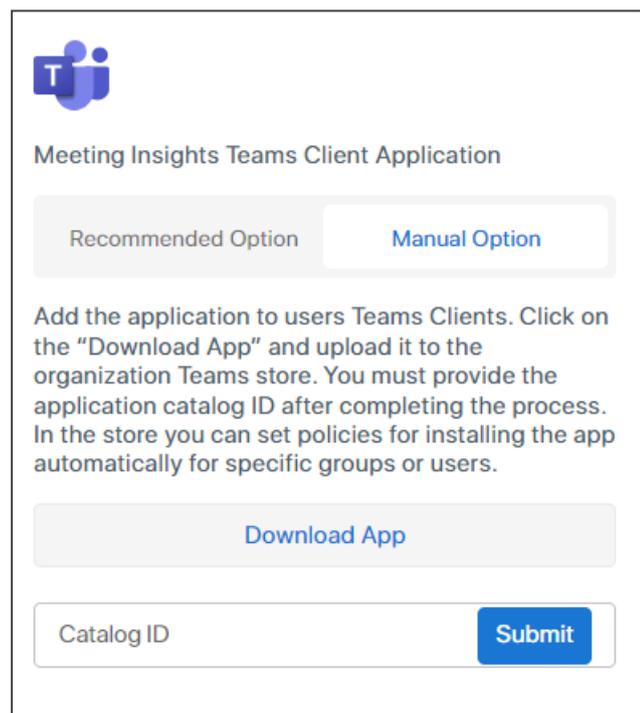
1. 「System Settings」メニューで、Tools オプションをクリックします。
2. 「Meeting Insights Teams クライアント アプリケーション」で次のいずれかを実行します。
  - Recommended Option をクリックし、Publish in your Teams Store をクリックします  
-または-
  - Meeting Insights アプリを Teams クライアントに手動で追加します (たとえば、組織向けにカスタマイズされていて、Meeting Insights が Teams アプリの公開権限を要求することに懸念がある場合)。
    - i. アプリパッケージをダウンロードします。
    - ii. Teams ストアに手動で追加します。Teams 管理者センターで、「アプリの管理」ページを開き、次の図に示すようにアップロードします。



- iii. 生成され、アプリに割り当てられたカタログ ID を見つけます。



iv. Meeting Insights の Tools > Manual Option で更新します。



v. 「Catalog ID」フィールドに入力し、Submit をクリックします。





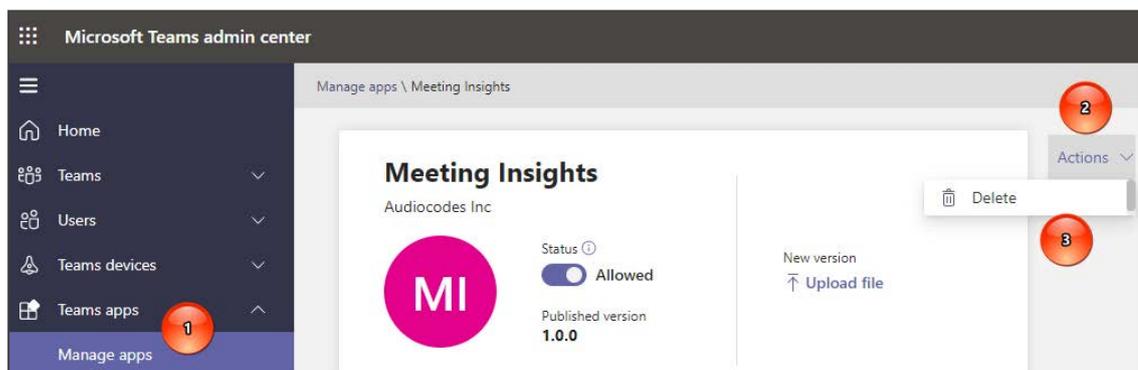
または、[こちら](#)に示されているように「M365に接続」ページで初期セットアップ中にアプリを追加します(最後のステップ)。

## TAC 経由で組織の Teams ストアにアプリを追加する

このセクションでは、Microsoft の Teams 管理者センター (TAC) を介して、組織の Microsoft Teams ストアに Meeting Insights アプリを追加する方法について説明します。

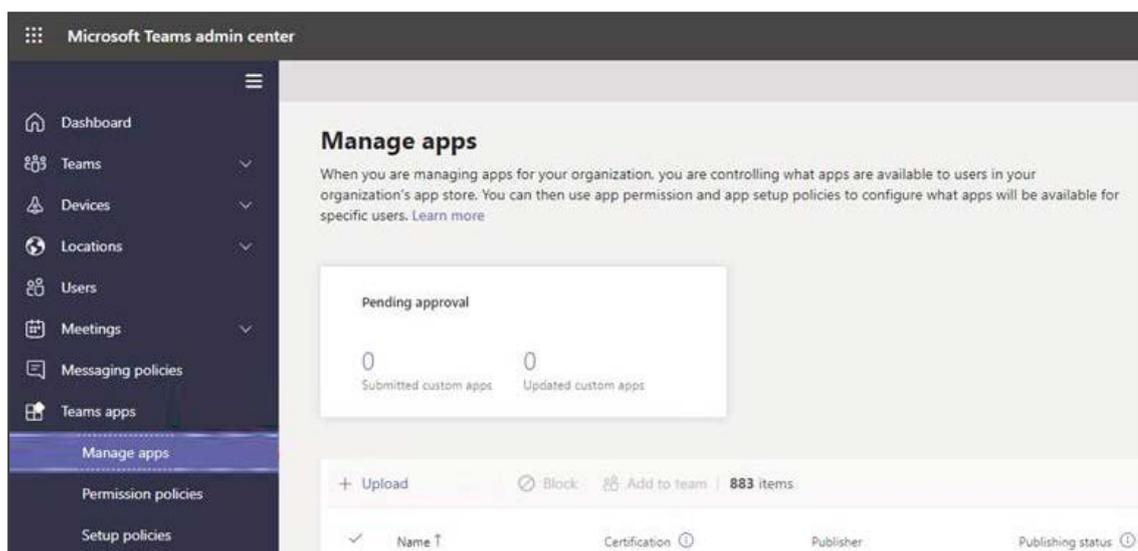
### ➤ Teams 管理者センター経由で Teams ストアに Meeting Insights アプリを追加するには:

1. 組織の Teams 管理者センターに Office 365 管理者アカウントでサインインします。
2. Teams ストアに以前のバージョンの Meeting Insights Teams アプリがある場合は、それを削除する必要があります。
  - a. 左側のナビゲーションメニューから、Teams apps > Manage apps に移動します。
  - b. Meeting Insights アプリを検索し、Actions ドロップダウンメニューから Delete を選択。

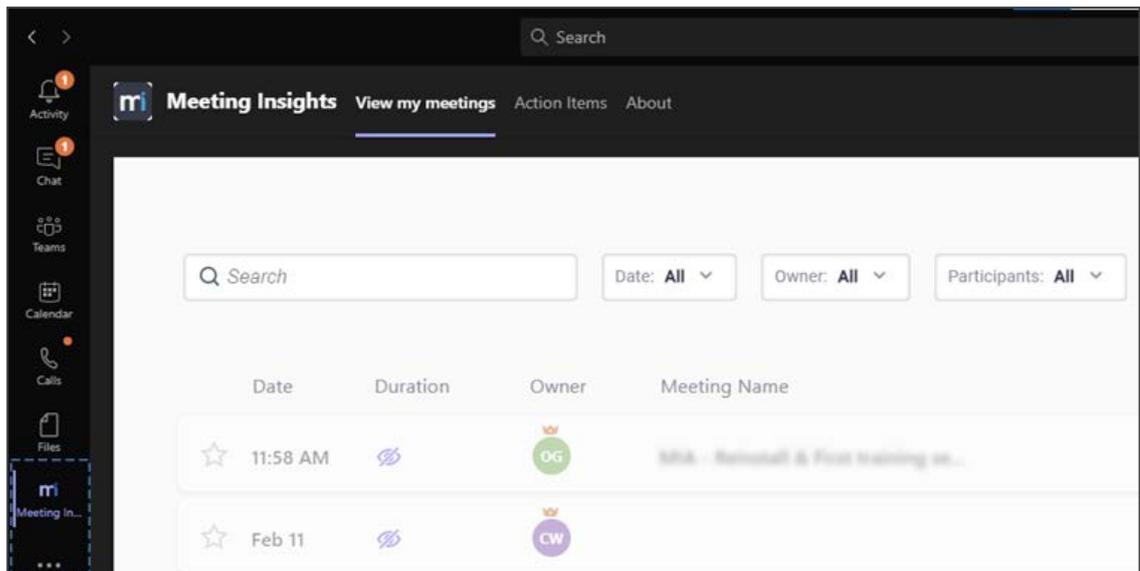


3. Meeting Insights Teams アプリのインストールファイルをアップロードします。

- a. 左側のナビゲーションメニューから、Teams apps > Manage apps に移動し、Upload をクリックします。







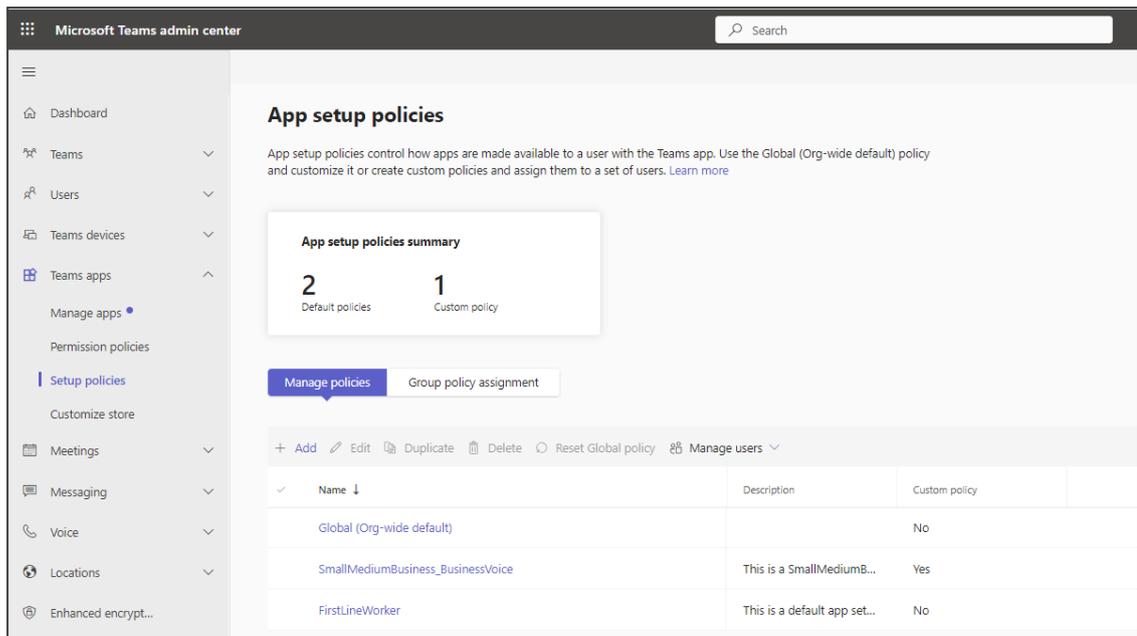
管理者は、Meeting Insights Teams アプリを組織全体またはアプリケーションを使用するユーザーグループに追加してピン留めすることをお勧めします。詳細については[こちら](#)をご覧ください。

### Meeting Insights Teams アプリを組織全体または特定のユーザーグループに追加し、ピン留めする

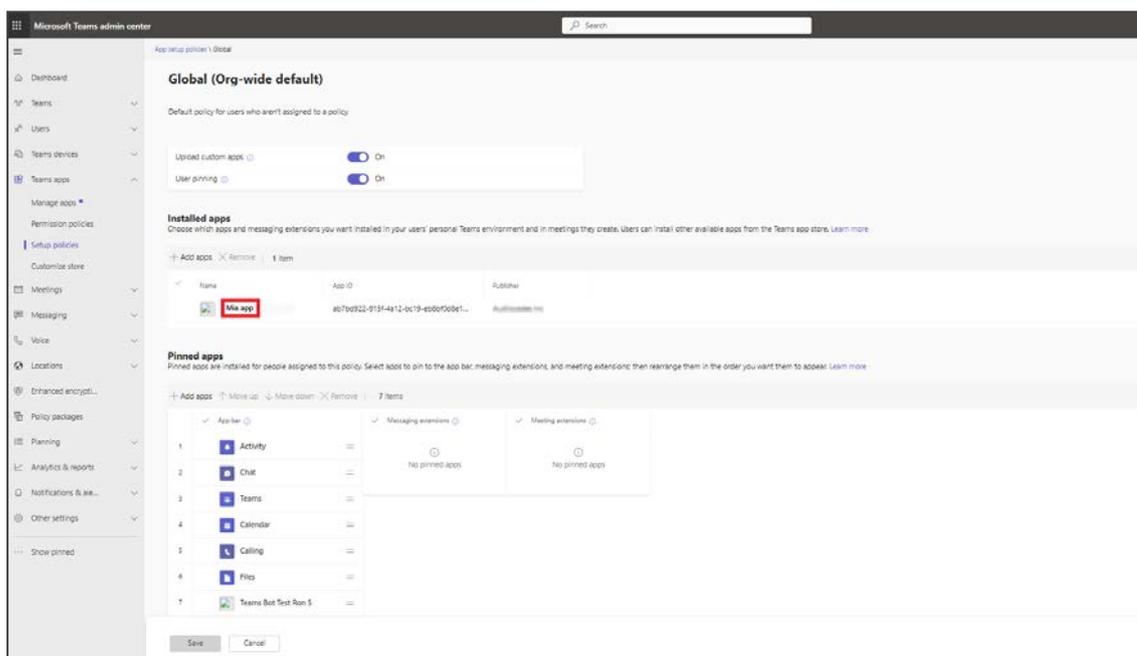
管理者は、Meeting Insights Teams アプリを組織全体またはアプリを使用するユーザーグループに追加してピン留めすることをお勧めします。

#### ➤ 組織全体またはユーザーグループに Meeting Insights Teams アプリを追加してピン留めするには:

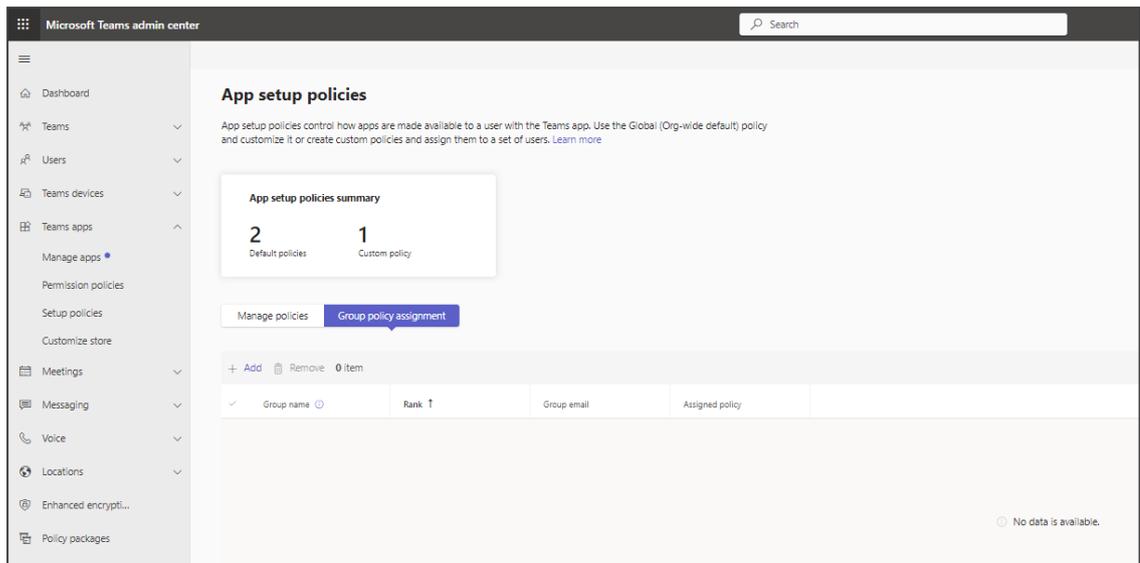
1. Microsoft Teams 管理者センター (TAC) を開いて組織ポリシーに追加するか、新しいポリシーを作成してユーザーまたはグループに割り当てます。



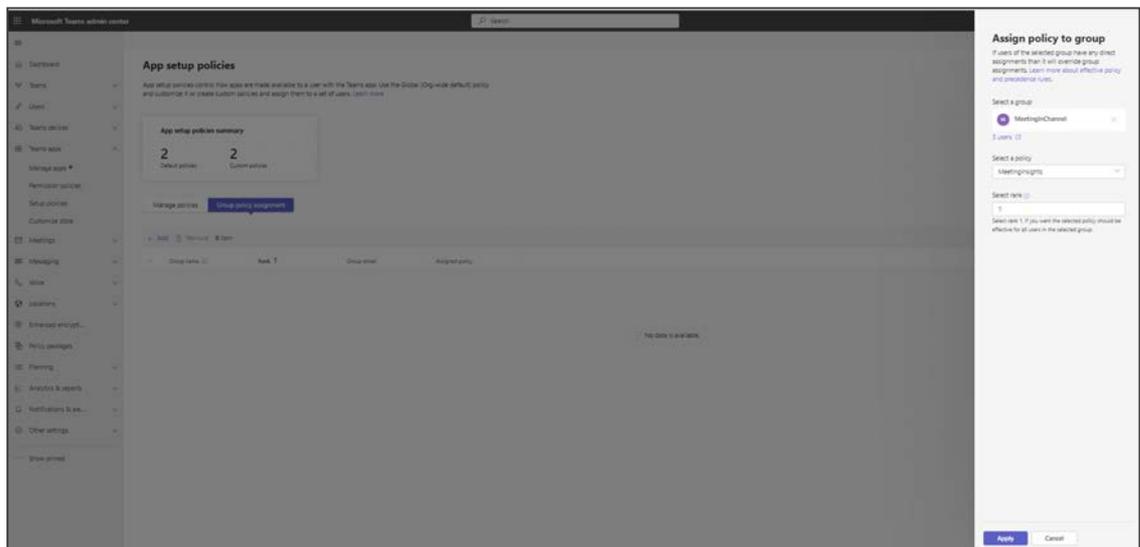
2. インストールされたアプリとピン留めされたアプリに Meeting Insights Teams アプリを追加して(推奨)、ユーザーに既定で表示されるようにします。



3. グループに適用するには、別のポリシーを作成し、インストールされてピン留めされたアプリに Meeting Insights Teams アプリを追加して、次に示すようにグループを割り当てます。
4. グループに割り当てるには、セットアップ ポリシー オプションの **Group policy assignment** をクリックします。



5. グループを割り当てるには、**Apply** をクリックします。

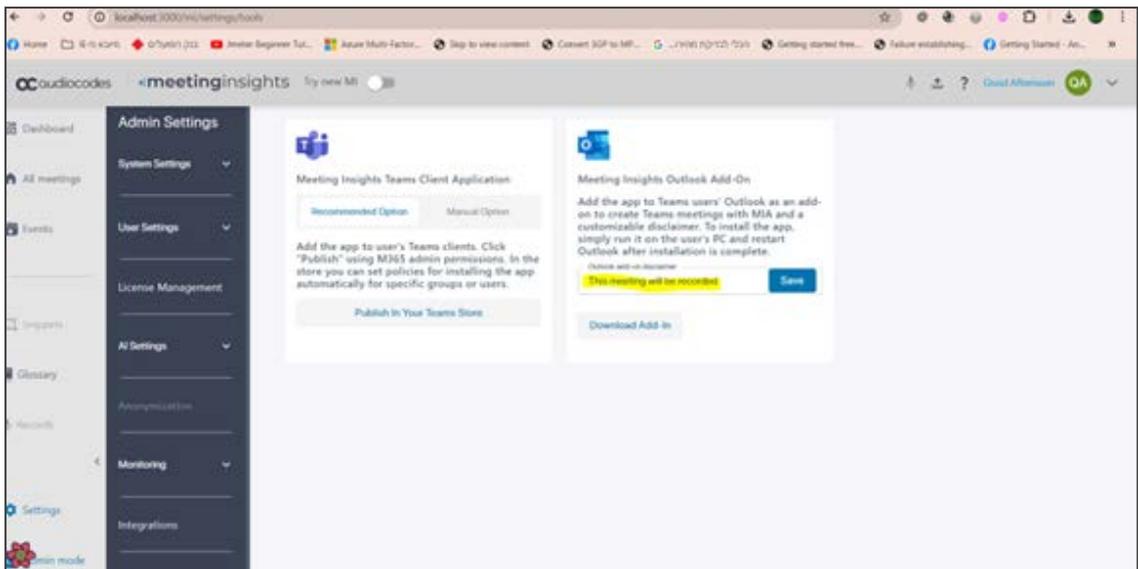


## Outlook アドインの設定

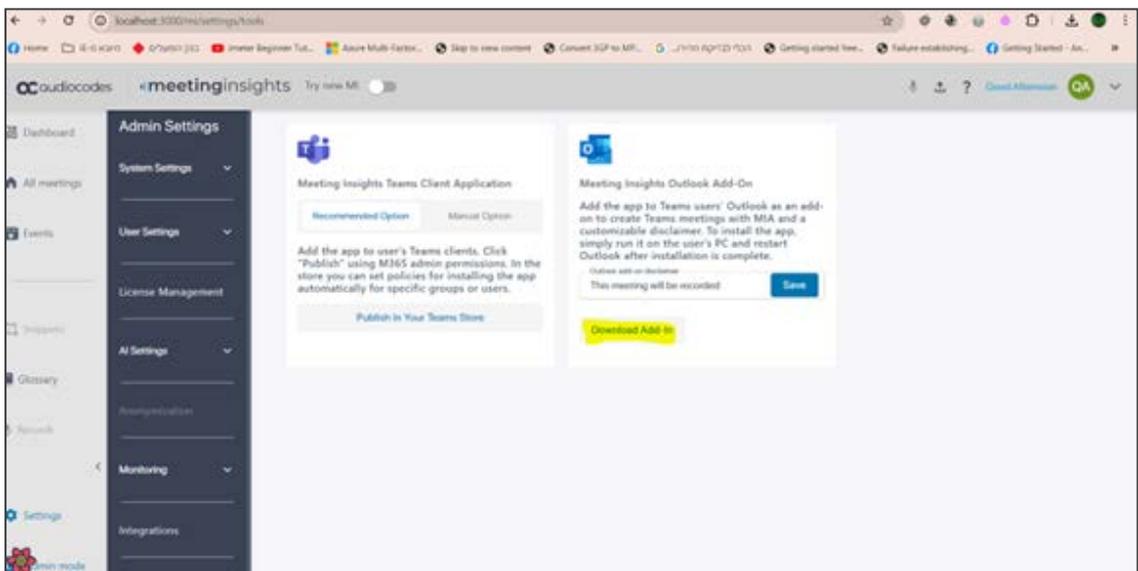
「ツール」ページを使用すると、管理者は Meeting Insights アプリをアドオンとして Teams ユーザーの Outlook に追加し、MIA を使用して Teams 会議を作成できます。以下の手順は、Microsoft Outlook アドインを設定する方法を示しています。

### ➤ Outlook アドインを設定するには:

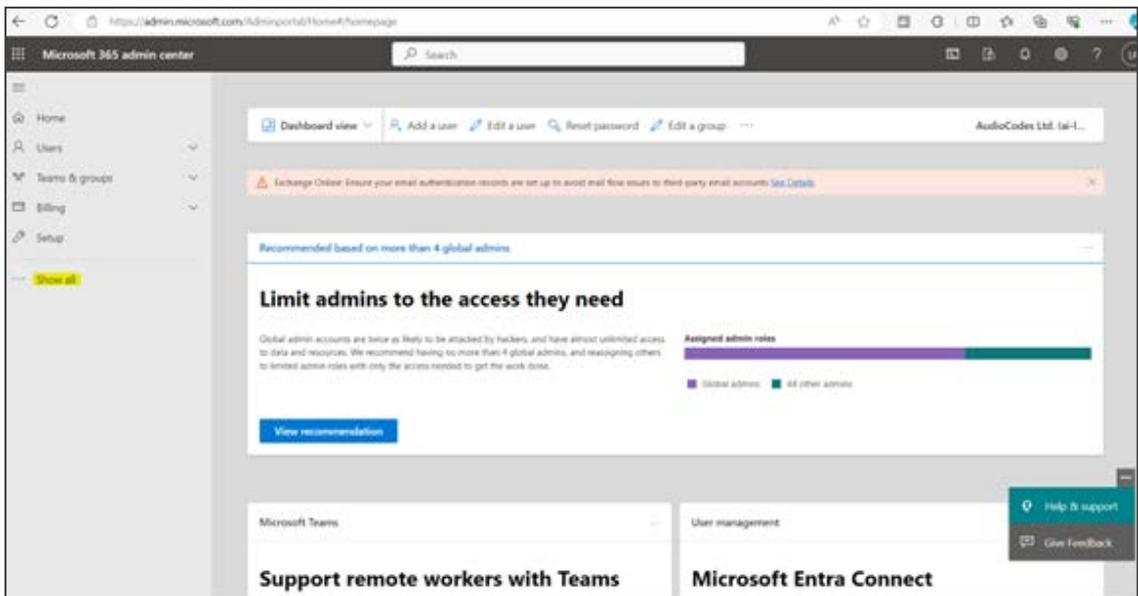
1. [推奨] 免責事項を Meeting Insights の「ツール」ページ (**Admin Settings > System Settings > Tools**) で設定します。



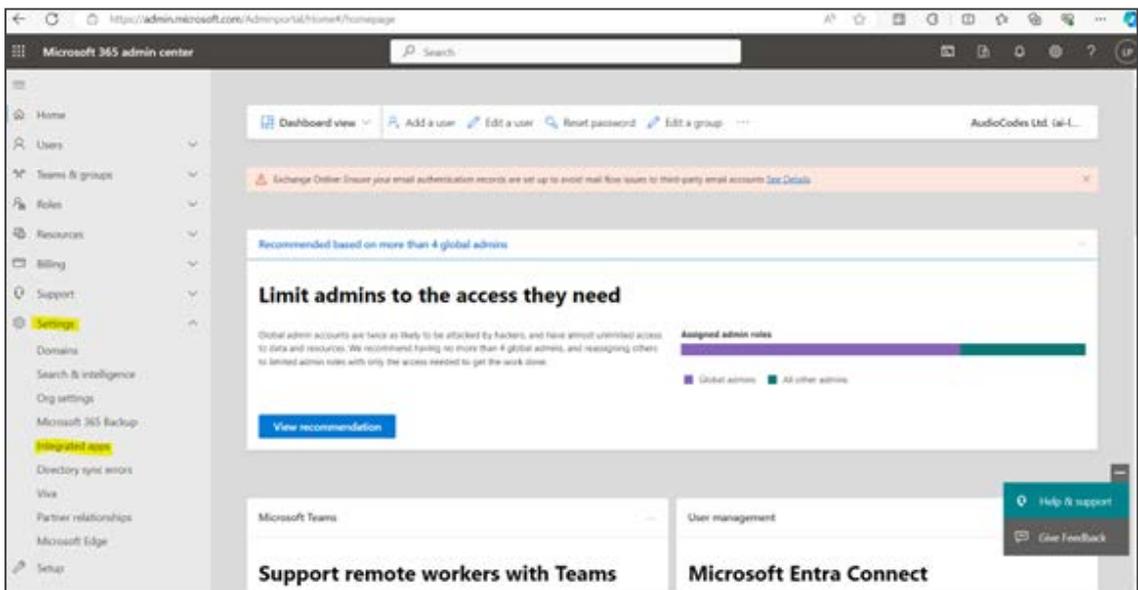
## 2. Download Add-In ボタンをクリックしてアドインをダウンロードします



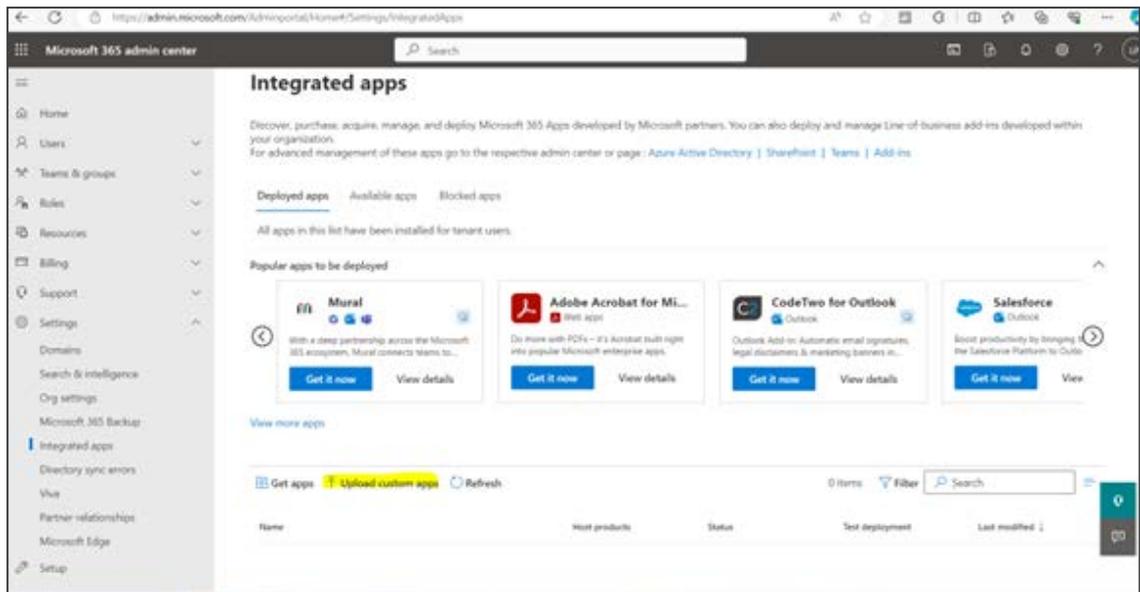
## 3. Microsoft 365 管理者センターを表示するには、<https://admin.microsoft.com/> にログインします。



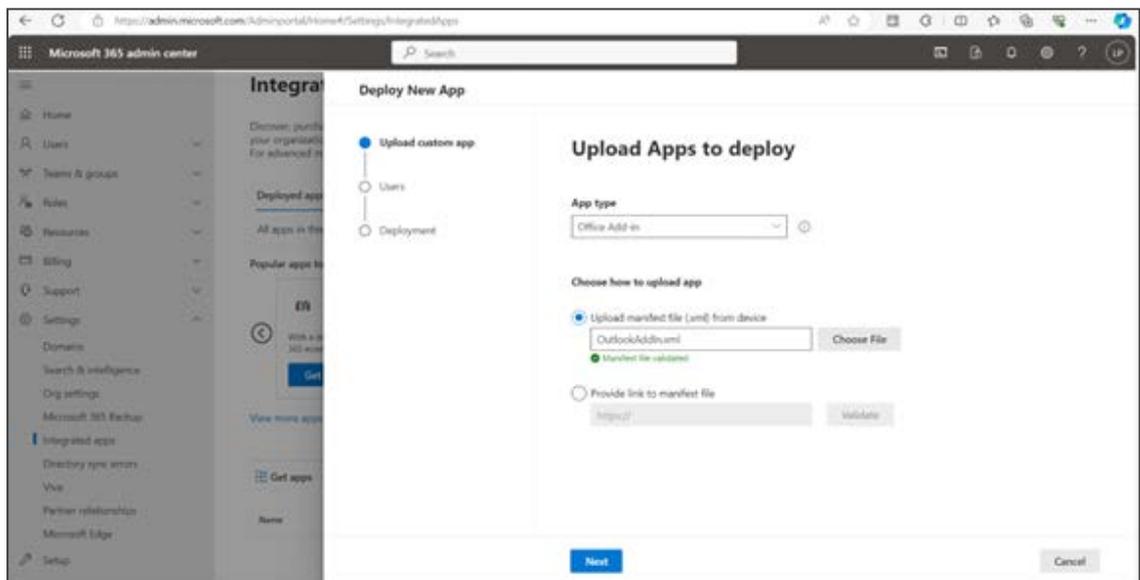
4. 前の図に示すように、Show All をクリックします。



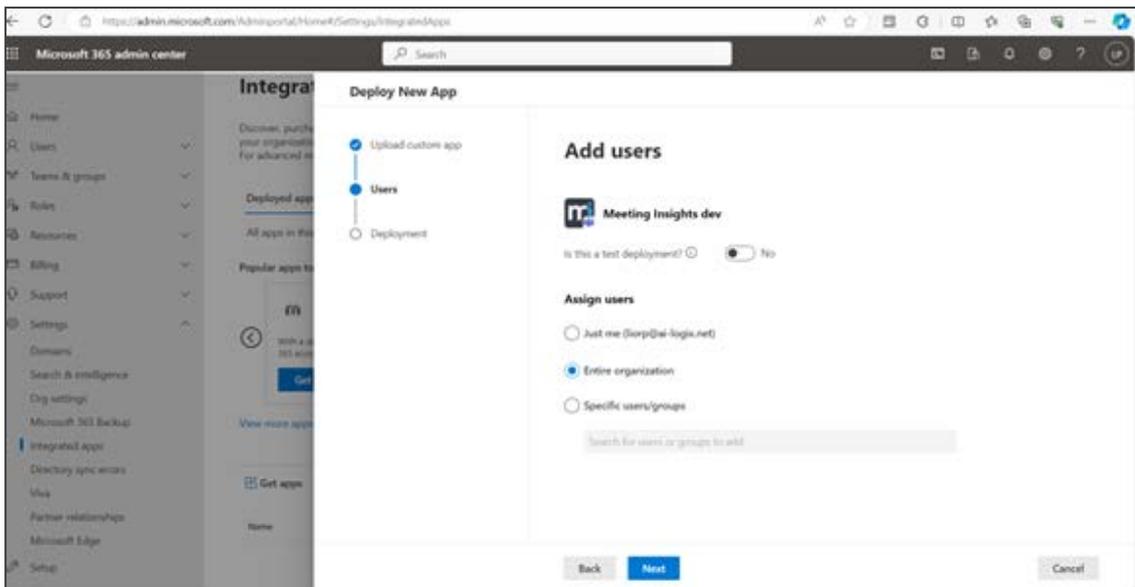
5. 上の図のように Settings メニューを展開し、Integrated apps オプションをクリックします。



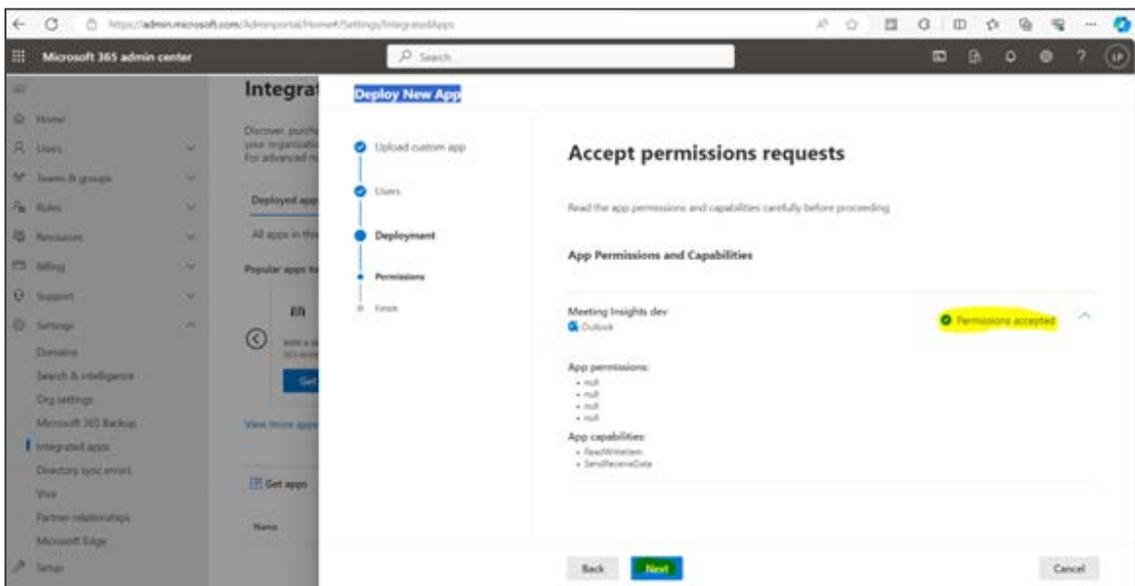
6. Upload custom apps オプションをクリックします。



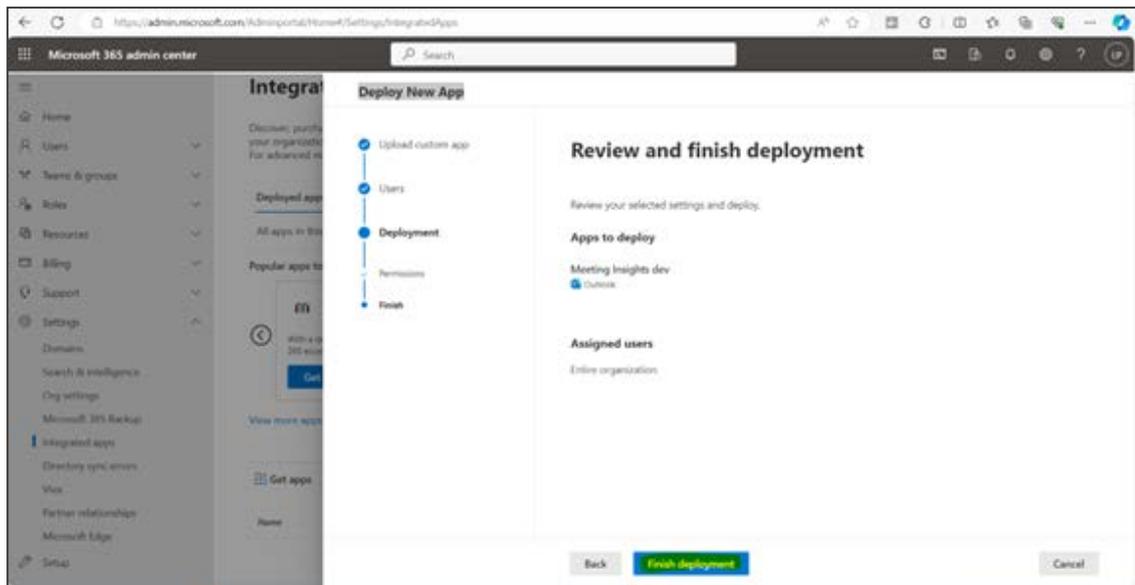
7. 「App type」ドロップダウンから、Office Add-in を選択し、Upload manifest (.xml) from device オプションを選択して、Choose File をクリックします。XML 検証後、Next をクリックします。



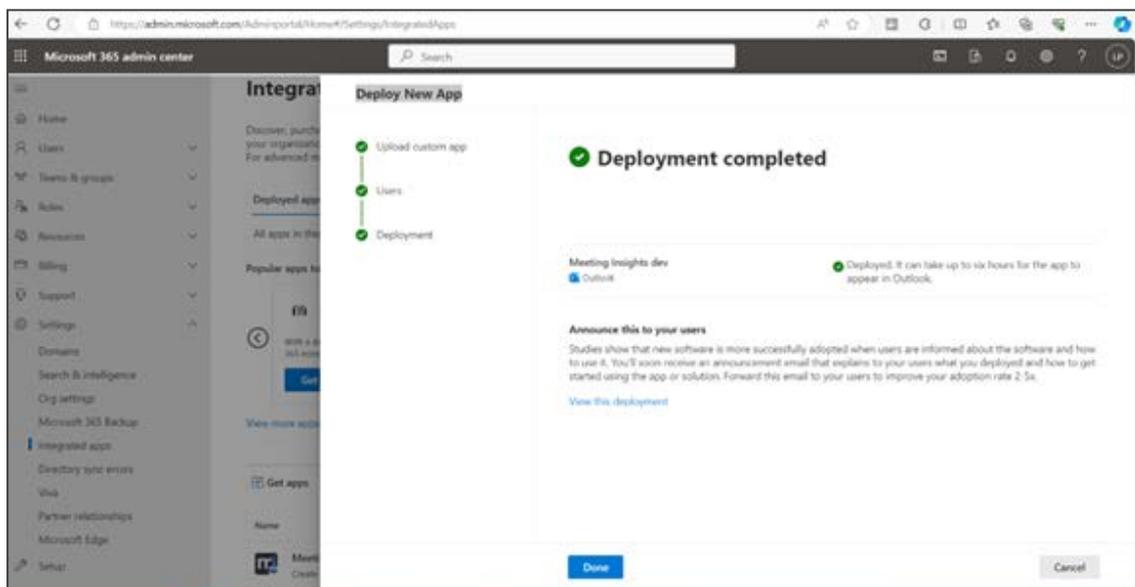
8. アドインを使用できるユーザーを選択し、Next をクリックします。



9. アプリケーションに必要な権限をクリックして承認し、Next をクリックします。



10. 展開を確認して、**Finish deployment** をクリックします。



展開が完了したら、上図に示す画面を表示します。

## ストレージ

デフォルトでは、Meeting Insights は、会議の録画音声、画面共有コンテンツ、生成された画像、文字起こし、AI 分析情報を、地域の設定に合わせて調整され、AudioCodes データセンターでホストされている別の Microsoft Azure Blob ストレージに保存します。

ただし、組織が独自の会議録画、文字起こし、および分析情報をホストする必要がある場合は、組織の Microsoft Azure Blob Storage アカウントまたは Amazon Web Services アカウント (Amazon S3 パケット) にストレージを有効にする Bring Your Own Blob Storage (BYOS) 機能を利用できます。この機能により、組織はストレージ インフラストラクチャの所有権を保持し、アクセス権限を管理し、完全な制御を維持できます。



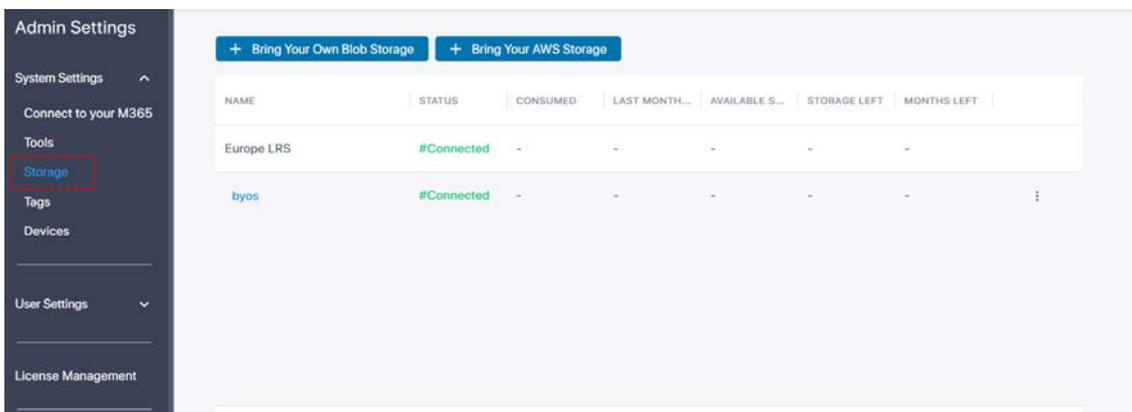
Bring Your Own Blob Storage には BYOS 機能キーが必要です。

さまざまなストレージ オプションの詳細については、次のセクションを参照してください。

- AudioCodes Azure Blob アカウントでホストされるストレージ
- 顧客の Azure BLOB アカウントでホストされるストレージ
- 顧客の Amazon S3 アカウントでホストされるストレージ

➤ Meeting Insights のストレージ アカウントを表示するには:

1. Admin Settings ナビゲーションメニュー ペインで、System Settings を展開し Storage をクリックします。デフォルトのストレージ アカウントが表示されます (例: Europe LRS)。



次の表は、テーブル列について説明しています。

表の列	説明
名前	ストレージ (LRS) が配置されている地域を表示します (例: 「Canada LRS」)。
状態	ストレージ アカウントへの接続の状態を表示します。 <ul style="list-style-type: none"> <li>■ 「接続済み」</li> <li>■ 「切断済み」</li> <li>■ 「失敗」</li> </ul>
消費済み	使用されているストレージ容量 (GB 単位) を表示します。 <b>注:</b> この列は、ローカル冗長ストレージ (LRS) と地理冗長ストレージ (GRS) に適用されます。
先月の成長	先月のストレージの変化を表示します。これは通常、増加 (成長) を示しますが、作成された会議録画よりも削除された会議録画の方が多く場合は、減少を示します。
Available Storage	利用可能なストレージ容量の合計 (GB 単位) を表示します。

表の列	説明
	注:この列は GRS にのみ適用されます。
Storage Left(ストレージ残量)	残りのストレージ容量(GB)を表示します。 注:この列は GRS にのみ適用されます。
Month Left(残り月)	ストレージがいっぱいになるまでの残り月数の推定値を表示します。

## AudioCodes Azure Blob アカウントでホストされるストレージ

Meeting Insights アプリケーションは、録画されたメディア (オーディオ、画面共有コンテンツ、生成された画像) とサマリー (文字起こし、概要、アクション項目、AI によって生成された分析情報) を、地域の設定に合わせて調整され、AudioCodes データセンターでホストされている個別の Azure Blob ストレージ コンテナに保存します。



ストレージが AudioCodes Azure Blob ストレージ アカウントでホストされている場合、会議の録画は**専用のアクセス制限されたストレージ**に保存されます。AudioCodes は、SaaS サービスのストレージ インフラストラクチャを所有しています。会議データの所有権 (コンテンツに対する権利と制御を含む) は、組織のみが保持します。

Meeting Insights は、次の Azure ストレージ オプションをサポートしています。

- **Local redundant storage (LRS):**これはローカルの冗長ストレージであり、データは同じ地域に複製されます。デフォルトでは、Meeting Insights は AudioCodes データセンターに単一のストレージ LRS プラットフォームを提供します。このストレージ プラットフォームには、ストレージ監視機能は含まれていません。
- **Geo-redundant storage (GRS):**これは地理的に冗長化されたストレージであり、データは2つの地域 (プライマリとセカンダリ) にわたって複製されます。GRS の利点は、地域的な停止が発生した場合でも録画が保護されることです。GRS が必要な場合は、AudioCodes からこの機能を購入できます。GRS は機能キーによって有効化され、ストレージ容量 (GB) も指定します。このストレージ プラットフォームを使用すると、ストレージを監視できます。

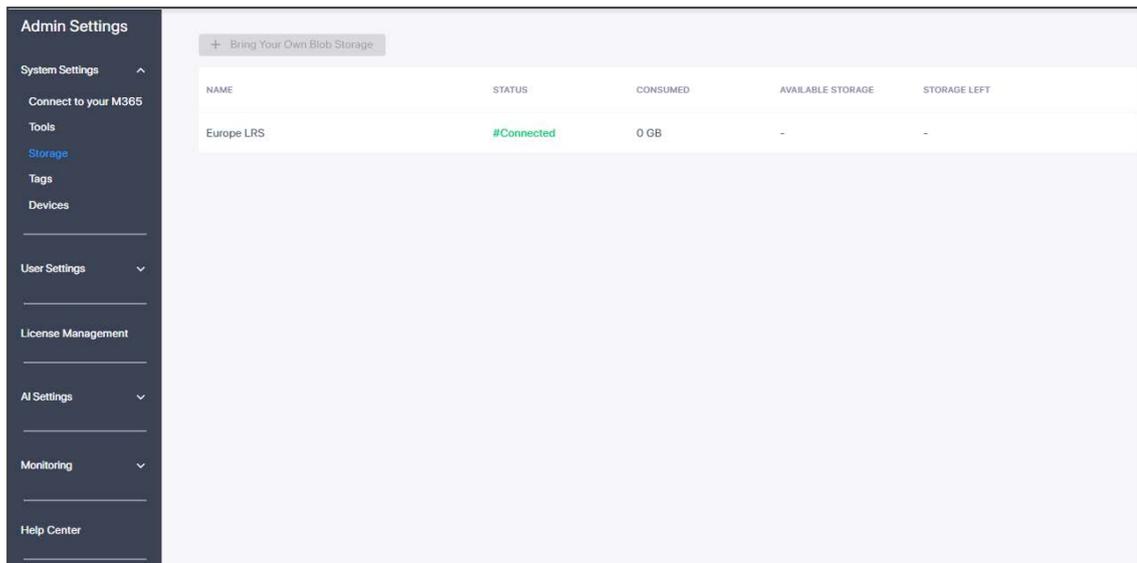
ストレージの接続状態と容量を監視するには、[ストレージの接続状態と容量の監視](#)を参照してください。



- Meeting Insights は、AudioCodes によってホストされている場合、ストレージを制限しません。
- Meeting Insights のデフォルトのストレージは LRS です。
- GRS は AudioCodes から購入できる機能です。

### ➤ AudioCodes がホストするストレージを表示するには:

- 「システム設定」メニューで、**Storage** オプションをクリックすると、デフォルトのストレージ アカウントが表示されます (例: Europe LRS)。



## 顧客の Azure BLOB アカウントでホストされるストレージ

組織が独自の会議録画、文字起こし、分析情報をホストする必要がある場合は、組織の Microsoft Azure Blob Storage アカウントにストレージを有効にする Bring Your Own Blob Storage (BYOS) 機能を利用できます。この機能により、組織はストレージ インフラストラクチャの所有権を保持し、アクセス権限を管理し、完全な制御を維持できます。



ストレージが組織の Azure Blob ストレージ アカウントでホストされている場合、会議の録画はこの Azure Blob ストレージに保存されます。組織はストレージ インフラストラクチャを所有し、アクセス権限を制御し、それを管理します (つまり、完全な制御を維持します)。この BYOS オプションは、内部または外部の規制に準拠するために会議の録画をネットワーク/データセンターでホストしておく必要がある組織を対象としています。

BYOS を構成した後、ユーザー プロフィールを使用してこれらのストレージ アカウントを特定のユーザーに割り当てることができ、これらのユーザー プロフィールに関連付けられたユーザーの録画が指定されたストレージの場所に保存されるようになります。

BYOS ストレージを追加するには、次の主な手順が含まれます。

1. Azure Blob ストレージ アカウントの設定。
2. ストレージ アカウントを使用して Meeting Insights を構成する (BYOS)。



- Bring Your Own Blob Storage には BYOS 機能キーが必要です。Meeting Insights アプリケーションで利用できない場合は、サービスプロバイダーにお問い合わせください。
- BYOS アカウントが Microsoft 365 テナントに登録されていることを確認します。
- ストレージの場所が Meeting Insights 展開インスタンスから地理的に離れている場合、パフォーマンスの遅延が発生する可能性があります。
- 表示名、電子メール、Azure OID などの顧客のユーザー情報、および時間、期間、件名、参加者、招待者などの録画された会議のメタデータは、顧客ごとに Meeting Insights の個別のデータベースに保存されます。
- ユーザーが複数のユーザープロフィールに割り当てられている場合、すべてのプロフィールを同じストレージで構成する必要があります。ユーザーが個別の保存場所を持つユーザープロフィールに割り当てられている場合、ユーザー録画は任意の保存場所に保存されます。
- アクティブな会議録画がない場合にのみ、追加された BYOS ストレージを削除できます。

### Azure Blob Storage アカウントの定義

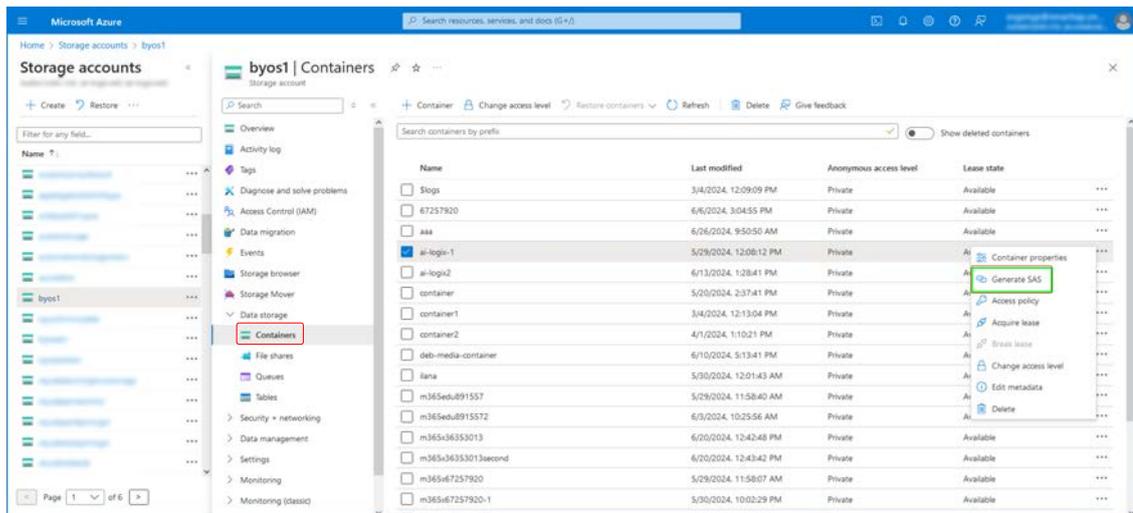
BYOS で Meeting Insights を構成する前に、まず Azure Blob Storage アカウントにストレージ コンテナを構成する必要があります。このプロセスには、Shared Access Signature (SAS) トークンと URL の生成が含まれます。これらは、後で Meeting Insights で BYOS を構成するときに必要になります。さらに、このプロセスには、SAS トークンの開始日時と有効期限の日時を指定することも含まれます。



このセクションでは、ストレージ コンテナを備えた Azure Blob Storage アカウントがあることを前提としています。

#### ➤ Azure Blob Storage アカウントを設定します。

1. (顧客テナントの) Microsoft Azure ポータルにログインします [アカウント](#)。
2. 「ストレージ アカウント」ページにアクセスし、関連する Blob ストレージ アカウントを選択します。
3. **Data storage > Containers** に移動し、メディアを保存するコンテナを選択します。
4. コンテナを右クリックし、ドロップダウンメニューから **Generate SAS** を選択すると、Generate SAS ダイアログボックスが開きます。



5. Generate SAS ダイアログボックスで、ストレージへのアクセス設定を構成します。
  - a. 署名方法グループで、Account key オプションを選択します。
  - b. 「Signing key」ドロップダウンリストから Key 1 を選択します。
  - c. 「Stored access policy」ドロップダウンリストから、共有アクセスポリシーを選択します。
  - d. 「Permissions」ドロップダウンリストから、リストされているすべての権限チェックボックスを選択 (チェック) します。
  - e. 「Start」フィールドと「Expiry」フィールドで、署名されたキーの開始日時と有効期限をそれぞれ定義します。



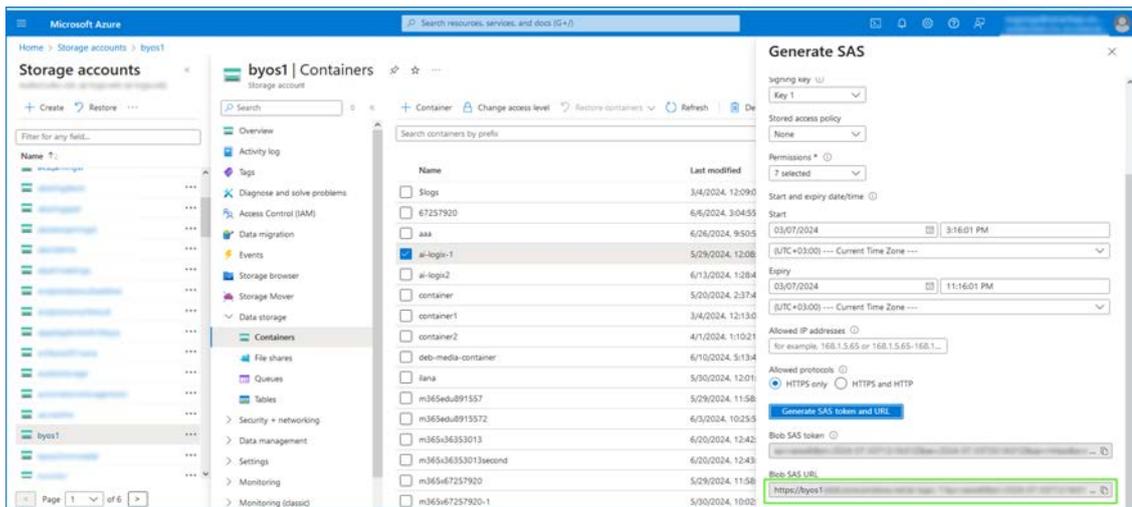
Meeting Insights の BYOC の場合、SAS トークンの有効期限は少なくとも 3 か月である必要があります。

- f. (推奨)「Allowed IP Addresses」フィールドに、Meeting Insights の IP アドレスを入力します。



- AudioCodes では、ネットワークへのアクセスを制限し、潜在的な脆弱性を軽減するために、このポイントツーポイント接続 (特定の IP アドレス) を使用することを推奨しています。
- IP アドレスを取得するには、AudioCodes の担当者にお問い合わせください。

- g. Allowed protocols group で HTTPS only オプションを選択し、HTTPS プロトコルを使用した要求のみを許可します。
- h. Generate SAS token and URL ボタンをクリックすると、共有アクセス署名 (SAS) トークンと URL が生成され、ボタンの下のフィールドに表示されます。



6. Blob SAS URL をコピーして安全な場所 (メモ帳など) に貼り付けます。このURL ( SAS トークンキーを含む ) は、Meeting Insights でこの BYOS ストレージを構成するときに必要になります ( [BYOS で Meeting Insights を構成する](#) 参照 ) 。

### BYOS で Meeting Insights を構成する

Azure Blob Storage アカウントを構成し、SAS URL を生成したら、BYOS を使用して Meeting Insights を構成できます。



Meeting Insights には BYOS ストレージ容量が表示されません。ストレージの監視は、Azure Blob ストレージ アカウントを通じてのみ実行できます。

#### ➤ BYOS で Meeting Insights を構成するには:

1. 「システム設定」メニューで、**Storage** オプションをクリックすると、デフォルトのストレージ アカウントが表示されます (例: Europe LRS)。
2. **Bring Your Own Blob Storage** ボタンをクリックすると、次のダイアログ ボックスが表示されません。

### Bring Your own Blob storage

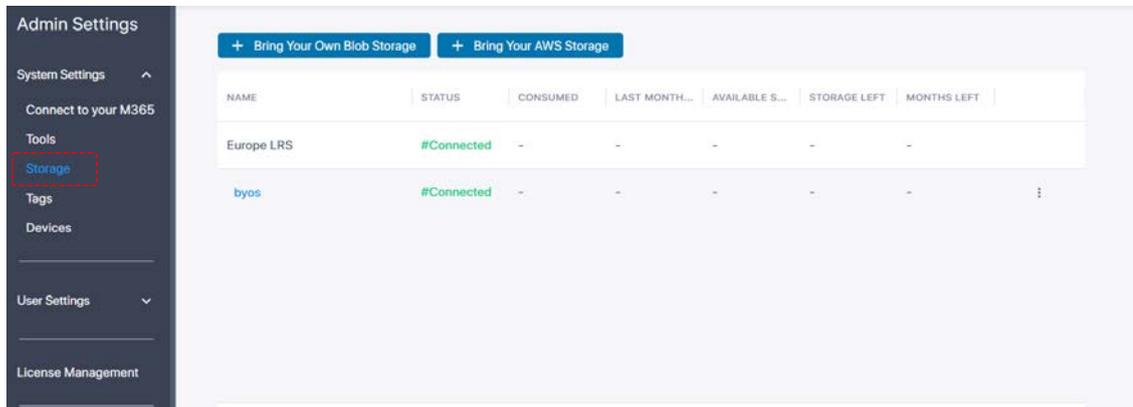
Friendly Name

Blob SAS URL

Cancel

Apply

3. 「Friendly Name」フィールドに、Blob ストレージ コンテナのわかりやすい名前を入力します。これは、後で簡単に識別できます。特に、複数の Blob ストレージ コンテナを追加する場合に便利です (例:「West US BYOS」または「North Europe BYOS」)。
4. 「Blob SAS URL」フィールドに、Azure Blob Storage アカウントからコピーした Blob SAS URL ( SAS トークンキーも含む ) を貼り付けます ( [Azure Blob Storage アカウントの定義](#) 参照 ) 。
5. **Apply** をクリックすると、BYOS が Meeting Insights に追加されます。



6. BYOS アカウントをユーザー プロフィールに関連付けるには、[ユーザー プロフィール](#) に示されているように、「Select Storage」ドロップダウン リストから選択します。

ストレージ接続ステータスの監視については、[ストレージの接続状態と容量の監視](#)を参照してください。

### BYOS ストレージへの接続の問題

Meeting Insights が BYOS ストレージにアクセスできない場合は、複数回の再試行後に録画が削除されます。BYOS ストレージへの接続が失われる原因としては、次のようなものがあります。

- ストレージが存在しない
- ネットワークの問題
- SAS トークンキーの有効期限が切れた

Meeting Insights では、30 日後、7 日後、有効期限当日に、電子メールとシステム アクティビティ ログの両方でトークン キーの有効期限が近づいたことを通知します。さらに、ストレージへの接続が失われた場合やトークン キーの有効期限が切れた場合、Meeting Insights はアラームをトリガーします。



- SAS トークン キーの有効期限は少なくとも 3 か月である必要があります。
- 停止や録画の潜在的な損失を防ぐために、期限が切れる前に新しい SAS トークン キーを生成し、新しいキーで Meeting Insights を更新することが重要です。

## 顧客の Amazon S3 アカウントでホストされるストレージ

ただし、組織が独自の会議録画、文字起こし、および分析情報をホストする必要がある場合は、組織の Amazon Web Services (AWS) ストレージ アカウント (Amazon S3 バケット) にストレージを有効にする Bring Your Own Blob Storage (BYOS) 機能を利用できます。



ストレージが組織の AWS ストレージアカウントでホストされている場合、すべての会議の録画はこの AWS ストレージに保存されます。組織はストレージ インフラストラクチャを所有し、アクセス権限を制御し、それを管理します (つまり、完全な制御を維持します)。この BYOS オプションは、内部または外部の規制に準拠するために会議の録画をネットワーク/データセンターでホストしておく必要がある組織を対象としています。

**ユーザー プロフィール**に指示されている通り、BYOS エンティティを設定したら、それを特定のユーザー (ユーザープロフィール) に割り当てる必要があります。これにより、ユーザー プロフィールに関連付けられたユーザーの会議の録画が、指定された Amazon S3 バケットに保存されるようになります。

Meeting Insights が会議の録画とデータを Amazon S3 バケットに送信できるようにするには、組織の AWS ストレージアカウントへのアクセス許可と、Amazon S3 バケットへの読み取り/書き込みアクセス許可を付与する必要があります。Meeting Insights は Microsoft Azure でホストされているため、クロスクラウド認証を実装し、AudioCodes AWS アカウントを使用して組織の AWS ストレージ アカウントで認証し、一時的な資格情報を取得します。Meeting Insights はこれらの認証情報を使用して組織の AWS ストレージアカウントに直接アクセスし、会議の録画とデータを Amazon S3 バケットに保存します。このプロセスは、Azure Entra ID と AWS Identity and Access Management (IAM) 間の信頼を確立するための OpenID Connect (OIDC) フェデレーションと、多層クライアント分離アーキテクチャを組み合わせることで、そして**永久的な資格情報を発行しないこと**で高度にセキュリティ保護されています。

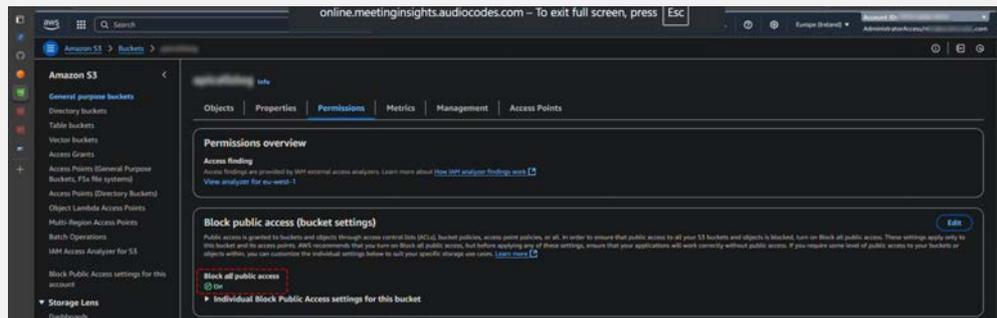
Amazon S3 バケットを作成したら、AWS ストレージアカウントには、AudioCodes にアカウントへの信頼とアクセス権を付与する定義済みの IAM ロールと、Amazon S3 バケットへの読み取り/書き込み権限を付与する関連 IAM ポリシーが必要です。

IAM リソース プロセスを容易にし、効率化するために、Meeting Insights は、組織の AWS ストレージ アカウント ID と Amazon S3 バケットの URL に基づいて、すぐに展開できる YAML ベースのスタック テンプレート (スクリプト) ファイルを自動的に提供します。必要なのは、AWS CloudFormation サービスを使用して、Amazon S3 バケット用のこの YAML ファイルをアップロードしたスタックを作成することだけです。アップロードされると、CloudFormation は適切なセキュリティを備えたすべての必要な AWS IAM リソースを自動的に作成します。

- AudioCodes のクロスクラウド ロール (AWS ストレージ アカウントへのアクセス) を信頼するための IAM ロール。
- 特定の Amazon S3 バケットへの読み取り/書き込み権限を付与する IAM ポリシー。
- 他の顧客グループを公開することなく適切な信頼関係を構築します。



- 組織のAWSストレージアカウントでBYOSを設定する場合は、管理者権限でサインインする必要があります。
- 組織のAWSストレージアカウントのセキュリティを確保するため、S3バケット用に取得された認証情報は一時的なものです。
- スクリプトファイルは、組織のAWSストレージアカウントIDのロールと、特定のAmazon S3バケットへのアクセスを許可するポリシーを作成します。同じAWSストレージアカウントに追加のBYOSを作成する必要がある場合は、追加のAmazon S3バケットにアクセスするためのポリシーを定義するスクリプトファイルのみをCloudFormationにアップロードする必要があります。
- AudioCodesと組織のAWSストレージアカウント間の専用の信頼「トンネル」は、アカウントの **Block all public access** 設定 (オフまたはオン) に影響されません。ただし、AudioCodesでは、セキュリティ上の理由から、すべてのパブリックアクセスをブロックすることをお勧めします。



AWS ベースのBYOSを追加するには、次の主な手順が含まれます。

1. Amazon S3 バケットの作成。
2. ストレージアカウントを使用して Meeting Insights を構成する (BYOS)。



- Bring Your Own Blob Storage にはBYOS機能キーが必要です。Meeting Insightsアプリケーションで利用できない場合は、サービスプロバイダーにお問い合わせください。
- ストレージの場所が Meeting Insights 展開インスタンスから地理的に離れている場合、パフォーマンスの遅延が発生する可能性があります。
- 表示名や電子メールなどの顧客のユーザー情報、および時間、期間、件名、参加者、招待者などの録画された会議のメタデータは、顧客ごとに Meeting Insights のデータベースに保存されます。
- ユーザーが複数のユーザープロフィールに割り当てられている場合、すべてのプロフィールを同じストレージで構成する必要があります。ユーザーが個別の保存場所を持つユーザープロフィールに割り当てられている場合、ユーザー録画は任意の保存場所に保存されます。
- アクティブな会議録画がない場合にも、追加されたBYOSストレージを削除できます。

## Amazon S3 バケットを作成

BYOSで Meeting Insights を構成する前に、Amazon S3 ストレージを構成する必要があります。これには主に、組織のAWSストレージアカウントにS3バケットを作成して構成することが含まれます。

➤ **Amazon S3 バケットを作成:**

1. 組織の **AWS** ストレージ アカウント。
2. Amazon S3 サービスにアクセスします。検索バーで「S3」を検索すると見つかります。
3. 左側のナビゲーション ペインで、**General purpose buckets** を選択します。
4. **Create bucket** ボタンをクリック。
5. 「Bucket name」には、バケットの一意の名前を入力します (例: 「meeting-insights」)。
6. バケットを配置する AWS 地域を選択します。
7. 必要に応じて、バケットのプロパティを構成するか、デフォルトのままにします。
8. **Create bucket** ボタンをクリックしてプロセスを完了します。これで、Amazon S3 にバケットが作成されました。



Amazon S3 バケットの作成の詳細については、[Amazon のドキュメント](#)を参照してください。

### **AWS ベースの BYOS 用に Meeting Insights を構成する**

Amazon S3 バケットを作成したら、Meeting Insights に AWS ベースの BYOS を追加する必要があります。



Meeting Insights には BYOS ストレージ容量が表示されません。ストレージの監視は、AWS ストレージ アカウントを通じてのみ実行できます。

➤ **AWS ベースの BYOS 用に Meeting Insights を構成するには:**

1. Admin Settings ナビゲーションメニュー ペインで **System Settings** を展開します。次に **Storage** をクリックします。「ストレージ」ページが表示され、Meeting Insights のデフォルト ストレージ (例: Europe LRS) が一覧表示されます。
2. **Bring Your Own Blob Storage** ボタンをクリックすると、次のダイアログ ボックスが表示されます。

## Bring Your AWS Storage

Cancel
Next

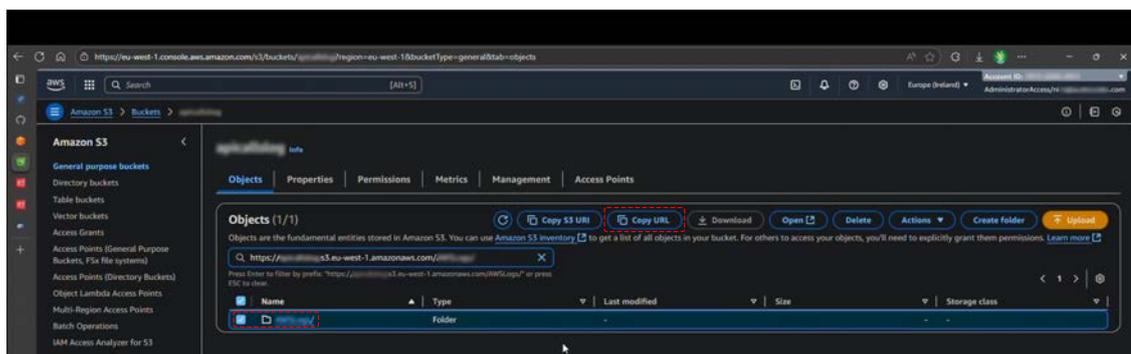
3. 「Friendly Name」フィールドに、Amazon S3 バケットのわかりやすい名前を入力します。これは、後で簡単に識別できます。特に、バケットが複数ある場合に便利です (例:「West US BYOS-AWS」または「North Europe BYOS-AWS」)。
4. 「AWS URL」フィールドに、Amazon S3 バケットのエンドポイント URL (例: `https://bucket-name.s3.eu-west-1.amazonaws.com/`) を貼り付けます。



URL を貼り付ける際は、「amazonaws.com」の後の**すべて**を削除します。たとえば、URL が `https://bucket-name.s3.eu-west-1.amazonaws.com/myobject/` の場合、`/myobject/` を削除します。

Amazon S3 コンソールから URL を取得できます。

- a. Amazon S3コンソールにサインインします。 <https://console.aws.amazon.com/s3/> をご覧ください。
- b. 左側のナビゲーション ペインで、**General purpose buckets** を選択します。
- c. 汎用バケットリストで、前の手順で作成したバケットの名前をクリックします ([Amazon S3 バケットを作成参照](#))。オブジェクト リストが表示されます。
- d. オブジェクト リストでバケットのオブジェクトを選択し、次に **Copy URL** をクリックします。URL がクリップボードにコピーされます:







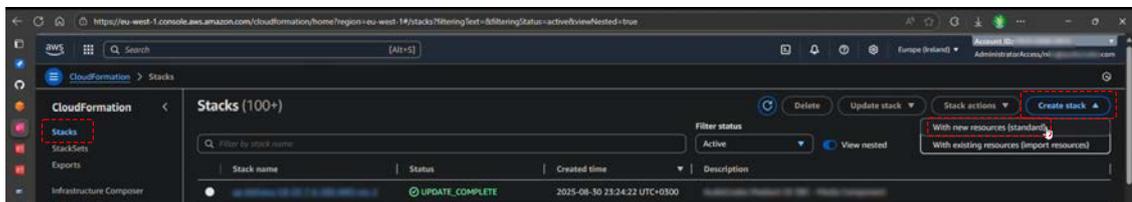
同じ AWS ストレージ アカウント ID で BYOS をすでに作成している場合は、YAML ファイルをダウンロードするためのリンクが **Assign role to storage (Create Role And Assign To Storage** の代わりに) を表示します。これは、ロールがすでに存在し、この AWS ストレージ アカウント ID に最初の BYOS を追加したときに作成されたためです。したがって、YAML ファイルでは、新しい BYOS に関連付けられた特定の Amazon S3 バケットにアクセスするための権限を Meeting Insights に付与するポリシーを作成するだけで済みます。

7. **Create Role And Assign To Storage** アイコンをクリックして、YAML ファイル (role-and-policy.yaml) をコンピューターにダウンロードし、次の操作を実行して、Amazon S3 バケットへの Meeting Insights のアクセス権限を付与し、AWS CloudFormation サービスを使用して、IAM リソースの YAML ファイルテンプレートに基づいてスタックを作成します。

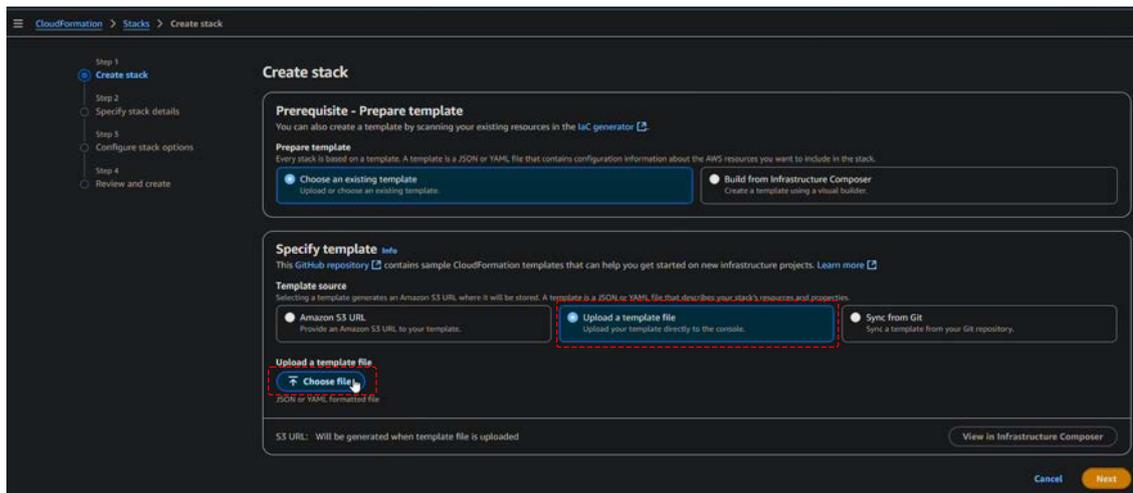


IAM リソースはグローバルで地域に依存しないため、単一の IAM ロールで複数の地域のバケットにアクセスでき、ポリシーにリストされているバケットが異なる AWS 地域に存在しても構わないため、このプロセスはどの AWS 地域でも実行できます。

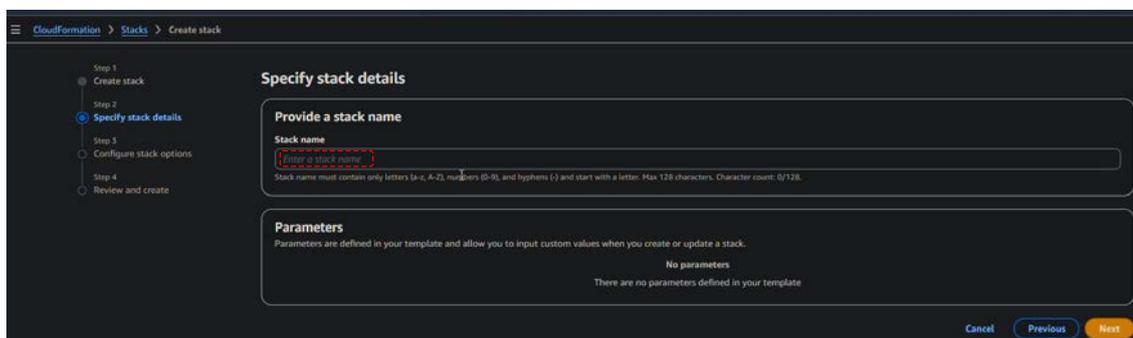
- a. 組織の **AWS** ストレージ アカウント。
- b. 検索バーに「CloudFormation」と入力し、結果から選択すると、AWS CloudFormation サービスのコンソールが表示されます。
- c. 左側のナビゲーションペインで、**Stacks** を選択し、次に **Create stack** ドロップダウンメニューから **With new resources (standard)** を選択してスタック作成ウィザードを開きます。



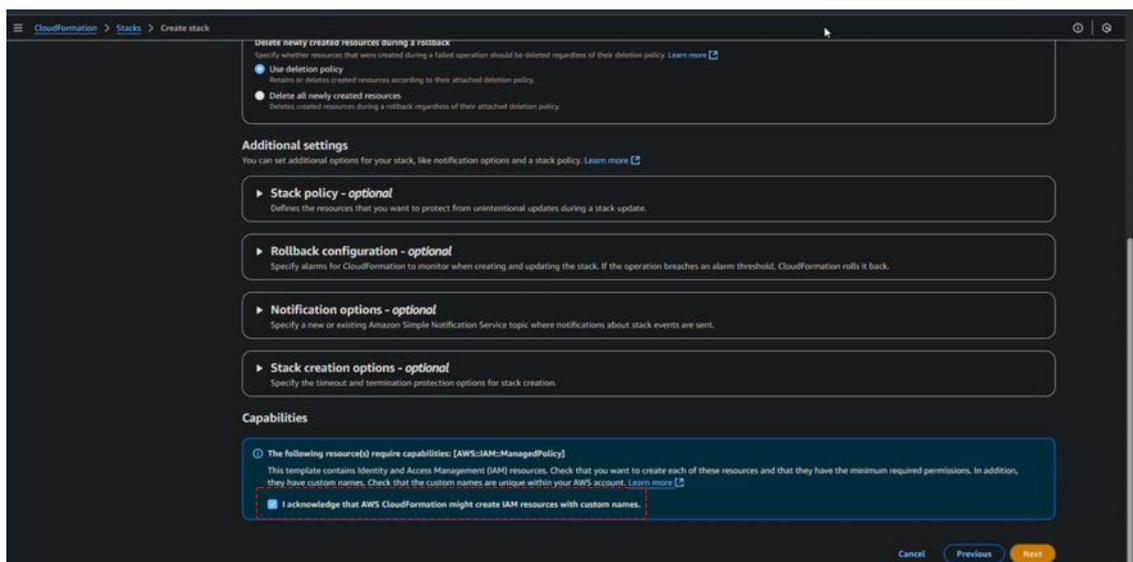
- d. スタックの作成ウィザード ページで、次の操作を行います。
  - i. **Prerequisite - Prepare template** 下で、**Choose an existing template** オプションを選択します。
  - ii. **Specify template** 下で、**Upload a template file** を選択し、**Choose file** をクリックします。次に Meeting Insights (上記) からダウンロードした YAML ファイルを選択します。



- e. ファイルのアップロードが完了したら、Next をクリックします。スタックの詳細を指定するウィザード ページが表示されます。
- f. 「Stack name」フィールドにスタックの名前を入力します。

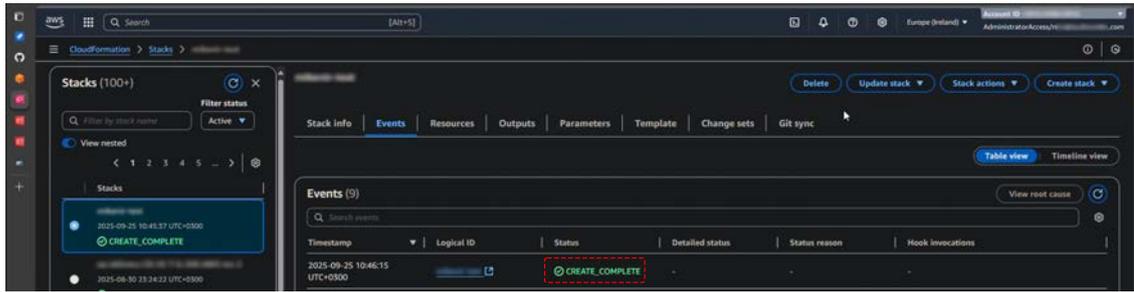


- g. Next をクリック。スタック オプションの構成 ウィザード ページが表示されます。
- h. ページの一番下までスクロールし、I acknowledge ... チェックボックスを選択します。



- i. Next をクリック。「確認と作成ウィザード」ページ (最後) が表示されます。

- j. 必要に応じて追加の設定を定義し、次に **Submit** をクリックします。スタックの作成は進行中です。これはスタックのページの「Status」フィールドに示され、作成が完了すると「CREATE\_COMPLETE」と表示されます。



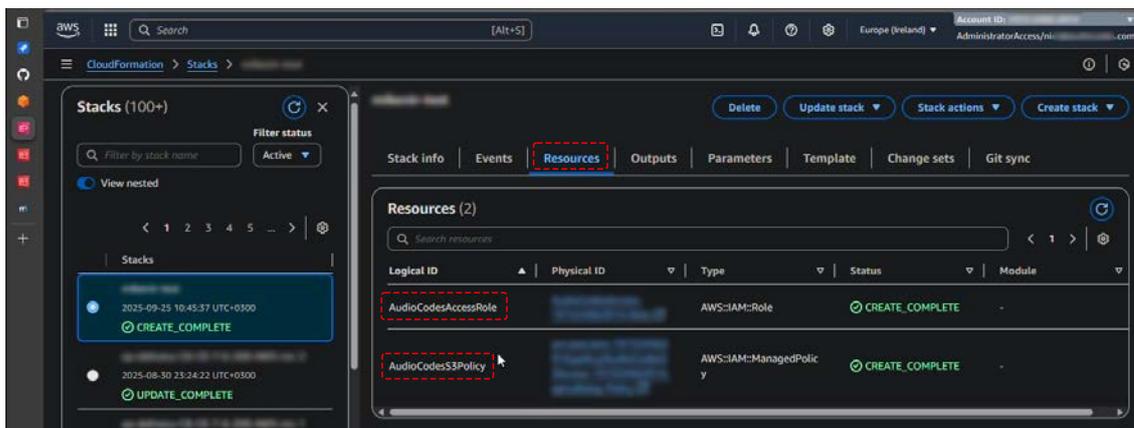
作成されたスタックのリソースを表示し、Meeting Insights に権限を付与したい場合は、リソースタブを選択します。次の2つのリソースが作成されます。

- **AudioCodesAccessRole:** AudioCodes を識別し、組織の AWS ストレージアカウントへのアクセス許可を許可する IAM ロール。
- **AudioCodesS3Policy:** 上記のロールの IAM ポリシーは、指定された Amazon S3 バケットに書き込む(会議の記録とデータを送信)ために、組織の AWS ストレージアカウントへの Meeting Insights の限定的なアクセス許可を付与します。



同じ AWS ストレージアカウント ID に対して BYOS をすでに作成している場合は、AudioCodesS3Policy リソースのみが表示されます。これは、ロール (AudioCodesAccessRole) がすでに存在し、この AWS ストレージアカウント ID に最初の BYOS を追加したときに作成されたためです。したがって、YAML ファイルでは、新しい BYOS に関連付けられた特定の Amazon S3 バケットにアクセスするための権限を Meeting Insights に付与するポリシーを作成するだけで済みます。

上記の各リソースをクリックすると、その定義を表示できます。または、ストレージページの Meeting Insights で省略記号をクリックして定義をダウンロードして表示することもできます。BYOS エンティティの省略アイコンをクリックし、ロールスクリプトを作成するまたはストレージスクリプトにロールを割り当てることができます。



- 8. Meeting Insights のユーザーインターフェースに戻り、開いたダイアログで **YAML ファイルを正常に実行しました** チェックボックスを選択します。

## Bring Your AWS Storage

To allow the application to access your Amazon S3 buckets, you must delegate access by granting the required permissions to the AudioCodes IAM role using a resource-based policy or role trust relationship.

**⚠ Important:** AWS Identity and Access Management (IAM) Administrator permissions are required to grant access to the IAM role.

Please follow the steps below to complete the configuration of your app:

1. Download the YAML file.
2. Run it in AWS CloudFormation (Read: [How to create IAM Role with Policy that grants access to the S3 bucket](#)).
3. Once complete, check the box below to finish setup.

### ↓ Create Role And Assign To Storage

If the role already exists, run the [Assign Role To The Storage](#) YAML instead.

I have successfully executed YAML file

Back

Continue Later

Finish

9. **Finish** をクリック。新しい BYOS AWS ストレージがストレージ ページにリストされ、「Status」列に「Pending」と表示されます。その後、組織の AWS ストレージ アカウントに接続されると、「Connected」と表示されます。

NAME	STATUS	CONSUMED	LAST MONTH...	AVAILABLE S...	STORAGE LEFT	MONTHS LEFT
Europe LRS	#Connected	-	-	-	-	-
byos	#Connected	-	-	-	-	-

10. BYOS ストレージ アカウントをユーザー プロフィールに関連付けるには、[ユーザー プロフィール](#)に示されているように、「Select Storage」ドロップダウン リストから選択します。

ストレージ接続ステータスの監視については、[ストレージの接続状態と容量の監視](#)を参照してください。

### BYOS ストレージへの接続の問題

Meeting Insights が Amazon S3 バケット ストレージにアクセスできない場合、接続を何度か再試行した後、会議の録画が削除されます。BYOS への接続が失われる原因としては、次のようなものがあります。

- Amazon S3 バケット はもはや存在しません
- ネットワークの問題

### ストレージの接続状態と容量の監視

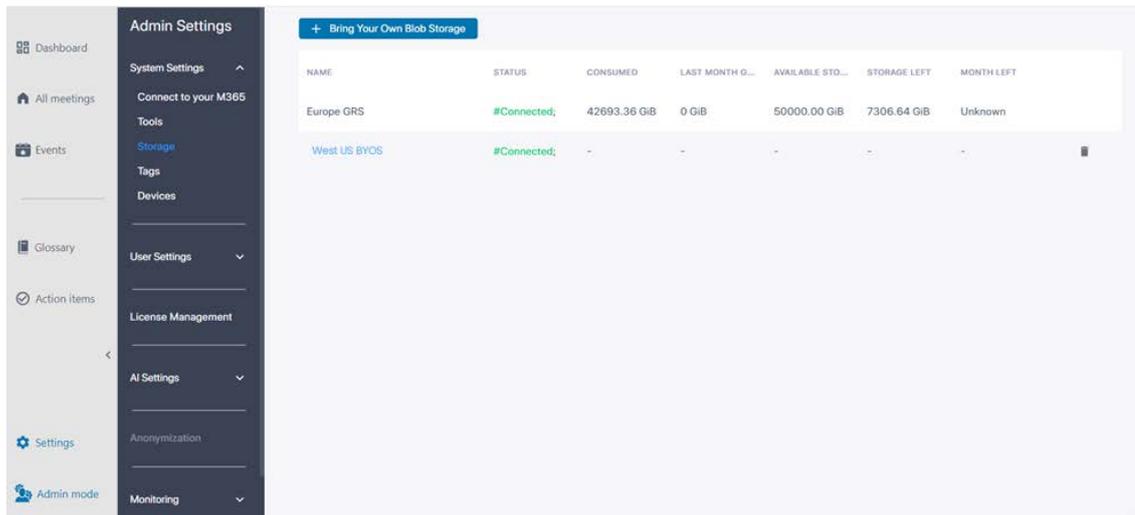
Meeting Insights を使用すると、ストレージの接続状態とストレージ容量 (ストレージ プラットフォームによって異なります) を監視できます。プラットフォームごとのストレージ監視のサポートは次のとおりです。

ストレージ プラットフォーム	ストレージ容量の監視
AudioCodes Azure Blob ストレージ アカウントによってホストされるストレージ	ストレージ監視は、Blob ストレージ オプションによって異なります。 <ul style="list-style-type: none"> <li>■ <b>LRS:</b> 監視が提供されません。</li> <li>■ <b>GRS:</b> 監視は、Meeting Insights (以下で説明) を通じて行われます。</li> </ul>
顧客の Azure Blob ストレージ アカウントまたは AWS アカウントによってホストされるストレージ	監視は、顧客の Azure Blob ストレージ アカウントまたは AWS アカウントを通じて行われます (Meeting Insights を通じてではありません)。

以下では、Meeting Insights を使用してストレージの接続状態とストレージ容量を監視する方法について説明します。

➤ **ストレージの接続性と容量を監視するには:**

- 「System Settings」メニューで、**Storage** オプションをクリックすると、ストレージ アカウントが表示されます。



ストレージの接続ステータスと容量は、ページ上の次のフィールドを使用して監視されます。

表の列	説明
名前	ストレージが配置されている地域を表示します (例: 「Canada LRS」、「Europe GRS」、「West US BYOS」)。
状態	ストレージ プラットフォームへの接続のステータスを表示します。 <ul style="list-style-type: none"> <li>■ 「接続済み」</li> <li>■ 「切断済み」</li> <li>■ 「失敗」</li> <li>■ 「保留中」</li> </ul>
消費済み	使用されているストレージ容量 (GB 単位) を表示します。 注:この列は、GRS 用の AudioCodes ホスト ストレージにのみ適用されま
先月の成長	先月のストレージの変化を表示します。これは通常、増加 (成長) を示しますが、作成された会議録画よりも削除された会議録画の方が多い場合は、減少を示します。 注:この列は、GRS 用の AudioCodes ホスト ストレージにのみ適用されま
Available	利用可能なストレージ容量の合計 (GB 単位) を表示します。

表の列	説明
Storage	<b>注:</b> この列は、GRS 用の AudioCodes ホスト ストレージにのみ適用されます。
Storage Left( ストレージ残量)	残りのストレージ容量( GB) を表示します。 <b>注:</b> この列は、GRS 用の AudioCodes ホスト ストレージにのみ適用されます。
Month Left ( 残り月)	ストレージがいっぱいになるまでの残り月数の推定値を表示します。 <b>注:</b> この列は、GRS 用の AudioCodes ホスト ストレージにのみ適用されます。

## BYOS エンティティの削除

BYOS エンティティを削除できます。



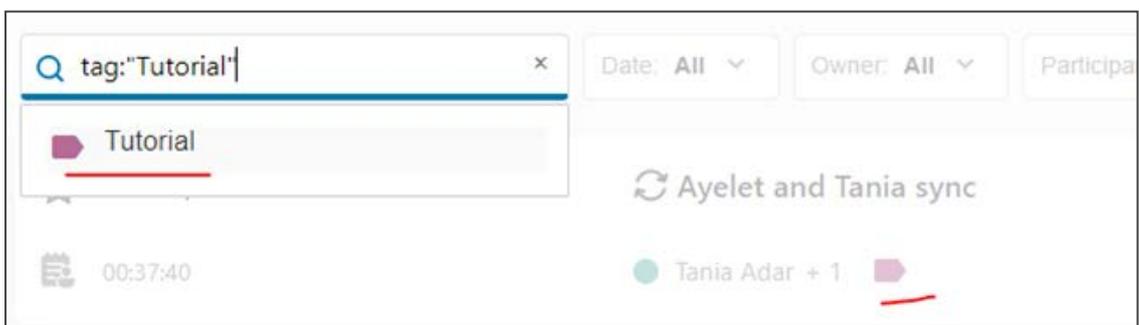
BYOS エンティティを削除すると、BYOS に関連付けられているそれ以降のすべての会議の録画とユーザーのデータ(ユーザー プロフィール) は保存されません。

### ➤ BYOS エンティティを削除するには:

1. Admin Settings ナビゲーションメニュー ペインで、**System Settings** を展開し、**Storage** をクリックします。Storage ページが表示されます。
2. 削除したい BYOS エンティティの省略記号 (3 つのドット) アイコンをクリックし、ドロップダウンメニューから **Delete** を選択すると、確認メッセージ ボックスが表示されます。
3. **Delete** をクリックして確定します。

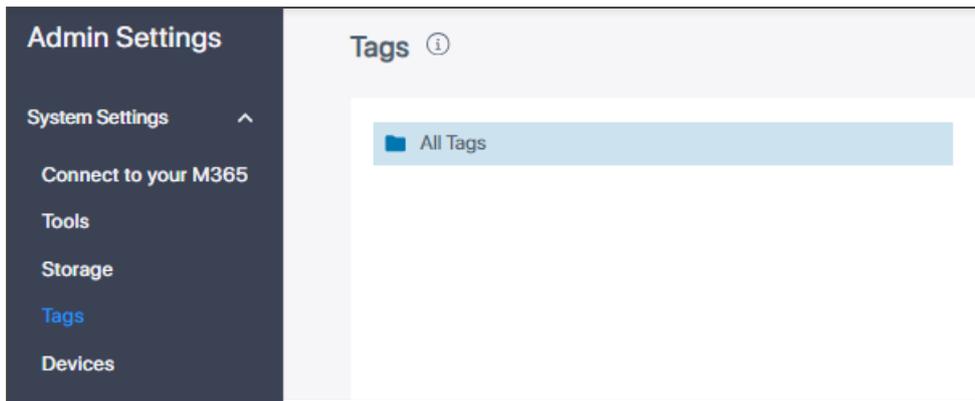
## タグ

会議の録画にタグを追加すると、録画内の特定の情報を簡単に検索できるようになります。

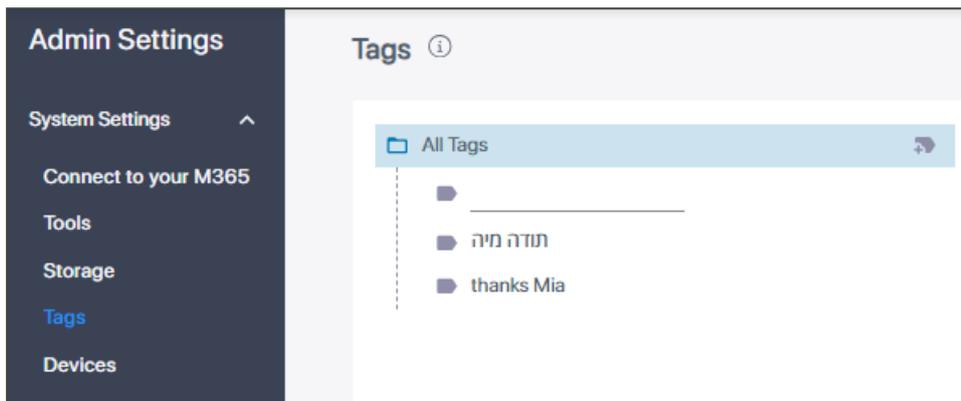


### ➤ タグを定義するには:

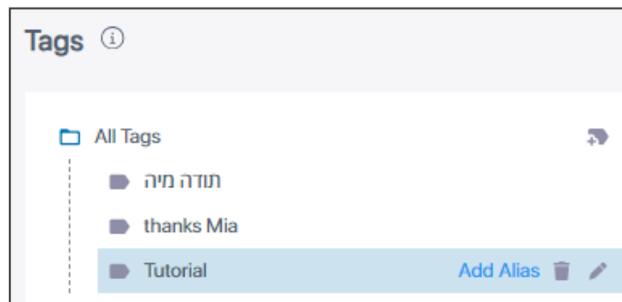
1. 「System Settings」メニューで、**Tags** オプションをクリックします。



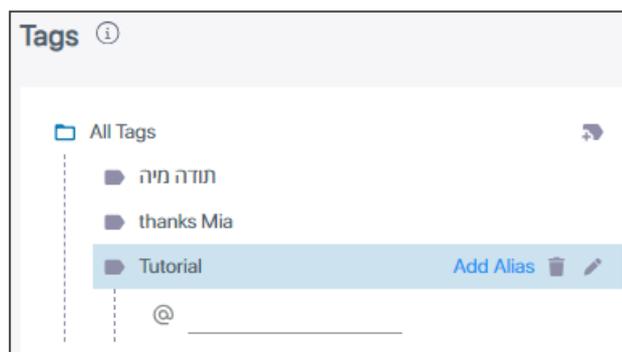
2. All Tags バーにマウスを移動し、👤アイコンをクリックします。



3. | \_\_\_\_\_ フィールドで、タグ名を入力して Enter キーを押します。



4. メニューから Add Alias を選択します。





タグの下に2つのカテゴリレベルの「エイリアス」を追加できます。これらのカテゴリレベルにより、企業会議を主題（製品など）ごとに整理しやすくなります。

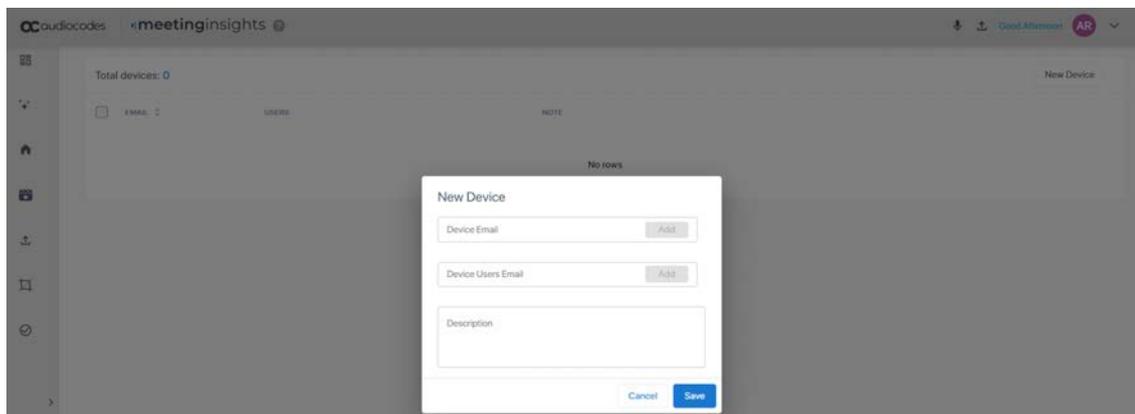
5. 必要に応じて、削除アイコンまたは編集アイコンを選択して、会議の節目の作成を容易にします。

## デバイス

管理者は、企業の物理的な会議室でデバイスを定義する必要があります。Meeting Insightsは、会議室に物理的に参加しているスピーカーを音声で識別しますが、特定のユーザーをデバイスに割り当てることはありません。部屋の電子メールアドレスを定義するだけで、デバイスを部屋に関連付けることができます。

### ➤ デバイスを構成するには:

1. 「System Settings」メニューで、**Devices** オプションをクリックします。



2. デバイスのメールを入力し、**Add** をクリックします。
3. デバイスユーザーのメールを入力し、**Add** をクリックします。

多数の出席者が座っている会議室に設置されたCAPに通話が着信し、そのデバイスが特定のユーザーに関連付けられていない場合、Meeting Insightsによる録画管理は実行できません。電子メールアドレスを定義するだけで、電話を特定のユーザーに関連付けて、録画管理が可能になります。

Meeting Insightsは、会議のすべての出席者の電子メールアドレスを使用してデバイス上でスピーカー検出を適用することに注意してください。つまり、招待されたユーザーの音声プリントが利用可能な場合は、それがデバイスのスピーカー検出に使用されます。

## 9 ユーザー設定の構成

管理者は次のユーザー設定を構成できます。

- ユーザープロフィール
- 管理者プロフィール
- ライセンスありのユーザー
- ライセンスなしのユーザー
- 会議の保持ポリシー
- 録画通知
- ユーザー設定

### ユーザープロフィール

ライセンスが割り当てられたユーザーのみが、自分のプロフィールに従って Meeting Insights にアクセスしたり、会議を録画したりすることができます。ライセンスを持たず会議に参加した残りのユーザーは、Meeting Insights にアクセスできません。Meeting Insights は情報をキャッシュし、会議情報に表示します。Meeting Insights を使用するには、ユーザーは少なくとも1つのユーザープロフィールに接続されている必要があります。Meeting Insights には3つのユーザープロフィールが提供されます。管理者はさらに作成できます。

[こちら](#)で「ライセンスのないユーザー」ページも参照してください。管理者は収集された情報を確認し、必要に応じて削除できます。ライセンスを持っていたものの、ライセンスの割り当てが解除されたユーザーもこのページに表示されます。

3つのプロフィールが提供されます。

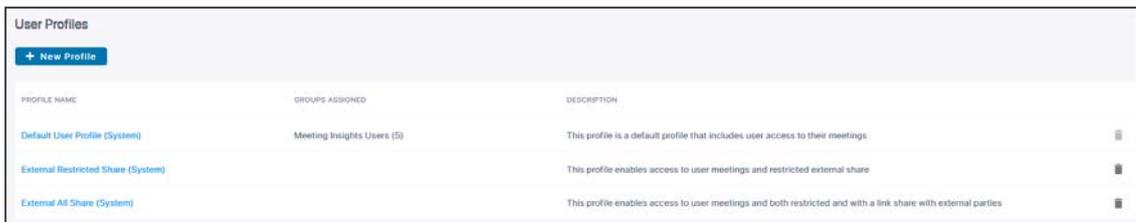
- **デフォルトのユーザープロフィール(システム)**。このプロフィールは、会議へのユーザーアクセスが含まれるデフォルトプロフィールです。
- **外部制限付き共有(システム)**。このプロフィールにより、ユーザー会議および制限された外部共有へのアクセスが可能になります。
- **外部全共有(システム)**。このプロフィールにより、ユーザー会議へのアクセスと、制限付きアクセス、および外部の関係者とのリンク共有の両方が可能になります。



- プロフィールが Microsoft Entra ID グループに割り当てられている間は、プロフィールを削除することはできません。プロフィールを削除する前に、グループを別のプロフィールに割り当てる必要があります。
- ユーザーにユーザープロフィールを割り当てるには、[ユーザーへの Meeting Insights ライセンスの割り当て](#)を参照してください。

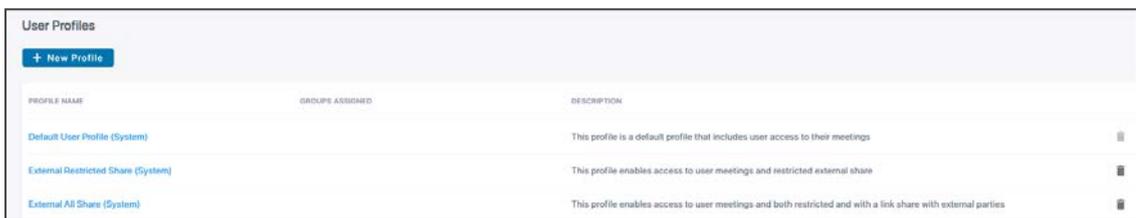
#### ➤ ユーザープロフィールを構成するには:

1. 「User Settings」メニューで、**User Profiles** オプションをクリックします。

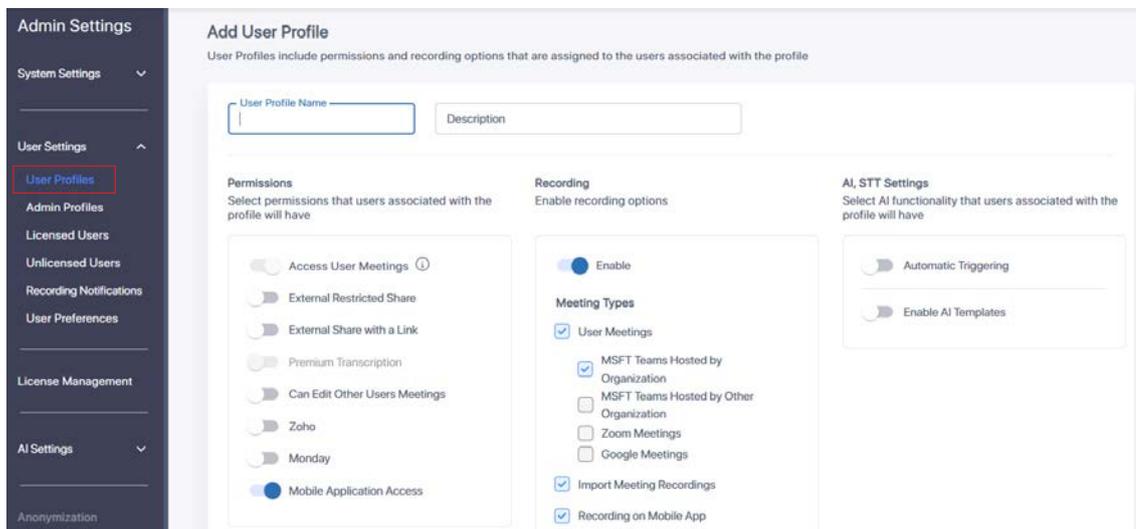


2. 3つのデフォルトプロフィールを表示します。

- 上の図は、ステップ3でライセンスを[こちら](#)に割り当てた際に実行した、**Default User Profile (System)**で割り当てられた**Meeting Insights Users (5)**を示しています。
- 下の図では、グループが割り当てられていません。ユーザープロフィールにグループを割り当てるには、[こちら](#)に示されたライセンスを割り当てるときにステップ3を参照してください。



3. すでに使用可能な3つのユーザープロフィールに別の(カスタマイズされた)ユーザープロフィールを追加するには、**New Profile**をクリックします。



4. 以下の表を参考にしてフィールドを設定します。

フィールド	説明
「User Profile Name」	後で効果的に管理できるように直感的な名前を入力します
「Description」	後で効果的に管理できるようにプロフィールの説明を入力します

フィールド	説明
<b>Permissions</b>	
<b>Access User Meetings</b>	このオプションは常に有効になっており、ユーザーが会議にアクセスするために使用されます。無効にすることはできません。このオプションはグレー表示されており、ユーザーは自分が主催または参加した会議、および自分と共有された会議に常にアクセスできることを示しています。このオプションは常に有効になっており、無効にすることはできません。
<b>External Restricted Share</b>	この設定を有効にすると、ユーザーは会議の録画を会議に参加した外部の関係者と共有できるようになります。会議の録画にアクセスするには、外部の関係者は電子メールの確認とコード アクセスのプロセスを実行する必要があります。 注:このオプションはデフォルトで無効になっています。
<b>External Share with a Link</b>	この設定を有効にすると、会議の録画をリンクで共有できるようになります。リンクを知っている人は誰でも録画にアクセスできるようになります。 注:このオプションはデフォルトで無効になっています。
<b>Premium Transcription</b>	「Premium Transcri」オプションはヘブライ語話者にのみ適用され、ほとんどの場合利用できません。テナントレベルで制御可能です。このオプションに興味がある場合は、サービスプロバイダーにお問い合わせください。 注:このオプションはデフォルトで無効になっています。
<b>Can Edit Other Users Meetings</b>	「Auto Can Edit」設定が有効になっているユーザーは、会議の前に自動的に「編集可能」権限を取得します。つまり、この権限により、会議の所有者と同じレベルの制御権が与えられ、共同所有者になります。閲覧、編集などが可能です。(会議の主催者と同じ)。これは、会議サイド パネルまたは会議共有オプションを通じて「Can View」を「Can Edit」に変更した場合に利用できる権限と同じです。 注:このオプションはデフォルトで無効になっています。
<b>Salesforce</b>	ユーザーは、AIによって生成された会議の概要を組織のSalesforceプラットフォームに送信できるようになります。 注:このオプションは、Meeting InsightsをSalesforceと統合した場合にのみ使用できます( <a href="#">Meeting InsightsとSalesforceの統合参照</a> )。
<b>Zoho</b>	ユーザーがアクション アイテムを組織のZohoプラットフォームに送信できるようにします。 注:このオプションは、Meeting InsightsをZohoと統合した場合にのみ使用できます( <a href="#">Meeting InsightsとZohoの統合参照</a> )。
<b>monday</b>	ユーザーが組織のmonday.comアカウント(ワークスペース、ボード、ダ

フィールド	説明
	<p>ループ) にアクション アイテムを送信できるようにします。</p> <p><b>注:</b>このオプションは、monday.com と Meeting Insights を統合した場合にのみ使用できます (<a href="#">Meeting Insights と monday.com の統合</a> 参照)。</p>
<b>Mobile Application Access</b>	<p>Meeting Insights スタンドアロン モバイル アプリへのアクセスと使用を有効にします。</p> <p><b>注:</b>このオプションはデフォルトで有効になっています。</p>
<b>Recording</b>	
<b>Enable</b>	<p>プロフィールに割り当てられたグループ内のユーザーが、開催する会議を録画できるようにします (会議の開催者である必要があります)。</p> <p><b>注:</b>このオプションはデフォルトで有効になっています。</p>
<b>User Meetings</b>	<p>プロフィールに割り当てられたユーザーが会議に招待され、そのユーザーが会議の主催者である場合、MIA がそのユーザーの会議を録画できるようになります。</p> <p>次のチェックボックスを 1 つ以上選択することで、さまざまなプラットフォームでこの機能を有効にできます。</p> <ul style="list-style-type: none"> <li>■ <b>MSFT Teams Hosted by Organization:</b> (デフォルト) 組織がホストする Microsoft Teams 会議。</li> <p><b>注:</b>このオプションはデフォルトで有効になっています。</p> <li>■ <b>MSFT Teams Hosted by Other Organization:</b> 他の組織がホストする Microsoft Teams 会議 (<a href="#">ユーザーが外部の Teams 会議を録画できるようにする</a> 参照)。</li> <p><b>注:</b>このオプションはデフォルトで無効になっています。</p> <li>■ <b>Zoom Meetings:</b> 組織または他の組織が主催する Zoom 会議 (<a href="#">ユーザーが Zoom 会議を録画できるようにする</a> 参照)。</li> <p><b>注:</b>このオプションはデフォルトで無効になっています。</p> <li>■ <b>Google Meetings:</b> 組織または他の組織が主催する Google Meet 会議 (<a href="#">ユーザーが Google Meet 会議を録画できるようにする</a> 参照)。</li> <p><b>注:</b>このオプションはデフォルトで無効になっています。</p> </ul>
<b>Import Meeting Recordings</b>	<p>ユーザーがサードパーティ ツールによって作成された会議の録画を Meeting Insights にインポートできるようにします。</p> <p><b>注:</b>このオプションはデフォルトで有効になっています。</p>
<b>Recording on Mobile App</b>	<p>Meeting Insights スタンドアロン モバイル アプリを使用しているときに、ユーザーが (携帯電話のマイクを使用して) 会話をアドホックに録画で</p>

フィールド	説明
	<p>きるようにします。</p> <p><b>注:</b></p> <ul style="list-style-type: none"> <li>■ このオプションはデフォルトで有効になっています。</li> <li>■ このオプションは、<b>Mobile Application Access</b> トグル ボタン (上記参照) がオンになっている場合にのみ利用可能です。</li> </ul>
<p><b>Select Storage</b></p>	<p>Meeting Insights では、会議の音声記録、画面共有コンテンツ、生成された画像、文字起こし、AI Insights が、地域の設定に合わせて調整され、AudioCodes データセンターでホストされる別の Azure Blob ストレージに保存されます。</p> <p>データの完全な制御と所有権を求めるお客様は、Bring Your Own Storage (BYOS) の Meeting Insights サポートを使用して、組織のプライベート ストレージ アカウントにのみデータを保存できます。次のアカウントが可能です。</p> <ul style="list-style-type: none"> <li>■ Microsoft Azure Blob Storage アカウント (さまざまな場所用)。詳細については、<a href="#">顧客の Azure BLOB アカウントでホストされるストレージ</a>を参照してください。</li> <li>■ AWS Amazon S3 アカウント (さまざまな場所用)。詳細については、<a href="#">顧客の Amazon S3 アカウントでホストされるストレージ</a>を参照してください</li> </ul> <p>BYOS をセットアップして構成したら、それらをユーザー プロフィールに割り当てて、これらのユーザープロフィールに割り当てられたユーザーの録画とデータを指定されたストレージに保存できるようになります。ストレージアカウントを構成するには、<a href="#">ストレージ</a>を参照してください。</p>
<p><b>Meeting Recordings Retention Period</b></p>	<p>会議録画の保持ポリシー(期間)を定義します。会議録画がこの期間を超えると、Meeting Insights によって削除されます。</p> <p>詳細については、<a href="#">会議の保持ポリシー</a>を参照してください。</p>
<p><b>Allow Users to Extend Recordings Retention</b></p>	<p>ユーザーは、会議を可能な限り最大の保存期間 (つまり、カスタム定義されている場合は3年以上) に設定することで、保存期間 (上記の <b>Meeting Recordings Retention Period</b> で定義) を上書きできます。</p> <p>詳細については、<a href="#">会議の保持ポリシー</a>を参照してください。</p>
<p><b>AI, STT Settings</b></p>	
<p><b>Automatic Triggering</b></p>	<p>会議の録画に対して AI を活用した分析情報の自動生成を有効にします。詳細については、<a href="#">AI の自動起動の有効化</a>を参照してください。</p> <p><b>注:</b> このオプションはデフォルトで無効になっています。</p>

フィールド	説明
Auto Approve Action Items	ユーザーの承認を必要とせずに、AIを活用したアクションアイテムを通常のアクションアイテムとして追加 (および要約メールに含める) できるようになります。無効にした場合は、それらは提案されたアクション項目として追加され、ユーザーの承認が必要です。
Enable AI Templates	AI生成の要約を特別なテンプレートに準拠させることができます。詳細については、 <a href="#">テンプレートベースのAIを活用したサマリーの有効化</a> を参照してください。 注: このオプションはデフォルトで無効になっています。

5. **Apply** をクリックします。このユーザープロフィールにユーザーグループを割り当てることができます。 [こちら](#)をステップ 3(ライセンスの割り当て)で参照してください。

## AIの自動起動の有効化

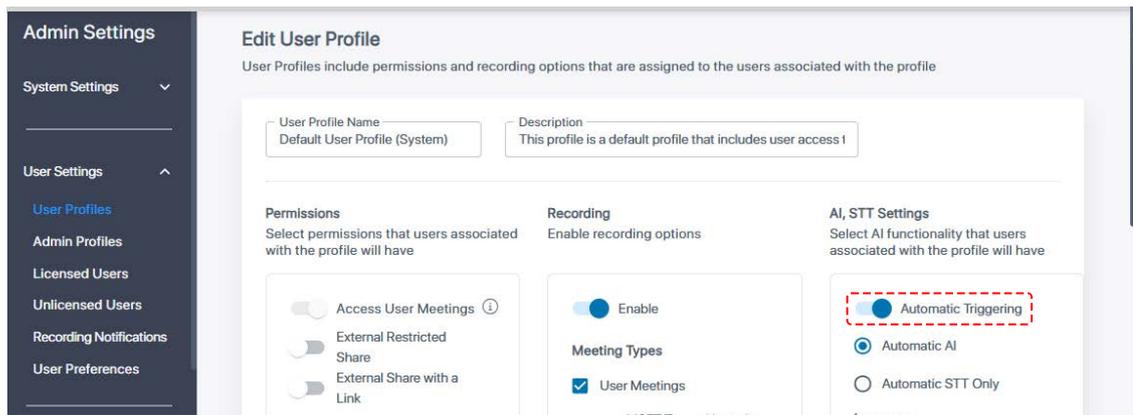
Meeting Insights を有効にすると、特定のユーザープロフィールに属するユーザーの会議録画に対してAIを活用したインサイトを自動的に生成できます。有効にすると、会議の開始時に言語を選択するようにユーザーに求めるメッセージは表示されません。



- アプリケーションに「Automatic AI Triggering」が含まれていないが、その機能を追加する場合は、サービスプロバイダーにお問い合わせください。
- AI生成は会議の終了時に行われ、時間がかかる場合があります (最大で会議の所要時間の半分まで)。
- 「Automatic Publish」が設定されているユーザーの場合、生成された分析情報を含む会議のサマリーは、生成が終了すると会議の内部参加者に自動的に送信されません。

### ➤ AIを活用した自動分析を有効にするには:

1. Admin Settings メニュー ペインで **User Settings** を展開し、**User Profiles** をクリックすると、「ユーザープロフィール」ページが表示されます。
2. User Profile を選択すると、「ユーザープロフィールの編集」ページが表示されます。
3. **AI, STT Settings** グループで、**Automatic Triggering** トグルスイッチをクリックしてオンにします。



4. 次のいずれかを選択します。

- **Automatic AI:** (デフォルト) AI を自動的にトリガーして、転写と分析情報を生成します。
- **Automatic STT Only:** AI を自動的にトリガーして、文字起こしのみを生成します。

5. Language 下で、次のいずれかを実行します。

- **Automatic Language Detection と Preferred Dialect:** (デフォルト) Meeting Insights が会議で話された主要言語を自動的に検出し、AI を活用した文字起こしとインサイトを生成できるようにします。言語に複数の方言がある場合、Meeting Insights では、音声テキスト変換サービスに使用する優先方言を選択できます。方言を選択すると、文字起こしの精度が向上し、音声テキスト変換サービスで話された単語を正しく識別して認識できるようになります。
  - i. 「Automatic Language Detection」チェックボックスを選択します。
  - ii. 「Select Preferred Dialect」ドロップダウンリストから、言語ごとに優先方言を選択します。



- 選択できるのは言語ごとに1つの方言です。たとえば、リストに英語とフランス語の複数の方言が含まれている場合、次の例に示すように、それぞれに対して1つの方言のみを選択できます。

**Language**

User language can be selected during the meeting, set in advance for English only speakers. Only one option can be selected.

Automatic Language Detection

Select Preferred Dialect

English

English (United States)

English (United Kingdom)

French

French (Belgium)

French (Canada)

French (France)

- ドロップダウンリストで利用可能な言語と方言を追加または削除するには、[AIを活用した文字起こしの有効化と構成](#)を参照してください。

- **デフォルトの会議言語:** AIを活用した文字起こしと分析のために、会議のデフォルト言語を設定できます。
    - 「Automatic Language Detection」チェックボックスをオフにします( 選択されている場合)。
    - ドロップダウンリストから特定の言語を選択するか、**Select Language During Meeting** を選択して会議中にユーザーに言語を選択するよう促します。
6. **Insights** の下で、対応するチェックボックスをクリックして、AIによって自動的に生成される Insights を選択します。
- サマリー( 以下のいずれかを選択) :
    - ◆ 箇条書き
    - ◆ 段落
    - ◆ 話者
  - アクションアイテム
  - 問題と解決策

- 質問と回答
- 準備



AIを活用したインサイトは、**自動 AI オプション**を選択した場合にのみ自動で生成されません(手順4を参照)。

7. **Meeting Types** 下で、すべての会議または特定の会議タイプでAIを自動的にトリガーするかどうかを選択します。
  - **All Meetings** - すべての会議でAIをトリガーします。
  - **Select Meeting Types**: 特定の種類の会議でAIをトリガーします。
    - ◆ **Meetings with External Parties**: 外部招待者との会議に対してのみAIをトリガーします。
    - ◆ **Meetings with <number> Invitees or More**: 指定された数以上の招待者がいる会議に対してのみAIをトリガーします。

#### Meeting Types

All Meetings  Select Meeting Types

Meetings with External Parties

Meetings with  Invitees or More

8. **Apply** をクリックします。

## テンプレートベースのAIを活用したサマリーの有効化

AI生成のサマリーをカスタムレイアウトテンプレートに準拠させるように設定できます。テンプレートを使用すると、会議の概要を特定の形式に準拠させることができます。たとえば、組織では、「会議の議題」、「主な懸念事項」、「望ましい目標」などの特定の用語を使用してサマリーを分類する必要がある場合があります。

テンプレートの使用が有効になっている会議の録画の所有者は、1つ以上のテンプレートに基づいてAIを活用したサマリーを実行できます。つまり、所有者は同じ会議録画の複数のサマリーを生成でき、それぞれが異なるテンプレートに基づいています。

Meeting Insightsでは、次の種類のテンプレートが提供されます。

- **カスタムテンプレート**: 組織の特定のニーズに合わせてカスタマイズします。利用可能なカスタムテンプレートを表示するには、[AIを活用したカスタムテンプレートの表示と命名](#)を参照してください。
- **ライブラリテンプレート**: ほとんどの組織に適した事前に構築されたテンプレート。利用可能なライブラリテンプレートを表示するには、[AIを活用したライブラリテンプレートの表示と命名](#)を参照してください。



利用可能なテンプレートの一覧を表示するには、AIを活用したカスタムテンプレートの表示と命名を参照してください。

➤ **テンプレート ベースの AI によるサマリーを有効にするには:**

1. Admin Settings メニュー ペインで、**User Settings** を展開し、**User Profiles** をクリックします。
2. **New Profile** をクリックして新しいユーザー プロフィールを追加するか、既存のユーザー プロフィールを選択します。
3. **AI, STT Settings** 下で、**Enable AI Templates** トグル ボタンをクリックし、AI 生成 サマリーのテンプレートをオンにします。
4. 「Select Templates」フィールドをクリックすると、セクターとそのテンプレートを一覧表示する次のダイアログ ボックスが表示されます。

Sectors	Templates
<input type="checkbox"/> (No Sector)	<input type="checkbox"/> template_test1
<input type="checkbox"/> USA_CUSTOM	<input type="checkbox"/> template_test2
<input type="checkbox"/> ADVANCED	<input type="checkbox"/> template_test3
<input type="checkbox"/> FFF	<input type="checkbox"/> tal test 1
<input type="checkbox"/> TAL TESTS	

Select Templates

5. **Sectors** ペイン下でセクターを選択し、次に**Templates**ペイン下で、必要なセクターのテンプレートを選択します。
6. 追加のセクターのテンプレートを選択する場合は、前の手順を繰り返します。
7. ダイアログ ボックスの外側の任意の場所をクリックしてダイアログ ボックスを閉じます。「Select Templates」フィールドに「Templates」と、選択したテンプレート の数が表示されます。
8. **Apply** をクリックします。

## ユーザー プロフィールごとの会議録画の種類

ユーザー プロフィールごとに、Meeting Insights ボット Mia で録画できる会議の種類を選択できます。これらの会議プラットフォームには、次のいずれかが含まれます。

- 自組織が主催する Microsoft Teams 会議これらの会議はデフォルトで許可されます。
- 他組織が主催する Microsoft Teams 会議( [ユーザーが外部の Teams 会議を録画できるようにする](#)参照)。
- 組織または他の組織が主催する Zoom 会議( [ユーザーが Zoom 会議を録画できるようにする](#)参照)。
- 組織または他の組織が主催する Google Meet 会議( [ユーザーが Google Meet 会議を録画できるようにする](#)を参照してください)。

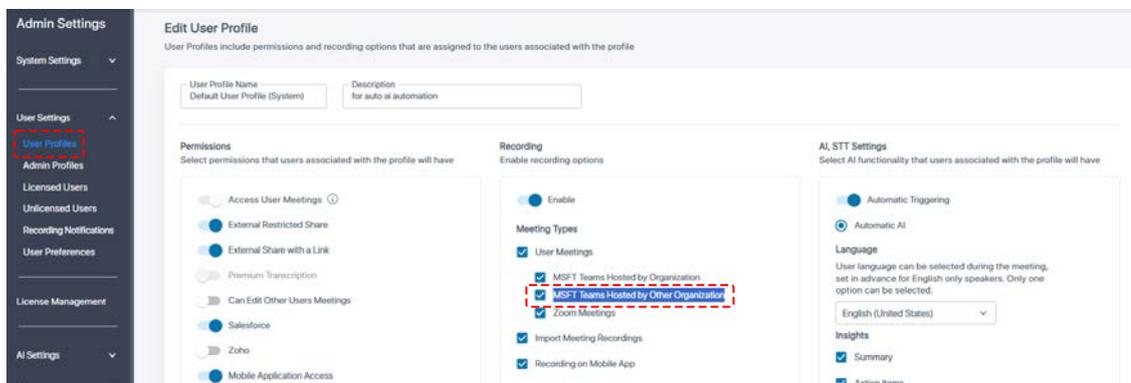
## ユーザーが外部の Teams 会議を録画できるようにする

特定のユーザー プロフィールに関連付けられたユーザーが、他の組織によってホストされる Microsoft Teams 会議 (外部 Teams 会議) を録画できるようにすることができます。

外部の Teams 会議に参加して録画する Meeting Insights ボットの名前をカスタマイズすることもできます。

### ➤ ユーザーが外部の Teams 会議を録画できるようにするには:

1. Admin Settings メニュー ペインで、**User Settings** を展開し、**User Profiles** をクリックします。
2. 外部の Teams 会議の録画を有効にするユーザーを含むユーザー プロフィールを選択すると、「ユーザープロフィールの編集」ページが表示されます。
3. **Recording** セクションの **Metering Types** グループで、「MSFT Teams Hosted by Other Organization」チェックボックスをオンにします。



4. **Apply** をクリックします。
5. (オプション) Meeting Insights ボットの名前をカスタマイズするには( [詳細はサードパーティの会議アプリ向けの Meeting Insights ボット名と通知のカスタマイズ](#)を参照してください):
  - a. Admin Settings メニュー ペインで、**Integrations** を展開し、**UC Recording** をクリックします。
  - b. **MSFT Teams Hosted by Other Organizations** の「Bot Name」フィールドで、ボット名を構成します。使用できるプレースホルダーを表示するには、**i** アイコンをクリックします。

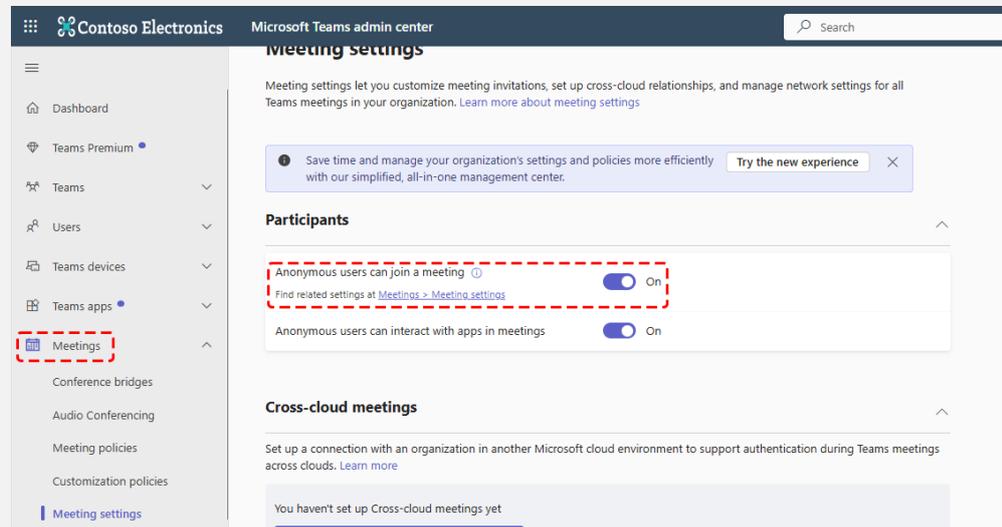
The screenshot displays the 'UC Recording Integration' configuration page. On the left, a dark sidebar lists various settings categories: 'User Settings' (expanded), 'User Profiles', 'Admin Profiles', 'Licensed Users', 'Unlicensed Users', 'Recording Notifications', 'User Preferences', 'License Management', 'AI Settings', 'Anonymization', 'Monitoring', 'Integrations', and 'Apps'. Under 'Apps', 'UC Recording' is selected and highlighted with a red dashed box. The main content area, titled 'UC Recording Integration', features a 'Bot Settings' section. It includes a 'Zoom' section with a 'Bot Name' field containing 'Stage Zoom'. Below it is the 'MSFT Teams Hosted by Other Organizations' section, where the 'Bot Name' field is highlighted with a red dashed box and contains the text '<UserFirstName>'s Meeting Assistant and Recorder'. At the bottom right of the settings area, there are 'Cancel' and 'Apply' buttons.

- c. **Apply** をクリックします。

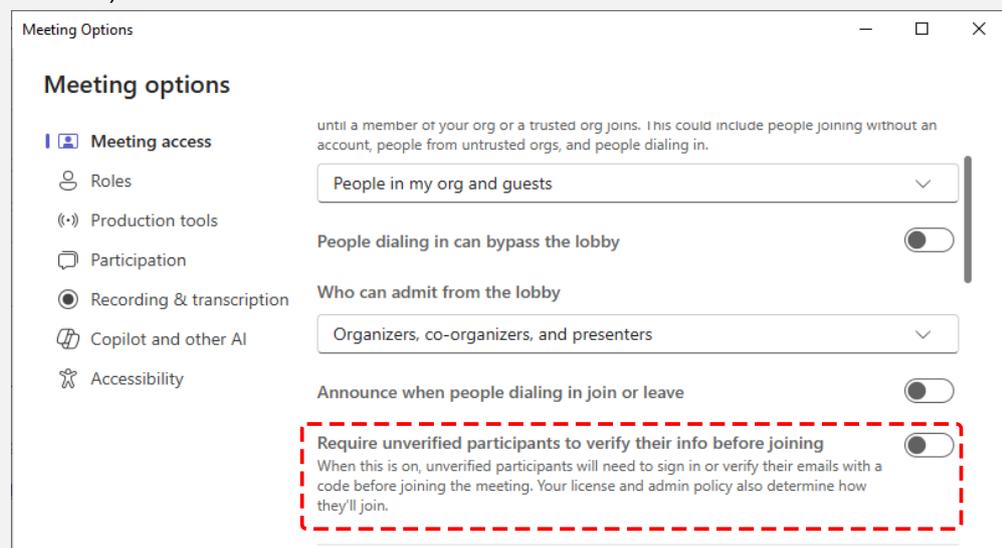


Meeting Insights で外部の Teams 会議を録画するには、他の組織の管理者が匿名ユーザーに Teams 会議への参加を許可する必要があります。他の組織の管理者は、匿名ユーザーを管理するさまざまな方法を持っています( 詳細の参照先: [匿名の参加者の管理に関する Microsoft のドキュメント](#) ):

- **組織全体のポリシー:** Teams 管理者センターで「Anonymous users can join a meeting」設定を有効にする必要があります(既定)。



- **特定の会議ポリシー:** 会議の主催者は、会議のポリシーで匿名ユーザーの参加が許可されていることを確認する必要があります。デフォルトでは、これは許可されています(「未確認の参加者は参加前に情報を確認する必要がある」は無効になっています)。

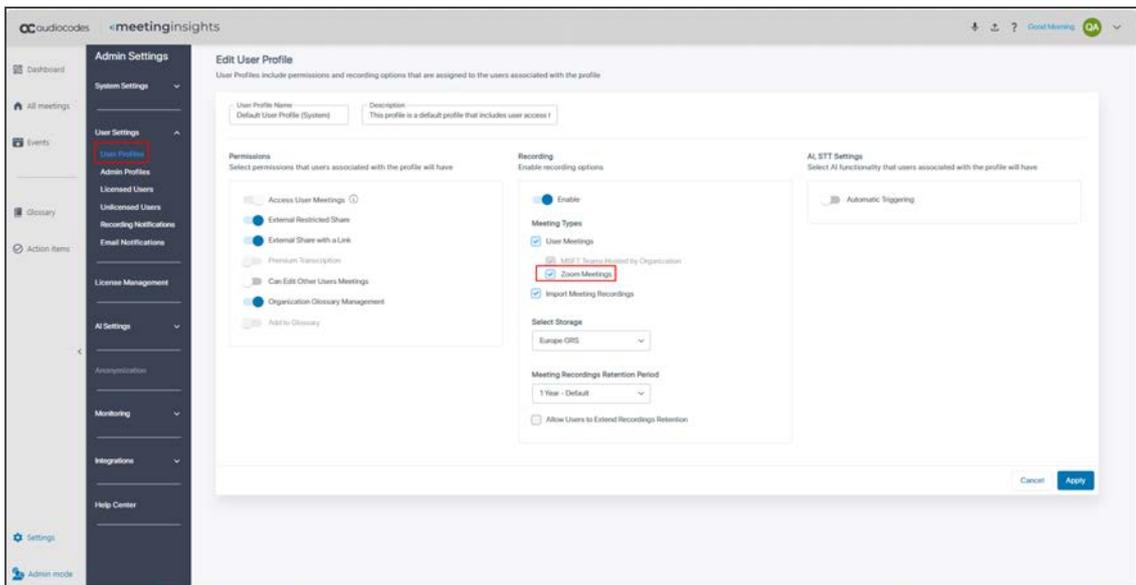


## ユーザーが Zoom 会議を録画できるようにする

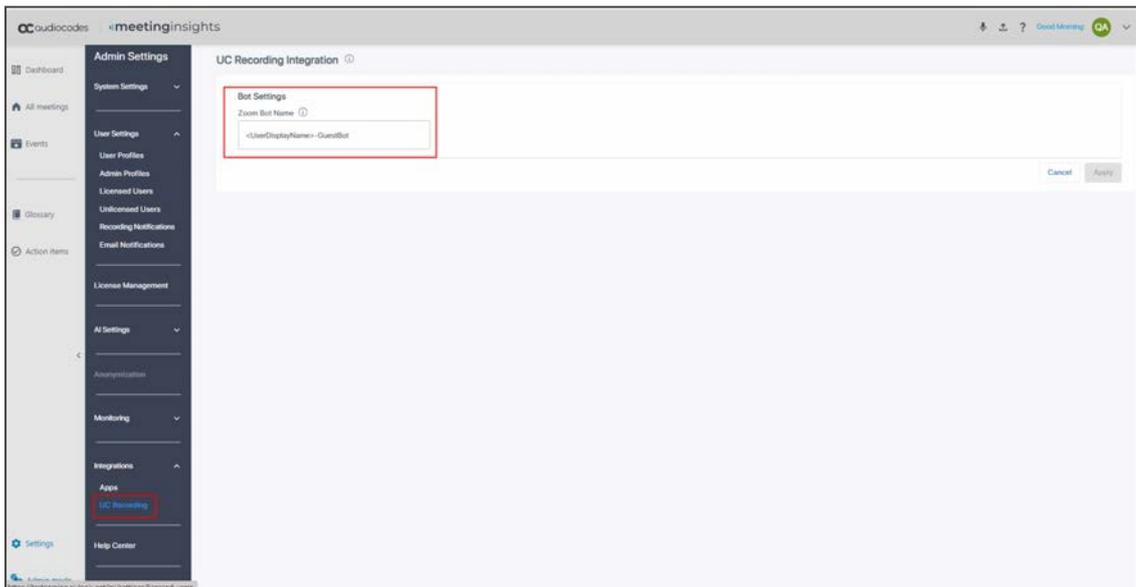
Zoom 会議を録画できるようユーザー(特定のユーザープロフィールに関連付けられている)を有効化できます。

### ➤ ユーザーが Zoom 会議を録画できるようにするには:

1. Zoom を有効にするユーザーが関連付けられているユーザープロフィールを選択します。



2. [オプション]「UC 録画統合」ページ(Admin Settings > Integrations > UC Recording)の「Bot Settings」の「Zoom Bot Name」フィールドで、Zoom ボット名を設定します。



3. 「Zoom Bot Name」の横にある i アイコンをクリックし、ツールヒントを参照として使用します。





- 「Zoom Bot Name」フィールドには、括弧で囲まれた <UserDisplayName> が含まれます。
- これは、Zoom Bot が会議に参加するために使用する名前です。

4. Apply をクリックします。

## ユーザーが Google Meet 会議を録画できるようにする

特定のユーザープロフィールに関連付けられたユーザーが、Meeting Insights によって Google Meet 会議を録画できるようにすることができます。Google Meet は、組織内または外部の組織(外部会議)でホストできます。

Google Meet 会議に参加して録画する Meeting Insights ボットの名前と、ボットが参加したときに表示される録画通知メッセージをカスタマイズすることもできます。詳細については、[サードパーティの会議アプリ向けの Meeting Insights ボット名と通知のカスタマイズ](#)を参照してください。



Meeting Insights で外部の Google Meet 会議を録画するには、**他の組織の管理者**が匿名ユーザーに会議への参加を許可する必要があります。他の組織の管理者は、匿名ユーザーを管理するさまざまな方法を持っています。詳細については、[Google のドキュメント主催者コントロールで会議へのアクセスを制御する](#)をご覧ください。

### ➤ ユーザーが Google Meet 会議を録画できるようにするには:

1. Admin Settings メニュー ペインで、**User Settings** を展開し、**User Profiles** をクリックします。
2. Google Meet 会議の録画を有効にするユーザーを含むユーザープロフィールを選択すると、「ユーザープロフィールの編集」ページが表示されます。
3. **Recording** セクションの **Metering Types** グループ下で、「Google Meetings」チェックボックスをオンにします。

The screenshot shows the 'Add User Profile' configuration page. On the left, the 'Admin Settings' sidebar is visible with 'User Settings' expanded and 'User Profiles' selected. The main content area is titled 'Add User Profile' and includes fields for 'User Profile Name' and 'Description'. Below these are three sections: 'Permissions', 'Recording', and 'AI, STT Settings'. The 'Recording' section is expanded, showing 'Enable recording options' set to 'Enable'. Under 'Meeting Types', the 'Google Meetings' checkbox is checked and highlighted with a red box. Other options like 'MSFT Teams Hosted by Organization', 'MSFT Teams Hosted by Other Organization', 'Zoom Meetings', and 'Import Meeting Recordings' are also visible.

4. Apply をクリックします。

## 管理者プロフィール

管理者プロフィールを設定できます。



デフォルトでは、管理者の数は5人に制限されています。さらに必要な場合は、サービスプロバイダーにリクエストできます。

### ➤ 管理者プロフィールを構成するには:

1. 「User Settings」メニューの下にある **Admin Profiles** オプションをクリックします。

Administrators (Full Access) ⓘ

Email Address Add

admin@M365x64321460.onmicrosoft.com | x

2. 追加する管理者のメールアドレスを入力し、**Add** をクリックします。



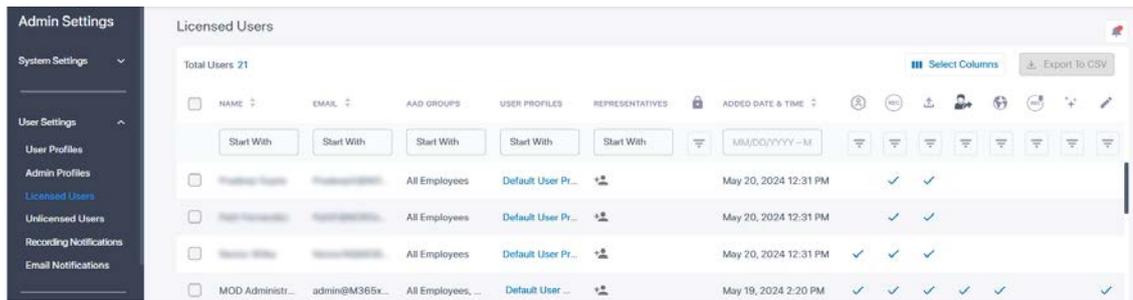
- 追加されたメールアドレスは、デフォルトの管理者となる管理者のメールアドレスです。
- デフォルトの管理者にはフルアクセス権限があり、すべての「Meeting Insights」ページにアクセスして、すべてを実行したり表示したりできます。
- アクセス権を失った場合、またはデフォルトの管理者アカウントが利用できないか削除されている場合は、サービスプロバイダーに連絡して、指定したアカウントを設定して管理者アカウントをリセットしてください。

## ライセンスありのユーザー

「ライセンスユーザー」ページでは、管理者はシステム内のすべてのライセンスユーザーとその権限を表示できます。このページでは、ユーザーが自分の録画に完全にアクセスするために別のユーザーを必要とする場合に備えて、管理者がユーザーに代表者を割り当てることもできます。たとえば、従業員が会社を退職する場合、割り当てられた担当者は退職する従業員の会議録画に対する所有者アクセス権を持ちます。

### ➤ ライセンスユーザーを管理するには:

1. 「User Settings」メニューで、「Licensed Users」オプションをクリックします。



2. ライセンスを取得したユーザーを1人選択するか、ライセンスを取得したユーザーを複数選択するか、またはNAME列の横にあるボックスをオンにして、ライセンスを取得したユーザーをすべて選択します。
3. 管理者権限アイコンや録画通知アイコンなどの権限アイコンの上にマウスを移動すると、アイコンを識別するツールヒントがポップアップ表示されます。
4. 必要な権限アイコンの下で、 ポップアップから、ALL、Enabled または Disabled を選択します。
5. [オプション] 代表者を追加: 代表者を追加するユーザーの隣にあるアイコンをクリックします。



6. 「Search」フィールドに、代表者として追加するユーザーの名前を入力します。



ライセンスを付与されたユーザーのみを他のユーザーの代表として追加できます。

7. ボックスにチェックを入れて、Apply をクリックします。代表者として追加したユーザーの名前は、「ライセンスユーザー」ページの REPRESENTATIVES 列に表示されます。



8. 「lock」アイコンが表示されている場合は表示します(前の図には示されていません)。



- 目的: 「lock」アイコンは、組織内でユーザー アカウントが変更されるまれな場合に表示されるセキュリティ機能です。
- 元従業員のユーザー プリンシパル名 (UPN) が再利用されると、アイコンが表示されます。これは、従業員が組織に戻った場合、または同じ UPN が新しい従業員に割り当てられた場合に発生する可能性があります。リストされているアカウントの横にこのアイコンが表示されている場合、組織の管理者がその従業員 (ユーザー) に退席した従業員の会議録画へのアクセスを許可するには、アイコンをクリックしてロックを解除します。新しい従業員にアクセスを許可したくない場合は、サービスプロバイダーのサポートにサポート チケットを開いて競合を解決してください。
- この機能で可能なこと:
  - ✓ 同じ UPN を持つユーザーが検出されると、アカウントはロックされます。
  - ✓ ロックにより、新しいユーザーが古いユーザーに代わって古い会議の録画にアクセスできなくなります。
  - ✓ ロックにより、新しいアカウントの新規録画とログインも停止されます。
- 管理者はユーザーのロックを解除することができ、ユーザーは以前のユーザーの会議録画にアクセスできるようになります。

- ユーザーを選択します。
- 🔒アイコンをクリックします。

## ライセンスなしのユーザー

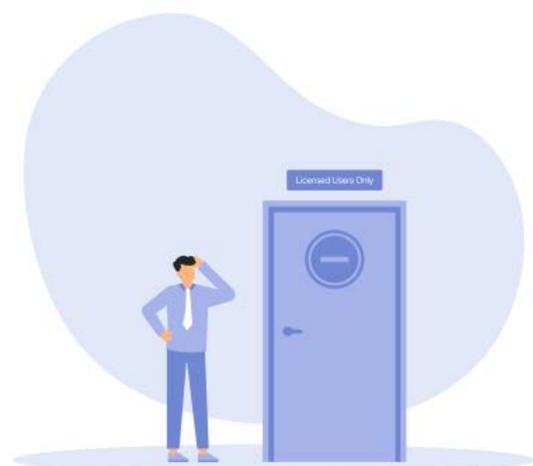
「ライセンスのないユーザー」ページでは、管理者はシステム内のすべてのライセンスのないユーザーを管理できます。ライセンスのないユーザーとは、ライセンスのあるユーザーの会議に参加し、参加した会議の一部として表示するために名前や UPN などの情報がシステム内に保持されているユーザー、または以前にライセンスを持っていたユーザーです。

ライセンスのないユーザーが Meeting Insights から、たとえばサマリーに関するメールを受信した場合、ユーザーが会議の録画にアクセスするためのボタンをクリックすると、次のメッセージが表示されます。

meetinginsights

### No license

You do not have a Meeting Insights license to view meetings.  
Please reach out to your admin to get a license.



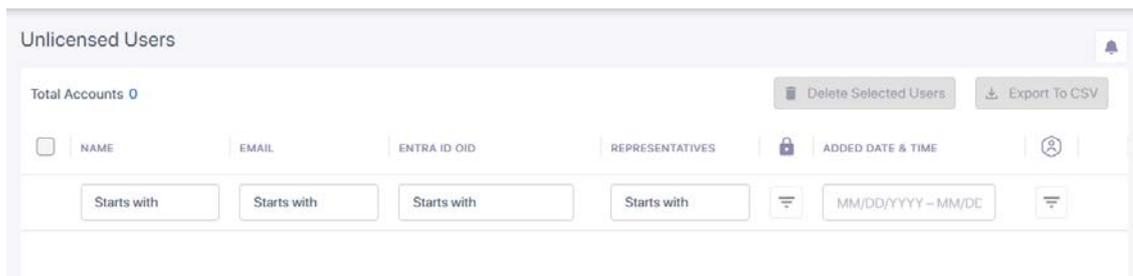
audiocodes



- 管理者は、ユーザーの情報を削除する必要がある場合、これらのユーザーを削除できます。
- 会議が削除された後にユーザーが会議に参加すると、ユーザーとその情報が再度追加されます。
- ページからユーザーを削除しても、会議からそのユーザーの表示名は削除されません。

### ➤ ライセンスのないユーザーを管理するには:

1. 「User Settings」メニューで、**Unlicensed Users** オプションをクリックします。



2. (オプション)「Name」の横にあるボックスをオンにして、ページにリストされているライセンスのないユーザーをすべて選択します。すべて選択解除するには、同じボックスをもう一度クリックします。
3. ライセンスのないユーザーを1人選択するか、各エントリの横にあるボックスをオンにしてライセンスのないユーザーを複数選択します。ライセンスのないユーザーの合計数のうち、選択したライセンスのないユーザーの数が表示されます。
4. (オプション) ページをフィルタリングする
  - 「Name」: 「Name」列の下の **Start With** フィールドに、名前の文字を入力します。
  - 「Email」: 「Email」列の下の **Start With** フィールドに、メールアドレスを入力します。
  - 「Entra ID OID」: 「Entra ID OID」列の下の **Start With** フィールドに、Microsoft Entra ID ユーザーのOIDを入力します。
  - 「Representatives」: 「Representatives」列の下の **Start With** フィールドに、代表者の名前を入力します。
  - : **ALL**、**Unlocked** または **Locked** のユーザーでフィルタリングします。
  - 「Added Date & Time」: **MM/DD/YY - MM/DD/YY** をクリックし、ポップアップ表示されるカレンダーで期間の開始日と終了日を選択します。



- ロックアイコンは、組織内でユーザーアカウントが変更される場合にまれに表示されるセキュリティ機能です。
- 元従業員のユーザープリンシパル名 (UPN) が再利用されると、アイコンが表示されます。これは、従業員が組織に戻った場合、または同じ UPN が新しい従業員に割り当てられた場合に発生する可能性があります。リストされているアカウントの横にこのアイコンが表示されている場合、組織の管理者がその従業員 (ユーザー) に退席した従業員の会議録画へのアクセスを許可するには、アイコンをクリックしてロックを解除します。新しい従業員にアクセスを許可したくない場合は、サービスプロバイダーのサポートにサポート チケットを開いて競合を解決してください。
- この機能で可能なこと:
  - ✓ 同じ UPN を持つユーザーが検出されると、アカウントはロックされます。
  - ✓ ロックにより、新しいユーザーが古いユーザーに代わって古い会議の録画にアクセスできなくなります。
  - ✓ ロックにより、新しいアカウントの新規録画とログインも停止されます。
- 管理者はユーザーのロックを解除することができ、ユーザーは以前のユーザーの会議録画にアクセスできるようになります。

## 会議の保持ポリシー

Meeting Insights を使用すると、会議の録画のユーザー (つまり、ユーザープロフィール) の保持ポリシー (期間) を定義できます。会議の録画の保持期間を超えると、Meeting Insights は関連データを削除します。

グローバル保存期間だけでなく、以下の特定の(例外)データの保存期間も定義できます:

- 会議記録のメディア(音声とビデオ)
- 会議録画の書き起こし
- 会議録画のAI生成インサイト (要約、会議準備、概要、アクション項目、質疑応答、問題と解決策)

メディアと文字起こしの保持期間をゼロ (0) に定義できます。これにより、Meeting Insights は AI 概要を生成し、録音や文字起こしを保存しません。



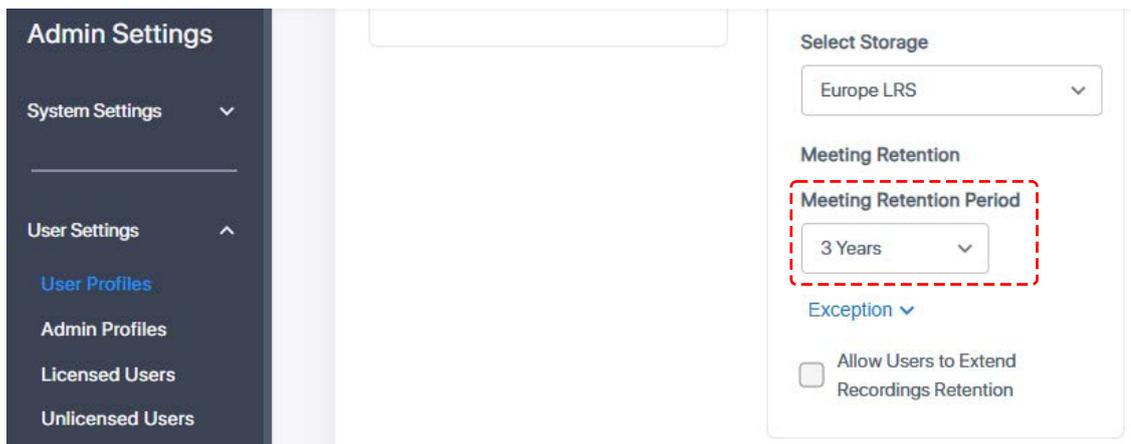
- このセクションでは、可能なすべての保持設定について説明します。ただし、これらの各保持オプションを利用できるかどうかは、購入した Meeting Insights プランによって異なります。
- 会議の録画は、会議の所有者/主催者に関連付けられたユーザープロフィールによって定義された保持期間を継承します。
- 保存期間を変更すると、ユーザープロフィールに関連付けられたユーザーが所有する過去と未来の両方のすべての会議の録画に適用されます。保持設定がすぐに有効になります。そして、新しい保持ポリシーに従って会議データを永久削除します。変更された保持期間が短い場合、この制限を超える既存の会議録画は直ちに削除されます。
- ユーザーを別のユーザープロフィールに再割り当てすると、そのユーザーの既存の会議録画すべてに、新しいユーザープロフィールの保持ポリシーが適用されます。新しいユーザープロフィールの保持期間を超えた会議の録画は、直ちに削除されます。
- メディア記録の保持期間がゼロ日の場合、ユーザーはサードパーティのオーディオファイル (wav) のみをインポートできます。または aac。形式 (ビデオファイルではありません)

#### ➤ 保持期間を定義するには:

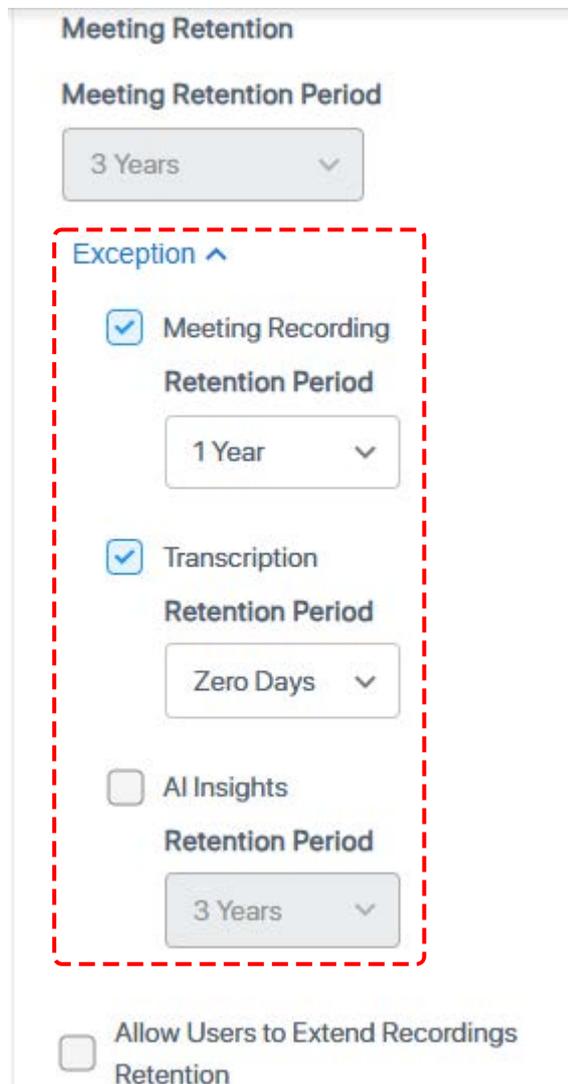
1. Admin Settings メニュー ペインで **User Settings** を展開し、**User Profiles** をクリックすると、「ユーザープロフィール」ページが表示されます。
2. User Profile を選択すると、「ユーザープロフィールの編集」ページが表示されます。
3. 会議録画のグローバル(メディア、文字起こし、AI生成のインサイト) 保持期間を構成するには:

**Recording** グループ下で、「Meeting Retention Period」ドロップダウンリストからグローバル保持期間を選択します。

- 90日間
- 180日間
- 1年 - デフォルト
- 2年(730日)
- 3年(1,095日)
- **Custom** をクリックし、特定の日数を入力します。



4. メディア、文字起こし、または AI 生成の分析情報の特定の保持期間を定義して、グローバル設定を上書きするには (手順 3)、次の手順を実行します。
  - a. Exception をクリックして内容を拡大:



- b. 会議の録画 (音声とビデオ) の保持期間を指定するには、「Meeting Recording」チェックボックスをオンにし、「Retention Period」ドロップダウンリストから保持期間を選択します。
- c. 会議の録画の文字起こしの保存期間を指定するには、「Transcription」チェックボックスをオンにし、「Retention Period」ドロップダウンリストから保存期間を選択します。
- d. AIによって生成されたインサイトの保持期間を指定するには、「AI Insights」チェックボックスをオンにし、「Retention Period」ドロップダウンリストから保持期間を選択します。



保持例外期間の場合:

- 例外期間は**2025年6月9日以降**に作成された会議の録画にのみ影響します。
- ゼロ日間の保持期間は、メディア(「会議記録」と文字起こし(「文字起こし」))に対してのみサポートされます。
- 例外の保存期間を定義すると、「Meeting Retention Period」フィールド(手順3を参照)には、**最高保存期間の例外と同じ値**が自動的に表示されます。

5. ユーザーが選択した会議記録の保存期間を可能な限り長く延長できるようにするには、**Allow Users to Extend Recordings Retention**チェックボックスをオンにします。これにより、以前に選択した保持期間が上書きされます。
6. **Apply** をクリック。設定に応じて、次のいずれかの確認メッセージが表示されます。
  - グローバル保持期間のみを定義した場合(「Meeting Retention Period」フィールド) :

### Meeting Retention Policy

The configured 'Meeting Recording Retention Period' will apply to all meetings — both past and future — owned by users associated with this profile. Retention settings take effect immediately upon application and may result in the permanent deletion of meeting data according to the new policy.

Cancel

Apply

- 例外保持期間を定義した場合:

### Meeting Retention Policy

The configured 'Meeting Recording Retention Period' will apply to all meetings — both past and future — owned by users associated with this profile. Retention settings take effect immediately upon application and may result in the permanent deletion of meeting data according to the new policy.

Note: The Meeting Retention Policy Exception applies only to meetings that took place after June 9, 2025.

Cancel

Apply

7. **Apply** をクリックして確認します。

## Microsoft 録画通知

Meeting Insights が有効になると、Teams 会議の Microsoft 録画通知をトリガーできます。有効にして会議を録画した場合に、Meeting Insights によって Microsoft が会議参加者に音声と視覚的な通知を提供するようになります。この設定は、Meeting Insights ユーザーによって上書きすることはできません。

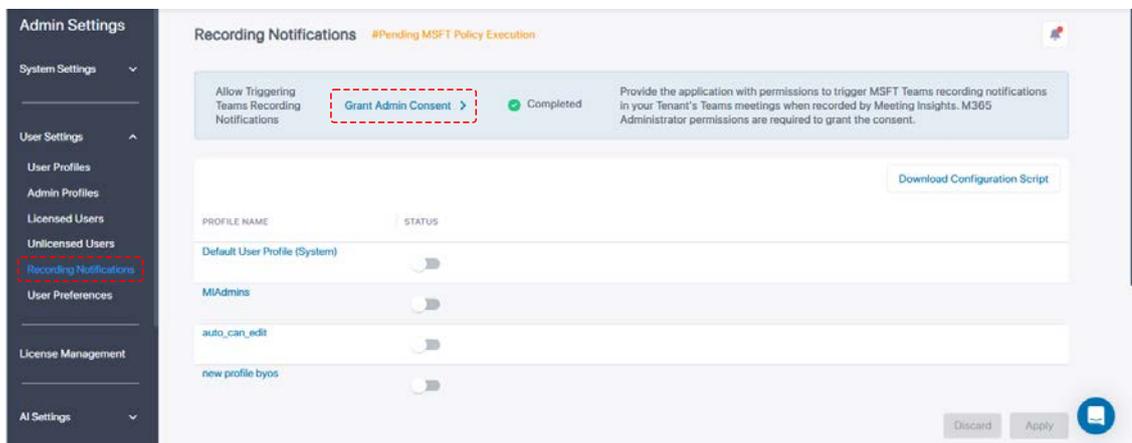
会議の録画は、所有者 (主催者) または録画通知が有効になっている参加者 (内部) が会議に参加した場合にのみ開始されます。所有者が会議を退席した場合でも、会議に参加している組織内の参加者のうち少なくとも 1 人が録画通知を有効にしている限り、録画は続行されます。所有者が会議を退席し、他の参加者に録画通知が有効になっていない場合、録画は一時停止されます。所有者または録画通知が有効になっている他の参加者が再度参加すると、録画が再開されます。Microsoft の録画通知機能が無効になっている場合は、所有者または他の参加者が会議に参加したか、退出したか、または参加も退出もしなかったかどうかに関係なく、録画は続行されます。



このセクションで説明する録画通知を有効にする手順には、**Teams 管理者の権限を必要とする Microsoft スクリプトの実行**が含まれます。

### ➤ Meeting Insights によって録画された会議中に録画通知をトリガーするには:

1. Admin Settings メニュー ペインで、**User Settings** を展開し、**Recording Notifications** をクリックします。



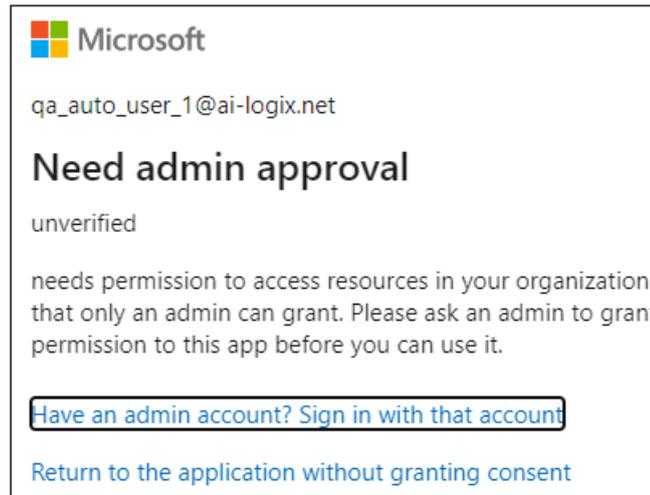
2. Meeting Insights によって録画された会議中に Teams の録画通知をトリガーできるように管理者の同意が与えられていることを確認します。

- ✔ は同意が得られたことを示します
- ✖ は同意がまだ与えられていないが、与えられる必要があることを示します



- 同意が得られていない場合は、ページを編集できません。
- 録画通知には、「M365に接続」ページから「Allow Meeting Insights to be Added to Ongoing Meetings」スクリプトを正常に実行する必要があります。このスクリプトにより、通知ボットが会議情報にアクセスできるようになります。

3. まだ同意が得られていない場合は、**Grant Admin Consent** をクリックします。



4. M365 管理者アカウントでサインインします。
5. Microsoft のアプリ権限を承認します。



admin@m365x30069440.onmicrosoft.com

## Permissions requested (1 of 2 apps)

Review for your organization

sandbox3mi-mia  
unverified

**This application is not published by Microsoft or your organization.**

This app would like to:

- ✓ Daemon Role (sandbox3mi-meetings)
- ✓ Bot Role (sandbox3mi-meetings)
- ✓ Access media streams in a call as an app
- ✓ Join group calls and meetings as an app
- ✓ Read online meeting details
- ✓ Read names and members of all chat threads
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Next

6. Next をクリックすると、次のアプリ権限ダイアログが表示されます。



← admin@m365x30069440.onmicrosoft.com

## Permissions requested (2 of 2 apps)

Review for your organization



**This application is not published by Microsoft or your organization.**

This app would like to:

- ✓ View users' basic profile
- ✓ Maintain access to data you have given it access to

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

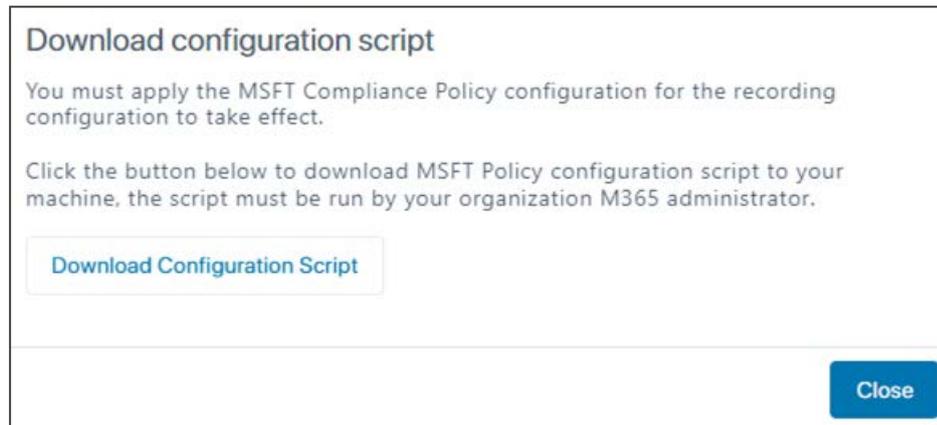
Accept

7. **Accept** をクリックします。
8. ユーザー プロフィールを有効にします。
  - たとえば、デフォルトのユーザープロフィール **Default User Profile (System)** を有効にします。
  - このプロフィールを持つすべてのユーザーは、自分が主催する会議中に録画通知を受け取ります。

- ユーザープロフィールを構成する方法については、[こちら](#)を参照してください。
9. ユーザープロフィールを変更すると、「録画通知」ページに次のメッセージが表示されます。

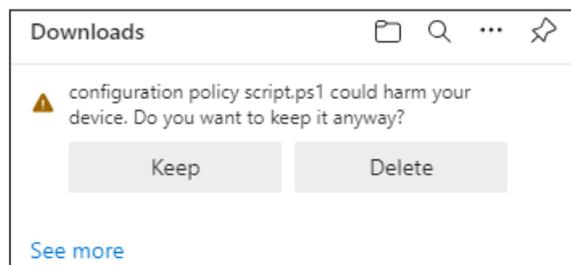


10. **Download Configuration Script** ボタンをクリックします。スクリプトは M365 管理者が実行する必要があります。



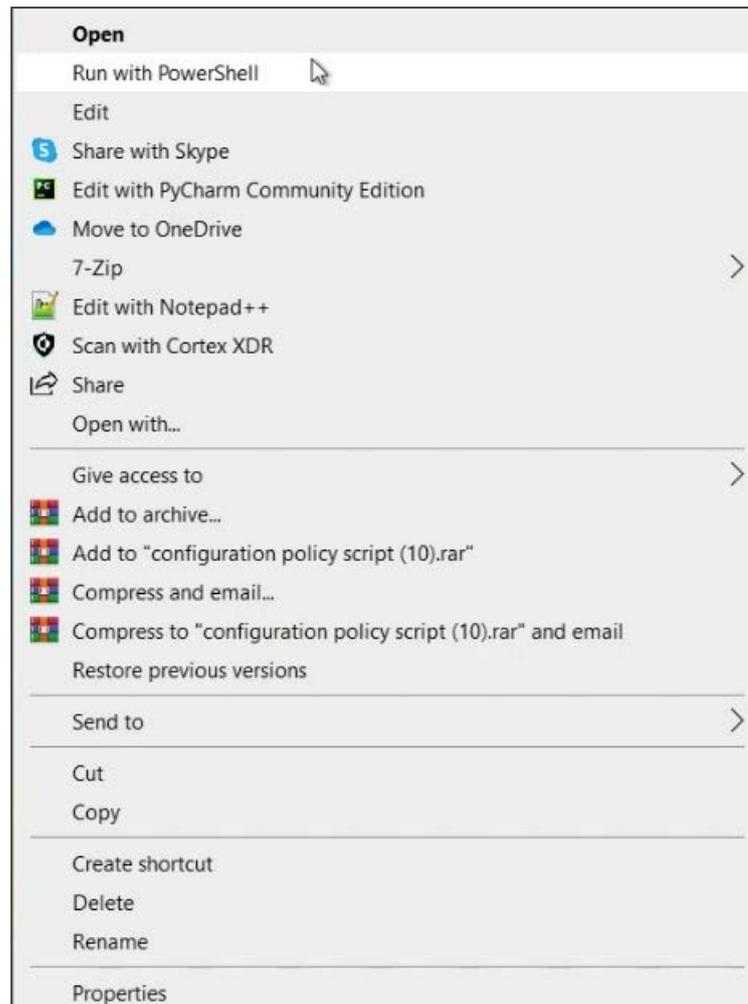
Microsoft で録画通知を有効にするには、スクリプトを実行する必要があります。Microsoft の構成が有効になるまでに時間がかかる場合があります。録画通知が有効になっているユーザーの会議は、Microsoft 側で構成が有効になるまで録画されません。

11. **Download Configuration Script** をクリックすると、次のプロンプトが表示されます。

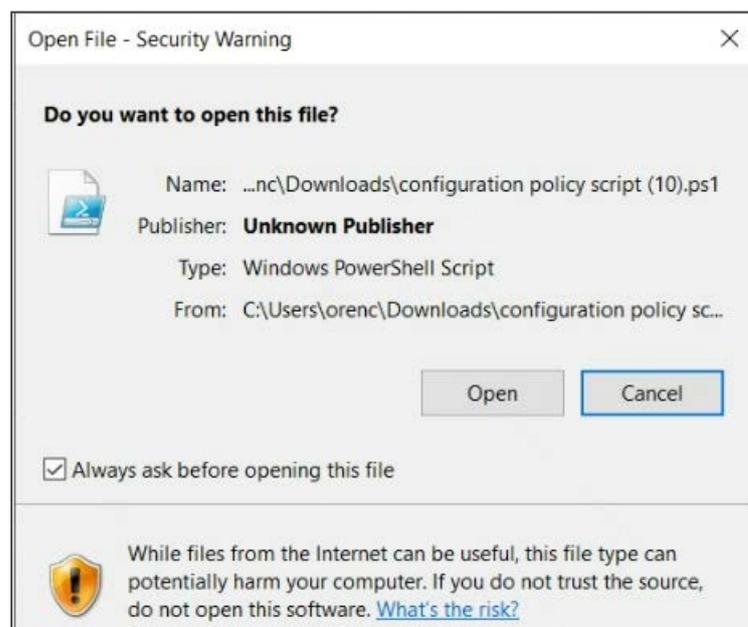


- Microsoft Edge のみで「Keep」プロンプトが表示されます。
- Chrome はすぐにダウンロード オプションを表示します。

12. (Edge の場合) **Keep** をクリックします。
13. (Chrome の場合) **ダウンロード アイコン**をクリックします。
14. ダウンロードした **policy script.ps1** ファイルを右クリックします。



15. Run with PowerShell オプションを選択します。

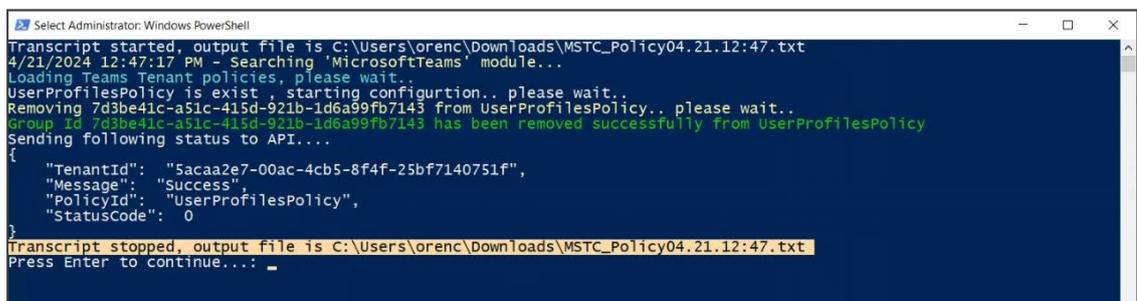


16. Open をクリックします。

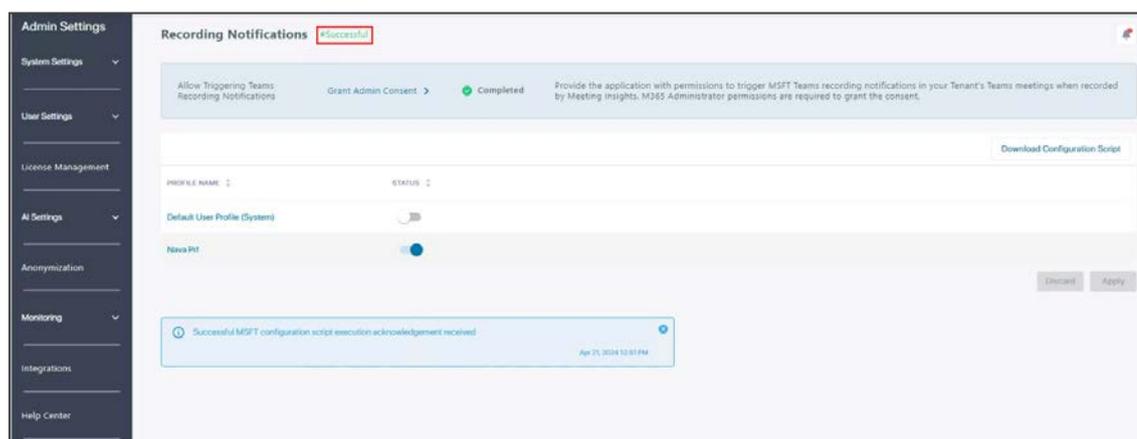


17. Yes をクリックします。

18. PowerShell で「A」と入力して Enter キーを押します。



19. スクリプトが実行されると、上の図に示すように「Transcript stopped」という表示と、下の図の「録画通知」ページに「Successful」というメッセージが表示されます。



- ユーザーに録画通知を有効にすると、ユーザーの通話確立が遅くなる可能性があります。
- Microsoft Entra ID グループを削除したり、通知の録画が有効になっているユーザープロフィールに Microsoft Entra ID グループを追加したりするには、変更を有効にするためにスクリプトをダウンロードして実行する必要があります。

## ユーザー設定

ユーザーに対して次の設定を構成できます。

- メール通知の設定 - [メール通知](#) 参照
- 会議録画の公開時間の設定 - [公開時間の設定](#) 参照

### メール通知

Teams のテナントでの会議中にユーザーに対して Microsoft の録画通知を有効にする権限を使用して、Meeting Insights を構成できます。

#### ➤ 電子メール通知を管理するには:

1. 「User Settings」メニューで、**User Preferences** オプションをクリックします。電子メール通知オプションは、**Default User Email Notifications** グループの下に表示されます。

Default User Email Notifications

Owner	Recipient
AI finished: Ready or Failed <input type="checkbox"/>	Action item was assigned to you in a meeting you were not invited to <input type="checkbox"/>
Meeting Processing Failure email notification <input type="checkbox"/>	Get meeting recap email once a meeting is published <input checked="" type="checkbox"/>
Transcription finished: Ready or Failed <input type="checkbox"/>	Get meeting recap UPDATE email once it is updated and sent by owner <input checked="" type="checkbox"/>
Weekly unpublished meetings reminder <input type="checkbox"/>	Get a notification email once a meeting is shared/unshared with you <input type="checkbox"/>
Added/Removed as a Representative for someone else <input type="checkbox"/>	Meeting recording is ready (Video ready) <input type="checkbox"/>
Get recap email once it's ready (for meetings not published yet) - only for cases you are configured as 'Not AutoPublish' <input checked="" type="checkbox"/>	Use Hebrew recap email template if recap is in Hebrew <input checked="" type="checkbox"/>

2. **Owner** で、会議録画の所有者への電子メール通知を構成します。

メール通知	説明
<b>所有者</b>	
AI 終了: 準備完了または失敗	AI サマリーが完了し、そのステータスが準備完了   失敗したことを示す電子メール通知をユーザーに送信する   送信しない場合は、オン   オフを切り替えます。
会議処理失敗のメール通知	会議処理が失敗したことを示す電子メール通知をユーザーに送信   送信しない場合は、オン   オフを切り替えます。
文字起こし終了: 準備完了または失敗	オン   オフにすると、文字起こしが完了し、そのステータスが準備完了   失敗であることを示す通知がユーザーに送信されます   送信されません。
毎週の未公開会議のリマインダー	未公開の会議についてユーザーに通知する電子メール通知を毎週送信するかどうかをオン   オフに切り替えます。

メール通知	説明
他の人の代表として追加/削除されました	オン   オフにすると、ユーザーが他のユーザーの代表として追加された   削除されたことを示す通知がユーザーに送信されます   送信されません。
準備ができたならサマリーメールを受け取る(まだ公開されていない会議の場合) - 「自動公開しない」に設定されている場合のみ	オン   オフにすると、サマリーの準備ができたことを示す電子メールがユーザーに送信されます   送信されません(未公開の会議の場合)。ユーザーが「自動公開しない」に設定されている場合のみ適用されます。

3. Recipient で、会議録画の参加者への電子メール通知を構成します。

- a. 各電子メール通知タイプに対応するトグルボタンをクリックして、オンとオフを切り替えます。

メール通知	説明
<b>受信者</b>	
招待されていない会議でアクションアイテムが割り当てられました	招待されていない会議でアクションアイテムがユーザーに割り当てられた後に、ユーザーに通知を送信する   送信しない場合はオン   オフを切り替えます。
会議が公開されたら会議のサマリーメールを受け取る	会議の録画が公開されたことを示す通知をユーザーに送信   送信しない場合は、オン   オフを切り替えます。
会議のサマリーが更新され、オーナーによって送信されたら、更新メールを受け取る	会議のサマリーが所有者によって更新されたことを示す通知メールをユーザーに送信   送信しない場合は、オン   オフを切り替えます。
会議があなたと共有/共有解除されたら通知メールを受け取る	オン   オフにすると、会議の録画がユーザーと共有された   共有解除されたことを示す通知メールがユーザーに送信されます   送信されません。
会議の録画準備完了(ビデオ準備完了)	会議の録画準備完了(ビデオ準備完了)を通知する通知をユーザーに送信   送信しない場合は、オン   オフを切り替えます。
サマリーがヘブライ語の場合は、ヘブライ語のサマリーメールテンプレートを使用します。	サマリーがヘブライ語の場合に使用するヘブライ語サマリー電子メールテンプレートのオン   オフを切り替えます。

## 公開時間の設定

Meeting Insights では、次の公開時間オプションがサポートされています。

- **Auto Publishing:** (デフォルト) Meeting Insights は、会議の終了後すぐに会議の録画を自動的に公開します。
- **Manual Publishing:** ユーザーは会議の録画を手動で公開する必要があります (会議の録画の **Publish** ボタンをクリックします)。
- **Delayed Publishing:** Meeting Insights は、会議の録画を終了後 3 日 (72 時間) 後に自動的に公開します。

会議の録画の公開に関して、組織のユーザー向けに次のような設定を行うことができます。

- 上記の公開オプションの 1 つをデフォルトとして選択します。
- ユーザーが上記の公開オプションのいずれかを選択できるようにします。それ以外の場合は、デフォルトの公開オプションのみが利用可能です。
- 各ユーザーの現在選択されている公開オプションをデフォルト オプションにリセットします。

#### ➤ 公開設定を構成するには:

1. 「User Settings」メニューで、**User Preferences** オプションをクリックすると、「ユーザー設定」ページが表示されます。
2. **Meeting Publishing Settings** グループまで下にスクロールします。

#### Meeting Publishing Settings

**Default Publishing Time:**

Auto Publishing

Manual Publishing

Delayed Publishing (72 hours)

---

**Allow User to Select Publishing Settings**

Reset all Users to Default Settings

**UPDATE**

3. 「Default Publishing Time」で、ユーザーのデフォルトの公開オプション (**Auto Publishing**、**Manual Publishing**、または **Delayed Publishing (72 hours)**) を選択します。各オプションの説明はこのセクションの冒頭にあります。
4. ユーザーが公開オプションを選択できるようにするには、**Allow User To Select Publishing Settings** トグル ボタンをクリックしてオンにします。公開オプションをユーザーに提供 (表示) せず、デフォルトの公開オプションのみを使用するようにしたい場合は、トグルボタンをクリックしてオフにします。
5. ユーザーが優先公開オプションを選択できるようにしている場合 (ステップ 4 のトグル ボタンをオンにするを参照)、すべてのユーザーが現在選択している公開オプションを強制的に

(上書きして) デフォルトの公開オプションに変更することができます (ステップ 3 を参照)。これを有効にするには、「Reset all Users to Default Settings」チェックボックスをオンにします。

6. 設定を適用するには、**Update** をクリックします。



- デフォルトの公開オプションを変更し、すべてのオプションがユーザーに利用可能 (つまり、**Allow User To Select Publishing Settings** トグルボタンがオン) であるが、「Reset all Users to Default Settings」チェックボックスがオフになっている場合：
  - ✓ 現在選択されているオプションが以前のデフォルト オプションではなかったユーザーの場合、選択されたオプションは保持されます (つまり、デフォルトに変更されません)。
  - ✓ 現在選択されているオプションが以前のデフォルト オプションであったユーザーの場合、そのオプションは新しいデフォルト オプションに変更されます。
- デフォルトの公開オプションを変更し、すべてのオプションがユーザーに利用可能 (つまり、**Allow User To Select Publishing Settings** トグルボタンがオン) で、「Reset all Users to Default Settings」チェックボックスをオンにした場合、**すべてのユーザーが新しいデフォルト オプションに強制的に変更されます。**
- ユーザーが公開オプションを選択できないようにした場合 (つまり、**Allow User To Select Publishing Settings** トグルボタンがオフになっている場合)、公開オプションはユーザーに表示されず、すべてのユーザーに同じ公開オプション (デフォルト) が設定されます。

## 10 AI 設定

Meeting Insights は、さまざまな人工知能 (AI) 機能をサポートしています。

- AI を活用した文字起こしの有効化と構成
- AI を活用した Insights の設定
- 声紋の表示とリセット
- AI を活用したカスタム テンプレートの表示と命名

### AI を活用した文字起こしの有効化と構成

Meeting Insights を有効にすると、AI を使用して会議の記録の文字起こしを作成できます。



AI を活用した文字起こし機能はデフォルトで有効になっています。

➤ AI を活用した文字起こしを構成するには:

1. 管理者設定メニューペインで、**AI Settings**を展開し、次に**Transcription**をクリックします。「文字起こし」ページが表示されます:

The screenshot shows the 'Transcription' settings interface. At the top, the title 'Transcription' is displayed. Below it, there is a toggle switch for 'Transcription' which is currently turned on. Underneath, the 'Languages' section contains a dropdown menu with five selected options: 'English (United States)', 'French (France)', 'English (United Kingdom)', 'French (Belgium)', and 'Japanese (Japan)'. At the bottom of the settings area, there is a 'Transcription Activation' dropdown menu set to 'Anyone'.

2. AI を活用した文字起こし機能をオンにするには、**Transcription** トグル ボタンをクリックします。
3. ユーザープロフィールを設定する際に選択できるようにする言語と方言を選択します ([AI の自動起動の有効化](#) 参照):
  - a. 「Languages」ペインで下向き矢印▼をクリックします。ドロップダウン リストが表示され、言語と方言が表示されます。

- b. 必要な言語と方言を選択すると、選択した言語と方言が「言語」ペインに追加されます。
    - c. 言語または方言を削除するには、「Languages」ペインで削除したい言語または方言の✕アイコンをクリックします。
  4. 会議録画の AI による文字起こしをトリガーできるユーザーを構成します。
    - a. 「Transcription Activation」ドロップダウンリストから、次のいずれかを選択します。
      - ◆ **Meeting Owner** - 所有者または編集権限を持つユーザーのみが AI を活用した文字起こしを起動できます。
      - ◆ **Anyone** - 会議の録画にアクセスできる誰でも AI による文字起こしを有効化できます。

## AI を活用した Insights の設定

Meeting Insights は AI を活用した Insights をサポートします。



- AI Insights 機能はデフォルトで有効になっています。
- AI Insights 機能を無効にすると、管理者は古い会議の AI を表示できますが、新しい会議をトリガーすることはできません。

### ➤ AI を活用した Insights を構成するには:

1. 「AI Settings」メニューで、AI Insights を選択します。

2. AI トグル ボタンをクリックして、AI を活用した Insights 機能をオンにします。
3. 「AI Activation」ドロップダウンから、会議録画の AI 生成分析情報をトリガーできるユーザーを選択します。
  - **Anyone** - 会議の録画にアクセスできるすべてのユーザー (デフォルト)。
  - **Meeting Owner** - 所有者または編集権限を持つユーザーのみ。
4. 免責事項をカスタマイズするには:
  - a. 免責事項の言語に対応する鉛筆アイコンをクリックします。

- b. 免責事項のテキストを入力し、チェックアイコンをクリックします。
- c. 免責事項のプレビューを表示するには、「免責事項のプレビュー」ドロップダウンリストから、免責事項を選択してください。

## 声紋の表示とリセット

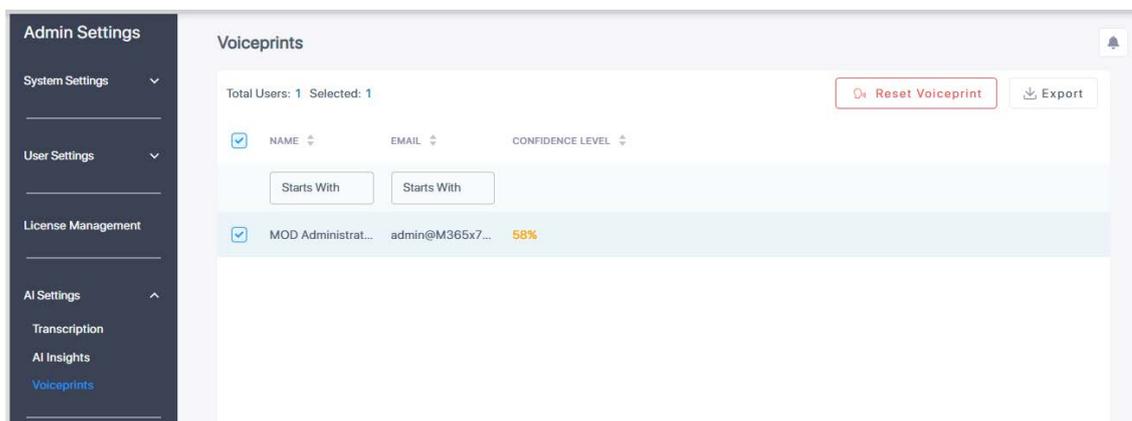
管理者はユーザーの声紋と信頼度レベルを表示できます。管理者は声紋をリセットすることもできます。



声紋鑑定は、既知の声と未知の声の聴覚およびインストルメンタルによる比較を使用してスペクトログラムを解釈します。彼らは、スペクトログラフで録画された音の時間、周波数、強度を調べます。ピッチ、方言、共鳴、呼吸パターン、その他の音声特性が登録されます。

### ➤ ユーザーの声紋と信頼度レベルを表示するには:

1. 「声紋」ページを開きます (Admin Settings > AI Settings > Voiceprints)。



2. 各声紋とその(色分けされた)信頼度レベルを表示します。

- 赤 = 声紋なし
- 黄色 = 不十分
- 緑 = 良い

### ➤ 声紋をリセットするには:

1. 「声紋」ページで、リセットする声紋を選択します。
2. **Reset Voiceprint** ボタンをクリックすると、確認メッセージが表示されます。
3. 確認するには **RESET** をクリックします。

## AI を活用したカスタム テンプレートの表示と命名

AI を活用した要約に使用できるすべてのカスタム テンプレートのリストを表示できます。テンプレートの名前を変更して、ユーザーへの表示方法を制御することもできます。

カスタム テンプレートは、組織の特定の要件を満たすように設計されています。会議の要約が標準形式に従う必要がある場合に特に役立ちます。たとえば、要約に「会議の議題」、「主な懸念事項」、「望ましい目標」などのセクションを含めることができます。

テンプレートは通常、セクター(例:「営業」および「人事」)に割り当てられます。これらは、特定のユーザー プロフィールのユーザーに適したテンプレートを見つけて選択するのに役立つ論理グループです。AI による要約を有効にし、ユーザー プロフィールのテンプレートを選択するには、[テンプレート ベースの AI を活用したサマリーの有効化](#)を参照してください。



- テンプレート「Name」は管理者専用ですが、「Custom Name」を設定しないとエンドユーザーに表示されます。
- テンプレートの「Custom Name」は一意である必要があります。

### ➤ テンプレートを表示したり、カスタム名を変更するには:

1. **Admin Settings** メニュー ペインで、**AI Settings** を展開し、次に **Custom Templates** をクリックします。リストにはすべてのカスタム テンプレートが表示されます。

NAME	DESCRIPTION	SECTOR	CUSTOM NAME
template_test1	Prompt created by automation in REST		
template_test2	Prompt created by automation in REST		

2. テンプレートの名前を構成するには:

- a. 必要なテンプレートに対応するアイコンをクリックすると、次のダイアログ ボックスが表示されます。

## Edit Template

Template Name

Deep Dive

Custom Name

Cancel

Save

- b. 「Custom Name」フィールドにテンプレートの名前を入力します。
- c. **Save** をクリックします。

## AI を活用したライブラリテンプレートの表示と命名

AI を活用した要約に使用できるすべてのテンプレートのリストをテンプレート ライブラリで表示できます。テンプレートの名前を変更して、ユーザーへの表示方法を制御することもできます。

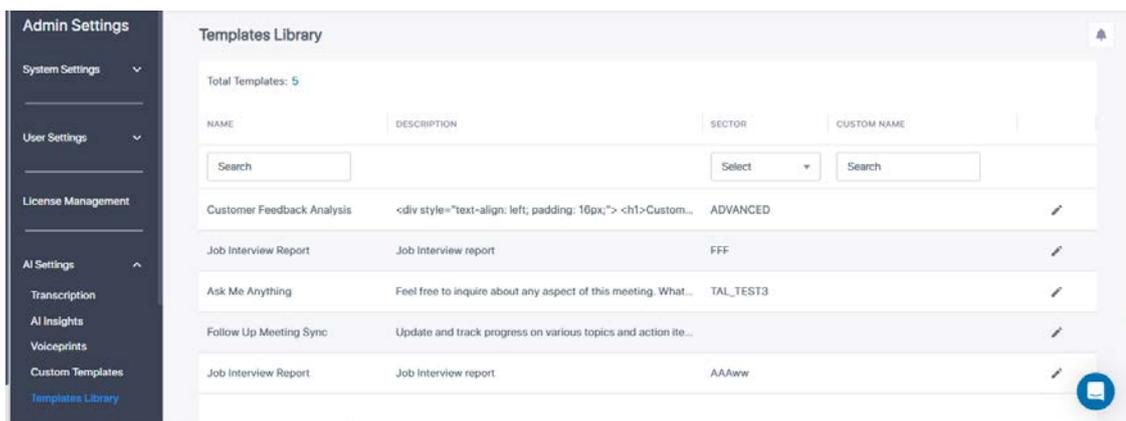
ライブラリ内のテンプレートは AudioCodes によって事前に構築されており、ほとんどの組織で使用できるように設計されています。テンプレートは通常、セクター(例:「営業」および「人事」)に割り当てられます。これらは、特定のユーザープロフィールのユーザーに適したテンプレートを見つけて選択するのに役立つ論理グループです。AI による要約を有効にし、ユーザープロフィールのテンプレートを選択するには、[テンプレート ベースの AI を活用したサマリーの有効化](#)を参照してください。



- テンプレート「Name」は管理者専用ですが、「Custom Name」を設定しないとエンドユーザーに表示されません。
- テンプレートの「Custom Name」は一意である必要があります。

### ➤ ライブラリテンプレートを表示したり、名前を変更したりするには:

1. **Admin Settings** メニュー ペインで、**AI Settings** を展開し、**Templates Library** をクリックすると、インストールされているテンプレートのリストが表示されます。



## 2. テンプレートの名前を構成するには:

- a. 必要なテンプレートに対応するアイコンをクリックすると、次のダイアログボックスが表示されます。

### Edit Template

Template Name

Deep Dive

Custom Name

Cancel Save

- b. 「Custom Name」フィールドにテンプレートの名前を入力します。
- c. **Save** をクリックします。

# 11 監視

次の2つのメニュー オプションが利用可能です。

- 監査証跡
- システム アクティビティ ログ

## 監査証跡

Meeting Insights には、Meeting Insights で実行された管理者およびユーザーのアクティビティを将来の参照用に録画する「監査証跡」機能があります。



Meeting Insights は監査ログ (監査証跡) を1年間保持します。

### ➤ 監査証跡を監視するには:

1. 「Monitoring」メニューで、**Audit Trail** オプションをクリックします。

Audit Trail						
Total: 9927						Export
DATE & TIME	NAME	ROLE	ACTIVITY	ITEM	MEETING SUBJECT	DESCRIPTION
MM/DD/YYYY - MM/DD/YYYY	Select name		Select		Contains	
Dec 25, 2023 8:51 AM	Shirel Megidish	Admin	Accessed	Meeting Page		
Dec 25, 2023 8:45 AM	Shirel Megidish	Admin	Changed	Group		Added "Test" Group
Dec 25, 2023 8:45 AM	Shirel Megidish	Admin	Downloaded	User Profile Group		Added association of user profile "Default Us...
Dec 25, 2023 8:44 AM	Shirel Megidish	Admin	Added	System Automatic AAD ...		Added automatic AAD groups synchronizatio...
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Deleted	Group		Added "team-1" Group
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Added	User Profile Group		Added association of user profile "Default Us...
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Executed	Manual AAD Synchroniz...		Executed manual AAD groups synchronization
Dec 25, 2023 8:40 AM	Shirel Megidish	Admin	Deleted	System Automatic AAD ...		Deleted automatic AAD groups synchronizati...
Dec 25, 2023 8:39 AM	Shirel Megidish	Admin	Added	System Automatic AAD ...		Added automatic AAD groups synchronizatio...
Dec 25, 2023 8:39 AM	Shirel Megidish	Admin	Deleted	System Automatic AAD ...		Deleted automatic AAD groups synchronizati...
Dec 25, 2023 8:37 AM	QA_Auto_User_1	User	Accessed	Page		

2. [オプション] ユーザーがシステム内で実行するアクション (アクセス、変更、ダウンロード、追加、削除など) によってページをフィルターするには、Activity フィルターを選択します。より効果的な管理のために、他のフィルターを選択して、ページから不要な情報を除外することもできます。たとえば、ユーザーグループのユーザープロフィールが変更された後、監査証跡ページの Activity フィルターを使用すると、変更が行われた時刻、変更を行ったユーザー、どのユーザーグループのユーザープロフィールが変更されたか、どのプロフィールからどのプロフィールに変更されたかなどの詳細を確認できます。

Audit Trail						
Total: 8 <span style="float: right;">Export</span>						
DATE & TIME	NAME	ROLE	ACTIVITY	ITEM	MEETING SUBJECT	DESCRIPTION
MM/DD/YYYY - MM/DD/YYYY	Select name		Changed		Contains	
Jan 10, 2024 10:04 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 9, 2024 11:01 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 3:35 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 1:21 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 12:25 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 10:59 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 7, 2024 3:06 PM	MOD Administrator	Admin	Changed	User Profile Group		ON
Jan 7, 2024 2:47 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON



- 全ユーザーのログイン/ログアウトがすべて録画されます。
- **Deleted** アクティビティは **Meeting deletion** アイテムにも関連付けられているため、このアクティビティを選択すると、この項目も表示されます。
- **Downloaded** アクティビティは、**Meeting Downloaded** や **Recap downloaded** などのアイテムに関連付けられています。
- アクティビティ **Accessed** に関連付けられたアイテムはありません。アクティビティはコンテンツへの一般的なアクセスを意味します。そうでない場合は、アイテムは会議と会議の件名を示します。
- アクティビティ **Added** | **Deleted** | **Changed** に関連付けられたアイテムは、たとえば Participant | ActionItem | Highlight | EditPermissions | External share などです。このアクティビティを選択すると、これらのアイテムが表示されます。

3. [オプション] Date フィルターを選択します。カレンダー アイコンをクリックし、ポップアップ カレンダーから月 | 日 | 年を選択します。この日付に行われたアクティビティのみがページに表示されます (この日付に行われなかったアクティビティは除外されます)。
4. [オプション] Meeting Subject フィルターを選択します。会議の件名を入力します。件名が入力したテキストと一致する会議に関連付けられたアクティビティのみが表示されます (件名がテキストと一致しない会議に関連付けられたアクティビティは除外されます)。
5. [オプション] Name フィルターを選択します。ドロップダウン矢印をクリックし、表示される「Search」フィールドにユーザーの名前を指定すると、そのユーザーに関連するエントリのみが表示されます。



アクティビティ、日付、会議の件名、名前など、複数のフィルターを適用できます。

6. **Export to CSV** オプションをクリックすると、監査証跡を CSV 形式でエクスポートして、他のユーザーと簡単に共有できます。

## システム アクティビティ ログ

「システム アクティビティ ログ」ページを使用すると、管理者は、管理者操作 (グループの管理者 マッピングまたはユーザーの追加により追加されたライセンス) の後に発生するシステム アクティビティを表示できます。

ログに録画されたアクティビティは日時でフィルタリングできるため、その日時外に発生したシステム アクティビティは表示から除外されます。



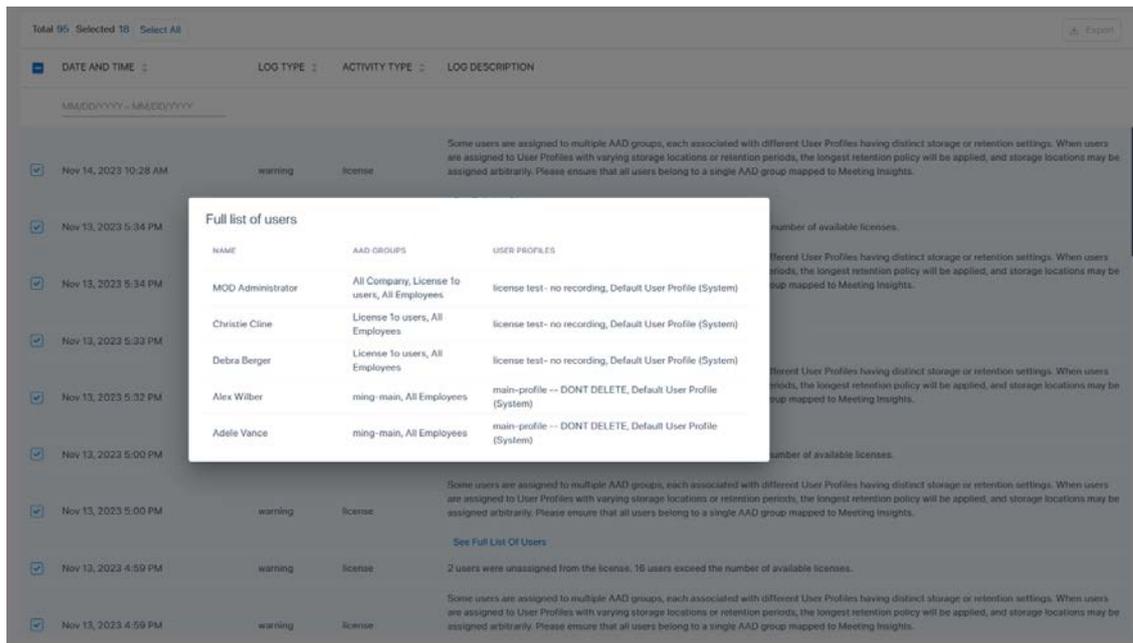
Meeting Insights はシステム アクティビティ ログを 6 か月間保持します。

### ➤ システム アクティビティ ログをフィルタリングするには:

1. 「Monitoring」メニューで、**System Activity Log** オプションをクリックします。

DATE AND TIME	LOG TYPE	ACTIVITY TYPE	LOG DESCRIPTION
<input checked="" type="checkbox"/> Nov 14, 2023 10:28 AM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights. <a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/> Nov 13, 2023 5:34 PM	warning	license	15 new users were assigned with the license. Overall 15 users exceed the number of available licenses.
<input checked="" type="checkbox"/> Nov 13, 2023 5:34 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights. <a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/> Nov 13, 2023 5:33 PM	info	license	18 users were unassigned from the licenses.
<input checked="" type="checkbox"/> Nov 13, 2023 5:32 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights. <a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/> Nov 13, 2023 5:00 PM	warning	license	2 new users were assigned with the license. Overall 18 users exceed the number of available licenses.
<input checked="" type="checkbox"/> Nov 13, 2023 5:00 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights. <a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/> Nov 13, 2023 4:59 PM	warning	license	2 users were unassigned from the license. 16 users exceed the number of available licenses.
<input checked="" type="checkbox"/> Nov 13, 2023 4:59 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.

2. (オプション)「Date and Time」の横にあるボックスをオンにしてすべてのログを選択します。すべて選択解除するには、同じボックスをもう一度クリックします。
3. 1つのログを選択するか、各ログ エントリの横にあるボックスをオンにして複数のログを選択します。使用可能なログの合計数のうち、選択したログの数が表示されます。
4. (オプション) ページを「Date and Time」、「Log Type」または「Activity Type」の列でフィルターするには、列 ヘッダーをクリックします。
5. (オプション) 期間別にページをフィルタリングします。MM /DD/YY - MM/DD/YY をクリックし、ポップアップ表示されるカレンダーで開始日と終了日を選択します。
6. 「Log Description」列の下にあるログの行の「See Full List Of Users」リンクをクリックします。



7. ログでは、たとえば、ライセンスにユーザーが追加された回数やライセンスから削除された回数 (カウント) などを表示します。
8. (オプション) ページの右上隅にある **Export** ボタンをクリックし、形式プロンプトで **Export to Excel** ボタンをクリックします。

## 12 統合

Meeting Insights は、次のサードパーティアプリケーションと統合できます。

- Microsoft Planner - [Meeting Insights と Microsoft Planner の統合 参照](#)
- Zoho - [Meeting Insights と Zoho の統合 参照](#)
- monday.com - [Meeting Insights と monday.com の統合 参照](#)
- Salesforce 顧客関係管理 (CRM) プラットフォーム - [Meeting Insights と Salesforce の統合 参照](#)

### Meeting Insights と Microsoft Planner の統合

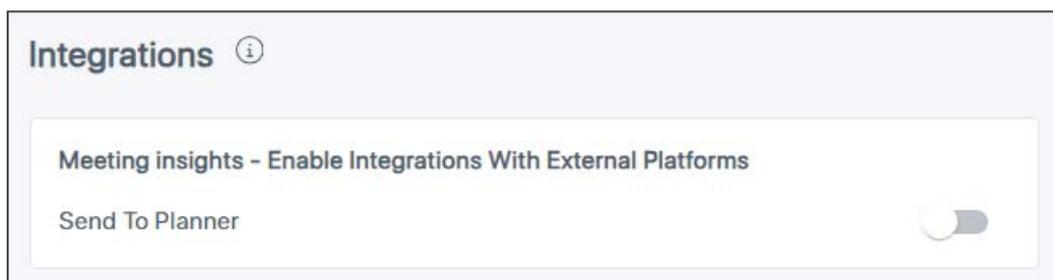
ここでの手順では、Microsoft Planner と Meeting Insights を統合する方法を示します。



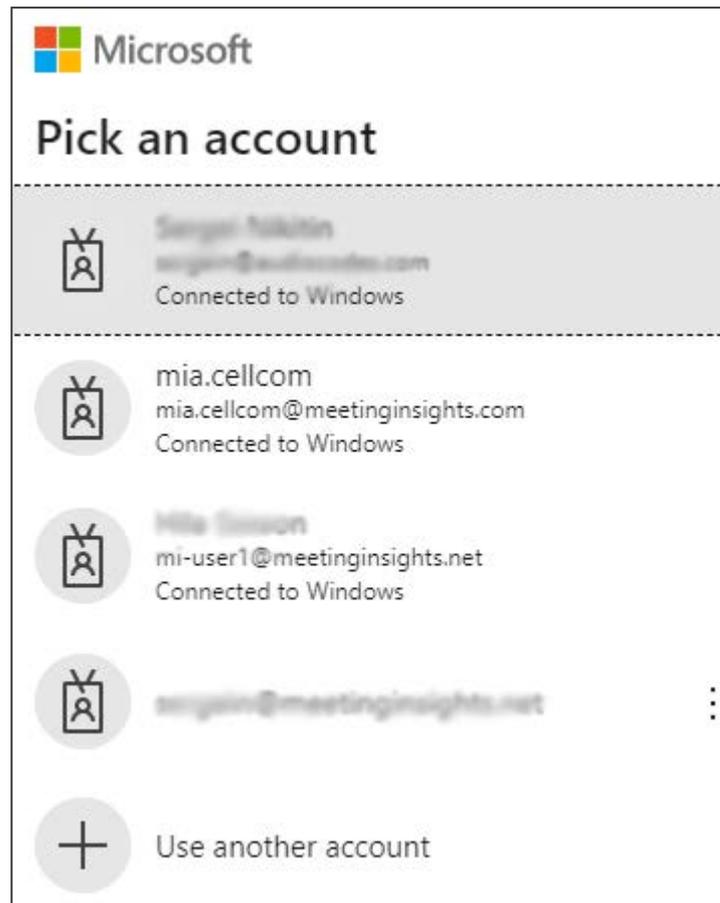
Microsoft Planner を統合する前に、ログインしているユーザーには、Meeting Insights の「管理者」権限と Azure の「テナント管理者」権限が必要です。

#### ➤ Microsoft Planner を統合するには:

1. 「Settings」メニューの下にある **Integrations** オプションをクリックします。



2. **Send to Planner** 設定を有効にすると、次の Microsoft 管理者ログインプロンプトにリダイレクトされます。



3. アカウントを選択してください。



sergein@meetinginsights.net

## Permissions requested

### Review for your organization

ronlab-auth-app  
**unverified**

**This app may be risky. Only continue if you trust this app.** [Learn more](#)

This app would like to:

- ^ Create, read, update, and delete user's tasks and task lists  
Allows the app to create, read, update, and delete the signed-in user's tasks and task lists, including any shared with the user.  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ^ View users' basic profile  
Allows the app to see your users' basic profile (name, picture, user name)  
This is a permission requested to access your data in Audiocodes ltd - MI.
- ^ Maintain access to data you have given it access to  
Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.  
This is a permission requested to access your data in Audiocodes ltd - MI.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

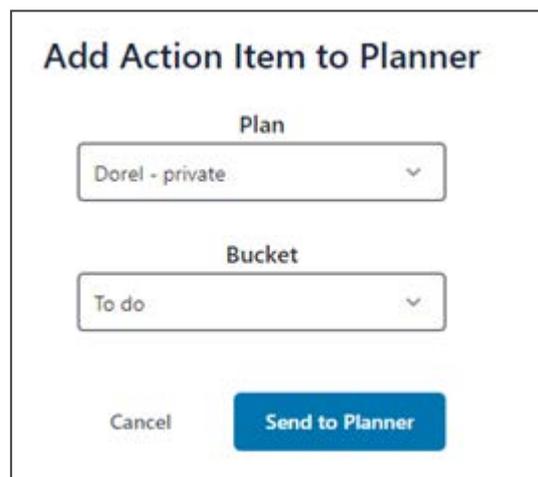
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

4. **Accept** をクリックすると、プロンプトに示されているように、サインインしたユーザーのタスクとタスクリストを作成、読み取り、更新、削除する権限をアプリに付与することになります。「設定」ページにリダイレクトされます。**Integrations** タブをクリックして、有効になっていることを確認します。
5. ライブ会議中にユーザーが Microsoft Planner にアクションアイテムを送信する次の例を参考にしてください。



6. **Action Items** メニューをクリックします。
7. プランとバケットを選択し、**Send to Planner** をクリックします。

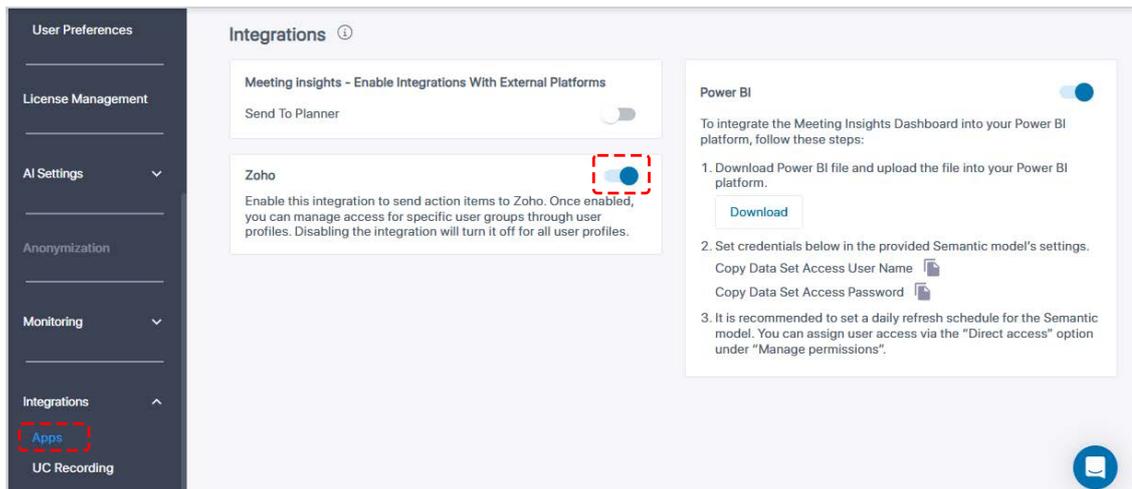


## Meeting Insights と Zoho の統合

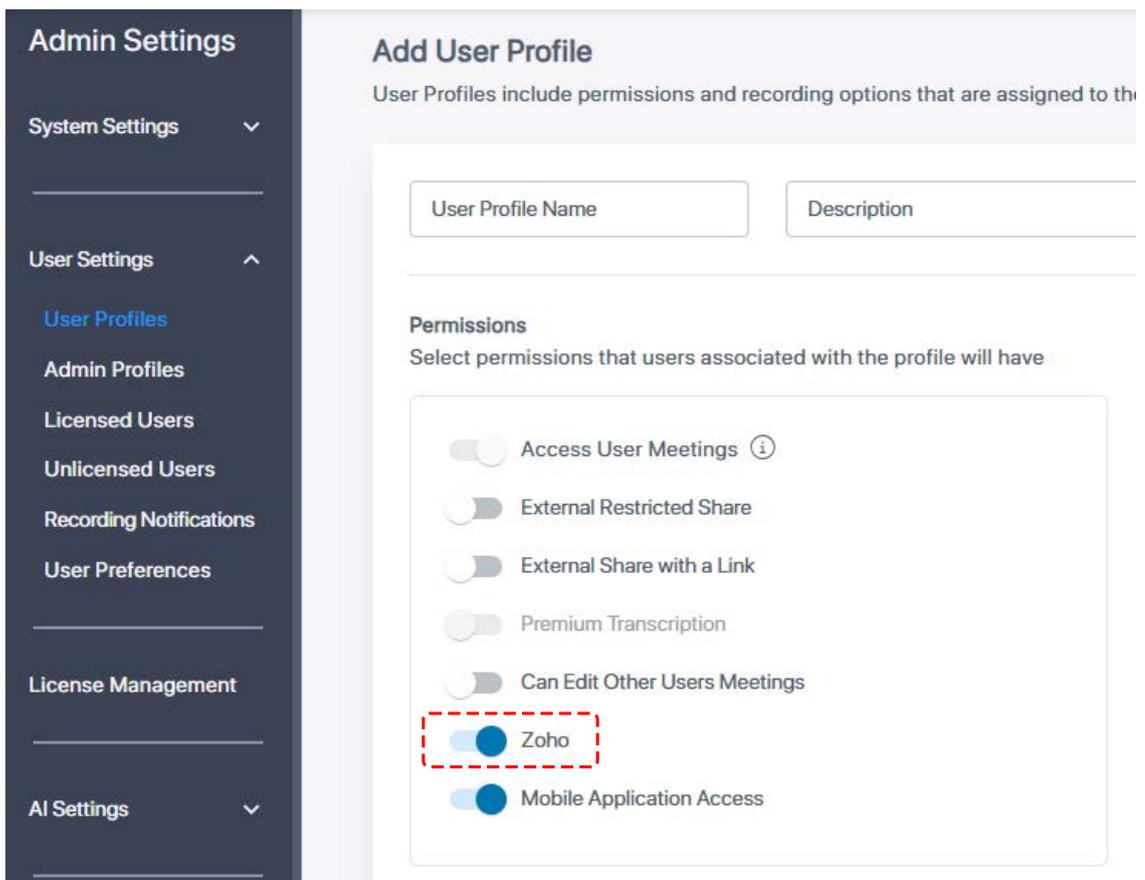
ユーザー (ユーザー プロフィールごと) がプロジェクト内の Zoho アカウントのタスクリストにアクションアイテムを送信できるように Meeting Insights を Zoho と統合するには、まず統合を有効にする必要があります。

### ➤ Zoho 統合を有効にするには:

1. 管理者設定メニューペインで、**Integrations** を展開し、**Apps** をクリックします。
2. **Zoho** トグルスイッチをクリックして統合をオンにします。



3. 特定のユーザープロフィールに対して Zoho を有効にする( [ユーザープロフィール](#)参照):
  - a. Admin Settings メニュー ペインで、**User Settings** を展開し、**User Profiles** をクリックします。
  - b. 新しいユーザープロフィールを追加するか、既存のユーザープロフィールを編集します。
  - c. 「権限」グループの下にある **Zoho** トグルボタンをクリックしてオンにします。



4. **Apply** をクリックします。

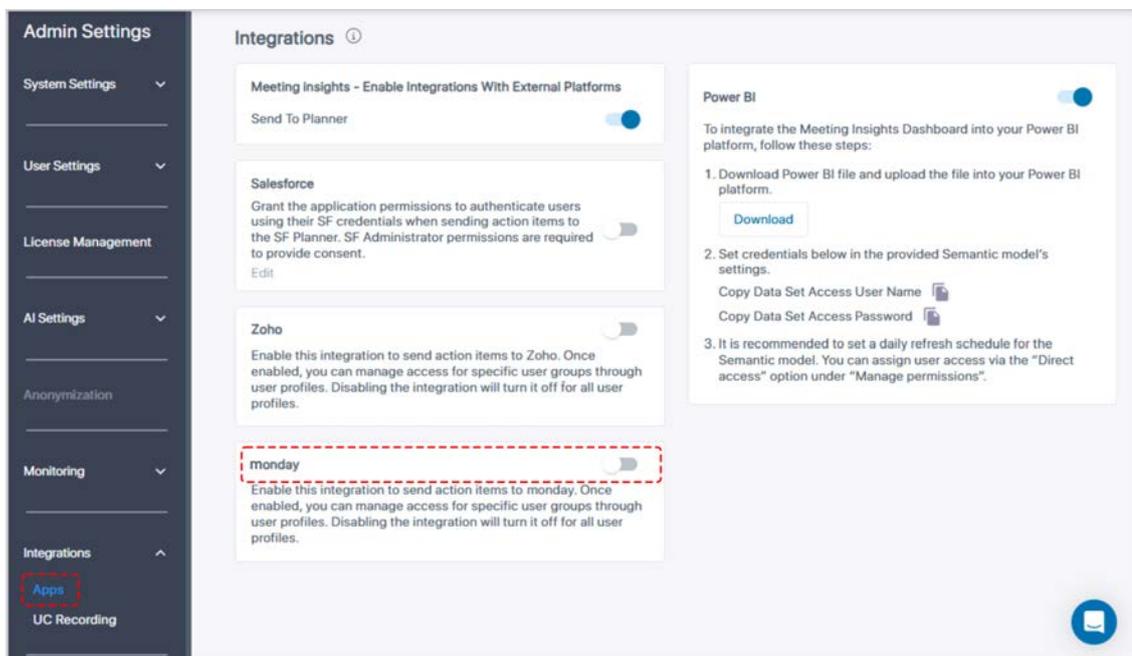
## Meeting Insights と monday.com の統合

Meeting Insights を組織の monday.com アカウントと統合して、ユーザーがアクション アイテムを monday.com (ワークスペース、ボード、グループ) に送信できるようにすることができます。

特定のユーザー(ユーザー プロフィールごと) が monday.com アカウントにアクションアイテムを送信できるようにするには、Meeting Insights を [monday.com](#) と統合する必要があります。これは、monday.com プラットフォームに monday.com 用の Meeting Insights アプリをインストールし、ワークスペースを選択して、アプリに付与された権限を承認することによって行われます。

### ➤ Meeting Insights を monday.com と統合するには:

1. 管理者設定メニュー ペインで、Integrations を展開し、Apps をクリックします。
2. Monday のトグルボタンをクリックします。



次のダイアログ ボックスが表示されます。

### monday.com Integration

Visit [this URL](#) and enable the Meeting Insights app (monday Administrator permissions are required).

Click Validate to confirm your monday.com integration setup by logging in to your monday account.

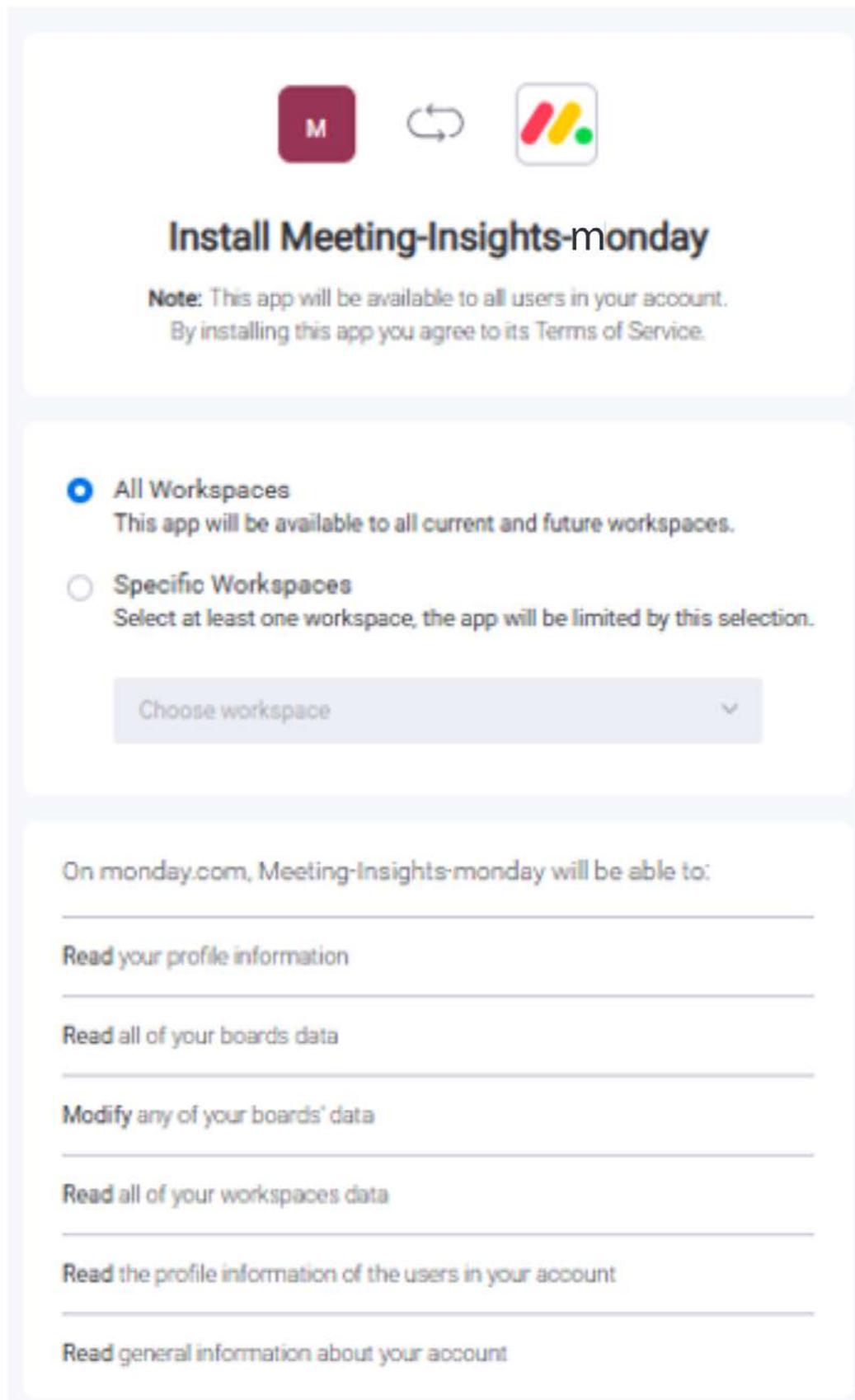
Cancel

Validate

3. This URL リンクをクリックして、monday.com に Meeting Insights アプリをインストールします。monday.com にリダイレクトされます (monday.com のアカウントにまだログインしていない場合は、ログインするように求められます)。



Meeting Insights アプリをインストールするには、**管理者権限**で monday.com にログインする必要があります。



## Install Meeting-Insights-monday

**Note:** This app will be available to all users in your account.  
By installing this app you agree to its Terms of Service.

**All Workspaces**  
This app will be available to all current and future workspaces.

**Specific Workspaces**  
Select at least one workspace, the app will be limited by this selection.

Choose workspace 

On monday.com, Meeting-Insights-monday will be able to:

---

Read your profile information

---

Read all of your boards data

---

Modify any of your boards' data

---

Read all of your workspaces data

---

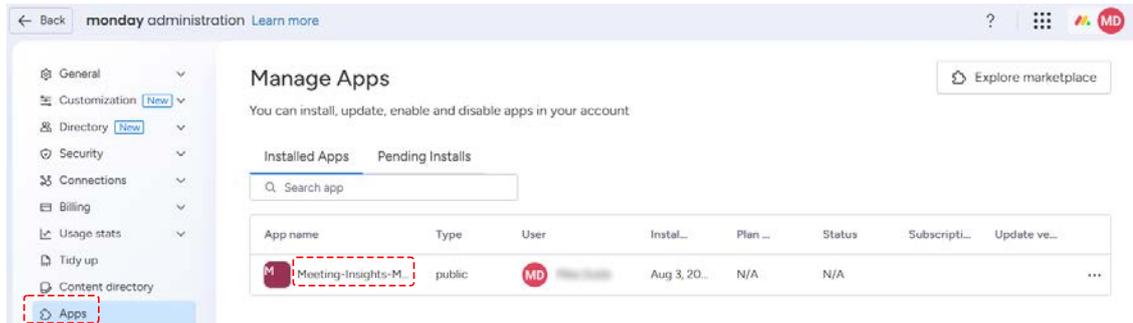
Read the profile information of the users in your account

---

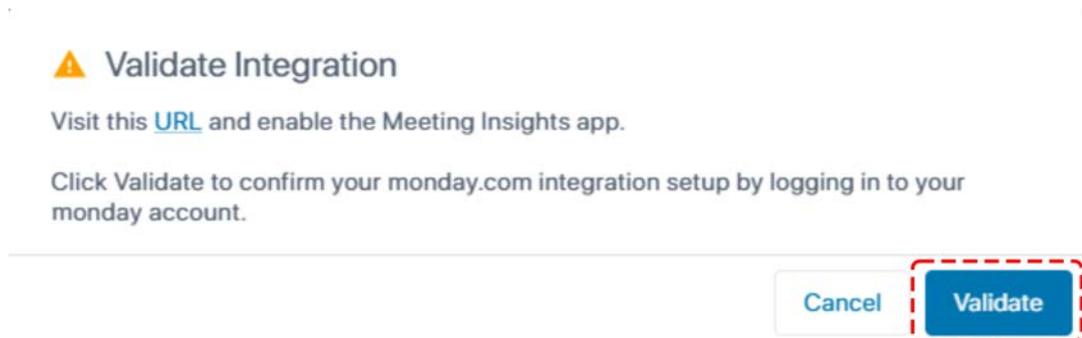
Read general information about your account

4. 次のいずれかのオプションを選択して、許可されたワークスペースを選択します。

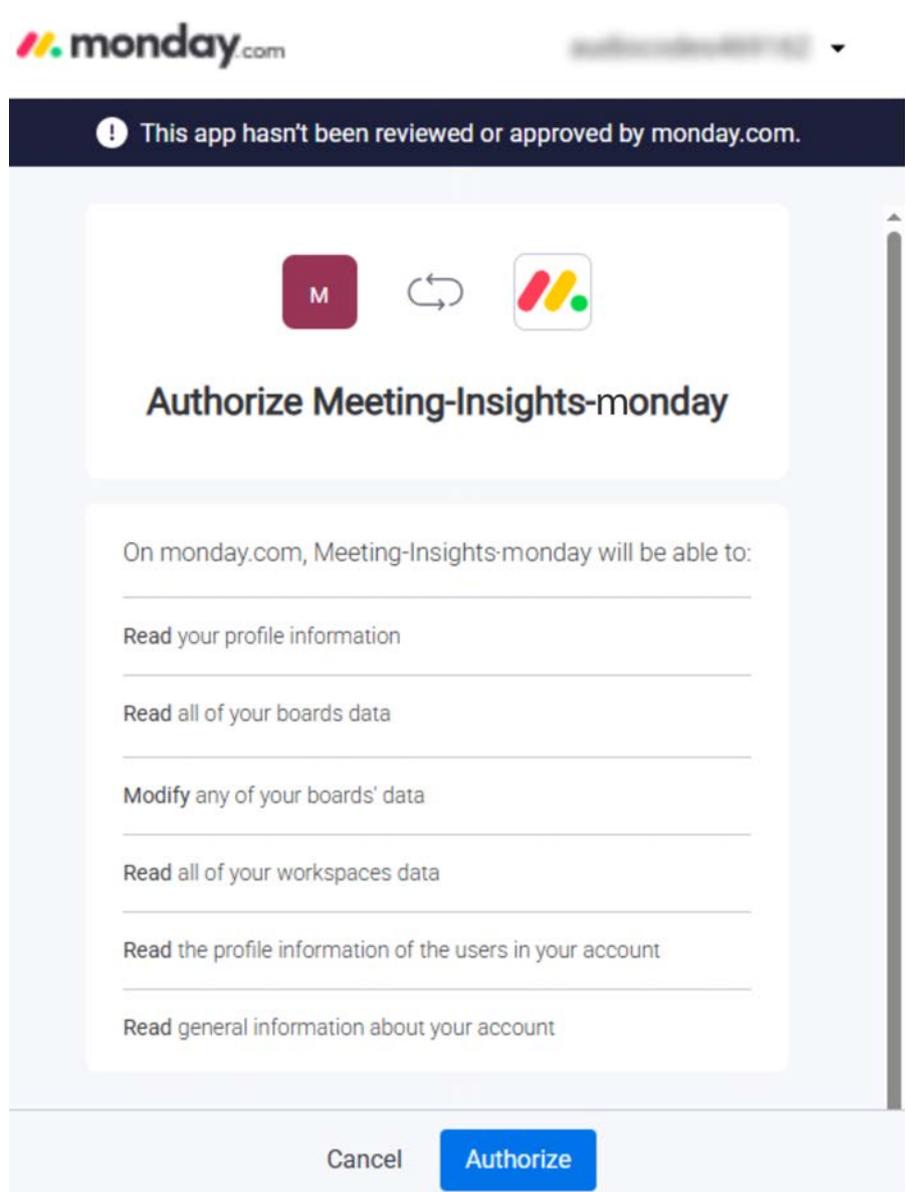
- **All Workspaces:** ユーザーが組織の monday.com アカウント内の任意のワークスペースにアクションアイテムを送信できるようになります。
  - **Specific Workspaces:** ユーザーがアクションアイテムを特定のワークスペースにのみ送信できるようになります。ドロップダウンリストから必要なワークスペースを選択します。
5. **Install** をクリックすると、monday.com の Meeting Insights アプリのインストールが開始されます。インストールが完了すると、monday.com アカウントの「アプリの管理」ページでインストールされたアプリを確認できます。



6. アプリが monday.com にインストールされたら、以下に示すように **Validate** をクリックします。



Monday.com に再度リダイレクトされ、monday.com の Meeting Insights アプリに付与された権限を承認します。

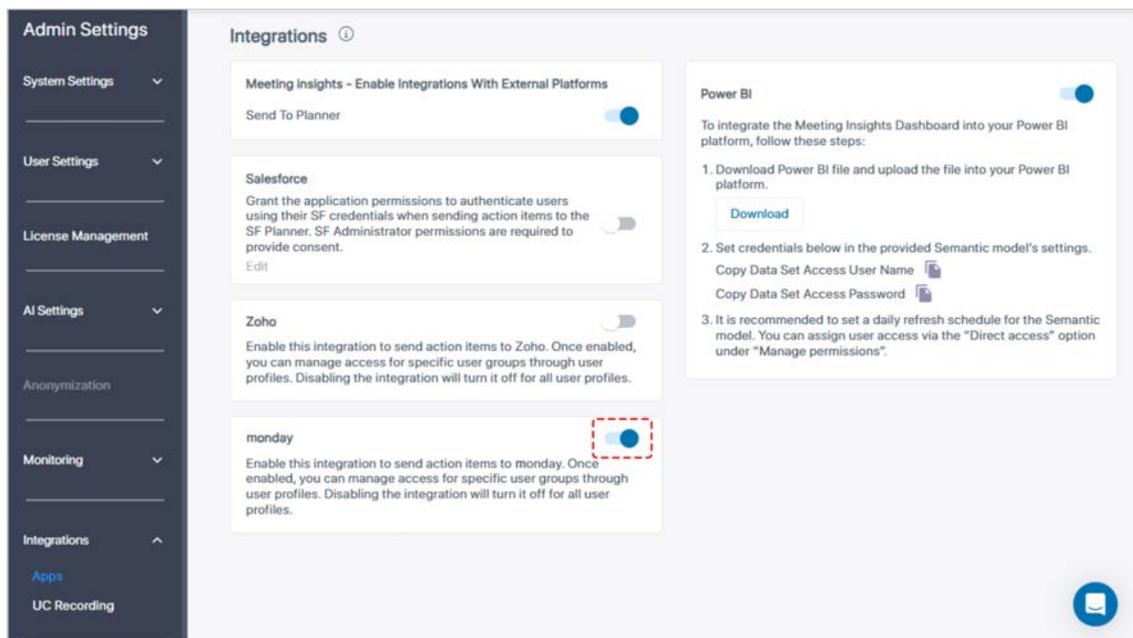


さまざまな権限の説明を次の表に示します。

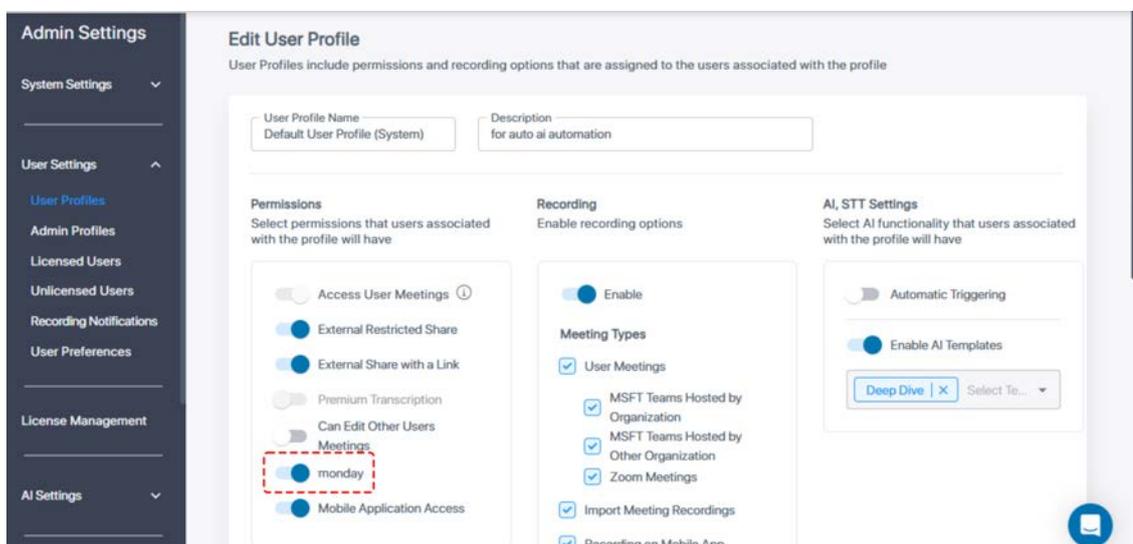
権限	タイプ	対象範囲	説明	目的
プロフィール情報を読み取る	読み取り	プロフィール	認証されたユーザーのID、名前、メールを取得します。ユーザー固有のアクションを識別またはパーソナライズするためによく使用されます。	OAuth 2.0 認証のユーザーデータを取得します。
すべてのボードデータを読み	読み取り	ボード	アイテム、グループ、列、更新、構造などのデータをボードから取得します。ボードのコンテンツを分析または表示するために必	Meeting Insights がユーザーのUIに表示できるようにします。

権限	タイプ	対象範囲	説明	目的
取る			要です。	
ボードのデータを変更する	書き込み	ボード	アプリがアイテムを作成/更新したり、アイテムを移動したり、列の値を変更したり、グループを作成/削除したり、ボード構造を変更したりできるようにします。	Meeting Insights がボード上のアクション項目を更新できるようにします。
すべてのワークスペースデータを読み取る	読み取り	ワークスペース	アプリがワークスペース構造を一覧表示してアクセスし、どのボードがどこに属しているかを確認できるようにします。データアクセスを整理またはスコープ設定するために重要です。	ワークスペースと、ワークスペースとボードの関係を取得し、UIに表示します。
アカウント内のユーザーのプロフィール情報を読み取る	読み取り	ユーザー	アカウント全体のユーザーデータ (ID、メール、名前) へのアクセスを許可します。ユーザーをアイテムに割り当てたり、ユーザーベースのレポートを生成したり、通知を送信したりするために必要です。	アクションアイテム所有者の電子メールと monday.com ユーザー間の相関関係を許可し、アクションアイテムをボードに割り当てることができます。
アカウントに関する一般情報を読む	読み取り	アカウント	プランの種類、階層、アカウント ID などの高レベルのアカウントデータへのアクセスを提供します。機能の適格性チェックやレポートに役立ちます。	OAuth 2.0 認証プロセスに必要な権限。

7. **Authorize** をクリックして権限を確認します。 **monday** のトグルボタンが自動的にオンになり、Meeting Insights が monday.com アカウントに統合されたことが示されます。



8. 特定のユーザープロフィールに対して monday.com を有効にする( [ユーザープロフィール参照](#)):
  - a. Admin Settings メニュー ペインで、**User Settings** を展開し、**User Profiles** をクリックします。
  - b. 新しいユーザープロフィールを追加するか、既存のユーザープロフィールを編集します。
  - c. Permissions グループの下にある **monday** トグル ボタンをクリックしてオンにします。



9. **Apply** をクリックします。

## Meeting Insights と Salesforce の統合

Meeting Insights を組織の Salesforce プラットフォームに統合することで、AI によって生成された会議概要の力を活用できます。この統合により、ユーザーはアカウント オブジェクトなどの特

定の Salesforce オブジェクトにサマリーを送信し、「ACompany」などの指定されたフィールドにデータを入力できます。これにより、営業会議の主要な議論ポイントに Salesforce 内で簡単にアクセスできるようになり、機会が最新の状態に保たれ、営業効率が向上します。



- AI を活用した箇条書きのサマリーのみが Salesforce に送信されます。
- 次の Salesforce オブジェクトのみがサポートされます。
  - ✓ アカウント
  - ✓ Opportunity
- Meeting Insights が AI を活用したサマリーを使用して Salesforce オブジェクト フィールドを更新すると、新しいコンテンツが既存のコンテンツに追加されます。
- Salesforce 統合を無効にすると、テナントの関連データと設定がすべて削除されます。

統合には次の主な手順が含まれます。

- Salesforce の設定と Meeting Insights に必要な情報の取得 ([Salesforce の設定と必要な情報の取得](#) 参照)。
- Salesforce プラットフォームと統合するための Meeting Insights の構成 ([Salesforce 統合のための Meeting Insights の設定](#) を参照してください)。

## Salesforce の設定と必要な情報の取得

組織の Salesforce プラットフォームと統合するように Meeting Insights を構成する前に、Salesforce で次の操作を行う必要があります。

1. Meeting Insights との統合のための接続アプリを作成する - [Salesforce で接続アプリを作成する](#) を参照してください。
2. Meeting Insights に関する次の情報を取得します。
  - Salesforce ドメイン URL - [Salesforce ドメイン URL の取得](#)。
  - 接続されたアプリケーションのクライアント ID とクライアントの秘密鍵 - [Salesforce 接続アプリのクライアント ID とシークレットの取得](#)。
  - Meeting Insights が AI を活用した会議サマリーを送信できるアカウントおよび機会の Salesforce オブジェクトのフィールド (API) 名 - [Salesforce オブジェクトフィールド \(API\) 名の取得](#)。

### Salesforce で接続アプリを作成する

接続アプリは、API と標準プロトコルを使用して外部アプリケーション (Meeting Insights など) を Salesforce と統合できるようにするフレームワークです。

#### ➤ 接続アプリを作成するには:

1. Salesforce アカウントにサインインします。
2. 右上隅にある歯車 ⚙️ アイコンをクリックし、**Setup** を選択します。
3. 左側のナビゲーションメニューで **Apps** を展開し、**App Manager** を選択します。

4. **New External Client App** ボタンをクリックすると、「新しい接続アプリ」ページが表示されます。
5. **Basic Information** を展開し、次の操作を行います。
  - 「External Client App Name」フィールドに、接続されたアプリの名前を入力します。
  - 「Contact Email」フィールドに、この統合の連絡先のメールアドレスを入力します。

▼ Basic Information

\* External Client App Name

\* Contact Email

Contact Phone

Logo Image URL

[Choose one of our sample logos.](#)

Description

6. **API (Enable OAuth Settings)**を展開し、次の操作を行います。
  - a. 「Enable OAuth」チェックボックスを選択します。

▼ API (Enable OAuth Settings)

Enable OAuth

- b. **App Settings** の「Callback URL」フィールドに、以下の URL すべて、または地域に応じた URL を入力します。
  - ◆ **EMEA:** <https://emea.meetinginsights.com/mi/redirect/salesforce>
  - ◆ **オーストラリア:** <https://au.meetinginsights.com/mi/redirect/salesforce>
  - ◆ **アメリカ大陸:** <https://americas.meetinginsights.com/mi/redirect/salesforce>

**App Settings**

\* Callback URL

- c. **OAuth Scopes** で、右側の **Selected OAuth Scopes** ペインのリストから次のスコープを選択します。
- ◆ **Full access (full)**
  - ◆ **Manage user data via APIs (api)**
  - ◆ **Perform requests at any time (refresh\_token, offline\_access)**



- d. **Flow Enablement** の下で、「Enable Client Credentials Flow」チェックボックスをオンにします。

#### Flow Enablement

- Enable Client Credentials Flow
- Enable Authorization Code and Credentials Flow
- Enable Device Flow
- Enable JWT Bearer Flow
- Enable Token Exchange Flow

- e. **Security** の下で、次のチェックボックスをオフにします。
- ◆ 「Require secret for Web Server Flow」
  - ◆ 「Require secret for Refresh Token Flow」
  - ◆ 「Require Proof Key for Code Exchange (PKCE) extension for Supported Authorization Flows」

#### Security

- Require secret for Web Server Flow
- Require secret for Refresh Token Flow
- Require Proof Key for Code Exchange (PKCE) extension for Supported Authorization Flows
- Enable Refresh Token Rotation
- Issue JSON Web Token (JWT)-based access tokens for named users

7. **Save** をクリックすると、接続されたアプリが作成され、External Client App Manager リストに表示されます。
8. 外部クライアント アプリマネージャーリストで、新しく接続されたアプリに対応する下向き矢印をクリックし、ドロップダウンメニューから **Edit Policies** を選択して、次の操作を行います。
  - a. **OAuth Policies** を展開します。
  - b. **Plugin Policies** の「Permitted Users」ドロップダウンリストから、「All users can self-authorize」を選択します。

### Plugin Policies

\* Permitted Users

All users can self-authorize ▼

- c. **OAuth Flows and External Client App Enhancements** で、「Enable Client Credentials Flow」チェックボックスをオンにし、Salesforce 管理者のメールアドレスを入力します。

### OAuth Flows and External Client App Enhancements

- Enable Client Credentials Flow

\* Run As (Username)

Enter an email address...

- d. **App Authorization** の「Refresh Token Policy」では、**Expire refresh token after specific time** オプションを選択し、「Refresh Token Validity Period」フィールドに 24 と入力し、「Refresh Token Validity Unit」を時間に設定することをお勧めします。つまり、ユーザーが Meeting Insights から Salesforce にログインすると、24 時間後に再度ログインするだけで済みます。

### App Authorization

#### Refresh Token Policy

- Refresh token is valid until revoked  
 Immediately expire refresh token  
 Expire refresh token after specific time  
 Expire refresh token if not used for specific time

\* Refresh Token Validity Period

24

9. **Save** をクリックします。

## Salesforce ドメイン URL の取得

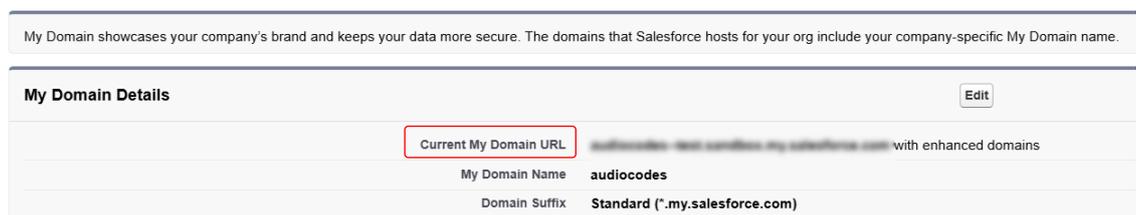
次の手順では、Meeting Insights を構成するために必要な組織の Salesforce ドメイン URL を取得する方法について説明します。

### ➤ クライアント ID とシークレットを取得するには:

1. Salesforce アカウントにサインインします。
2. 右上隅にある歯車アイコンをクリックし、**Setup** を選択します。
3. 左側のナビゲーションメニューで **Company Settings** を展開します。次に **My Domain** を選択します。

ドメイン URL は「Current My Domain URL」フィールドに表示されます。

#### My Domain Settings

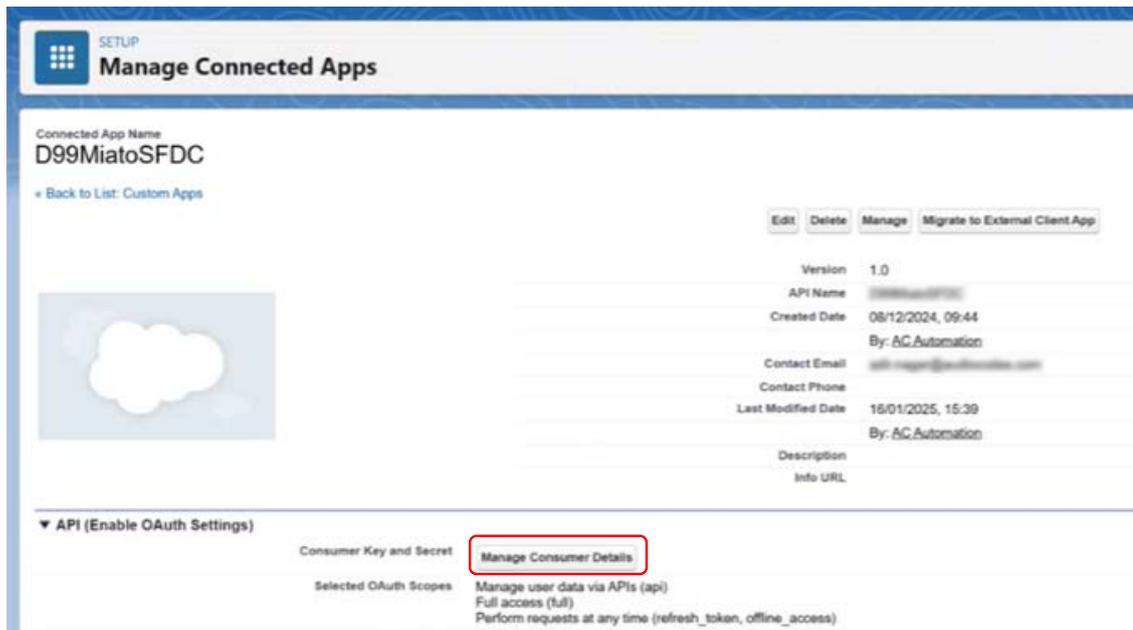


## Salesforce 接続アプリのクライアント ID とシークレットの取得

Meeting Insights 統合用の接続アプリケーションを作成したら、Meeting Insights の構成に必要なクライアント ID とクライアント シークレットを取得できます。

### ➤ クライアント ID とシークレットを取得するには:

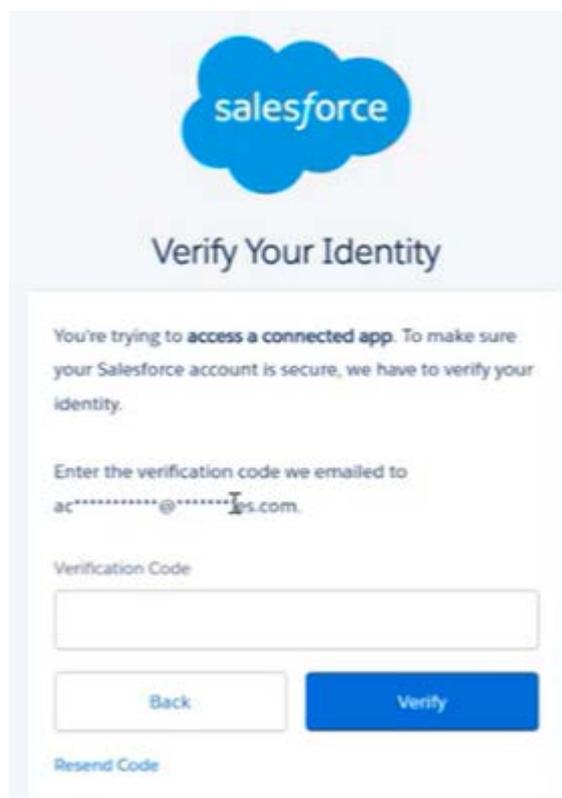
1. Salesforce アカウントにサインインします。
2. 右上隅にある歯車アイコンをクリックし、**Setup** を選択します。
3. 左側のナビゲーションメニューで **Apps** を展開し、**App Manager** を選択します。
4. App Manager リストで、新しく接続されたアプリに対応する下向き矢印をクリックし、ドロップダウンメニューから **View** を選択します。
5. **Manage Consumer Details** ボタンをクリックします。



The screenshot shows the 'Manage Connected Apps' interface in Salesforce. The app name is 'D99MiatoSFDC'. There are buttons for 'Edit', 'Delete', 'Manage', and 'Migrate to External Client App'. The app details include: Version 1.0, API Name, Created Date 08/12/2024, 09:44, Contact Email, Contact Phone, Last Modified Date 16/01/2025, 15:39, and Description. Under the 'API (Enable OAuth Settings)' section, the 'Consumer Key and Secret' field has a 'Manage Consumer Details' button highlighted with a red box. The 'Selected OAuth Scopes' are 'Full access (full)' and 'Perform requests at any time (refresh\_token, offline\_access)'.

確認コードがあなたのメールアドレスに送信されます。

- 表示されたダイアログボックスの「Verification Code」フィールドにコードを入力します。



The screenshot shows the 'Verify Your Identity' dialog box. It features the Salesforce logo at the top. The text reads: 'You're trying to access a connected app. To make sure your Salesforce account is secure, we have to verify your identity. Enter the verification code we emailed to ac\*\*\*\*\*@\*\*\*\*\*.com.' Below this is a 'Verification Code' input field. At the bottom, there are 'Back' and 'Verify' buttons, and a 'Resend Code' link.

- Verifyをクリックすると、クライアント ID が「Consumer Key」フィールドに表示され、クライアントシークレットが「Consumer Secret」フィールドに表示されます。



## Salesforce オブジェクトフィールド (API) 名の取得

次の手順では、アカウントのオブジェクトと機会のオブジェクトのフィールド名を取得する方法について説明します。これらは、Meeting Insights を構成するために必要な API フィールド名である必要があります。

### ➤ オブジェクト フィールド名を取得するには:

1. Salesforce アカウントにサインインします。
2. 右上隅にある歯車アイコンをクリックし、**Setup** を選択します。
3. 左側のナビゲーションメニューで **Object Manager** を選択し、オブジェクト (例: アカウント) を選択します。
4. **Fields & Relationships** をクリックし、必要なフィールドを検索します。次の例に示すように、API フィールド名は「Field Name」列に表示されます。



## Salesforce 統合のための Meeting Insights の設定

Salesforce アカウントから必要な情報を取得したら( [Salesforce の設定と必要な情報の取得参照](#) )、Meeting Insights を Salesforce と統合するように構成できます。

### ➤ Salesforce 統合用に Meeting Insights を構成するには:

1. 「Admin Settings」メニューで **Integrations** を展開し、**Apps** をクリックすると、「統合」ページが表示されます。
2. Salesforce グループの下にあるトグルボタンをクリックして、Salesforce 統合を有効にします。

### Integrations ⓘ

**Meeting insights - Enable Integrations With External Platforms**

Send To Planner

**Salesforce**

Grant the application permissions to authenticate users using their SF credentials when sending action items to the SF Administrator permissions are required to provide consent.

[Edit](#)

次のダイアログ ボックスが表示されます。

#### Salesforce Connection

Domain

Client ID

Client Secret

Environment Type

Sandbox
▼

Salesforce Object to Update	Salesforce Field to Update
Account Summary	
Opportunity Summary	

### 3. Salesforce 接続を構成します。

- a. 「Domain」フィールドに、組織の Salesforce プラットフォームのドメイン URL を入力します。ドメイン URL の取得については、[Salesforce ドメイン URL の取得](#)を参照してください。
- b. 「Client ID」フィールドに、Salesforce 接続アプリのクライアント ID を入力します。クライアント ID の取得については、[Salesforce 接続アプリのクライアント ID とシークレットの取得](#)を参照してください。
- c. 「Client Secret」フィールドに、Salesforce 接続アプリのクライアント シークレット キーを入力します。クライアントシークレットを取得するには、[Salesforce 接続アプリのクライアント ID とシークレットの取得](#)を参照してください。

- d. 「Environment Type」ドロップダウンリストから、展開のニーズに合った Salesforce 環境を選択します。
  - ◆ **Sandbox:**このオプションを使用すると、ライブ Salesforce インスタンス (本番環境) に展開する前に、安全な環境で Meeting Insights の統合をテストおよび検証できます。これにより、実稼働データに影響を与えることなく、構成と機能を検証できます。
  - ◆ **Production:**このオプションを使用して、Meeting Insights をライブ Salesforce 環境に直接展開します。
4. 「Salesforce object to update」の下にリストされている各 Salesforce オブジェクト (アカウントまたは機会) について、対応する「Salesforce Field to Update」列に Salesforce フィールド名を入力します。これらは、Meeting Insights が会議のサマリーを送信するフィールドです (ユーザーが選択した場合)。



- フィールド名は **API** フィールド名 でなければなりません。API フィールド名を取得するには、[Salesforce オブジェクトフィールド \(API\) 名の取得](#)を参照してください。
- フィールド名が Salesforce に表示されるものとまったく同じであることを確認します。
- 現在 Meeting Insights では、アカウントおよび機会の Salesforce オブジェクトのみがサポートされます。
- Meeting Insights が AI を活用したサマリーを使用して Salesforce オブジェクト フィールドを更新すると、新しいコンテンツが既存のコンテンツに追加されます。

5. **Submit** をクリックします。
6. ユーザー プロフィールに Salesforce を有効にする:
  - a. **User Settings** メニューを展開し、**User Profiles** をクリックします。
  - b. 新しいユーザー プロフィールを追加するか、既存のユーザー プロフィールを編集します。
  - c. **Permissions** グループの下にある **Salesforce** トグル ボタンをクリックしてオンにします。

## Edit User Profile

User Profiles include permissions and recording options that are assigned to th

User Profile Name Default User Profile (System)	Description This profile is a default profile that ir
--	--

### Permissions

Select permissions that users associated with the profile will have

- Access User Meetings ⓘ
- External Restricted Share
- External Share with a Link
- Premium Transcription
- Can Edit Other Users Meetings
- Organization Glossary Management
- Add to Glossary
- Salesforce

7. **Apply** をクリックします。

## サードパーティの会議アプリ向けの Meeting Insights ボット名と通知のカスタマイズ

サードパーティアプリ (Zoom、外部組織が主催する Microsoft Teams 会議、Google Meet など) が主催する会議の記録を有効にしている場合は、これらの会議に参加して記録する Meeting Insights ボットの名前をカスタマイズできます。Google Meet では、ボットが参加して録画を開始したときに表示される通知メッセージをカスタマイズすることもできます。

ボット名を定義するときにプレースホルダー (変数またはテンプレート) を使用できます。これは、Meeting Insights によって実際の値に置き換えられます。たとえば、ユーザーの名前が Bob の場合、「<UserFirstName>'s Meeting Assistant」として定義されたボット名は「Bob's Meeting Assistant」と表示されます。デフォルトのボット名は、「<UserFirstName>'s Meeting Assistant and Recorder」です。

Meeting Insights を有効にしてサードパーティアプリで主催される会議を記録する方法の詳細については、次のセクションを参照してください。

- ユーザーが Zoom 会議を録画できるようにする
- ユーザーが Google Meet 会議を録画できるようにする
- ユーザーが外部の Teams 会議を録画できるようにする

➤ Meeting Insights のボット名と録画通知をカスタマイズするには:

1. Admin Settings メニュー ペインで、Integrations を展開し、UC Recording をクリックします。

**UC Recording Integration** ⓘ

**Bot Settings**

Zoom ⓘ

Bot Name \*  
<UserFirstName>'s Meeting Assistant and Recorder

**MSFT Teams Hosted by Other Organizations** ⓘ

Bot Name \*  
forward\_test\_bot

**Google Meet** ⓘ

Bot Name \*  
google\_meet\_bot

Bot Chat Notifications Message  
<CompanyName>'s Meeting Insights (Mia) has joined. This meeting is recorded and analyzed to generate advanced insights and summaries. Learn more: <MeetingInsightsURL>

## 2. Zoom 会議

Zoomの「Bot Name」フィールドで、ボット名を設定します。サポートされているプレースホルダーを表示するには、i アイコンをクリックします。

### 3. Microsoft Teams 会議:

MSFT Teams Hosted by Other Organizations の「Bot Name」フィールドで、ボット名を構成します。サポートされているプレースホルダーを表示するには、i アイコンをクリックします。

### 4. Google Meet 会議:

Google Meet 下で:

- **ボット名:** Zoomの「Bot Name」フィールドで、ボット名を設定します。サポートされているプレースホルダーを表示するには、i アイコンをクリックします。
- **録音通知メッセージ:**「Bot Chat Notifications Message」フィールドに、Meeting Insights ボットが会議に参加して記録するときに Google Meet チャット ウィンドウに表示する記録通知メッセージを入力します。メッセージを表示したくない場合は、フィールド内のすべてのテキストを削除します (つまり、空のフィールドになります)。

### 5. Apply をクリックします。

## 13 スケジュールされた会議へのMIAの自動招待の設定

管理者は、特定のユーザーまたはユーザーグループが主催するスケジュールされた Teams および Zoom 会議に、Meeting Insights Assistant (MIA) を自動的に招待するように構成できます。ユーザーが会議をスケジュールすると、MIA が自動的に招待者リストに追加され、次の免責事項 (例) がすべての招待状の本文に追加されます。

**免責事項: 会議は録画されます**



会議の主催者が会議の招待状を開いたときに、免責事項は会議の主催者には表示されません。これは、会議招待状の他のすべての受信者に表示されます (招待状の本文の上部)。

スケジュールされた会議へのMIAの自動招待を構成するには、次の3つの手順を実行します。

1. Microsoft 360 管理者センターでメールが有効なセキュリティグループを追加します。方法は[こちら](#)を参照してください。



メールルールの一部にできるのは、メールが有効なセキュリティグループのみです。

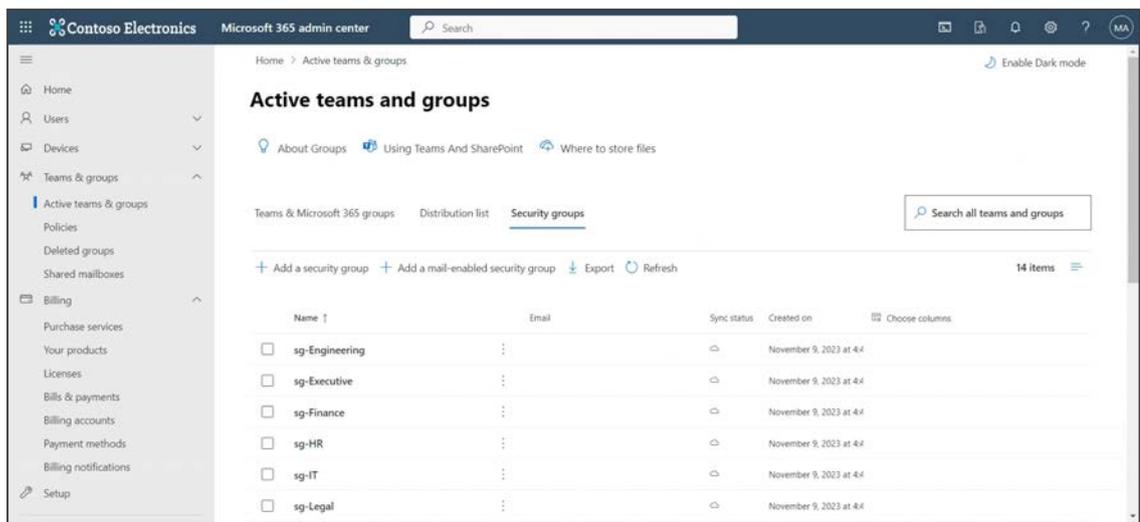
2. Exchange 管理者センターで自動招待ルールを定義します。方法は[こちら](#)を参照してください。
3. ルールをテストします。方法は[こちら](#)を参照してください。

### メール対応セキュリティグループを追加する

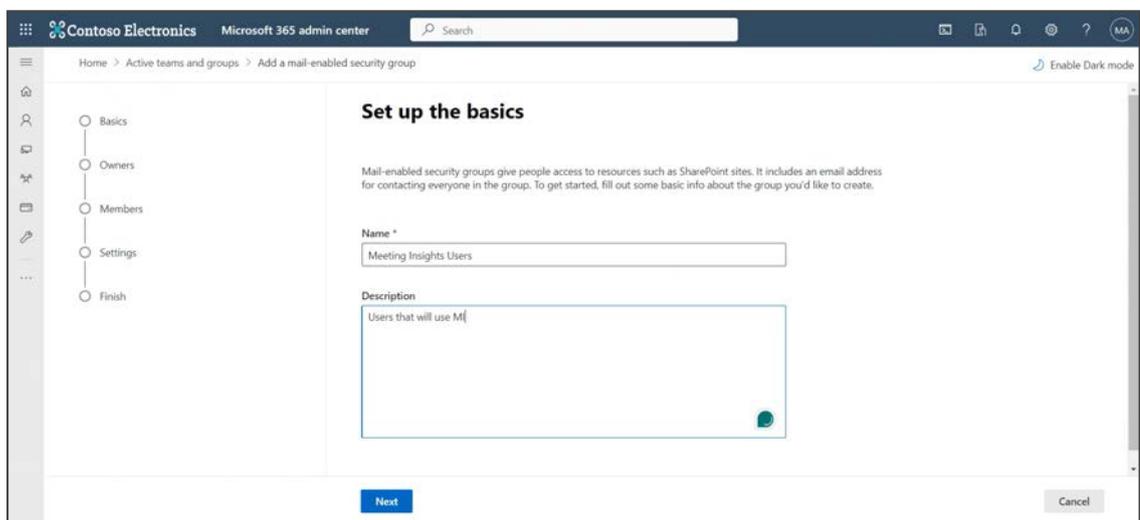
以下の手順では、Microsoft 365 管理者センターを通じてメールが有効なセキュリティグループを作成する方法に重点を置いています。

➤ **メールが有効なセキュリティグループを追加するには:**

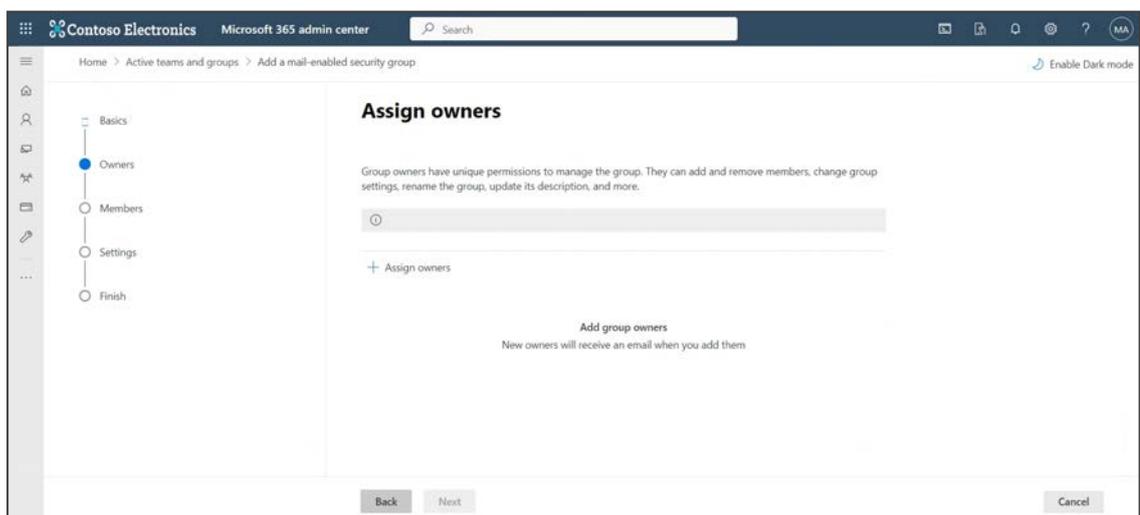
1. Microsoft 365 管理者センターで、Teams & groups > Active teams & groups > Security Groups タブに移動します。



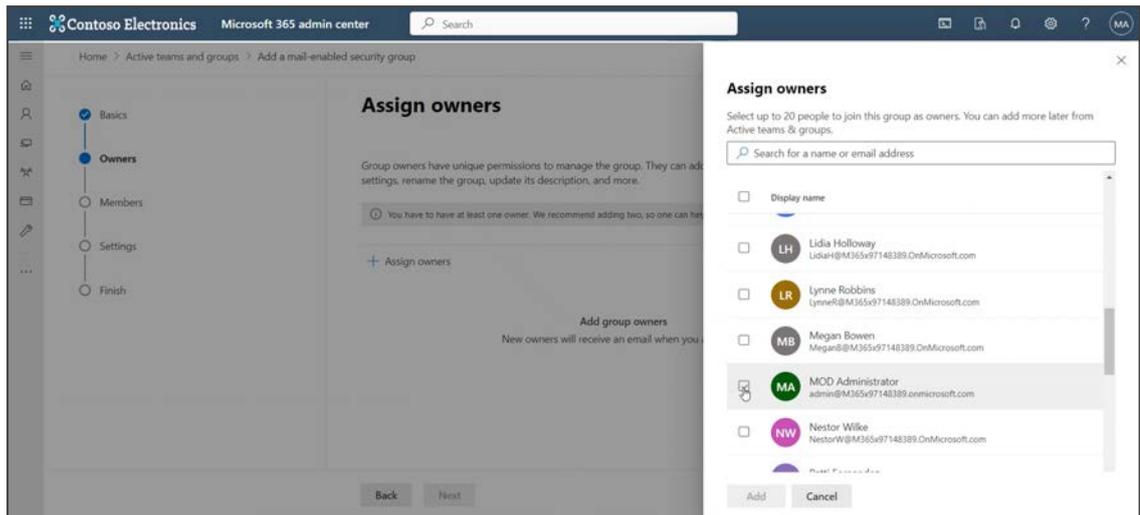
2. 上記の「アクティブなチームとグループ」ページで、+ Add a mail-enabled security group をクリックします。



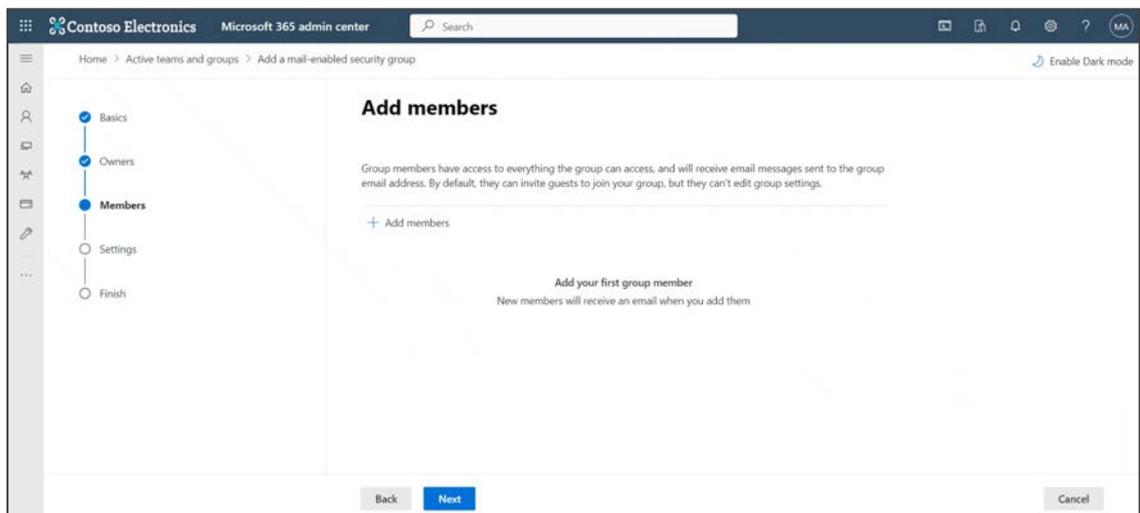
3. 上記の「基本設定」ページで、「Name」フィールドに Meeting Insights Users と入力し、後で効果的に管理できるように「説明」を入力して、Next をクリックします。



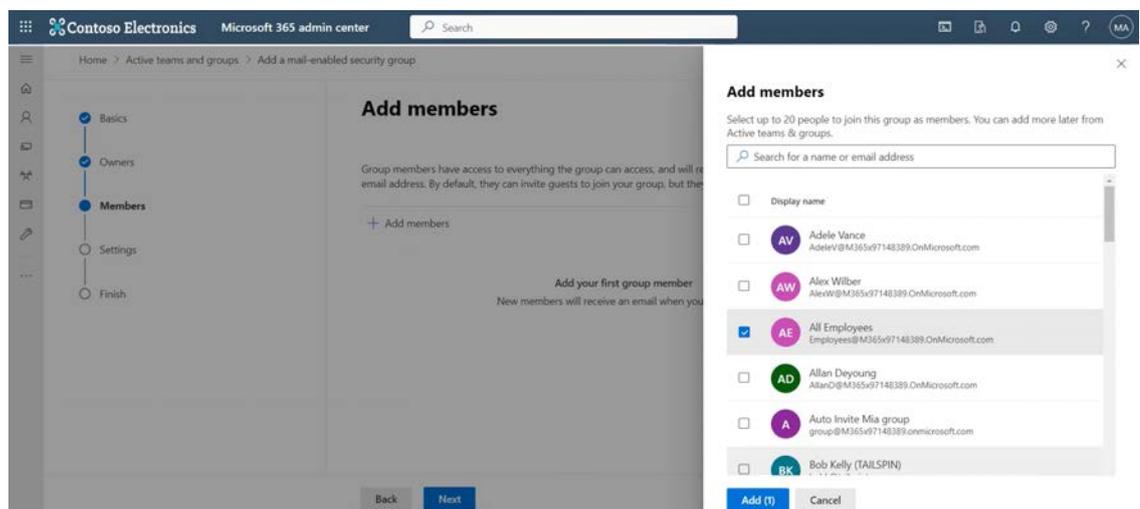
#### 4. 開いた「所有者の割り当て」ページで、+ Assign owners をクリックします。



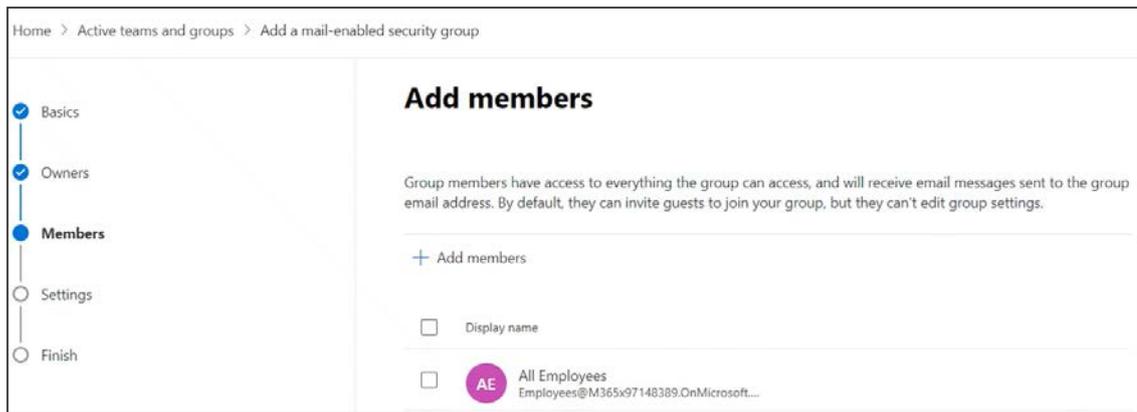
#### 5. 右側にポップアップ表示されるリストから所有者を選択し、Add をクリックします。



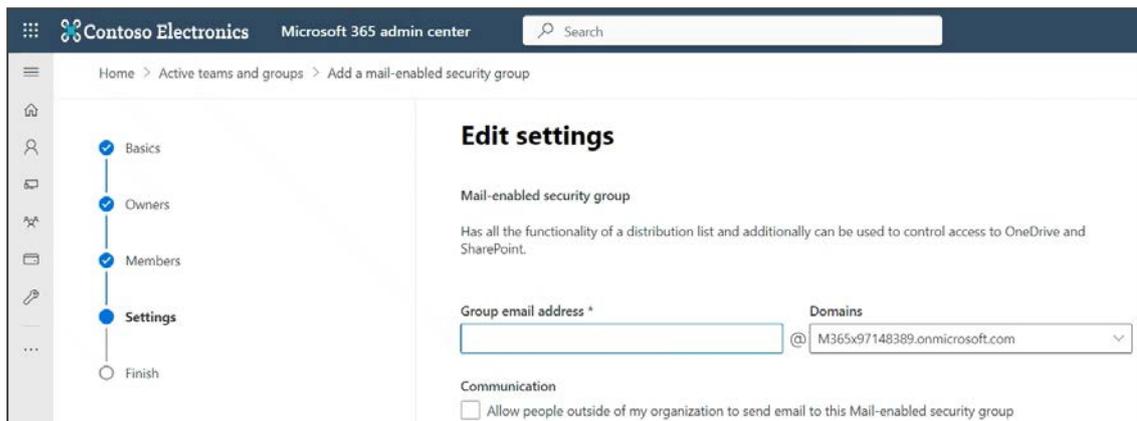
#### 6. 上記の「メンバーを追加」ページで、+ Add members をクリックします。



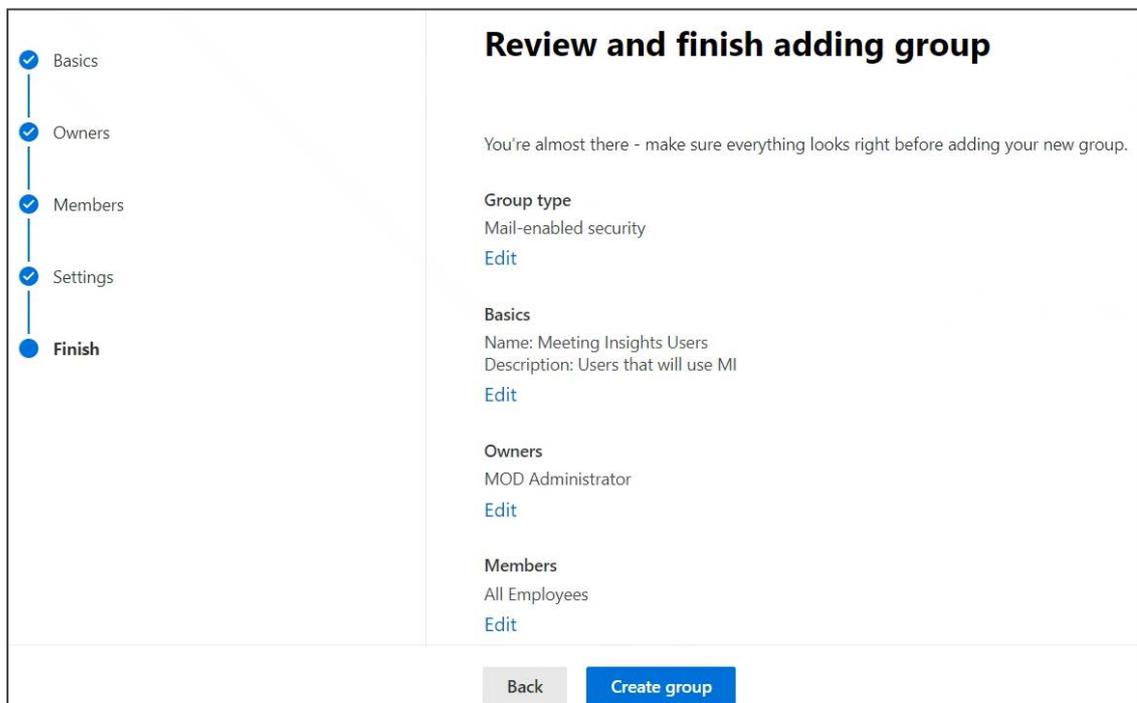
#### 7. グループに追加する個々のメンバーを選択し、Add をクリックします。



8. 選択したメンバーが追加されたことを確認し、**Next** をクリックします。



9. 「Group email address」フィールドにグループ名 (例: MIGroup) を入力します。



10. **Create group** をクリックします。

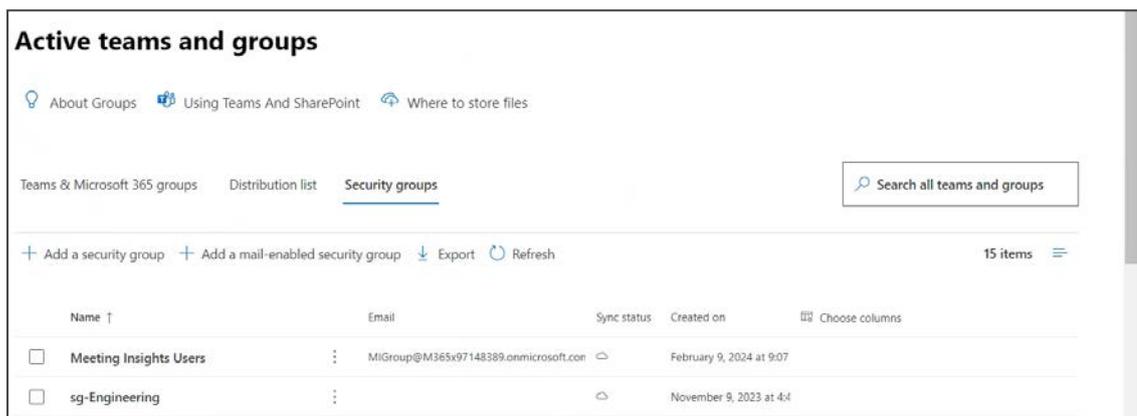
 **Meeting Insights Users group created**

It can take up to an hour for Meeting Insights Users group to appear in your Active teams & groups list. If you don't see your new group yet, go to the [Exchange admin center](#)

**Next steps**

[Add another Mail-enabled security group](#)

11. **Close** をクリックします。「アクティブなチームとグループ」ページにリストされている、新しく作成されたメール対応セキュリティグループを表示します。



**Active teams and groups**

About Groups Using Teams And SharePoint Where to store files

Teams & Microsoft 365 groups Distribution list **Security groups** Search all teams and groups

+ Add a security group + Add a mail-enabled security group Export Refresh 15 items

Name ↑	Email	Sync status	Created on	Choose columns
<input type="checkbox"/> Meeting Insights Users	MIGroup@M365x97148389.onmicrosoft.com	☑	February 9, 2024 at 9:07	
<input type="checkbox"/> sg-Engineering		☑	November 9, 2023 at 4:4	

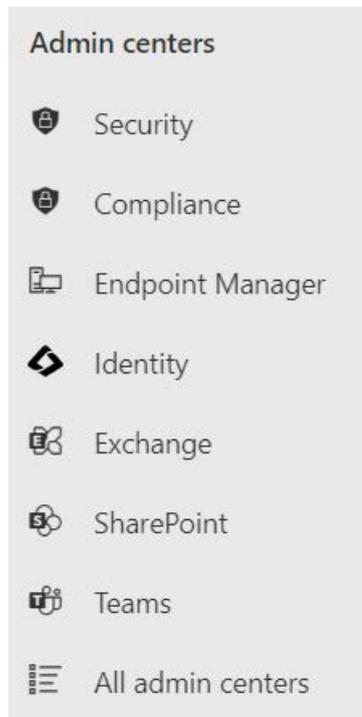
次に「自動招待」ルールを[こちら](#)に示されているように設定します。

## 自動招待ルールを設定する

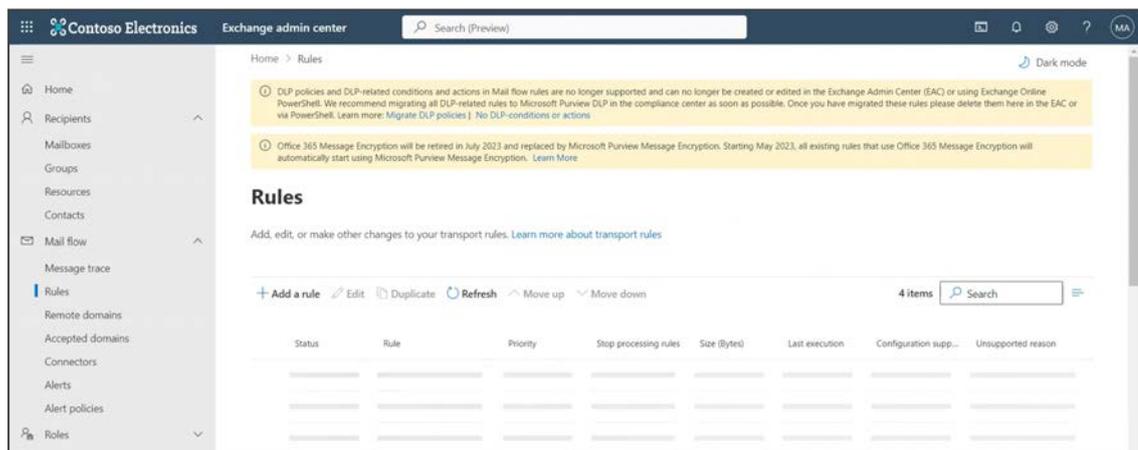
以前に示されているようにメール対応セキュリティグループを追加した後、管理者は、Microsoft の Exchange 管理者センターから「自動招待」ルールを設定できます。Microsoft 360 管理者センターから Exchange ルールを構成するには、メッセージがカレンダー イベントであることや、Teams 会議の場合は「Microsoft Teams 会議」、Zoom 会議の場合は「Zoom 会議」というテキストが含まれていることなど、特定の条件を定義する必要があります。

### ➤ 「自動招待」ルールを設定するには:

1. Microsoft 365 管理者センター (メールが有効なセキュリティグループを追加した場所) に表示される管理センターの一覧から、**Exchange** をクリックします。



2. Exchange 管理者センターで、Mail flow > Rules に移動します。



3. 「ルール」ページで、+ Add a rule をクリックします。

**New transport rule**

- Set rule conditions
- Set rule settings
- Review and finish

## Set rule conditions

Name and set conditions for your transport rule

**Name \***  
Auto Invite MIA

**Apply this rule if \***

The message properties include the message type  
The message type is 'Calendaring'

**And**

The subject or body subject or body includes any of these words  
The subject or body includes any of these words 'Microsoft Teams meeting' or 'Microsoft Teams' or 'Join Zoom Meeting'

**And**

The sender is a member of this group  
The sender is a member of 'MIGroup@M365x97148389.onmicrosoft.com'

4. 上の図を参考に、次のルール条件を設定します。
  - a. ルールの名前を設定します (例: Auto Invite Mia)。
  - b. 2つの **Apply this rule if** ドロップダウンから、それぞれ **The message properties** および **include the message type** を選択します。メッセージの種類として **Calendaring** を選択します。
  - c. + をクリックします。2つの **And** ドロップダウンから、それぞれ **The subject or body** および **subject or body includes any of these words** を選択します。単語として **Microsoft Teams 会議**、**Microsoft Teams**、または **Zoom 会議に参加** と入力します。
  - d. + をクリックします。2つの **And** ドロップダウンから、それぞれ **The sender** および **is a member of this group** を選択します。前の手順で作成したグループを選択します。上の図では、**MIGroup@M365x97148389.onmicrosoft.com** になります。
5. 下にスクロールし、下の図を参考にしてルール条件の設定を続けます。
  - a. 2つの **Do the following** ドロップダウンから、それぞれ **Apply a disclaimer to the message** および **prepend a disclaimer** を選択します。
    - i. 免責事項については、組織に必要な免責事項を定義します。例:「免責事項: 会議は録画されます」。
    - ii. 免責事項を挿入できない場合にフォールバックするアクションとして「折り返し」を選択します。
  - b. + をクリックします。2つの **And** ドロップダウンから、それぞれ **Add recipients** および **to the To box** を選択します。To boxの電子メールを定義します。
  - c. 2つの **Except if** ドロップダウンから、それぞれ **The message** および **To or Cc box contains this person** を選択します。その人の電子メールアドレスを定義します。

- d. 2つのOrドロップダウンから、それぞれ **The subject or body** および **subject matches these text patterns** を選択します。テキストパターン **^Canceled** を定義します:

**New transport rule**

- Set rule conditions
- Set rule settings
- Review and finish

**Do the following \***

Apply a disclaimer to the message    prepend a disclaimer    +    🗑️

Prepend 'Disclaimer: The meeting will be recorded' and fall back to action 'Wrap' if the disclaimer can't be inserted    ✎

---

**And**

Add recipients    to the To box    🗑️

Add these recipients to the To box 'mia.Tania-8389@meetinginsights.com'    ✎

---

**Except if**

The message    To or Cc box contains this person    +    🗑️

The To or Cc box contains 'mia.Tania-8389@meetinginsights.com'    ✎

---

**Or**

The subject or body    subject matches these text patterns    🗑️

The subject matches these text patterns '^Canceled:'    ✎

**Next**

6. **Next** をクリックします。

**New transport rule**

- ✓ Set rule conditions
- Set rule settings
- Review and finish

## Set rule settings

Set settings for your transport rule

**Rule mode**

- Enforce
- Test with Policy Tips
- Test without Policy Tips

**Severity \***

Not specified

Activate this rule on

2/9/2024 - 4:00 PM

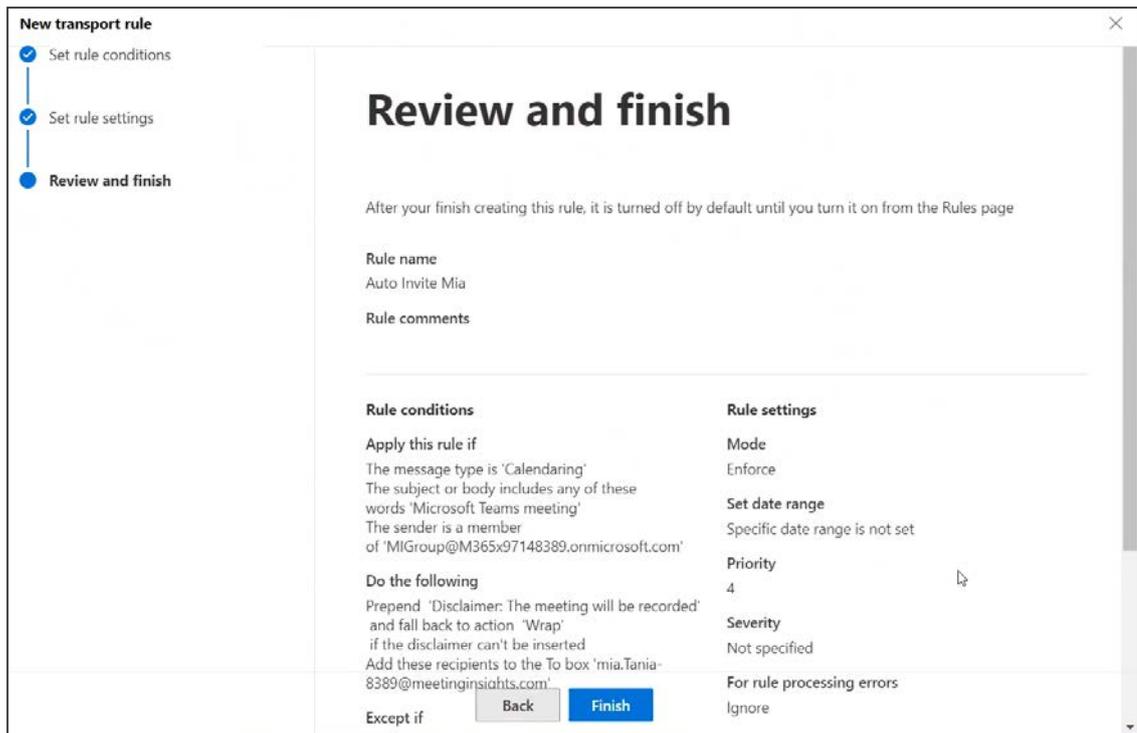
Deactivate this rule on

2/9/2024 - 4:00 PM

Stop process

Back Next

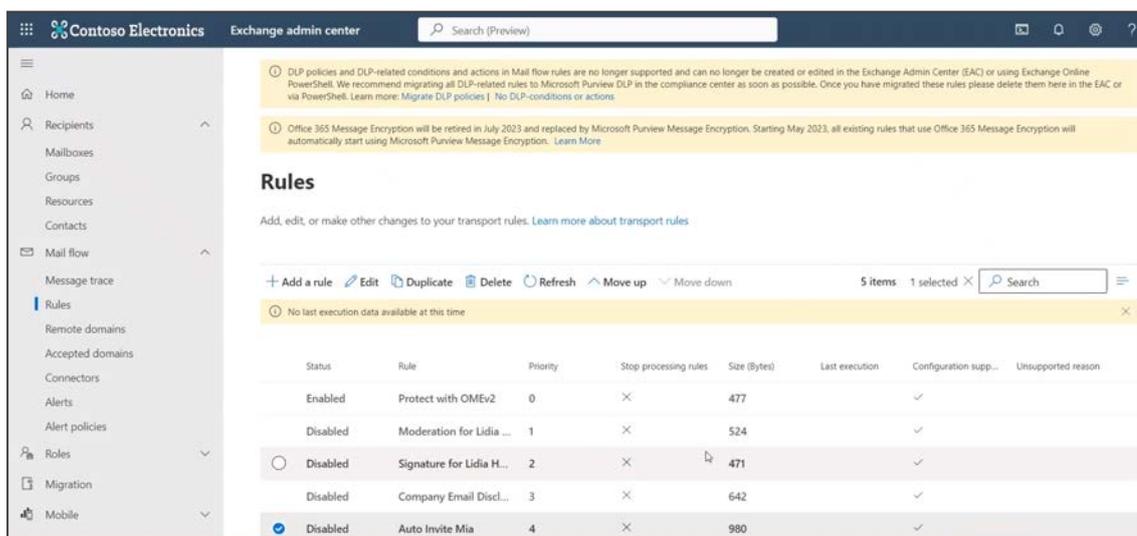
7. ルール設定を次のように設定します。
  - a. 「Rule mode」はデフォルトの **Enforce** のままにします。
  - b. 「Severity」レベルのドロップダウンでは、必要に応じてこのフィルターを **Not specified** のままにするか、組織の要件に応じて設定します(レポートを使いやすいするため)。
  - c. 「Activate this rule on」を選択し、すぐに有効になるように設定します。
  - d. 「Match sender address in message」ドロップダウンから、**Header** を選択します。
8. **Next** をクリックします。



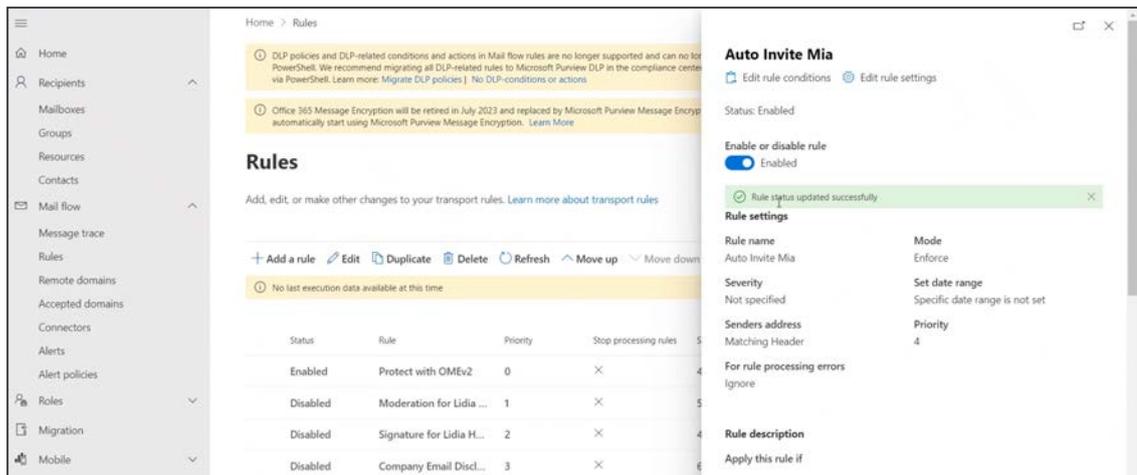
9. これまでの説明どおりにすべての設定が構成されていることを確認し、**Finish** をクリックします。



10. 新しく構成されたルール(以下の例では「Auto Invite Mia」)がExchange 管理者センターにリストされていることを確認します。



11. ルールを有効にします。



すべてのユーザーに対してデフォルトで MIA 自動招待を有効にすることをお勧めします。会議を録画したくないユーザーは、録画を一時停止するか、MIA 参加者を会議から削除することができます。

次に[こちら](#)に示されているようにルールをテストします。

## ルールをテストする

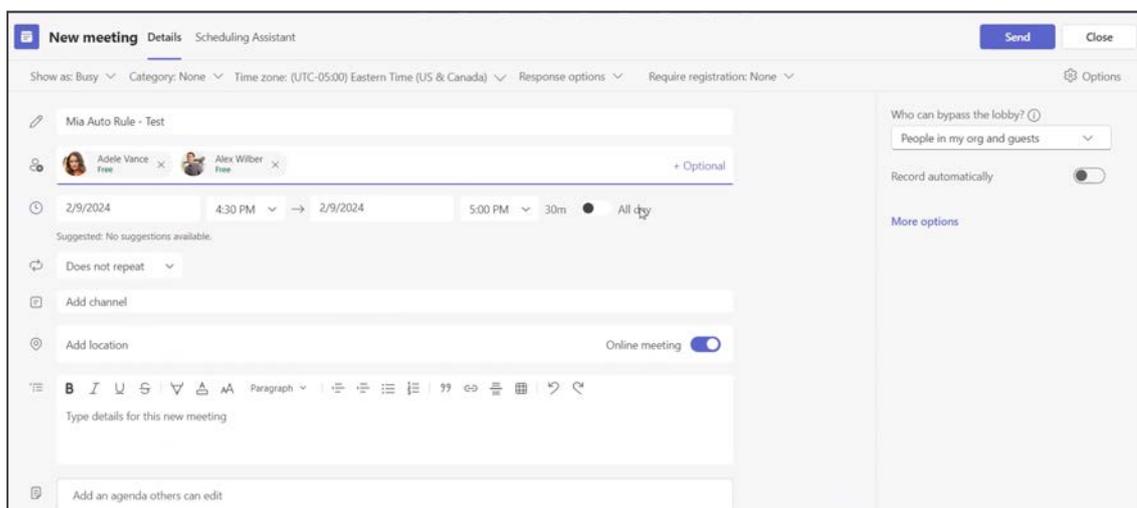


MIA の「自動招待」ルールが有効になるまでに最大 30 分かかります。

管理者は MIA の「自動招待」ルールをテストして、期待どおりに機能することを確認できます。

### ➤ MIA の「自動招待」ルールをテストします。

1. 管理者の Teams アプリにログインし、カレンダーを開いて **+ New meeting** をクリックします。
2. 会議のタイトル(例:「MIA 自動ルール-テスト」)を入力し、必要な出席者を追加します。



3. **Send** ボタンをクリックすると、ルールが有効になります。
4. Outlook で、招待状が届き、MIA が招待されたことを確認します。

## Teams 会議のロビーの管理

管理者は、Microsoft Teams 管理者センター (TAC) の「Meeting join and lobby」設定を使用して、会議に参加するユーザーを管理したり、Teams 会議のロビーを管理したりできます。「Meeting join and lobby」の構成は、ポリシーに割り当てられているユーザーの会議に有効になる会議ポリシーの一部です。



[下図参照]

- 会議ポリシー設定に**緑** (下記) が設定されている場合、MIA はこのポリシーに割り当てられているユーザーの会議ロビーをバイパスします。
- 会議ポリシー設定に**赤** (下記) が設定されている場合、MIA はこのポリシーに割り当てられているユーザーの会議ロビーにルーティングされます。

### Meeting join & lobby

Meeting join and lobby settings let you control how people join meetings and allow you to manage the lobby for Teams meetings.  
[Learn more about meeting join and lobby settings](#)

Anonymous users can join a meeting ⓘ  On  
Find related settings at [Meetings > Live events policies](#) and [Meetings > Meeting settings](#)

Anonymous users and dial-in callers can start a meeting ⓘ  Off

Who can bypass the lobby ⓘ People in my org ▼

People dialing in can bypass the lobby ⓘ

People can join external meetings hosted by ⓘ

### Meeting engagement

Meeting engagement settings let you control how people

Meeting chat ⓘ Only organizers and co-organizers ▼  
Find related settings at [Messaging > Messaging policies](#)

External meeting chat ⓘ  On

## 14 Power BI Analytics 使用状況レポートの作成

管理者は、Meeting Insights Analytics ダッシュボードを Microsoft Power Business Intelligence (BI) に統合できます。

方法は以下のリンクを参照

1. Meeting Insights で Power BI 統合を有効にする( [こちら](#)を参照)
2. Power BI をインストール | 構成する( [こちら](#)を参照)
3. レポートから使用状況統計を確認する( [こちら](#)を参照)
4. Power BI 統合を無効にする( [こちら](#)を参照)

### Meeting Insights で Power BI 統合を有効にする

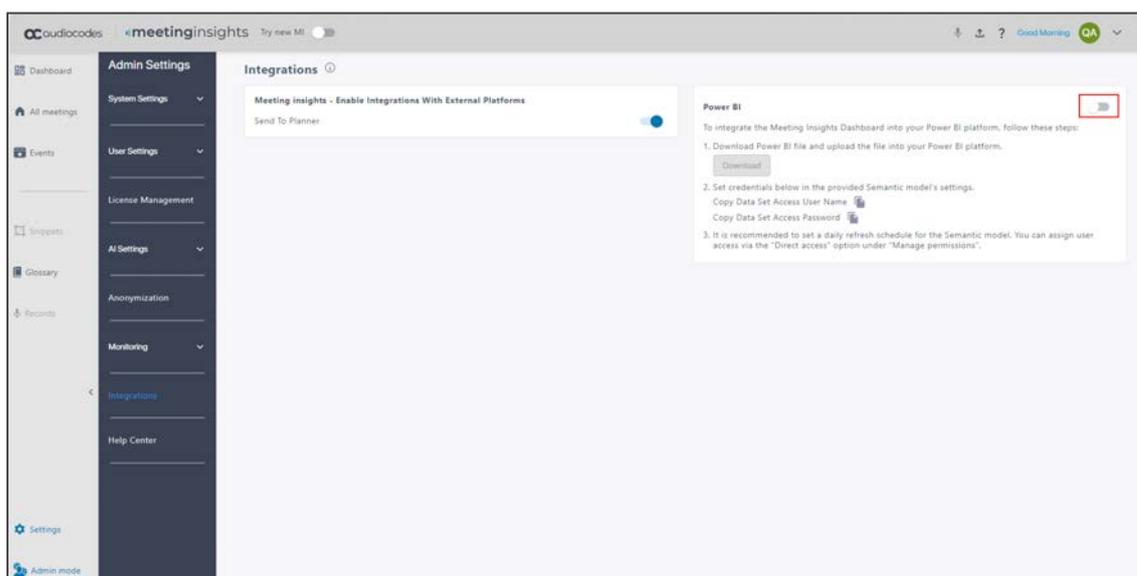
以下の手順は、管理者が Meeting Insights で Power BI 統合を有効にする方法を示しています。



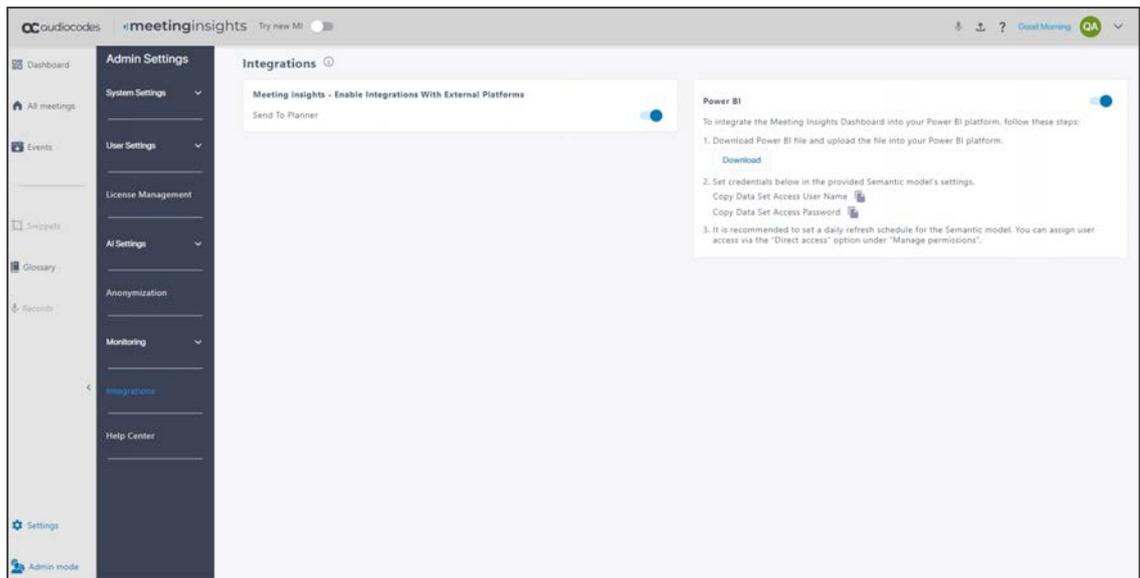
- 管理者は、アプリケーションで統合が有効になっている場合にのみ統合を表示しません。
- これをお持ちでなく、ご希望の場合は、サービスプロバイダーにお問い合わせください。

#### ➤ Meeting Insights で Power BI 統合を有効にするには:

1. Meeting Insights で、統合 ページを開きます。



2. 上図に示すスイッチを ON にスライドします。



3. 上の図に示されている **Download** ボタンをクリックして、Power BI レポート ファイル (.pbix) をダウンロードし、Power BI プラットフォームにアップロードします。
4. 資格情報をコピーしてステップ 5 に進みます。詳しい手順については、[こちら](#)をご覧ください。

## インストール | Power BI Analytics の構成

ここで説明する手順は、Meeting Insights Power BI Analytics をインストール | 構成する方法を示しています。

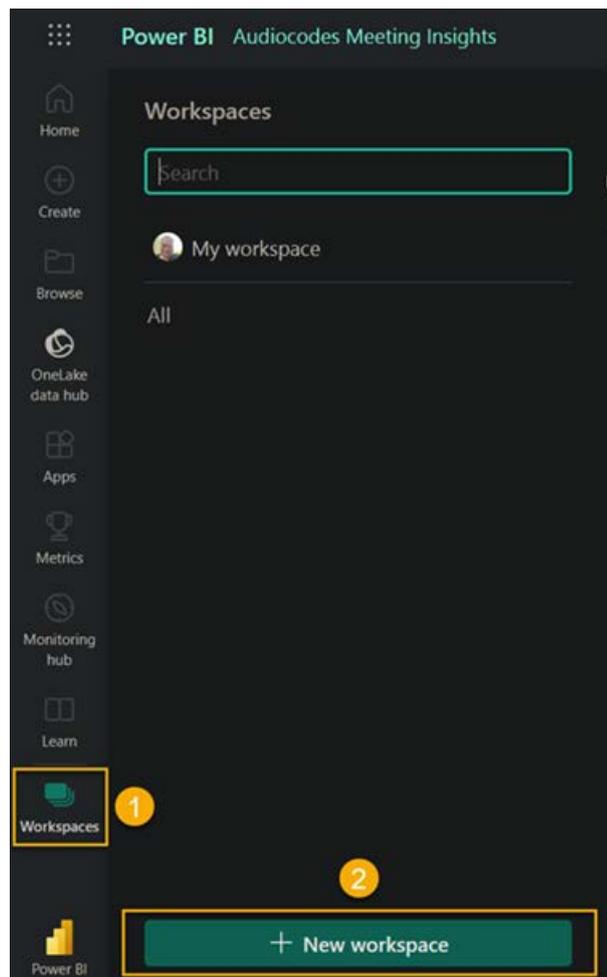


### 前提条件

- Office 365 E5 顧客アカウント、または個別の Power BI Pro ライセンスが添付された任意の Office 365 ライセンス アカウント。
- Microsoft E5 ライセンスには、Power BI Pro ライセンスが 1 つ含まれています。

### ➤ Power BI をインストール | 構成するには:

1. <https://app.powerbi.com/> で Microsoft Power BI ポータルにサインインします。



2. + New workspace をクリックします。

**Create a workspace**

Name \*

MeetingInsights PBI

Available

Description

Describe this workspace

Domain (preview) ▾

Assign to a domain (optional) ▾

[Learn more about workspace settings](#) ↗

Workspace image

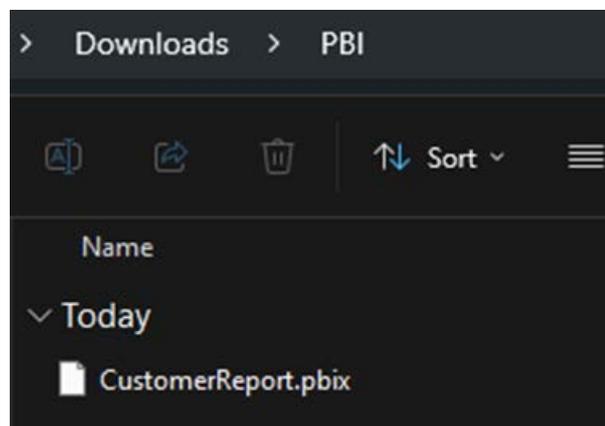
Upload

Reset

Advanced ▾

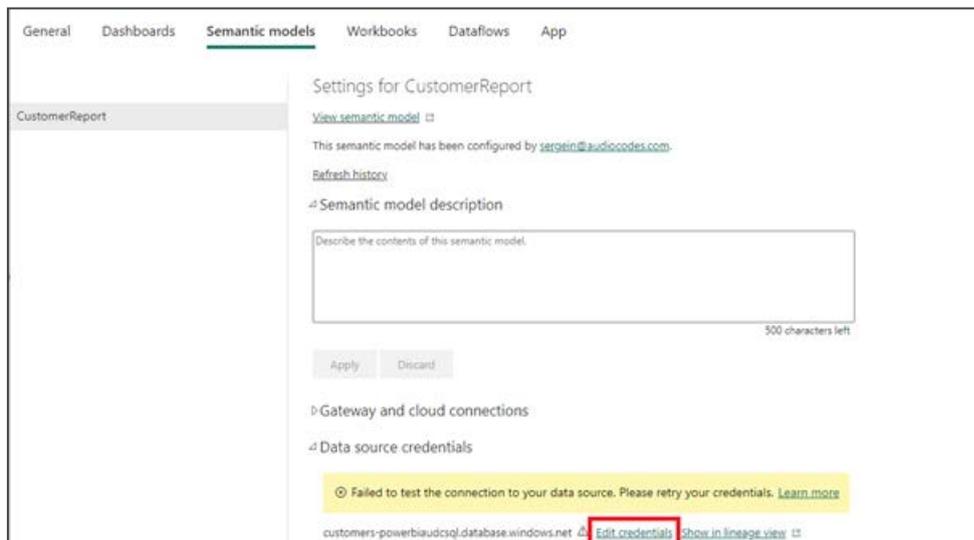
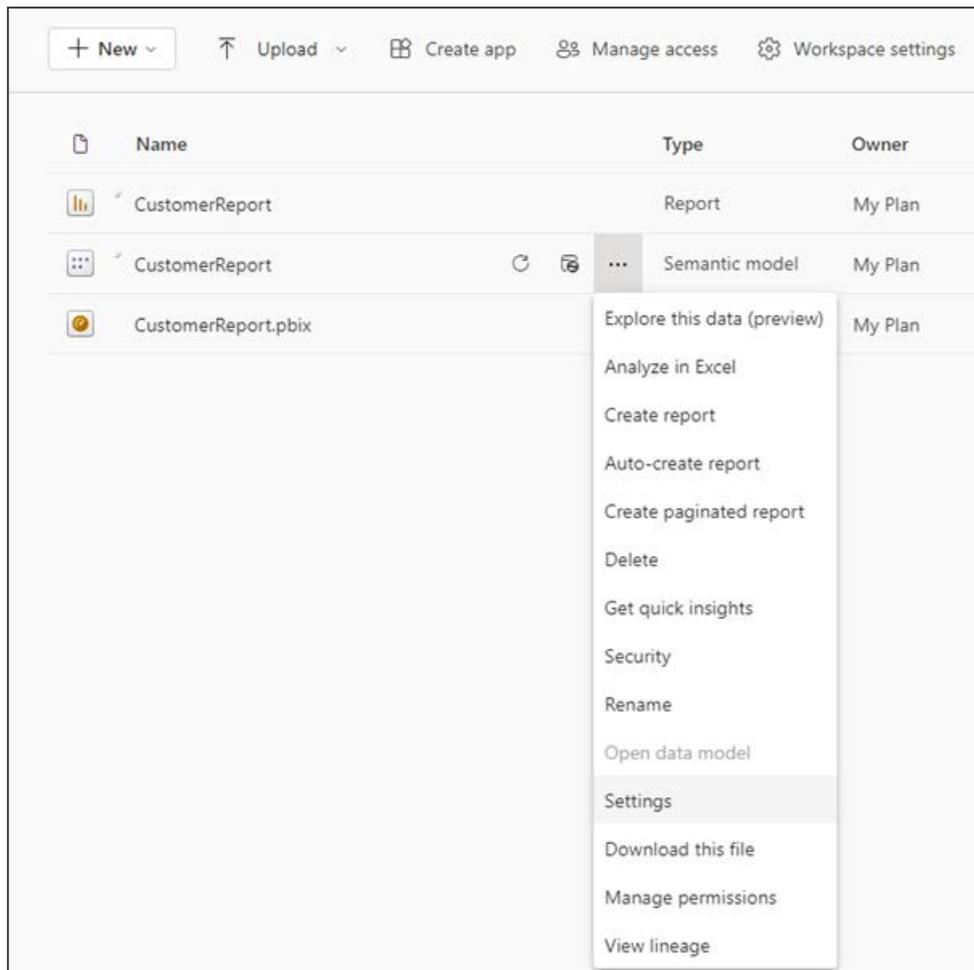
Apply Cancel

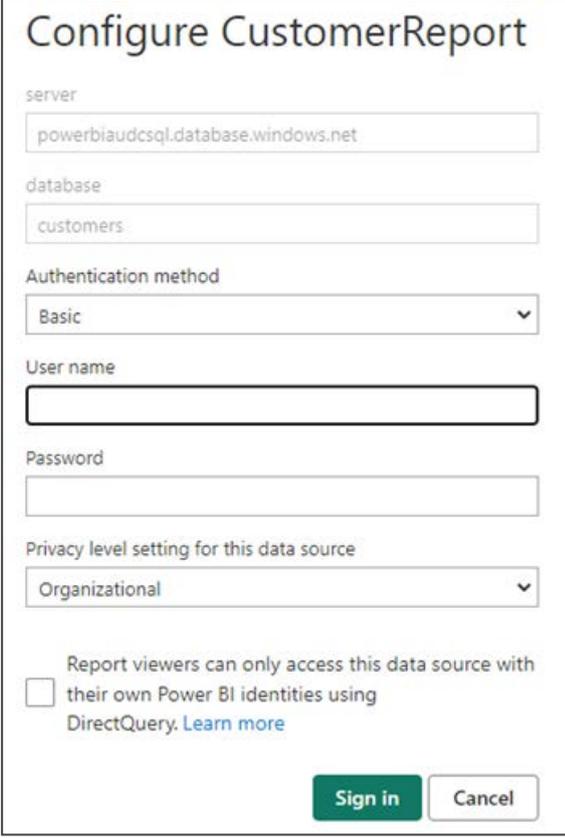
3. 新しいワークスペースの名前を入力し、**Apply** をクリックします。
4. ステップ 3 [こちら](#) に示すように、Meeting Insights の統合 ページを使用してダウンロードした Power BI レポート ファイル (.pbix) をインストールします。



5. レポートの資格情報を設定するには、次の図を参照してください。[こちら](#)に表示されている統合ページを使用して資格情報をコピーします。

+ New ▾    ↑ Upload ▾    📦 Create app    👤 Manage access    ⚙️ Workspace settings			
📄	Name	Type	Owner
📊	CustomerReport	Report	My Plan
📊	CustomerReport	Semantic model	My Plan
📄	CustomerReport.pbix	Dashboard	My Plan





**Configure CustomerReport**

server  
powerbiaudcsql.database.windows.net

database  
customers

Authentication method  
Basic

User name  
[Empty field]

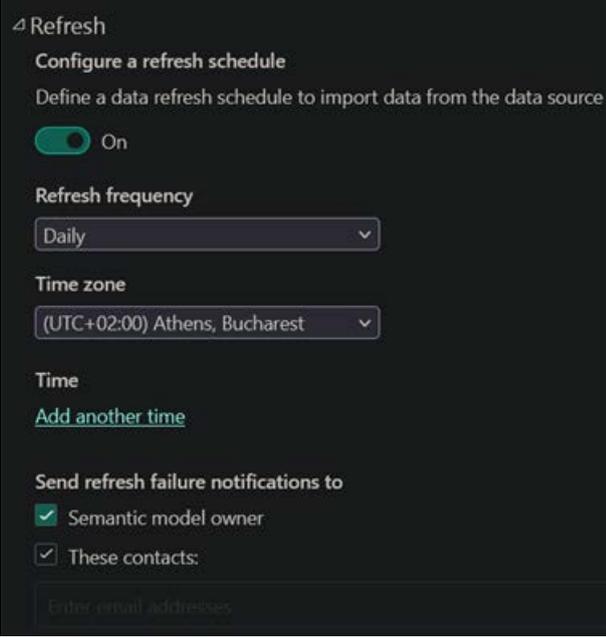
Password  
[Empty field]

Privacy level setting for this data source  
Organizational

Report viewers can only access this data source with their own Power BI identities using DirectQuery. [Learn more](#)

Sign in Cancel

6. [推奨] Semantic model の毎日の更新スケジュールを設定します。「Manage permissions」の Direct access オプションを使用してユーザー アクセスを割り当てることができます。



Refresh

Configure a refresh schedule

Define a data refresh schedule to import data from the data source

On

Refresh frequency  
Daily

Time zone  
(UTC+02:00) Athens, Bucharest

Time  
[Add another time](#)

Send refresh failure notifications to

Semantic model owner

These contacts:

Enter email addresses

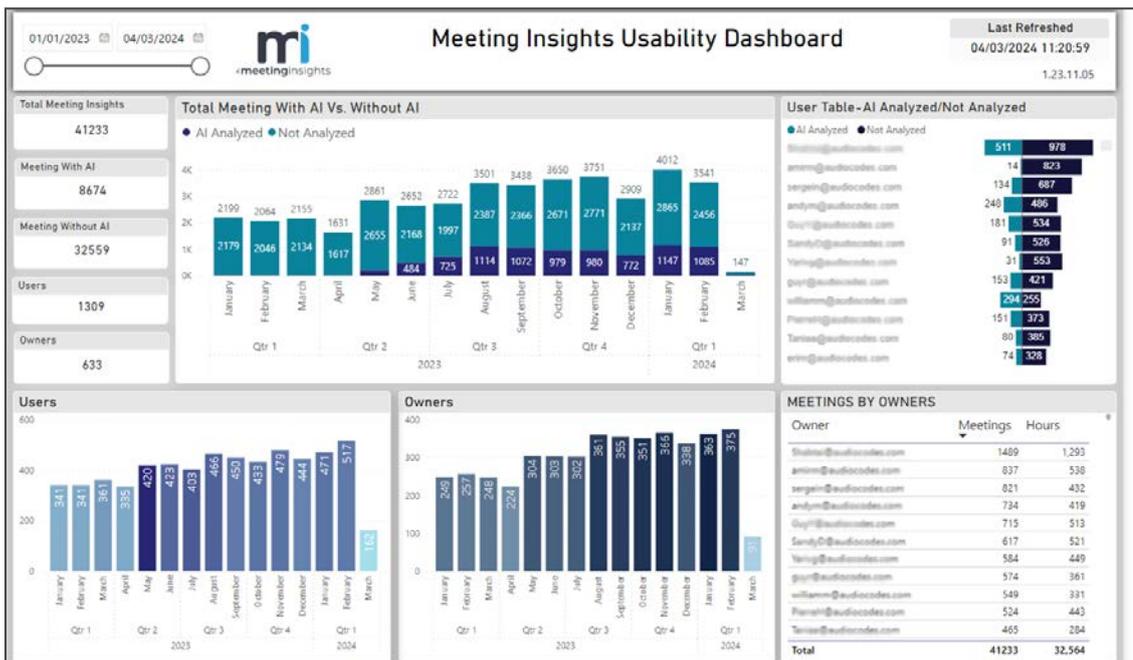
7. 「ワークスペース」ページに戻り、「Semantic model」アイテムの Refresh now をクリックします。

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Included in app
CustomerReport	Report	My Plan	3/10/24 9:24:19 AM	—	—	—	<input type="checkbox"/>
CustomerReport	Semantic model	My Plan	3/10/24 9:24:19 AM	N/A	—	—	<input type="checkbox"/>
CustomerReportLgkls	Dashboard	My Plan	—	—	—	—	<input type="checkbox"/>

## レポートを使用して製品の使用状況統計を確認する

Meeting Insights を Microsoft の Power Business Intelligence (BI) と統合すると、管理者や経営陣は、企業内のユーザーが Meeting Insights とその機能をどのように、どの程度利用しているかを示すビジネス分析レポートを作成できます。

下の図は、Usability Dashboard レポートを示しています。



- Usability Dashboard レポートは、管理者や経営陣に、Meeting Insights とその主要機能である AI の価値提案を示すことができます。
- レポートの統計とグラフは管理者にユーザーがアプリケーションとその主要機能である AI をどの程度、およびどれくらいの深度で使用しているかを知ることができます。
- レポートは、管理者に受け入れられる Microsoft Power BI テンプレートで生成されます。

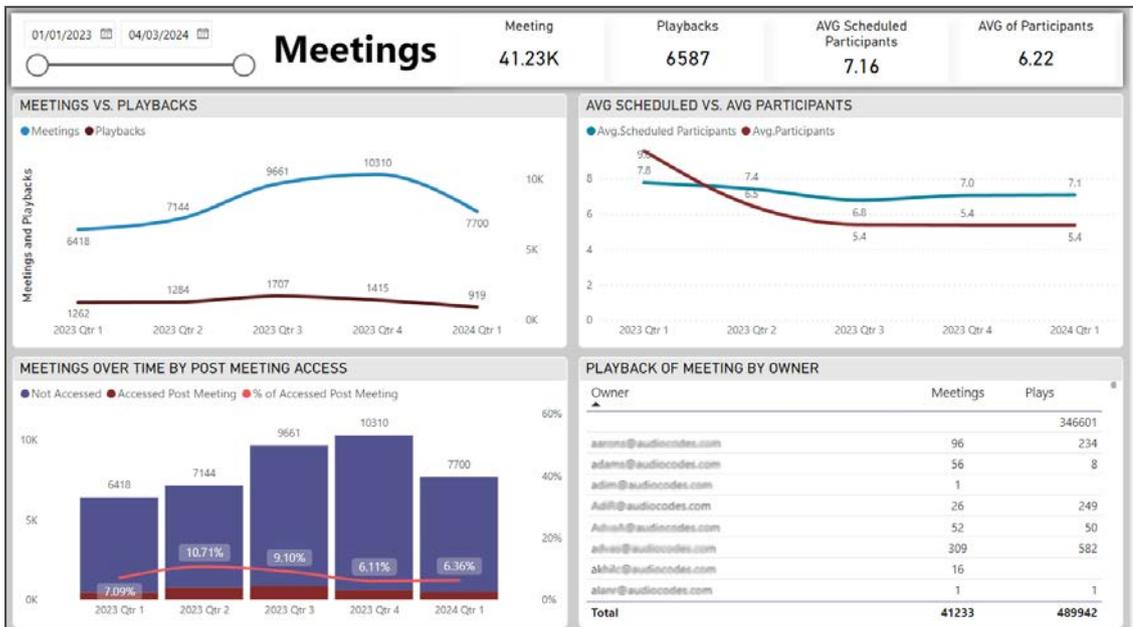
[前の図を参照] 管理者は、ページの左上隅で定義された期間内に、企業内で Meeting Insights を使用して合計何回の会議が開催されたかを一目で確認できます。さらに管理者は、AI を使用して分析された会議の数と分析されなかった会議の数を評価できます。さらに管理者は、会議後にユーザーが実行した分析の数と、所有者が実行した分析の数をすぐに確認できます。

管理者は、ページの右側にある User Table-AI Analyzed/Not Analyzed ペインで、ユーザーごとにこれらの統計を表示できます。このペインには、ユーザーの順序付きリスト、定義された期間

内に各ユーザーが行った会議の数、および各ユーザーが会議に費やした時間数が表示されます。

その下の **Meetings by Owners** ペインには、各所有者が開催した会議の数と、各所有者が会議に費やした時間が表示されます。このペインには、すべての所有者が開催した会議の合計数と、すべての所有者が会議に費やした合計時間数も表示されます。

下の図は **Meetings** レポートを示しています。



[前の図を参照] 管理者は、ページの左上隅で定義された期間にわたって、ユーザーと所有者が製品にどれくらいの深度で関与したかをすぐに測定できます。**Meetings vs. Playbacks** グラフには、組織内で開催された会議の数と実行された再生の数が表示されます。たとえば、再生機能がほとんど利用されていない場合 (前の図のグラフに示すように、会議と再生の曲線の間に大きなギャップがあることで示されます)、ユーザー | 所有者は会議を再生せずに製品を表面的に使用する傾向があることを示している可能性があります。対照的に、再生機能が最大限に活用された場合 (2つの曲線が両方とも高い使用率を示している)、ユーザー | 所有者がそれを有効活用したことを示します。したがって、グラフは機能の有効性を示しています。

**Average Scheduled vs. Average Participants** グラフには、会議に招待された招待者の数と、それらの会議に積極的に参加した招待者の数が表示されます。これらの統計は製品の有効性を示し、管理者や経営陣が投資から利益 (使用率) を得ているかどうかを評価するのに役立ちます。

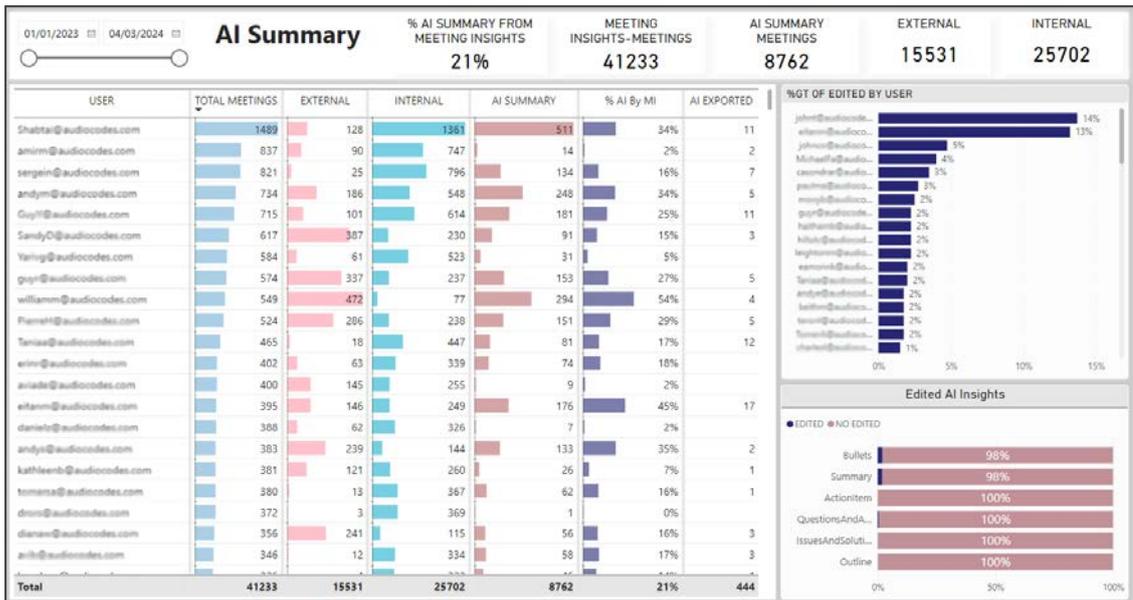
グラフ **Meetings over Time by Post Meeting Access** では、時間の経過に伴う会議終了後の録画にアクセスしたユーザーの数と割合が管理者に表示されます。このグラフも、製品の有効性とユーザーが Meeting Insights の機能をどの程度活用しているかを示しています。

**Playback of Meeting by Owner** グラフは、会議の所有者が Meeting Insight の再生機能をどの程度活用したかを示します。グラフには、所有者ごとの行動と、すべての所有者の合計行動が表示されます。管理者は一目で次のことを判断できます:

- 所有者の数と、所有者が実行する再生回数の比較

■ 各所有者が行った会議の数と、各所有者が実行した再生回数の比較

下の図は AI Summary レポートを示しています。



[前の図を参照] 管理者はこのレポートを使用して、一定期間にわたる AI Summary の使用状況をグローバルおよび外部 | 内部ユーザーごとにすばやく確認できます。このレポートにより、管理者や経営陣は、Meeting Insights の AI Summary 機能が組織に提供しているメリットを把握できます。

レポートのタイトルバーを使用すると、管理者は AI Summary (l-r から) のグローバル統計をすばやく確認できます。

- **% AI Summary from Meeting Insights** には、AI Summary 機能が使用された会議の割合が表示されます。前の例では、期間中に開催されたすべての会議の 21% で AI Summary 機能が使用されました。
- **Meeting Insights - Meetings** には、期間中に開催された Meeting Insights の会議数が表示されます。前の例では、41233 回の会議が開催されました。
- **AI Summary Meetings** には、AI Summary 機能が使用された Meeting Insights の会議の数が表示されます。前の例では、この機能は 8762 回の会議で使用されました。
- **External** には、期間中に各ユーザーが Meeting Insights を使用して行った外部会議の数が表示されます。前の例では、すべてのユーザーが Meeting Insights を使用して 15531 件の外部会議を開催しました。
- **Internal** には、期間中に各ユーザーが Meeting Insights を使用して行った内部会議の数が表示されます。前の例では、すべてのユーザーが Meeting Insights を使用して 25702 件の社内会議を開催しました。

レポートのメイン ペインでは、管理者は次の列 (l-r から) でユーザーごとの AI Summary 使用状況統計を確認できます。

- **Total Meetings** には、期間中に各ユーザーが Meeting Insights を使用して行った会議の合計数が表示されます。列は、会議数の多い順、または会議数の少ない順で並べ替え

ることができます。管理者は、Meeting Insights を使用して、組織内でどのユーザーが最も多くの会議を行ったか、どのユーザーが最も少ない会議を行ったかを簡単に判断できます。

- **External** には、ユーザーが Meeting Insights を使用して行った外部会議の数が表示されます。列は、最大から最小、または最小から最大の順に並べ替えることができます。管理者は、Meeting Insights を使用して、外部会議を最も多く行ったユーザーと、最も少なく行ったユーザーを簡単に判断できます。
- **Internal** には、ユーザーが Meeting Insights を使用して行った内部会議の数が表示されます。列は、最大から最小、または最小から最大の順に並べ替えることができます。管理者は、どのユーザーが最も多くの社内会議を行ったか、どのユーザーが最も少ないかを簡単に判断できます。
- **AI Summary** には、AI がトリガーされた会議の数 (期間中に開催された会議の合計数に対する相対値) が表示されます。
- **% AI by MI** には、ユーザーごとに AI Summary が生成された会議の割合が表示されます。管理者は統計を使用して、期間中に各ユーザーが機能をどの程度使用したかを判断できます。
- **AI Exported** には、期間中にアクセス権を持つユーザーによって AI がエクスポートされた回数が表示されます。



- 各列には *global usage* も表示されます。
- ✓ % AI by MI 列には合計パーセンテージが表示されます。
- ✓ その他の列には合計数が表示されます。

レポートの %GT of Edited by User ペインを使用すると、管理者はユーザーごとに、会議の数に対するユーザーが実行した編集の割合を判断できます。これもまた、次のことを示している可能性があります。

- 各ユーザーがアプリの編集機能にどの程度、そしてどれだけの深度で関与しているか
- 編集機能に関するアプリの価値提案
- 編集機能の観点から見たアプリの ROI
- 組織がサービスから得ている利益

レポートの Edited AI Insights ペインを使用すると、管理者は編集パターンを決定できます。前の例では、箇条書きに対して 2% の編集が行われ、サマリーに対して 2% の編集が行われました。たとえば、アクション アイテムはまったく編集されませんでした。これらのパターンは、次のことを示す指標としても役立ちます。

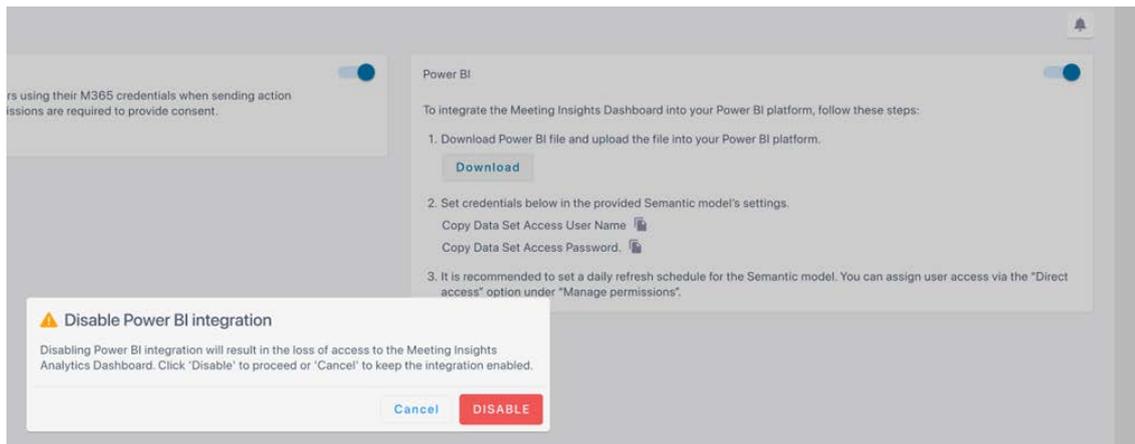
- ユーザーがアプリにどの程度、そしてどれだけの深度で関与しているか
- アプリの価値提案
- アプリの ROI
- 組織がサービスから得る利益

## Power BI 統合を無効にする

管理者はオプションで、Meeting Insights の Microsoft Power Business Intelligence (BI) 分析を無効にすることができます。

➤ **Meeting Insights Power BI を無効にするには:**

1. Meeting Insights で、統合 ページを開きます。
2. Power BI スイッチをオフにスライドすると、次の通知が表示されます。



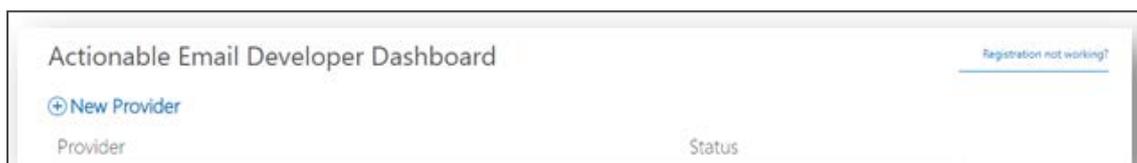
3. **DISABLE** をクリックします。

## 15 実用的な要約メールの有効化

管理者は、新しい Outlook Office プロバイダーを作成することで、アクション アイテム メール の受信者がメール内でステータスを「Done」に設定できるようにすることができます(DONE ボタンをクリックすることによって)。

➤ **新しい Outlook Office プロバイダーを作成するには:**

1. <https://aka.ms/publishoam> に進みます。
2. 会議の録画の送信先のユーザーと同じテナントに属する Teams テナント 管理者でログインすると、次の画面が表示されます。



3. **New Provider** をクリックすると、次の画面が表示されます。

# Actionable Email Developer Dashboard

[← Back](#)

## 1. New Provider

Friendly Name \*

Please enter a name for provider

Provider Id (originator)

11ed39bc-efd3-4a20-9ba1-f3eeb2a7ce0a

Organization Info

AudioCodes Ltd. (ai-logix.net)(ad41d6c3-67f0-47cc-9de3-e07fd185c1c7)

Sender email address from which actionable emails will originate \*

expense-notification@contoso.com

[Add another email address](#)

Target URLs \*

(HTTPS URLs which will be invoked by the actions from the message card. Regex can be used to club mutiple URLs)

https://www.api.contoso.com/ or regex:https://.+\.contoso\.com/

[Add another actions URL](#)

Public Key

(Provide your own public key if you want to send [signed card payloads](#))

<RSAKeyValue>...</RSAKeyValue>

[Add another public key](#)

Logo

Logo must be of type .png, .jpg or .gif and no greater than 60 kb



## 2. Scope of submission

Who are you enabling this for? \*

- Test Users (Test your provider on users from same tenant, auto-approved)
- Organization (You will be submitting this request to your organization's Exchange administrators)
- Global (Please note that rollout takes 2 weeks after this submission is approved)

## 3. Additional Information

Email addresses of other people who should be notified.

expense-notification@contoso.com

[Add another email address](#)

Comments

Any additional detail for your administrator to easily approve this request.

I accept the terms and conditions of the [App Developer Agreement](#)

You must accept the terms and conditions

Save

Cancel

4. **New Provider** グループで、次のフィールドに入力します。
  - 「Friendly Name」: プロバイダーの任意の名前を入力します (例: 「be304qf4BE」)。
  - 「Provider Id」: (読み取り専用) この値は自動的に生成されます。AudioCodes に提供してください。
  - 「Sender email address from which actionable emails will originate」: アクション アイテムメールの送信元となる MIA のメールアドレス (AudioCodes により提供) を入力します。
  - 「Target URLs」: ユーザーがアクション アイテムメールで DONE をクリックしたときに呼び出される URL (AudioCodes によって提供) を入力します。
5. **Scope of submission** グループで、**Organization** オプションを選択します。
6. **Additional information** グループで、通知先の他の人の電子メールアドレスを入力し、この電子メール通知のメッセージを入力します。
7. 利用規約に同意し、**Save** をクリックします。

## 16 Meeting Insights データセキュリティについて



ネットワーク内のセキュリティ製品 (ファイアウォールなど) が Meeting Insights の正しい動作を妨げないことを確認してください。スキャンと操作から除外するには、サービスの FQDN と IP アドレスを適切なホワイトリストに追加します。

- **暗号化:**保存時 (256 ビット AES) および転送時 (256 ビット SSL/TLS 1.2 以降)
- **Azure Open AI データのプライバシー:** LLM のトレーニングにデータは使用されません (Azure Open AI セキュリティ)
- **GDPR、CCPA、CPRA:** 準拠
- **保持ポリシー:**顧客の設定に応じた自動データ保持ポリシー
- **アプリケーション アクティビティ:**ユーザーアクティビティの監査証跡
- **開発:** OWASP に準拠した安全なソフトウェア開発手法
- **ISO-27001 および ISO27032:** 認定
- **データセキュリティ:**
  - 保存時に暗号化 (ディスクとストレージの暗号化)
  - 転送中に暗号化された HTTPS 接続
- **プラットフォーム/ホスティングのセキュリティ:**
  - MSFT セキュリティおよびコンプライアンスの推奨事項に従った Azure サブスクリプション
- **アプリケーション セキュリティ:**
  - マネージド ID コンポーネント間認証
  - Imperva Incapsula – Web アプリケーション セキュリティ、DDoS 緩和など
- **認証:**
  - Microsoft Entra ID、Teams SSO

このページは意図的に空白のままになっています。

**AudioCodes 本社**

6 Ofra Haza Street  
Naimi Park  
Or Yehuda, 6032303, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Rd  
Piscataway, NJ 08854, USA  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

お問い合わせ: <https://www.audiocodes.com/corporate/offices-worldwide>

Web サイト: <https://www.audiocodes.com/>

ドキュメントのフィードバック <https://online.audiocodes.com/documentation-feedback>

©yyyy AudioCodes Ltd. AudioCodes、AC、HD VoIP、HD VoIP Sounds Better、IPmedia、Mediant、MediaPack、What's Inside Matters、OSN、SmartTAP、User Management Pack、VMAS、VoIPerfect、VoIPerfectHD、Your Gateway To VoIP、3GX、AudioCodes One Voice、AudioCodes Meeting Insights、および AudioCodes Room Experience は、AudioCodes Limited の商標または登録商標です。その他すべての製品または商標はそれぞれの所有者の財産です。製品の仕様は予告なく変更される場合がございます。

文書番号: LTRT-12764

