

Microsoft O365を使用したEメール暗号化アドインの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Cisco Secure Email Encryption Serviceアドインの導入に関するベストプラクティス](#)

[設定](#)

[Cisco Secure Email Encryption Serviceアドインアプリケーション登録](#)

[Cisco Secure Email Encryption\(CRES\)管理ポータルでのドメインとアドインの設定](#)

[Microsoft 365にマニフェストファイルをアップロードしてEメール暗号化サービスアドインを展開](#)

[確認](#)

[トラブルシューティング](#)

[リレーション情報](#)

はじめに

このドキュメントでは、Microsoft Office 365を介してCisco Eメール暗号化サービスアドインの集中導入を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CiscoセキュアEメールゲートウェイ
- Cisco Secure Email Encryption Service (旧称Cisco Registered Envelope Service)
- Microsoft O365スイート(Exchange、Entra ID、Outlook)

使用するコンポーネント

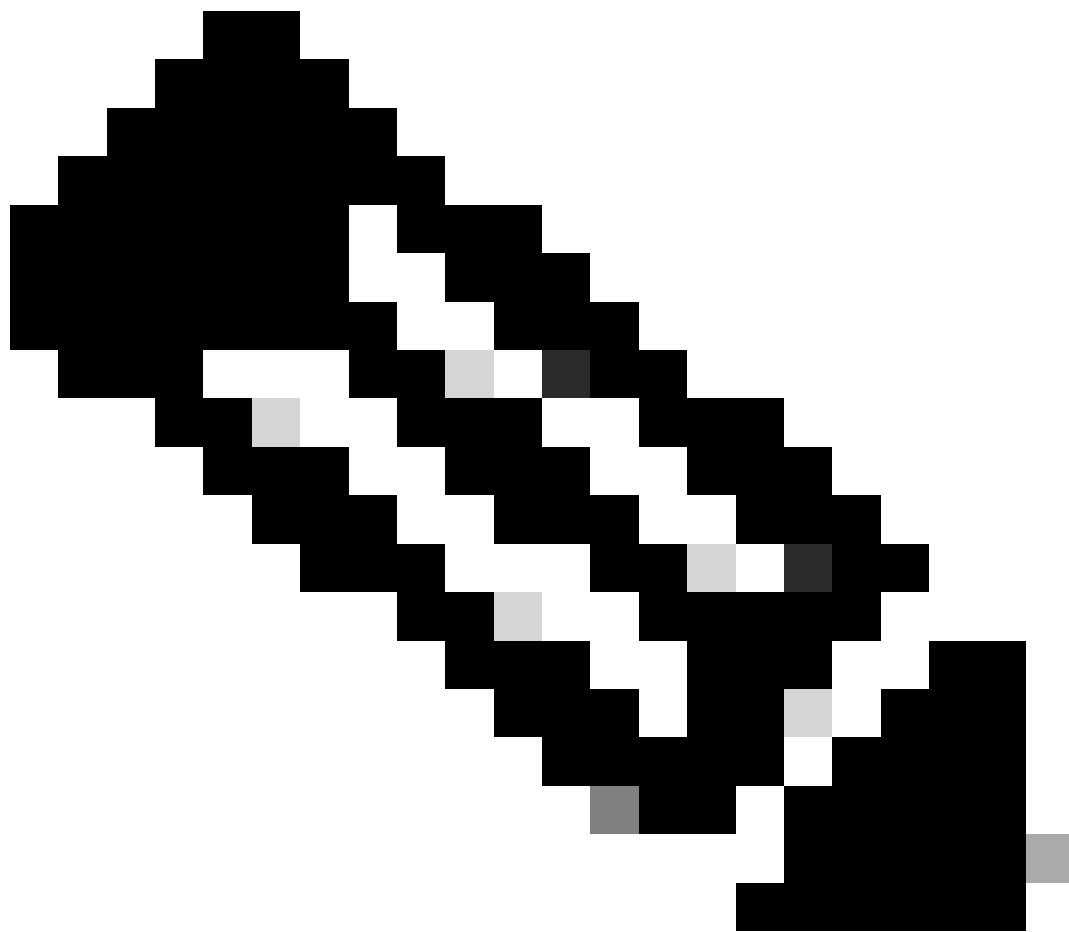
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Eメール暗号化アドイン10.0.0
- Microsoft Exchange Online
- Microsoft Entra ID (以前のAzure AD)
- Outlook for O365 (macOS、Windows)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Secure Email Encryption Serviceアドインを使用すると、エンドユーザはワンクリックでMicrosoft Outlookから直接メッセージを暗号化できます。このアドインは、Microsoft Outlook（WindowsおよびmacOS用）およびOutlook Web Appに展開できます。



注：このドキュメントは、アドインを使用するOffice 365/Microsoft 365サブスクリプションを使用する予定のすべてのエンドユーザに適しており、アドインを使用する予定のすべてのエンドユーザは登録Cisco Secure Email Encryption Service(CES)ユーザです。

Cisco Secure Email Encryption Serviceアドインの導入に関する

ベストプラクティス

- テストフェーズ：部門または部門内の少数のエンドユーザーにアドインを導入します。結果を評価し、成功したら次の段階に進みます。
- パイロットフェーズ：さまざまな部門や部門のエンドユーザーにアドインを導入します。結果を評価し、成功したら次の段階に進みます。
- 実稼働フェーズ：すべてのユーザーにアドインを導入します。

設定

Cisco Secure Email Encryption Serviceアドインアプリケーション登録

1. 少なくとも1人のクラウドアプリケーション管理者([Microsoft 365 Admin Center](#))としてMicrosoft 365 Admin Centerにログインします。
 2. 左側のメニューで展開Admin Centersし、「Identity」をクリックします。
 3. に移動して選択Identity > Applications > App registrationsします New registration.
-
-



注：複数のテナントにアクセスできる場合は、右上のメニューにある設定アイコンを使用して、アプリケーションを登録するテナントに[ディレクトリ+サブスクリプション]メニューから切り替えます。

-
4. アプリケーションの「表示名」を入力し、アプリケーションを使用できるアカウントを選択して、「Register」をクリックします。

Register an application ...

* Name

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

Cisco Secure Email Encryption Add-in

1



Supported account types

Who can use this application or access this API?

2

- Accounts in this organizational directory only (██████████ Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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.

Select a platform



e.g. https://example.com/auth

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

3

アプリケーションの登録

5. 登録が成功したら、Certificates & Secretsでクライアントシークレットを設定するアプリケーションに移動します。組織の法規制に従って有効期限を選択します。

Home > App registrations > Cisco Secure Email Encryption Add-in

Cisco Secure Email Encryption Add-in | Certificates & secrets

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets** 1
 - 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 a token (instead of a certificate 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)** 2 Federated credentials (0)

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

+ New client secret ←

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

Add a client secret ×

Description: 3

Expires: 3

4

クライアントシークレットの設定

6. 登録アプリケーションの概要ページから、Application (client) ID およびDirectory (tenant) IDをコピーします。前の手順で生成した証明書およびシークレットからClient Secret をコピーします。

Home > App registrations >

Cisco Secure Email Encryption Add-in

Search Delete Endpoints Preview features

- Overview**
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously).

Essentials

Display name : [Cisco Secure Email Encryption Add-in](#)

Application (client) ID : [redacted] 4d69-a6b3-787e7f5c85a1

Object ID : d0db75f5-c7ef-4458-a9c2-b07ab89f4b03

Directory (tenant) ID : [redacted] 4298-a0ad-f45d431104d8

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

Enter IDアプリケーションの概要

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
CRES Client Secret	30/04/2025	21-8Q~Wkyy5n6Ozt8VgfWFgePG6.Ukn1...	aa04c890-94d0-4081-8382-8fec90d4505d

クライアントシークレットのコピー

7. 登録済みEメール暗号化アプリケーションに移動し、API permissionsに進みます。Add a permissionをクリックし、必要なMicrosoft Graphアプリケーション権限を選択します。

- メール。読み取り
- メール。読み取り/書き込み
- メール送信
- ユーザー。読み取り。すべて

Request API permissions



< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

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](#)

mail. ←

Permission	Admin consent required
▼ Mail (3)	
<input checked="" type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as any user	Yes

Add permissions

Discard

Microsoft Graph 権限の設定

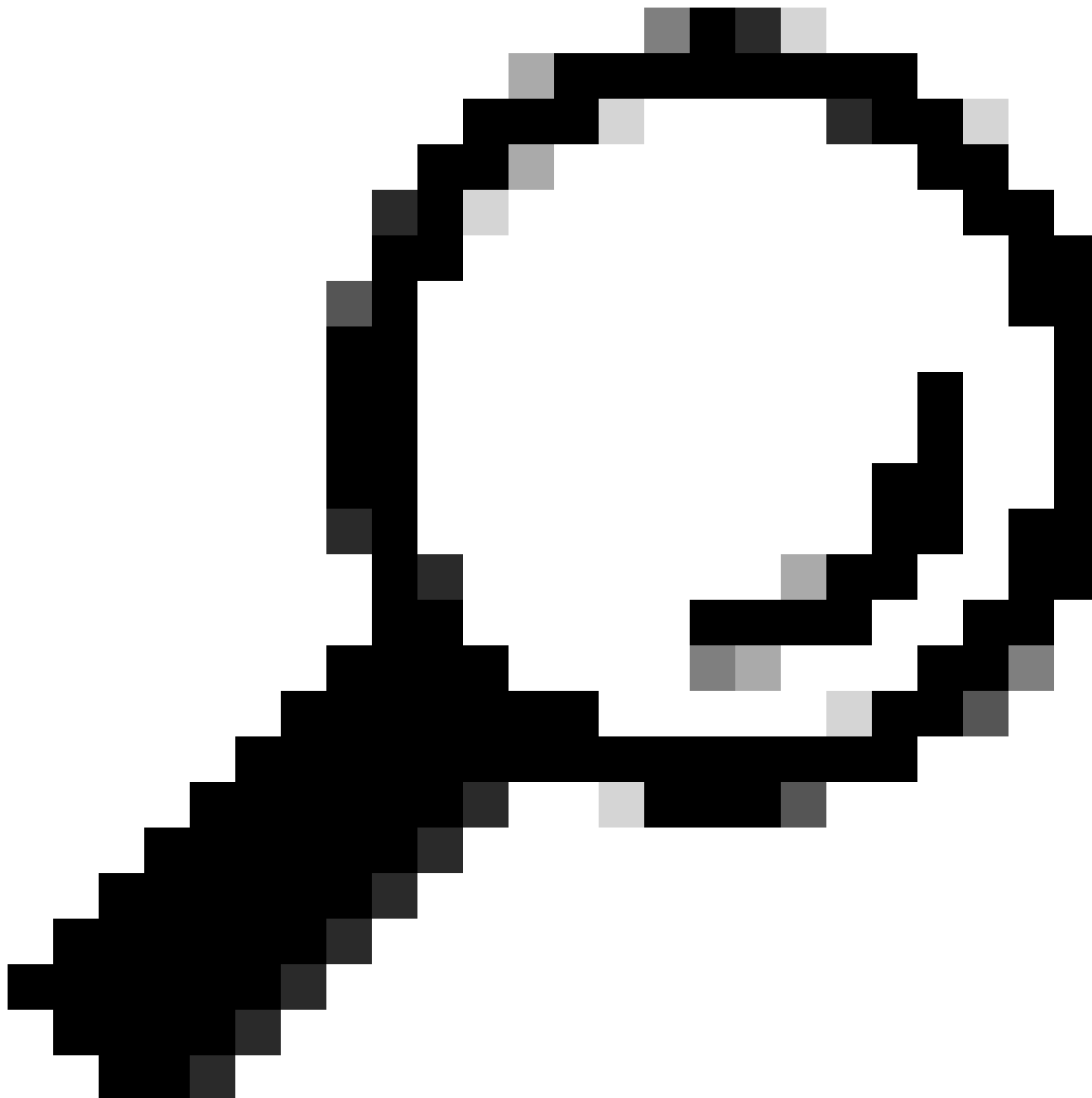
7. 「Grant Admin Consent for <tenant-name>」をクリックして、組織に代わってアプリケーションに権限を付与します。

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (4)				...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for [redacted] ...
Mail.Send	Application	Send mail as any user	Yes	✔ Granted for [redacted] ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for [redacted] ...

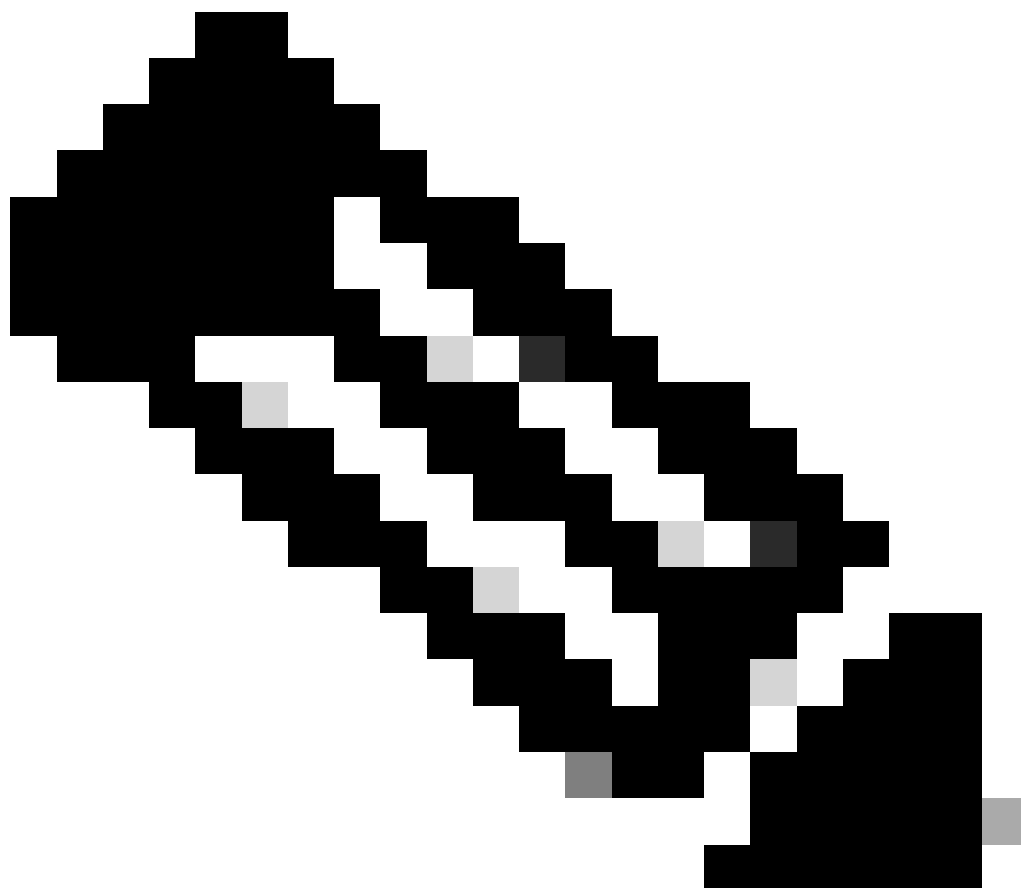
Microsoft Graph API 権限

Cisco Secure Email Encryption(CRES)管理ポータルでのドメインとアドインの設定

1. アカウント管理者としてCisco Secure Email Encryption Service(CRES)管理ポータルにログインします。(https://res.cisco.com/admin)
2. Accounts > Manage Accountsに移動します。組織に割り当てられているアカウント番号、または電子メール暗号化アドインを構成する予定のアカウントをクリックします。
3. に移動しProfiles、「ドメイン」として名前タイプを選択し、「値」の下に電子メール・ドメイン名を入力します。クリック **Add Entries** して5 ~ 10秒間待ちます。(ブラウザのページを更新したり、正常に追加されるまで別のページに移動したりしないでください)。



ヒント：同じ手順を繰り返して、組織でEメール暗号化サービスを使用する他のEメールドメインを追加します。



注:CRES管理ポータルに追加された電子メールアドレスを取得するには、Cisco Technical Assistance Center(TAC)にお問

い合わせください。

Details Groups Tokens Addin Config Rules **Profiles** Branding

Name **Domain** Or other

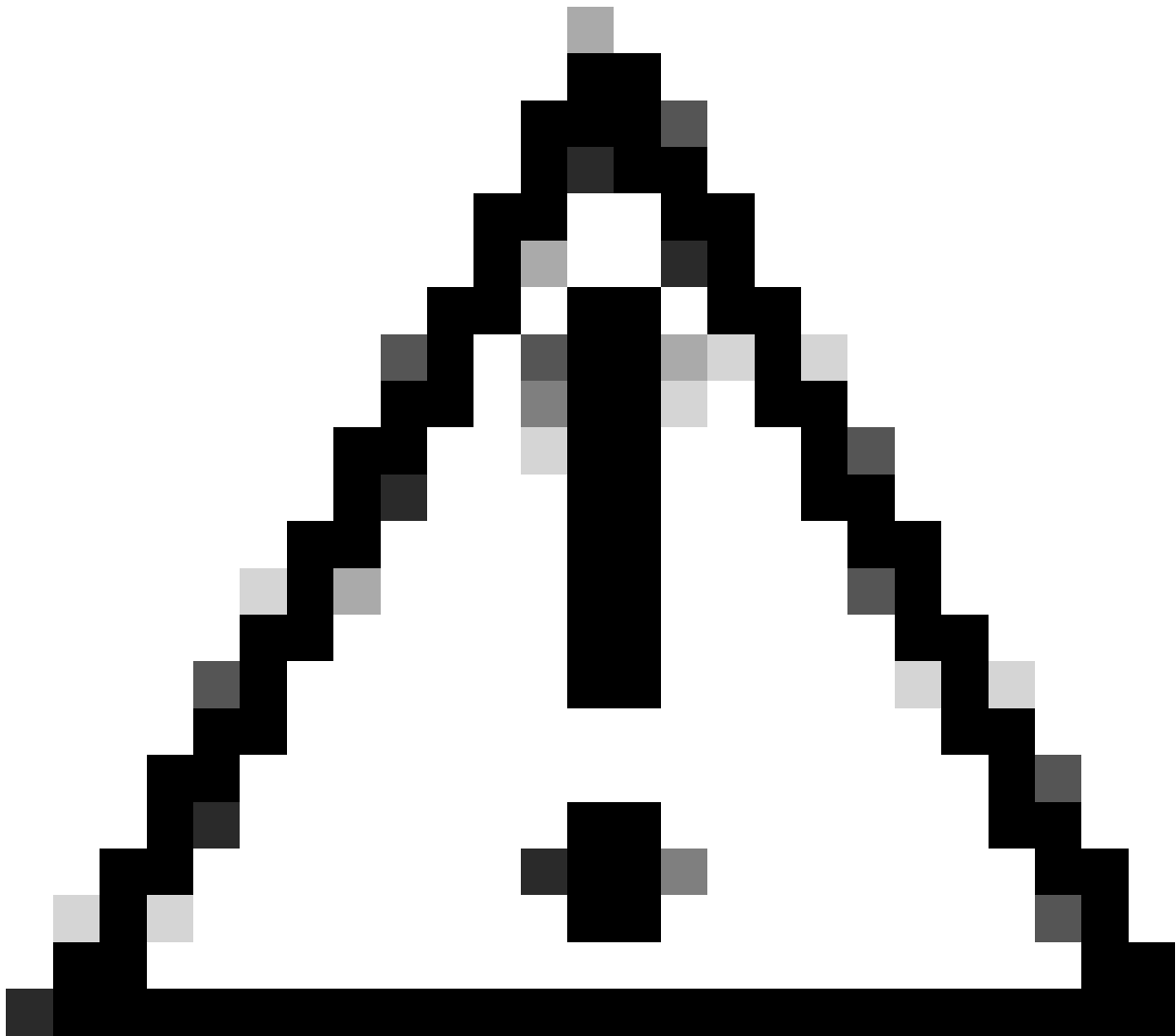
Values (comma or semicolon separated)* **Add Entries**

CRES管理ポータルプロファイル

4.Add-in Configタブに移動します。

ステップ1: Azure ADの詳細の下のEntra IDから取得したテナント、クライアントID、およびシークレットを入力します。をクリックします。Save Details

ステップ2: ドメインと暗号化タイプを選択し、Save Configurationをクリックします。追加したすべてのドメインに同じ設定を適用するには、すべてのドメインでSave Configurationを使用します。



注意：ステップ1.とステップ2.を同時に完了せずに別のページに移動しないでください。ステップ2.が同時に完了しない場合、Azure ADの詳細は保存されません。

ステップ3:Download Manifestをクリックします。

Details Groups Tokens **Addin Config** Rules Profiles Branding Features Migration Security Templates

1

Step 1: Configure the Office 365 Mailbox Settings ?

Azure AD Details: ?

Tenant ID*

Client ID* 2

Client Secret*

3 →

Step 2: Configure the Add-In Settings

Domain 4

Encryption Type 5

Password remembered in Add-In client for days

Flag Type Subject Flag Header Flag

Flag Value

6 →

Step 3: Download the Manifest File to Deploy the Cisco Secure Email Encryption Service Add-In to Your Organization's Users

7 →

CRES管理ポータルアドインの構成

Microsoft 365にマニフェストファイルをアップロードしてEメール暗号化サービスアドインを展開

1. Microsoft 365 Admin Centerに管理者としてログインします。(Microsoft 365管理センター)。

2. に移動しSettings > Integrated apps て、[アドイン]をクリックします。

admin.microsoft.com/Adminportal/Home#/Settings/IntegratedApps

Microsoft 365 admin center

Home > Integrated apps

Integrated apps

Discover, purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners. You can also deploy and manage l For advanced management of these apps go to the respective admin center or page : Azure Active Directory | SharePoint | **Add-ins** 3

Deployed apps Available apps Blocked apps

All apps in this list have been installed for tenant users.

Popular apps to be deployed

- Mural**

With a deep partnership across the Microsoft 365 ecosystem, Mural connects teams to...
- Adobe Acrobat for Mi...**

Do more with PDFs – it's Acrobat built right into popular Microsoft enterprise apps.
- CodeTwo for Outlooc**

Outlook Add-in: Automatic email sign legal disclaimers & marketing banners

View more apps

3. をクリックDeploy Add-inし、Upload Custom Appsを選択します。前の手順I have the manifest file (.xml) on this deviceでCisco Email Encryption Service(ESA)管理ポータルからダウンロードしたファイルを選択し、アップロードします。をクリックします。Upload

4. 次の手順で、Cisco Secure Email Encryption Serviceへのアクセスが必要なユーザを割り当てます。段階的に導入する場合は、を選択Specific Users/groupsし、をクリックDeployします。

Configure add-in



Cisco Secure Email Encryption Service By Cisco

Assign Users

Choose which users will have access to Cisco Secure Email Encryption Service

Everyone

Specific users / groups

Search for specific users or groups to add or remove

Start typing a name to search for users

Just me



Deployment Method

Fixed (Default)

The add-in will be automatically deployed to the assigned users and they will not be able to remove it from their ribbon.

Available

Users may install this add-in by clicking the Get More add-ins button on the home ribbon in Outlook and going to Admin-managed.

Optional

The add-in will be automatically deployed to the assigned users but they can choose to remove it from their ribbon.

2

Deploy

Cancel

After you choose Deploy, the add-in will be available on assigned users' ribbons the next time they open their app.

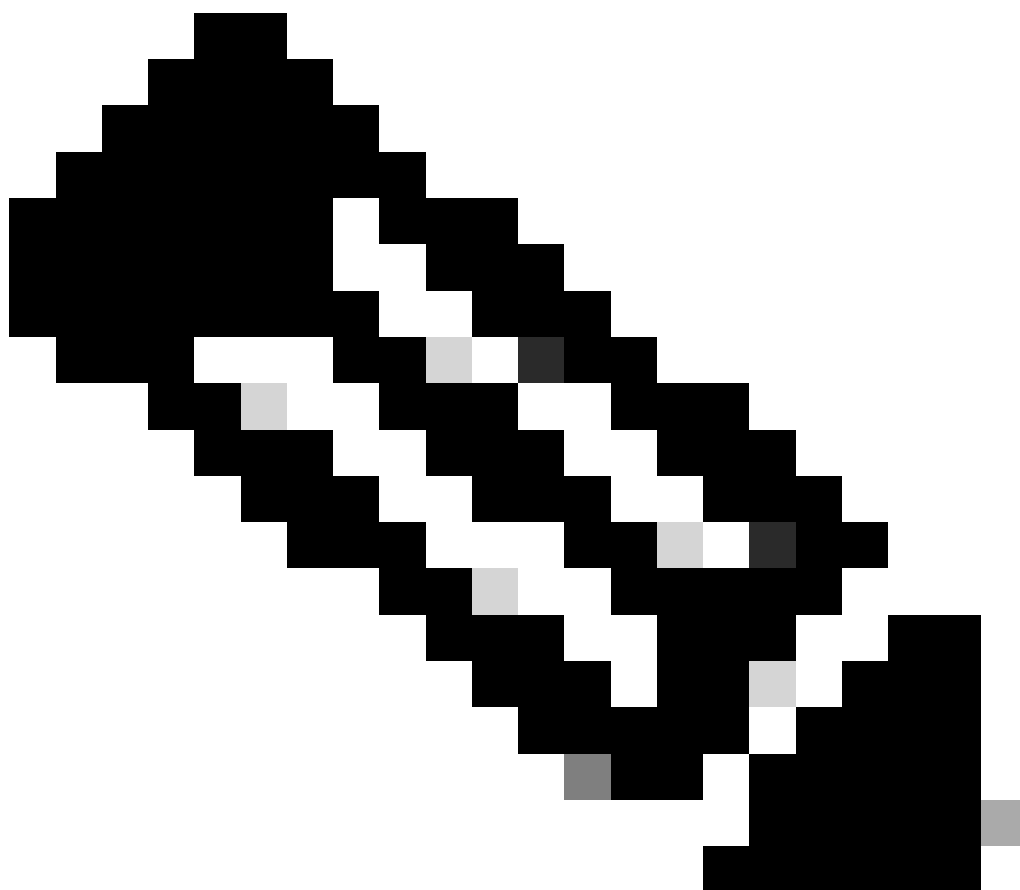
5. アドインが正常に展開されると、エンドユーザーのリボン (Outlookクライアント) に表示されるまでに最大で12時間かかる場

合があります。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. Outlook for Office 365/Microsoft 365またはOutlook Web Appを起動し、暗号化するメッセージを作成し、有効な受信者を少なくとも1人追加します。



注：暗号化の種類（管理者が設定）が[暗号化]の場合は、次の手順に進む前に、メッセージが完了し、有効な受信者が追加されていることを確認してください。ステップ3の後、メッセージは暗号化され、すぐに送信されます。

2. Cisco Secure Email Encryption Service アドインを開いてクリックします。

- Outlook Web Appで、（[送信]ボタンと[破棄]ボタンの近くにある）省略記号アイコンをクリックし、[Cisco Secure Email Encryption Service]をクリックします。
- Outlook for WindowsまたはMacOSで、リボンまたはツールバーの[暗号化]をクリックします。
- MacOSバージョン16.42以降のOutlookで新しいOutlookインターフェイスを使用している場合は、ツールバーの[Cisco Secure Email Encryption Service]をクリックします。

3. クレデンシャルを入力し、Sign inをクリックします。（暗号化タイプがフラグの場合のみ、Sendをクリックします）。

The screenshot displays the Outlook interface during the encryption process. The email header includes the sender 'Udupi Kris...', the recipient 'Udupi...', and the subject 'Testing New Encryption'. A file attachment 'securedoc_2024050...' is shown. The right sidebar features the 'Encryption Flow Summary' with the following steps:

- Encryption Initiated (May 1, 2024; 08:42:48 AM IST)
- Successfully Authenticated (May 1, 2024; 08:42:48 AM IST)
- Message Encrypted (May 1, 2024; 08:42:51 AM IST)
- Message Sent (May 1, 2024; 08:42:51 AM IST)

Red arrows point to the 'Message Encrypted' and 'Message Sent' steps in the summary.

Microsoft Outlook暗号化の状態

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

リリース情報

- [Cisco Secure Email Encryptionサービスアカウント管理者ユーザガイド](#)
- [Cisco Secure Email Encryptionサービスアドインユーザガイド](#)
- [Microsoft Entraアプリケーション登録ガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

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。