

Office365 OAuthを使用したWebex Connectメールアプリの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ1:Webex Connectでメールアプリの設定を開始します。](#)

[手順2: Microsoft Azureでアプリを作成する](#)

[ステップ3:Office365でメールボックスユーザーを構成します](#)

[ステップ4:Webex Connectで電子メールアプリケーションを設定する](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、オープン認証(OAuth 2.0)を使用してOffice 365の電子メールアプリケーションを設定する手順について説明します。

著者 : Cisco TACエンジニア、Andrius SuchankaおよびBhushan Suresh

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Webex Contact Center(WxCC)2.0
- 電子メールフローが設定されたWebex connectportal
- MS Azureアクセス
- MS Office 365アクセス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- WxCC 2.0
- Cisco Webex Connect
- Microsoft Azure
- Microsoft Office365

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ 1： Webex Connectでメールアプリの設定を開始する

Webex Connectプラットフォームで電子メールアプリケーションの設定を開始します。

- Webex Connectテナントにログインします。

-[Assets（資産）]->[Apps（アプリ）]に移動し、[Configure New App（新しいアプリの設定）]をクリックして[Email（メール）]を選択します。認証タイプとして[OAuth 2.0]を選択し、後の設定手順で[Forwarding Address]と[Call Back URL]をコピーして保存します。

< Configure New Application - Email
Enter the mail server settings for your account to start sending and receiving emails using Webex Connect.

Asset Name ①
Asset Name

Email ID
Email ID

Forwarding Address
b6b9072db2ce25198b45f08c9a9f Copy

Note: Emails sent to the asset email ID will be forwarded to this address.

Authentication Type
OAuth 2.0

SMTP Server Username

Port Security
None

Client ID Client Secret

Call Back URL
https://[redacted].us.webexconnect.io/callback

Microsoft側での設定に進みます。

ステップ 2： Microsoft Azureでアプリを作成する

Azureポータルにアプリを登録するには、「[Microsoft IDプラットフォームにアプリケーションを登録する](#)」のドキュメントを参照してください。

<https://portal.azure.com>にログインします。

-[Azure Active Directory]に移動し、[アプリの登録]を選択して[新しい登録]をクリックします。

-アプリケーション名を入力し、適切なアカウントタイプを選択し、Webの「リダイレクトURI」をテナント名(手順1で確認した<https://yourwebexconnectname.us.webexconnect.io/callback> as)を入力し、アプリケーションを登録します。

Register an application ...

* Name

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

 ✓

Supported account types

Who can use this application or access this API?

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

[Help me choose...](#)

Redirect URI (optional)

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

 ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

– アプリケーションの登録後、[Authentication]に移動し、[Implicit grand and hybrid flows]まで下にスクロールし、[Access tokens]オプションを選択して保存します。

Search

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication**
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Cisco Systems, Inc only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

⚠ Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes **No**

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock

Save Discard

-[Certificates & secrets]に移動し、[Client Secrets]を選択し、[New client secret]をクリックし、説明と有効期間を追加します。

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add a client secret

Description

Expires

Add Cancel

- クライアントシークレット値をコピーし、後で使用できるように保存します。

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
wxconnect	10/26/2024	L1e8Q~B5rzySjA6wI3PqgNqZkdVd1zpTJ...	5f7981e4-9b3e-43ff-b2cf-297606955fff

-[APIアクセス許可]に移動し、[アクセス許可の追加]をクリックし、[組織で使用するAPI]を選択し、検索フィールドに「office 365」と入力し、[Office 365 Exchange Online]を選択します。[Application permissions]を選択し、[Mail]セクションを展開して[Mail.Send]をオンにし、[Add permission]をクリックします。

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | API permissions

Search

Refresh Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Cisco Systems, Inc

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

office 365
Name
Office 365 Enterprise Insights
Office 365 Exchange Online
Office 365 Information Protection
Office 365 Management APIs
Office 365 SharePoint Online

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. The

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cisco Systems, Inc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Request API permissions

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
Other permissions	
<input type="checkbox"/> full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	
Exchange	
IMAP	
Mailbox	
MailboxSettings	
Mail (1)	
<input type="checkbox"/> Mail.Read Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadWrite Read and write mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.Send Send mail as any user	Yes
Organization	

Add permissions Discard

・ 当該許可を付与した後は、管理者の同意を得ること。[Grant admin consent]をクリックします

All services > Cisco Systems, Inc | App registrations > WebexConnect

WebexConnect | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Cisco Systems, Inc? This will update any existing admin consent records this application already

Yes No

Configured permissions




Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Cisco Systems, Inc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	
Office 365 Exchange Online (1)				
Mail.Send	Application	Send mail as any user	Yes	⚠ Not granted for Cisco S...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

-[Overview (概要)]に移動し、[Application (client) ID(アプリケーション(クライアント)ID)]と[Directory (テナント) ID(ディレクトリ(テナント)ID)]を書き留めて、さらに設定を行います

Search <<  Delete  Endpoints  Preview features

Overview

- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication

Essentials

Display name : [WebexConnect](#)

Application (client) ID : 56ba9bac-67be-4bd2-b551-47258e7ead62


Object ID : 3d6317c3-ed51-4ff2-955d-019ac1637beb




Directory (tenant) ID : 0f47778c-61c2-4b0a-8e94-3f05e737a1dd

Supported account types : [My organization only](#)

注： Azureで、[エンタープライズアプリケーション]の[同意とアクセス許可]の下で、アプリケーションに対するユーザーの同意が許可されていることを確認してください（これは既定の設定です）。

Home > Enterprise applications | Consent and permissions >

 Consent and permissions | User consent settings ...

<<  Save  Discard  Got feedback?

Manage

- User consent settings**
- Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps
All users can consent for any app to access the organization's data.

ステップ 3： Office 365でメールボックスユーザーを構成する

<https://admin.microsoft.com>にログインします。


-Users->Active Usersに移動します。

- Webex Connectと統合するメールボックスを持つユーザを選択します。

- 特定のユーザーを選択した後、[メール]に移動し、[メールアプリ]の[メールアプリの管理]をクリックします。[認証されたSMTP]が選択されていることを確認し、[変更の保存]をクリックします。



John

 [Reset password](#)

[Change photo](#)

[Account](#)

[Devices](#)

[Licenses and apps](#)

Mail

[OneDrive](#)

Mailbox storage

0.01% (5.791MB/50GB)

[Learn more about mailbox storage quotas](#)

Mailbox permissions

[Read and manage permissions \(0\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

Show in global address list

Yes

[Manage global address list visibility](#)

Automatic replies

Off

[Manage automatic replies](#)

Email apps

All apps allowed

[Manage email apps](#)

Email forwarding

Applied

[Manage email forwarding](#)

More actions

[Edit Exchange properties](#)



Manage email apps

Choose the apps where John can access Microsoft 365 email.


- Outlook on the web
- Outlook desktop (MAPI)
- Exchange web services
- Mobile (Exchange ActiveSync)
- IMAP
- Pop
- Authenticated SMTP

Save changes

-[Email Forwarding (メール転送)]で[Manage email forwarding (メール転送の管理)]をクリックし、[Forward all emails sent to this mailbox (このメールボックスに送信されたメールをすべて転送)]を選択し、ステップ1で確認したWebex Connectアプリケーション設定のエイリアスで[Forwarding email address (メール転送アドレス)]に入力し、[Save changes (変更を保存)]をクリックします。



John

 [Reset password](#)

[Change photo](#)

[Account](#)

[Devices](#)

[Licenses and apps](#)

[Mail](#)

[OneDrive](#)

Mailbox storage

0.01% (5.791MB/50GB)

[Learn more about mailbox storage quotas](#)

Mailbox permissions

[Read and manage permissions \(0\)](#)

[Send as permissions \(0\)](#)

[Send on behalf of permissions \(0\)](#)

Show in global address list

Yes

[Manage global address list visibility](#)

Automatic replies

Off

[Manage automatic replies](#)

Email apps

All apps allowed

[Manage email apps](#)

Email forwarding

Applied

[Manage email forwarding](#)

More actions

[Edit Exchange properties](#)



Manage email forwarding

Forward all emails sent to this mailbox

The mailbox owner will be able to view and change these forwarding settings.

Forwarding email address *

a41a0ba3566ed2091155f13e48e6d4f8@mail-us.imiconnect.io

Keep a copy of forwarded email in this mailbox

Save changes

– 外部メールアドレスへの送信メール転送がMicrosoft 365 Defenderポータルで許可されていることを確認します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。