Configurer l'application de messagerie Webex Connect avec Office365 Oauth

Table des matières

Introduction

Ce document décrit les étapes pour configurer une application de messagerie pour Office365 avec une autorisation ouverte (OAuth 2.0).

Contribution d'Andrius Suchanka et de Bhushan Suresh, Ingénieur TAC Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Webex Contact Center (WxCC) 2.0
- Webex connectportal avec flux de messagerie configurés
- Accès MS Azure
- Accès MS Office 365

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

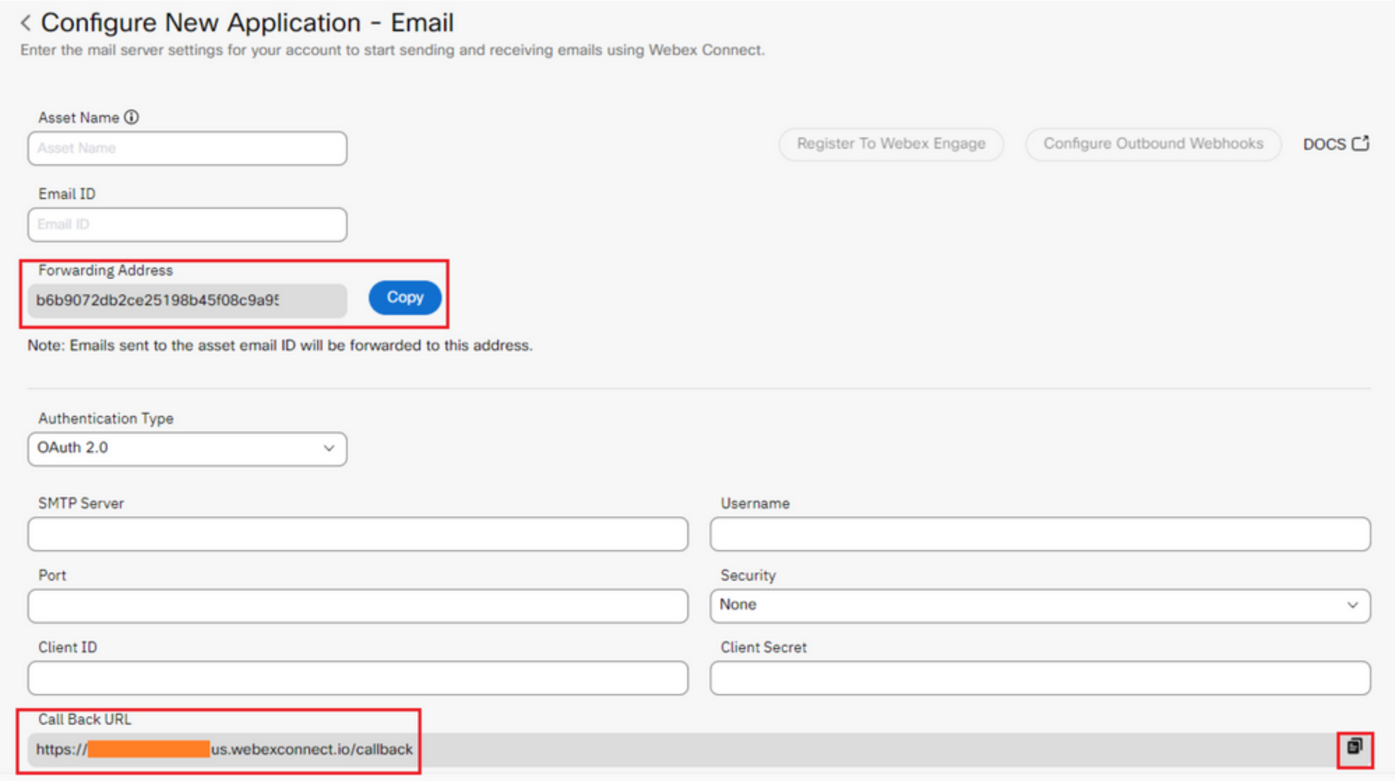
Configurer

Étape 1 : Démarrer la configuration de l'application de messagerie sur Webex Connect

Démarrez la configuration de l'application Email sur la plateforme Webex Connect.

- Connectez-vous à votre client Webex Connect ;

-Accédez à 'Actifs->Applications', cliquez sur 'Configurer une nouvelle application' et sélectionnez 'E-mail'. Sélectionnez « OAuth 2.0 » pour le type d'authentification, copiez et stockez « Forwarding Address » et « Call Back URL » pour les étapes de configuration ultérieures :



< Configure New Application - Email

Enter the mail server settings for your account to start sending and receiving emails using Webex Connect.

Asset Name: Asset Name

Email ID: Email ID

Forwarding Address: b6b9072db2ce25198b45f08c9a9!

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

Passez à la configuration côté Microsoft.

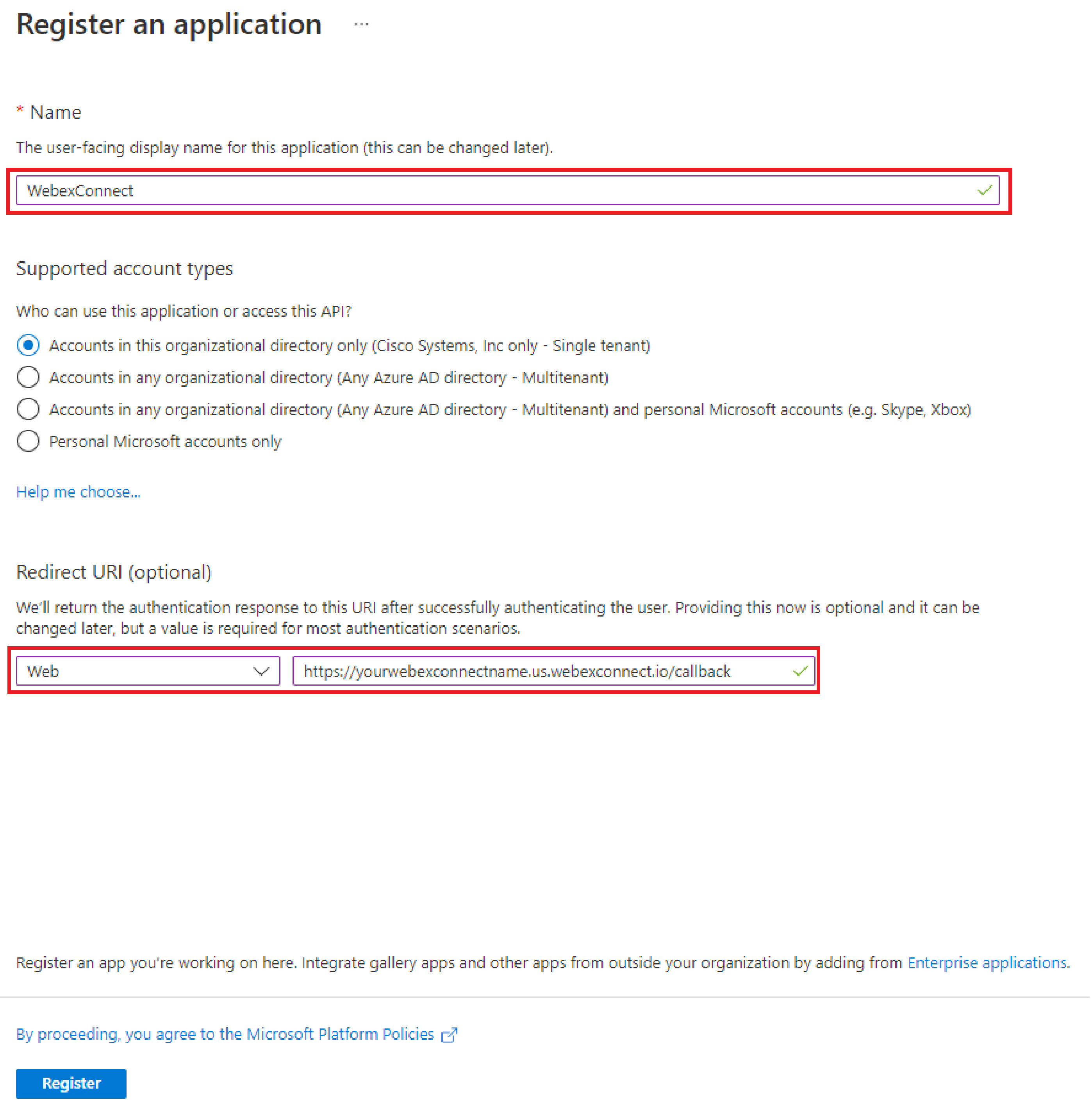
Étape 2 : Créer une application dans Microsoft Azure

Enregistrez une application dans le portail Azure conformément au document '[Enregistrer une application avec la plateforme d'identité Microsoft]'.

-Connectez-vous à [https://portal.azure.com ;]

-Accédez à 'Azure Active Directory', sélectionnez 'Inscriptions d'applications' et cliquez sur 'Nouvelle inscription';

-Fournissez le nom de l'application, sélectionnez le type de compte approprié, entrez l'URI de redirection Web avec le nom de votre locataire (c'est-à-dire https://yourwebexconnectname.us.webexconnect.io/callback as vu à l'étape 1) et enregistrez l'application :



Register an application ···

* Name

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

WebexConnect ✓

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)

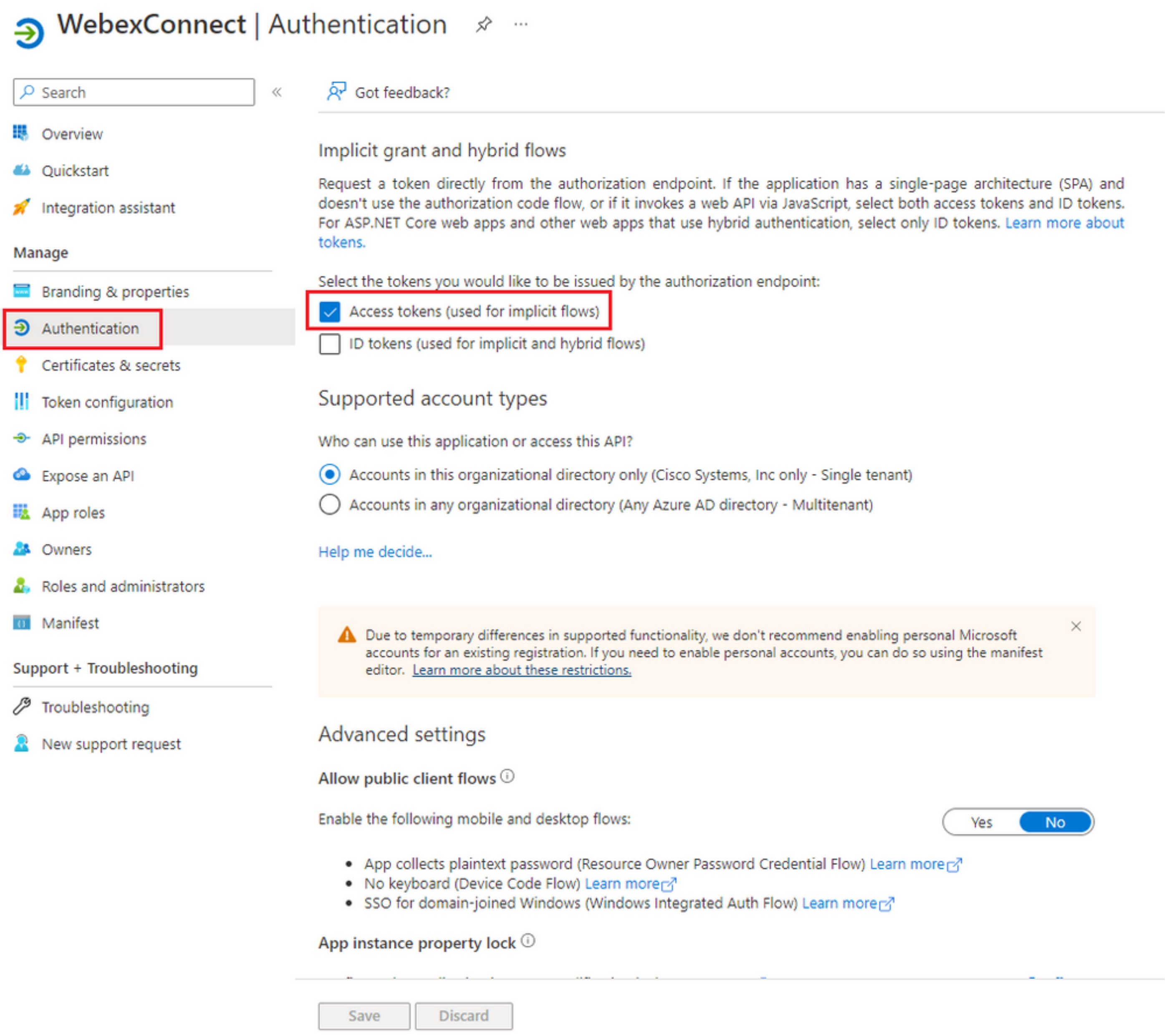
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://yourwebexconnectname.us.webexconnect.io/callback ✓

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

-Après l'enregistrement de l'application - naviguez jusqu'à 'Authentification', faites défiler jusqu'à 'Flux grand et hybride implicites', sélectionnez l'option 'Jetons d'accès' et enregistrez :



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

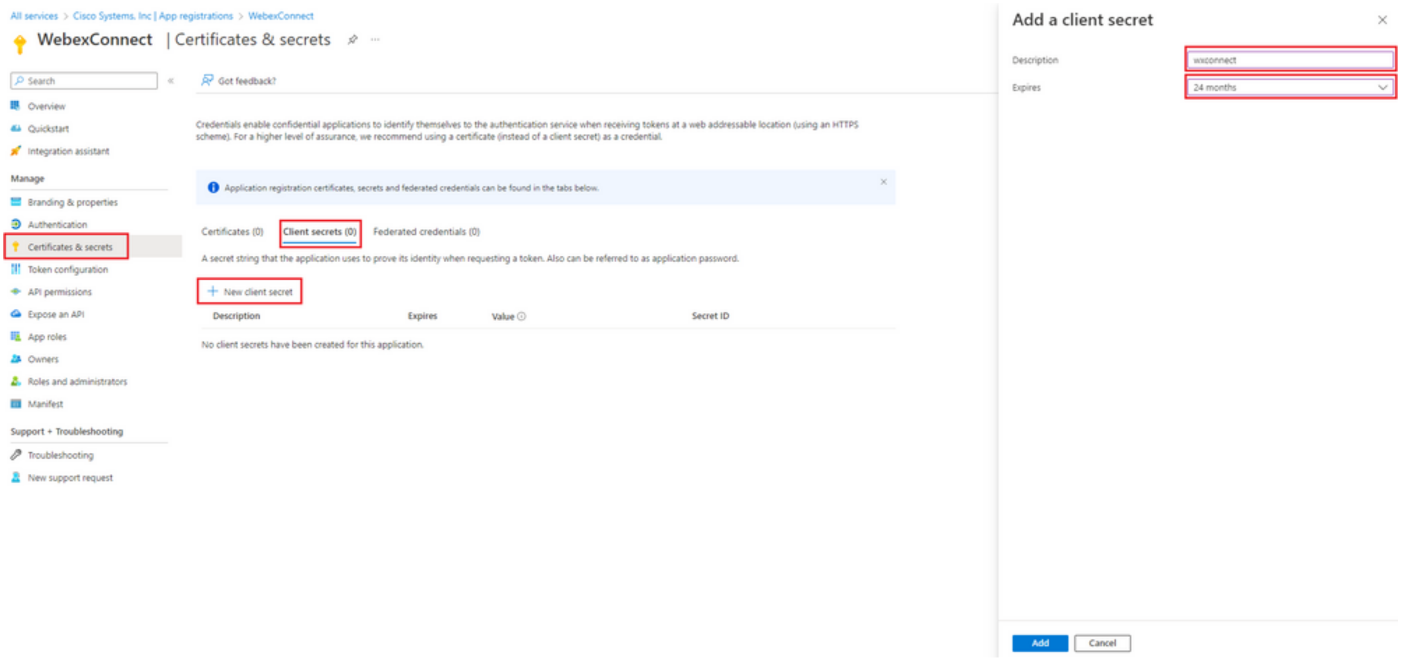
Allow public client flows

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

-Naviguez jusqu'à 'Certificates & secrets', sélectionnez 'Client Secrets', cliquez sur 'New client secret', ajoutez une description et une durée de validité :



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.

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

Description	Expires	Value	Secret ID

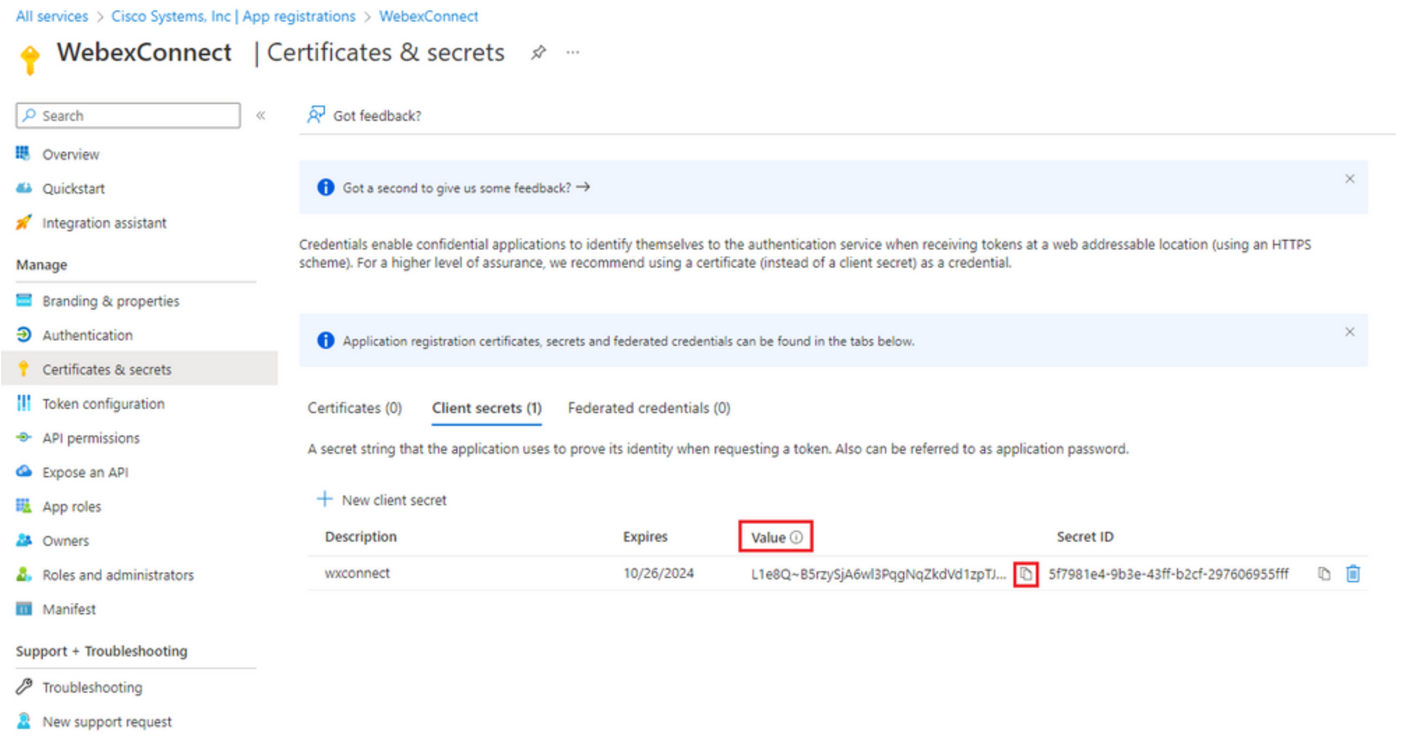
No client secrets have been created for this application.

Add a client secret

Description: wxconnect

Expires: 24 months

-Copiez la valeur secrète du client et stockez-la pour une utilisation ultérieure :



WebexConnect | Certificates & secrets

Got a second to give us some feedback? →

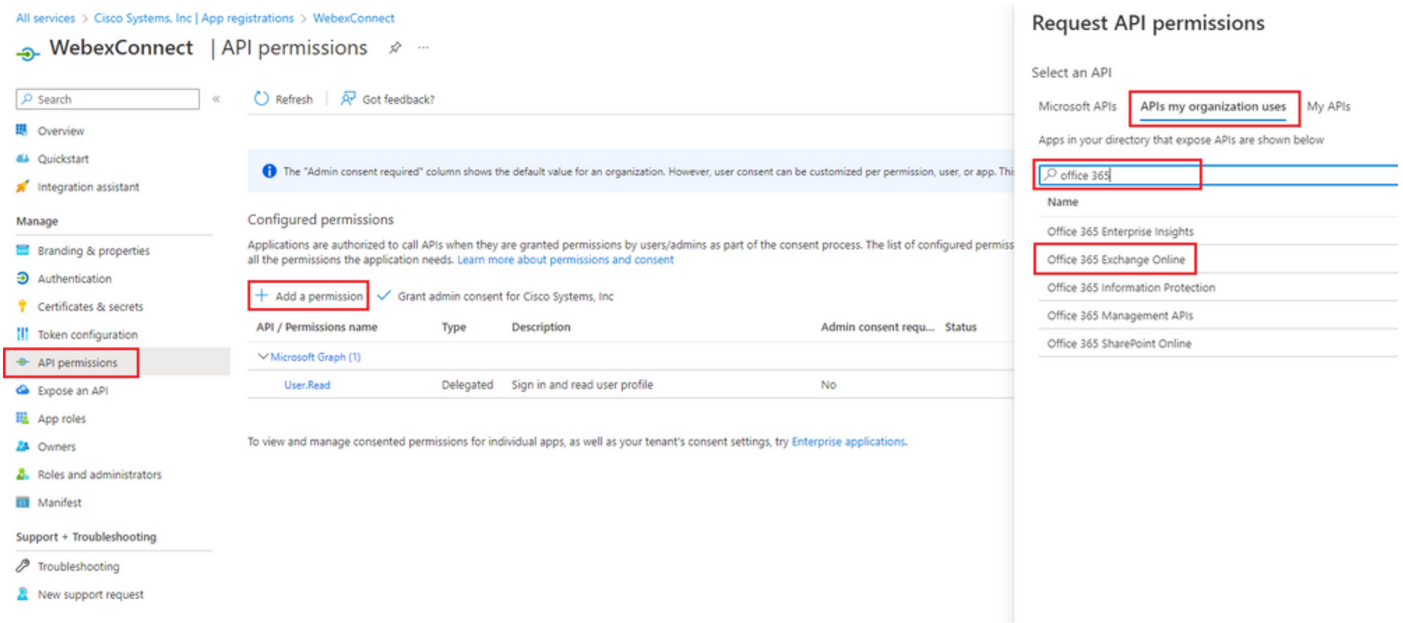
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

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

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

Description	Expires	Value	Secret ID
wxconnect	10/26/2024	L1e8Q~B5rzySjA6wl3PqgNqZkdVd1zpTJ...	5f7981e4-9b3e-43ff-b2cf-297606955fff

- Accédez à « Autorisations API », cliquez sur « Ajouter une autorisation », sélectionnez « API utilisées par mon organisation », dans le champ de recherche « Office 365 » et sélectionnez « Office 365 Exchange Online ». Sélectionnez « Autorisations d'application », développez la section « Courrier », cochez « Courrier.Envoyer » et cliquez sur « Ajouter une autorisation » :



WebexConnect | API permissions

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

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 permiss all the permissions the application needs. Learn more about permissions and consent

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.

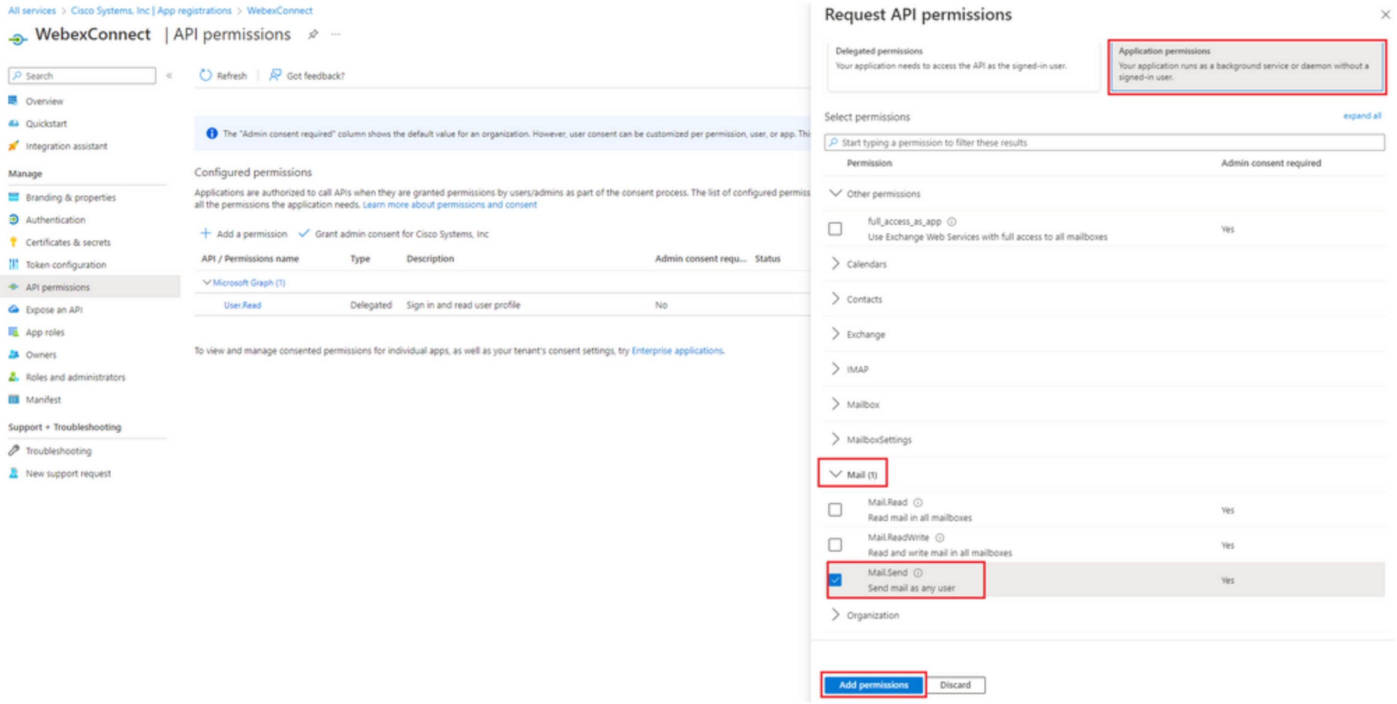
Request API permissions

Select an API

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



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

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 permiss all the permissions the application needs. Learn more about permissions and consent

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.

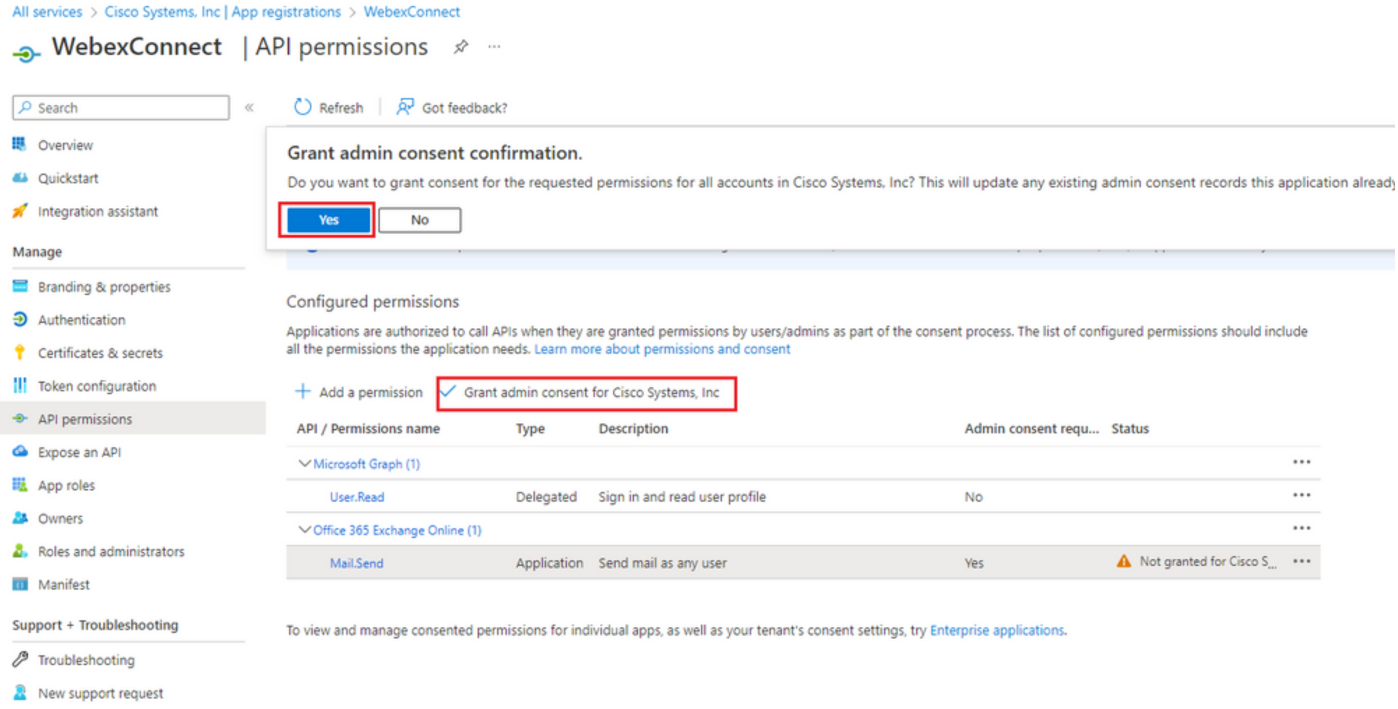
Select permissions

expand all

Start typing a permission to filter these results

Permission	Admin consent required
Other permissions	
□ full_access_as_app Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	
Exchange	
IMAP	
Mailbox	
MailboxSettings	
Mail (1)	
□ Mail.Read Read mail in all mailboxes	Yes
□ Mail.ReadWrite Read and write mail in all mailboxes	Yes
☑ Mail.Send Send mail as any user	Yes
Organization	

-Après l'ajout de cette autorisation, le consentement de l'administrateur doit être accordé. Cliquez sur « Accorder le consentement de l'administrateur » :



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

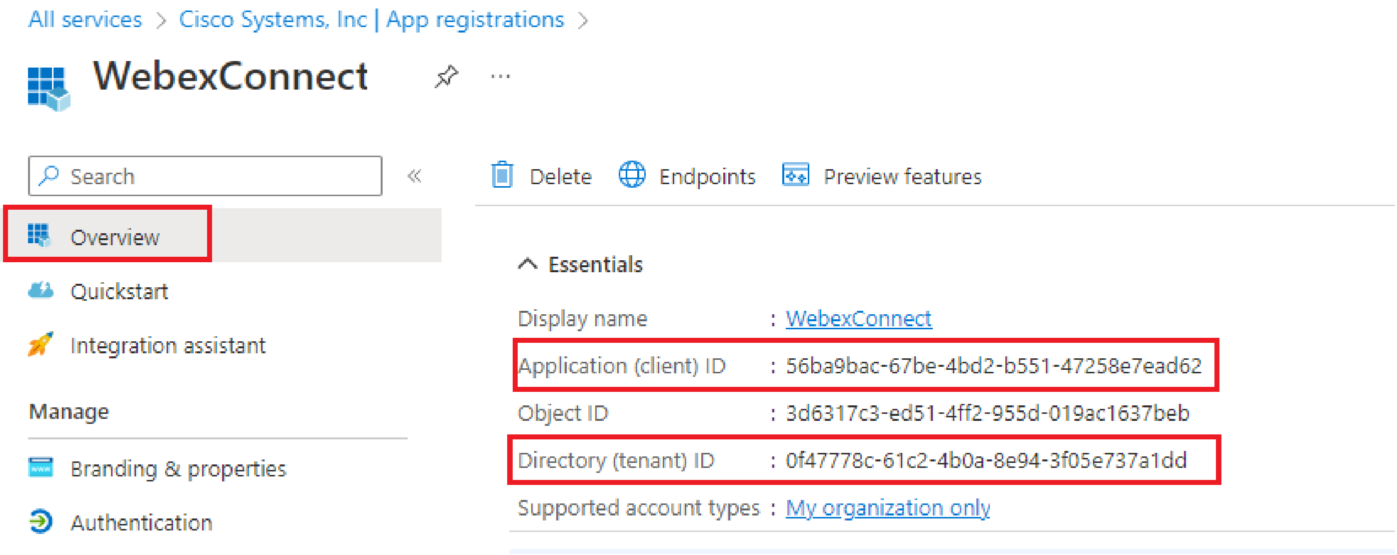
Configured permissions

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

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.

-Accédez à « Vue d'ensemble » et notez « ID d'application (client) » et « ID de répertoire (locataire) » pour une utilisation de configuration supplémentaire :



All services > Cisco Systems, Inc | App registrations >

WebexConnect

Display name : WebexConnect

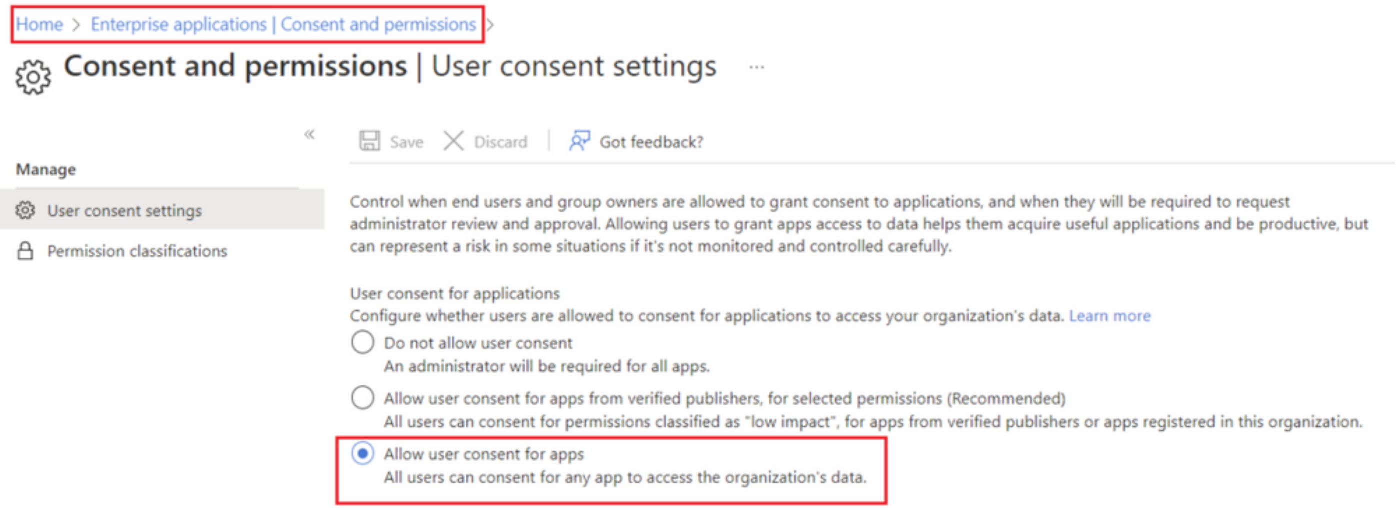
Application (client) ID : 56ba9bac-67be-4bd2-b551-47258e7ead62

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

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

Supported account types : My organization only

Remarque : assurez-vous que le consentement de l'utilisateur pour les applications est autorisé dans Azure sous « Consentement et autorisations » pour « Applications d'entreprise » (il s'agit d'un paramètre par défaut) :



Home > Enterprise applications | Consent and permissions >

Consent and permissions | User consent settings

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.

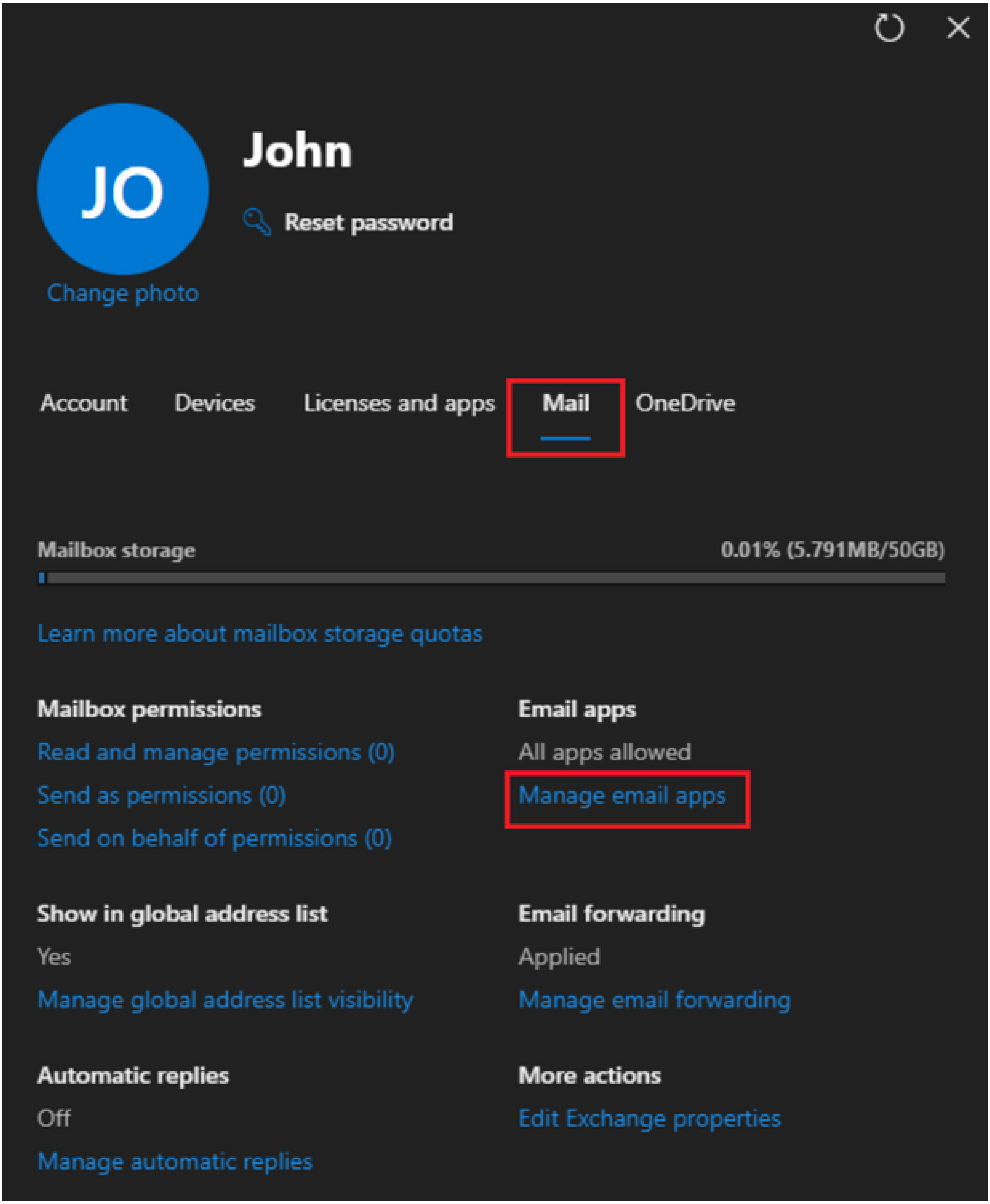
Étape 3 : Configurer l'utilisateur de boîte aux lettres sur Office365

-Connectez-vous à https://admin.microsoft.com ;

-Naviguez jusqu'à Utilisateurs->Utilisateurs actifs ;

-Sélectionnez un utilisateur avec une boîte de messagerie pour l'intégration à Webex Connect ;

-Après avoir sélectionné un utilisateur spécifique, naviguez jusqu'à 'Mail', sous 'Email apps', cliquez sur 'Manage email apps', assurez-vous que 'Authenticated SMTP' est sélectionné et cliquez sur 'Save changes' :



John

Reset password

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)

Email apps

All apps allowed

Manage email apps

Show in global address list

Yes

Manage global address list visibility

Email forwarding

Applied

Manage email forwarding

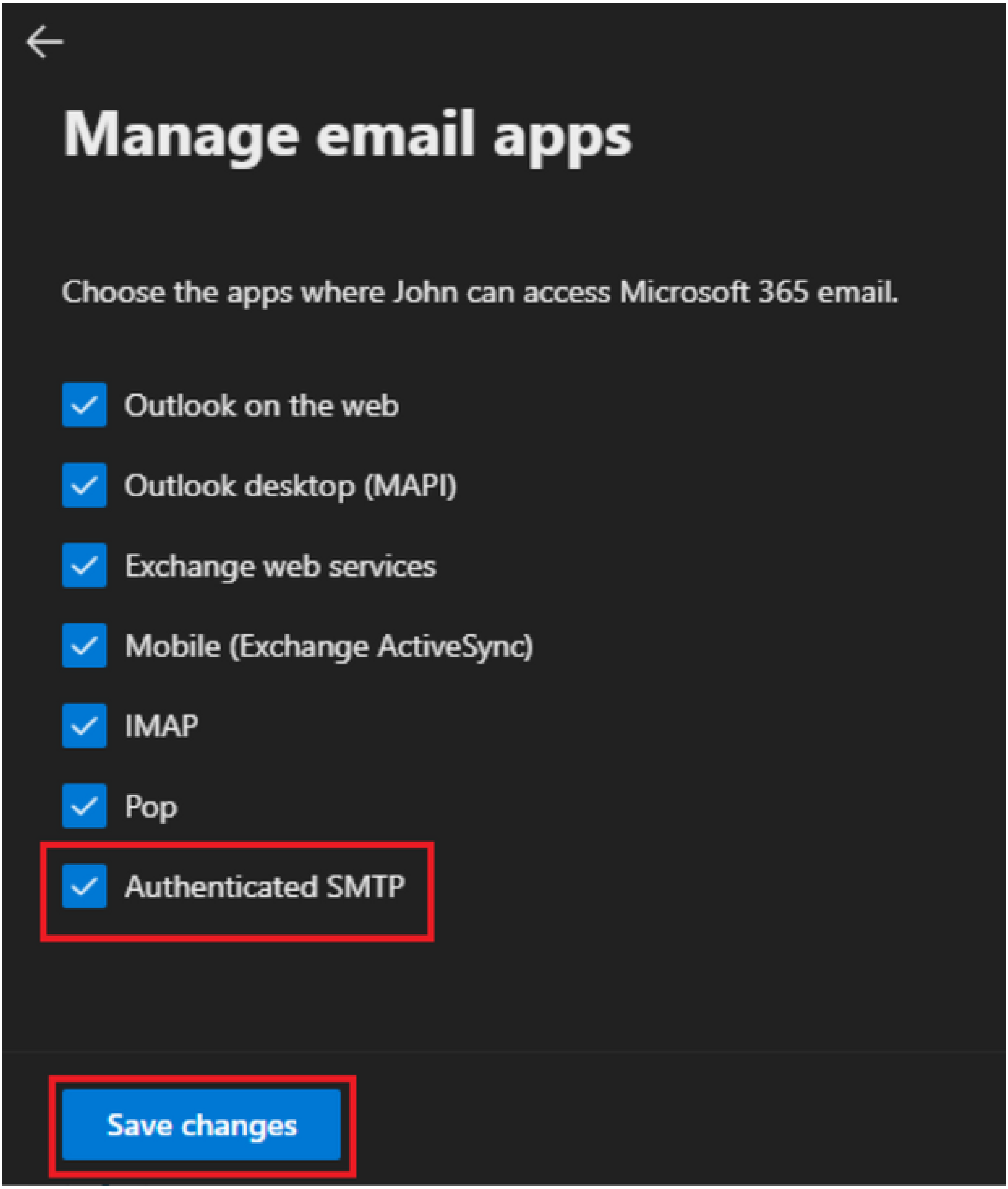
Automatic replies

Off

Manage automatic replies

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

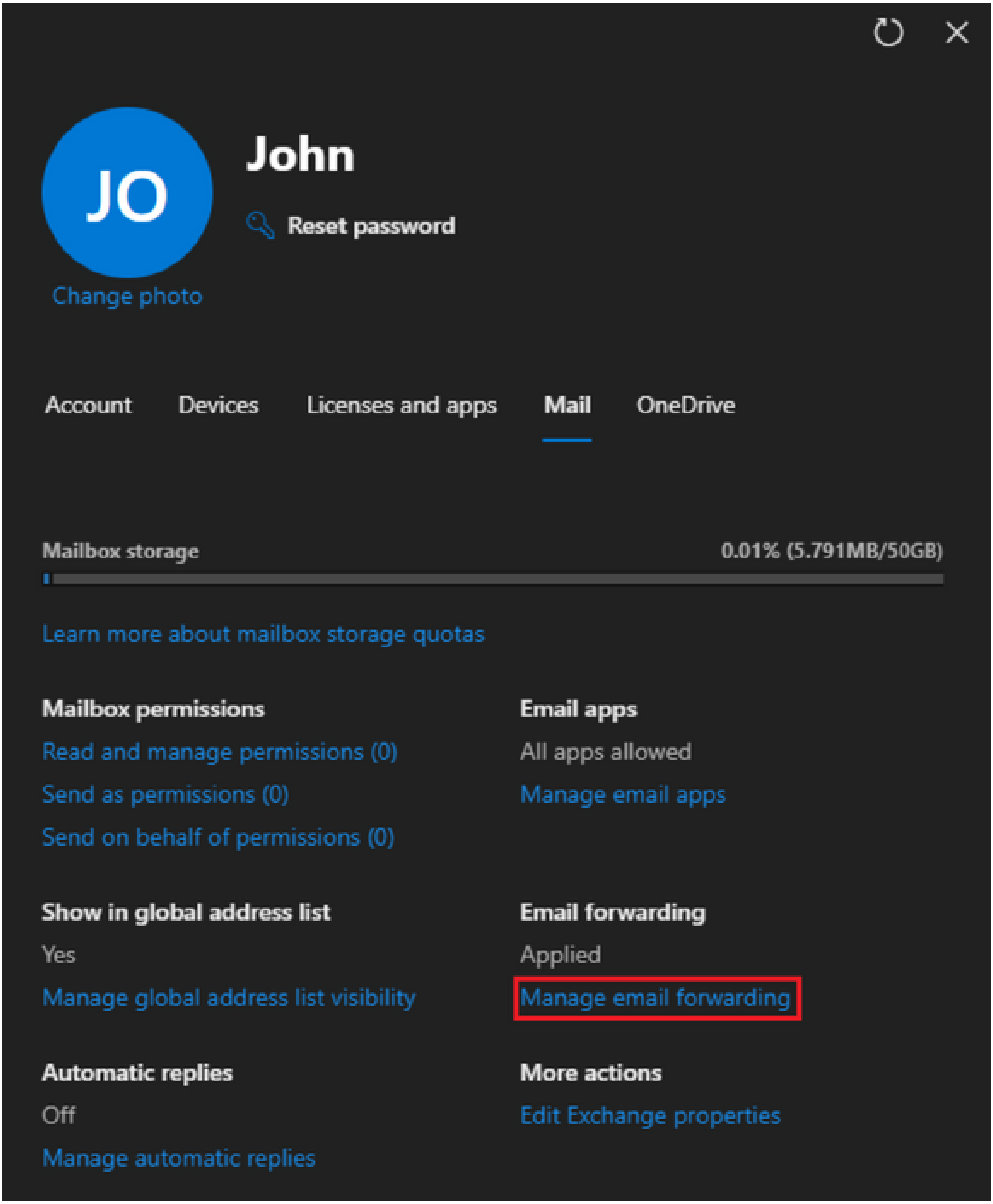
☑ Mobile (Exchange ActiveSync)

☑ IMAP

☑ Pop

☑ Authenticated SMTP

-Sous 'E-mail Forwarding', cliquez sur 'Manage email forwarding', sélectionnez 'Forward all emails sent to this mailbox', remplissez 'Forwarding email address' avec un alias de la configuration de l'application Webex Connect comme indiqué à l'étape 1 (en outre, si nécessaire, sélectionnez 'Keep a copy of forwarding email in this mailbox') et cliquez sur 'Save changes' :



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)

Email apps

All apps allowed

Manage email apps

Show in global address list

Yes

Manage global address list visibility

Email forwarding

Applied

Manage email forwarding

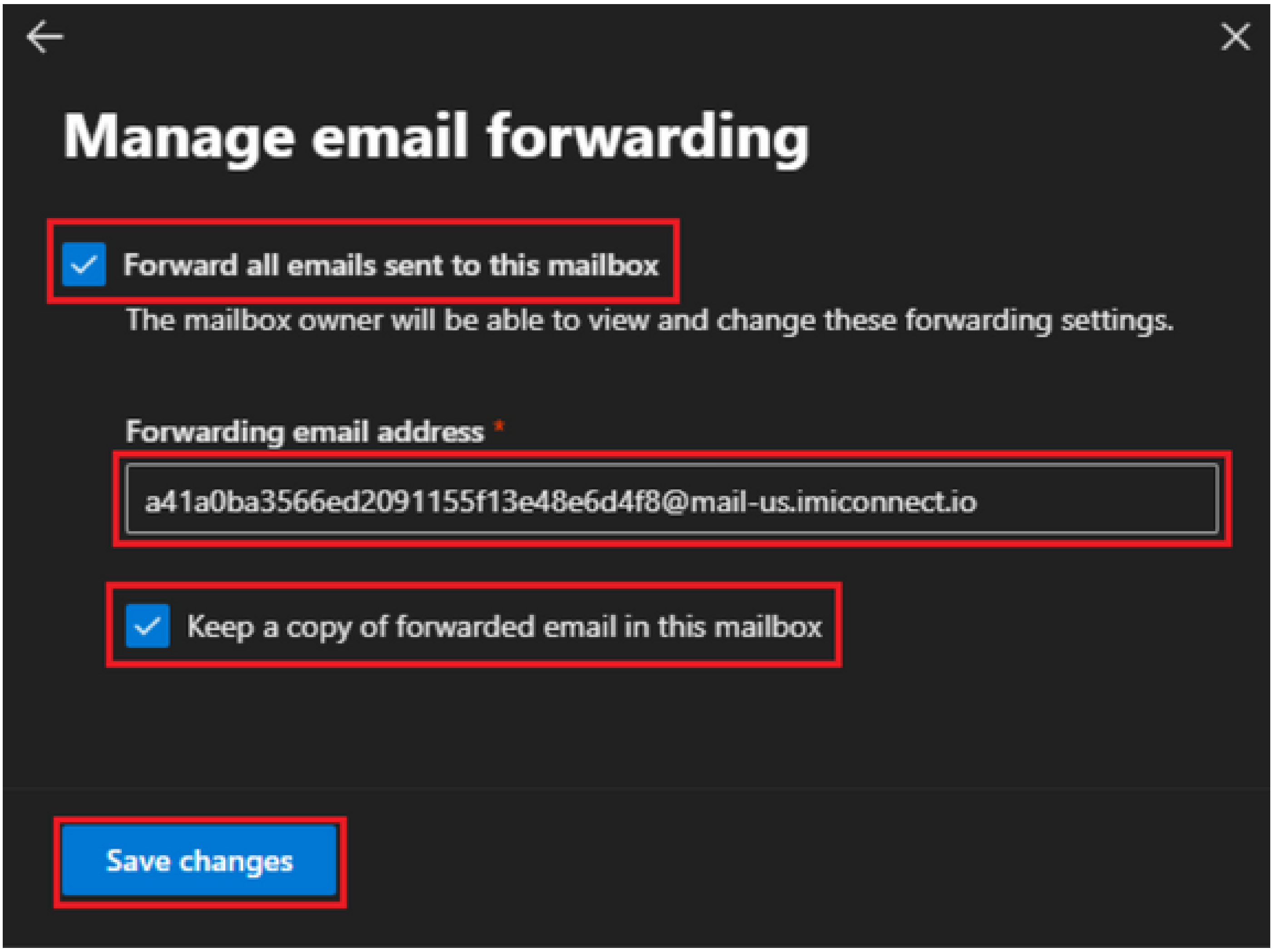
Automatic replies

Off

Manage automatic replies

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

-Assurez-vous que le transfert des e-mails sortants vers des adresses e-mail externes est autorisé dans votre portail Microsoft 365 Defender.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.