

Configurare il componente aggiuntivo Crittografia e-mail utilizzando Microsoft O365

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Procedure ottimali per l'implementazione del componente aggiuntivo del servizio Cisco Secure Email Encryption](#)

[Configurazione](#)

[Registrazione applicazione del componente aggiuntivo del servizio Cisco Secure Email Encryption](#)

[Configurazione delle impostazioni del dominio e dei componenti aggiuntivi sul portale di amministrazione Cisco Secure Email Encryption \(CRES\)](#)

[Carica file manifesto in Microsoft 365 per distribuire il componente aggiuntivo Servizio crittografia e-mail](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni sulla relazione](#)

Introduzione

In questo documento viene descritto come configurare la distribuzione centralizzata del componente aggiuntivo del servizio Cisco Email Encryption tramite Microsoft Office 365.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Gateway
- Cisco Secure Email Encryption Service (in precedenza Cisco Registered Envelope Service)
- Suite Microsoft O365 (Exchange, Entra ID, Outlook)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

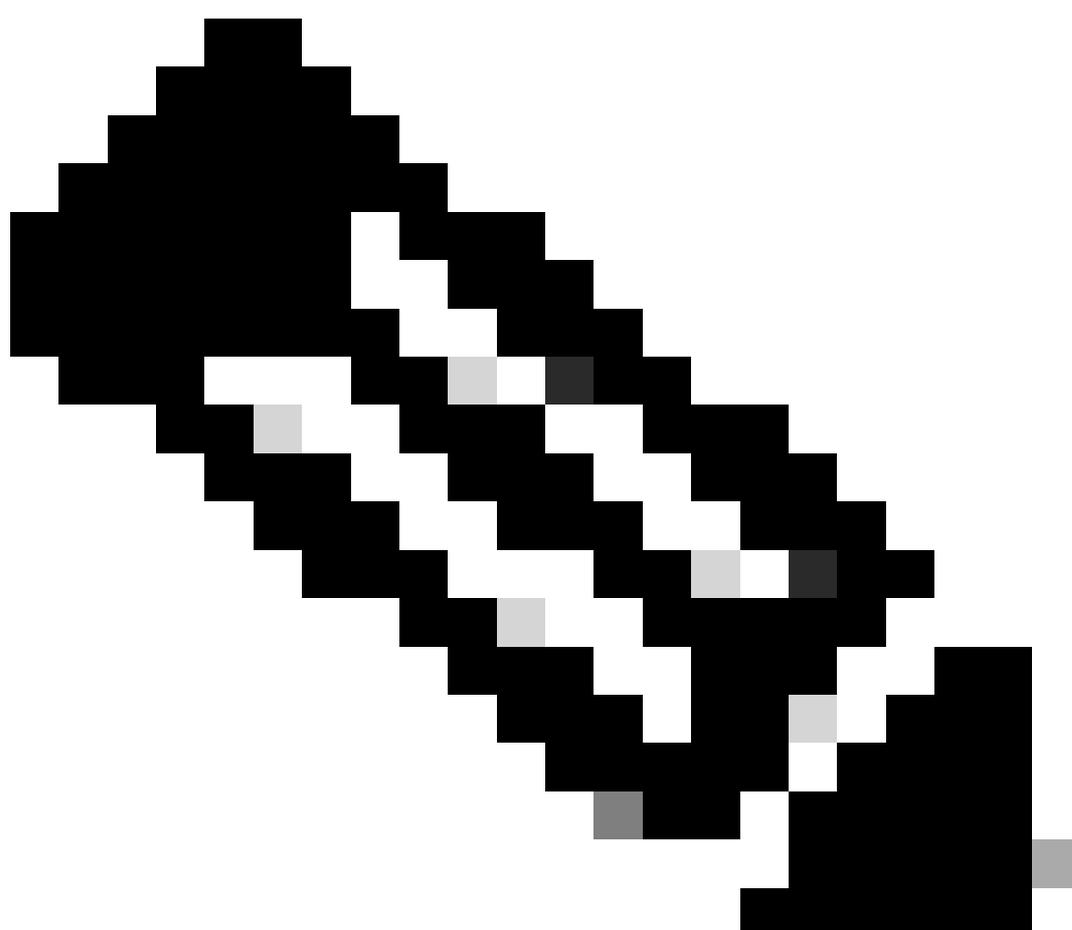
- Cisco Email Encryption Add-in 10.0.0

- Microsoft Exchange Online
- ID Entra Microsoft (in precedenza Azure AD)
- Outlook per O365 (macOS, Windows)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il componente aggiuntivo del servizio Cisco Secure Email Encryption consente agli utenti finali di crittografare i messaggi direttamente da Microsoft Outlook con un semplice clic. Questo componente aggiuntivo può essere distribuito in Microsoft Outlook (per Windows e macOS) e Outlook Web App.



Nota: questo documento è ideale per tutti gli utenti finali che intendono utilizzare il

componente aggiuntivo utilizzando l'abbonamento a Office 365/Microsoft 365 e per tutti gli utenti finali che intendono utilizzare il componente aggiuntivo sono utenti registrati del servizio Cisco Secure Email Encryption.

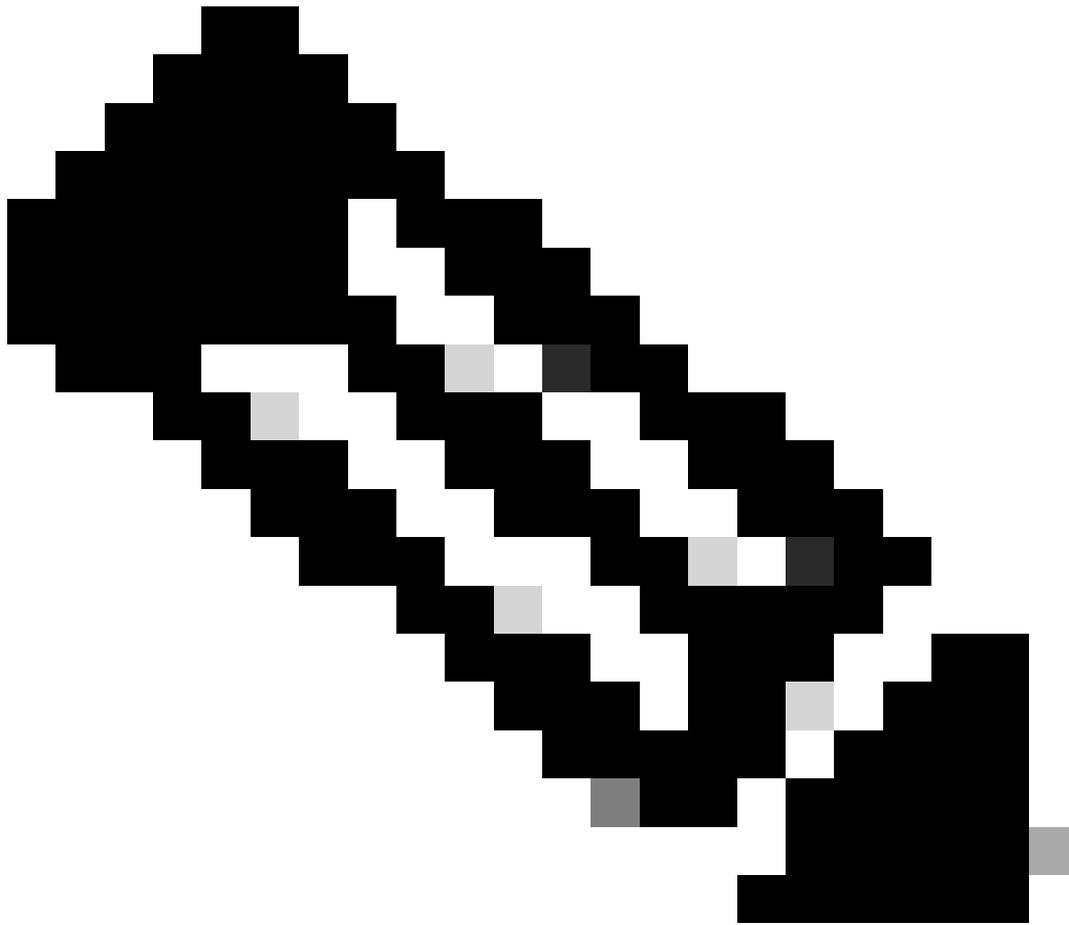
Procedure ottimali per l'implementazione del componente aggiuntivo del servizio Cisco Secure Email Encryption

- Fase di test: distribuzione del componente aggiuntivo a un piccolo gruppo di utenti finali all'interno di un reparto o di una funzione. Valutare i risultati e, se l'esito è positivo, passare alla fase successiva.
- Fase pilota: installazione del componente aggiuntivo per più utenti finali di diversi reparti e funzioni. Valutare i risultati e, se l'esito è positivo, passare alla fase successiva.
- Fase di produzione: distribuire il componente aggiuntivo a tutti gli utenti.

Configurazione

Registrazione applicazione del componente aggiuntivo del servizio Cisco Secure Email Encryption

1. Accedere a Microsoft 365 Admin Center come amministratore di applicazioni cloud ([Microsoft 365 Admin Center](#)).
 2. Nel menu a sinistra, espandere Admin Center e fare clic su Identity.
 3. Passare a Identity > Applications > App registration e selezionare New registration.
-
-



Nota: se si dispone dell'accesso a più tenant, utilizzare l'icona Impostazioni nel menu in alto a destra per passare al tenant in cui si desidera registrare l'applicazione dal menu Directory + Sottoscrizioni.

4. Inserire un nome visualizzato per l'applicazione, selezionare gli account che possono utilizzare l'applicazione e fare clic su Register.

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

Registra applicazione

5. Dopo aver completato la registrazione, passare all'applicazione in cui configurare il segreto client Certificates & Secrets. Scegliere la scadenza in base alla conformità normativa dell'organizzazione.

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

Configura segreto client

6. Dalla pagina Panoramica dell'applicazione registrata, copiare Application (client) ID e Directory (tenant) ID. Copiare il **Client Secret** da Certificati e segreti generati nel passaggio precedente.

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 : ██████████4d69-a6b3-787e7f5c85a1

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

Directory (tenant) ID : ██████████4298-a0ad-f45d431104d8

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

Panoramica dell'applicazione Entra ID

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

Copia segreto client

7. Passare all'applicazione Registered Email Encryption Application e andare a API permissions. Fare clic su Add a permission e selezionare le autorizzazioni necessarie per l'applicazione Microsoft Graph:

- Lettura.Mail
- Mail.ReadWrite
- Invia.posta
- User.Read.All

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
<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](#)

Configurazione autorizzazioni di Microsoft Graph

7. Fare clic su Grant Admin Consent for <tenant-name> per concedere all'applicazione l'accesso alle autorizzazioni per conto dell'organizzazione.

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] ...

Configurazione delle impostazioni del dominio e dei componenti aggiuntivi sul portale di amministrazione Cisco Secure Email Encryption (CRES)

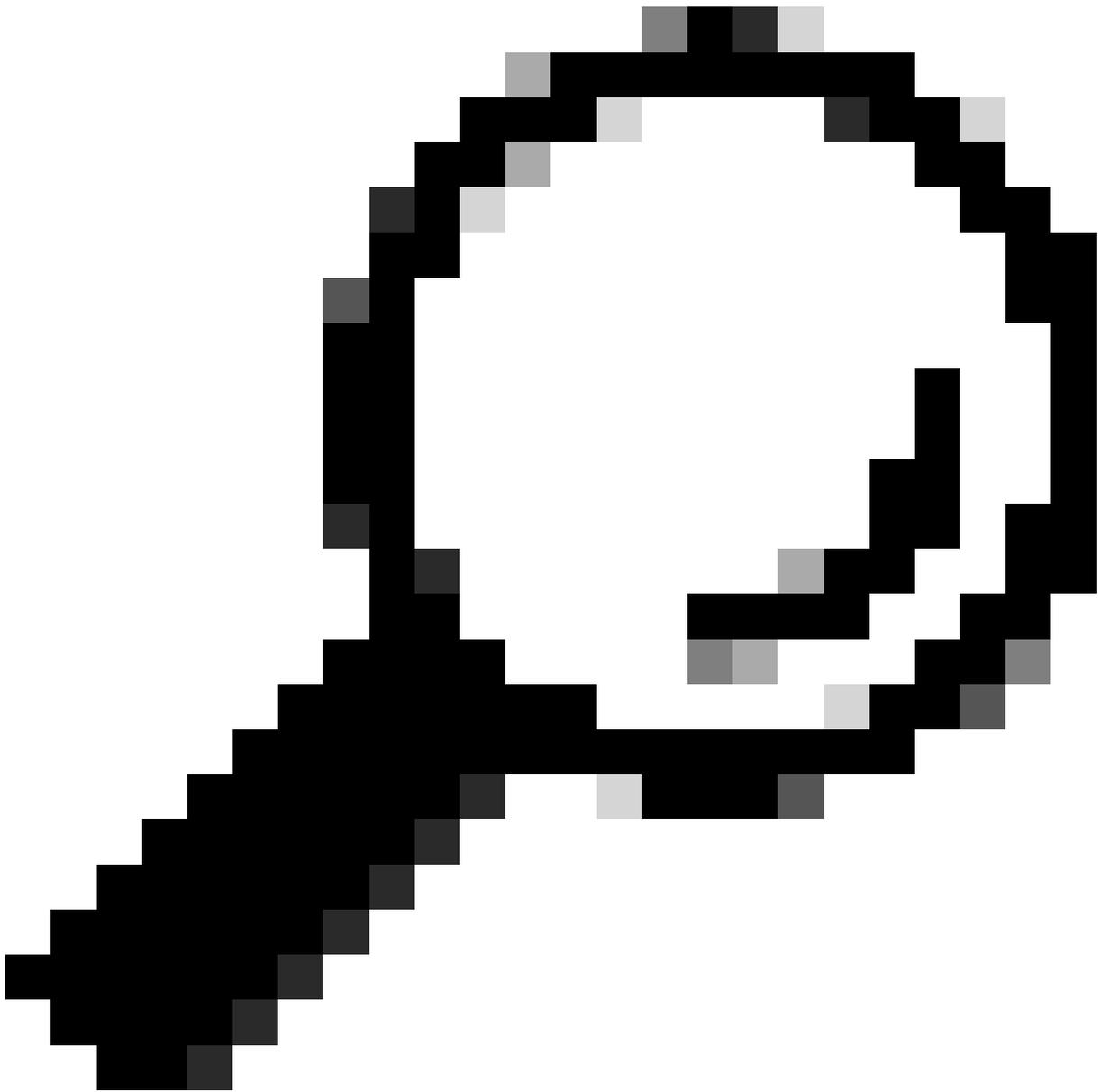
1. Accedere al portale di amministrazione di Cisco Secure Email Encryption Service (CRES) come amministratore di account.

<https://res.cisco.com/admin>

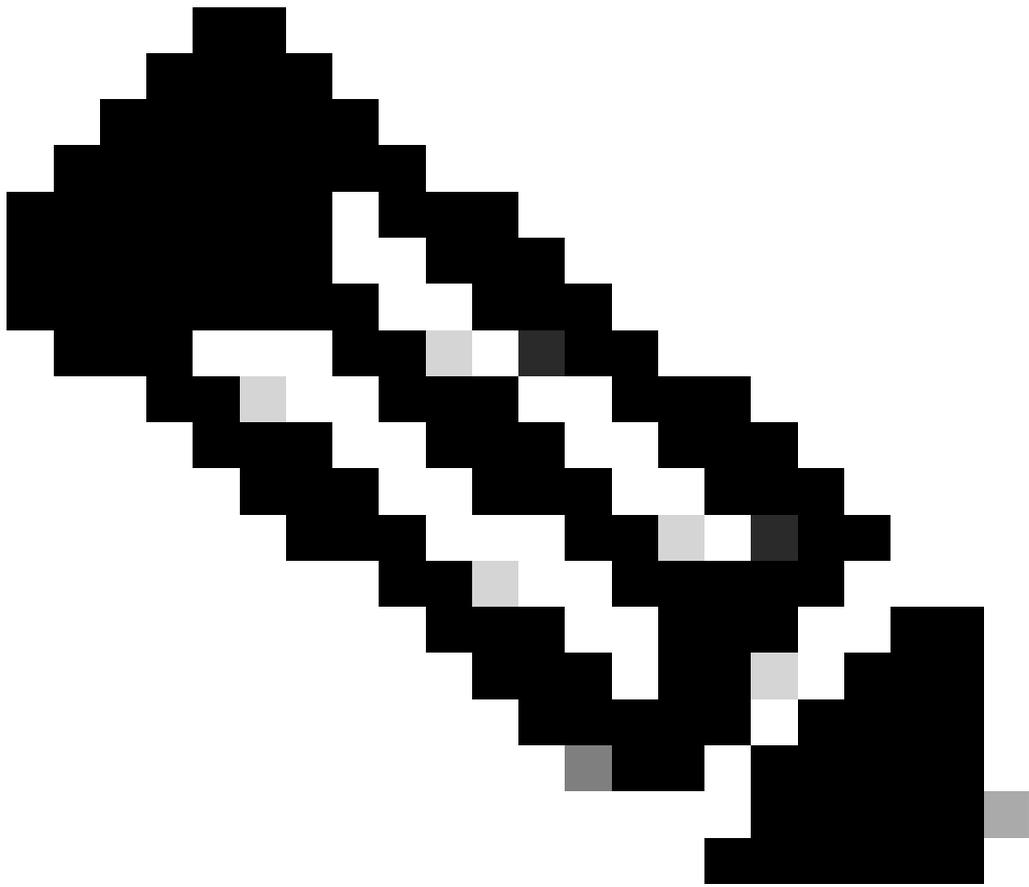
2. Passare a Accounts > Manage Accounts. Fare clic sul numero di account assegnato all'organizzazione o sull'account per il quale si intende configurare il componente aggiuntivo Crittografia e-mail.

3. Passare Profiles a, selezionare il tipo Nome come Dominio e immettere il nome del dominio e-mail in Valori. Fare clic su **Add Entries** e attendere 5-10 secondi. Non aggiornare la pagina del browser o passare a un'altra pagina finché non viene aggiunta correttamente.





Suggerimento: ripetere gli stessi passaggi per aggiungere altri domini e-mail che utilizzeranno il servizio di crittografia e-mail nell'organizzazione.



Nota: per aggiungere i domini e-mail sul portale di amministrazione di CRES, contattare il Technical Assistance Center di Cisco.

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

Name **Domain** Or other

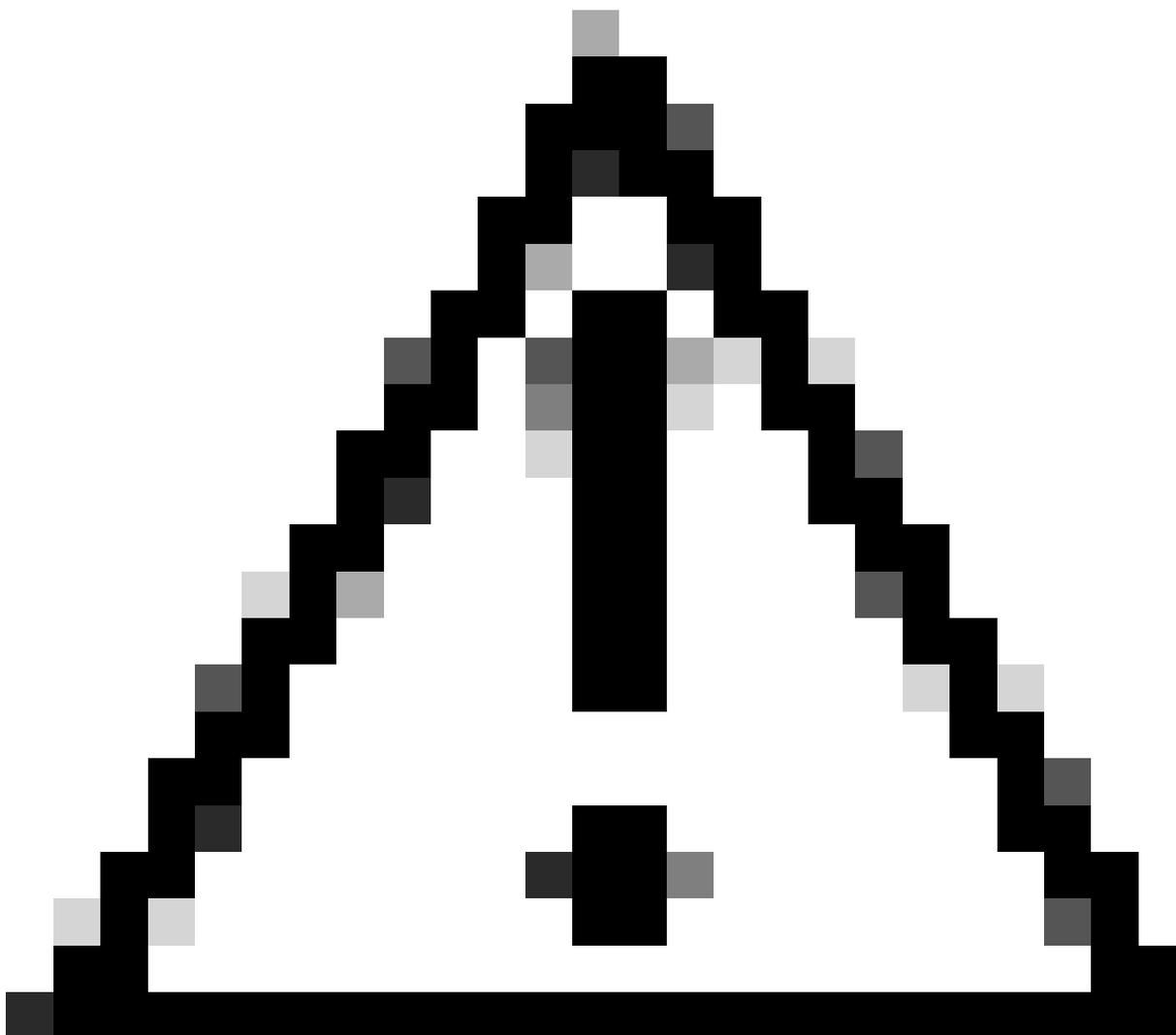
Values (comma or semicolon separated)* **Add Entries**

Profili portale di amministrazione CRES

4. Passare alla Add-in Configscheda.

Passaggio 1: immettere il tenant, l'ID client e il segreto ottenuti dall'ID Entra in Dettagli di Azure AD. Fare clic su .Save Details

Passaggio 2: selezionare il dominio, Tipo di crittografia e fare clic su Save Configuration. Utilizzare Save Configuration per tutti i domini per applicare le stesse impostazioni a tutti i domini aggiunti.



Attenzione: non passare a una pagina diversa senza completare contemporaneamente i passi 1 e 2.. Se il passaggio 2. non viene completato contemporaneamente, i dettagli di Azure AD non verranno salvati.

Passaggio 3: Fare clic su Download Manifest.

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* [redacted] c-a443-4298-a0ad-f45d431104d8

Client ID* [redacted] 6-09a9-4d69-a6b3-787e7f5c85a1 2

Client Secret* [redacted]

3 → Save Details Reset

Step 2: Configure the Add-In Settings

Domain [redacted] onmicrosoft.com 4

Encryption Type Encrypt 5

Password remembered in Add-In client for 30 days

Flag Type Subject Flag Header Flag

Flag Value [redacted]

6 → Save Configuration Save Configuration for All Domains

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

7 → Download Manifest

Configurazione del componente aggiuntivo del portale di amministrazione CRES

Carica file manifesto in Microsoft 365 per distribuire il componente aggiuntivo Servizio crittografia e-mail

1. Accedere a Microsoft 365 Admin Center come amministratore. ([Microsoft 365 Admin Center](#)).

2. Individuare Settings > Integrated apps e fare clic su Componenti aggiuntivi.

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...

Get it now View details
- Adobe Acrobat for Mi...**

Do more with PDFs – it's Acrobat built right into popular Microsoft enterprise apps.

Get it now View details
- CodeTwo for Outlook**

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

Get it now View deta

View more apps

3. Fare clic su Deploy Add-in scegliere Upload Custom Apps. Selezionare I have the manifest file (.xml) on this devicee caricare il file scaricato dal portale di amministrazione del servizio Cisco Email Encryption dal passaggio precedente. Fare clic su .Upload

4. Nella fase successiva, assegnare gli utenti che devono accedere al servizio Cisco Secure Email Encryption. Per una distribuzione in più fasi, scegliere Specific Users/groupse fare clic su Deploy.

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.

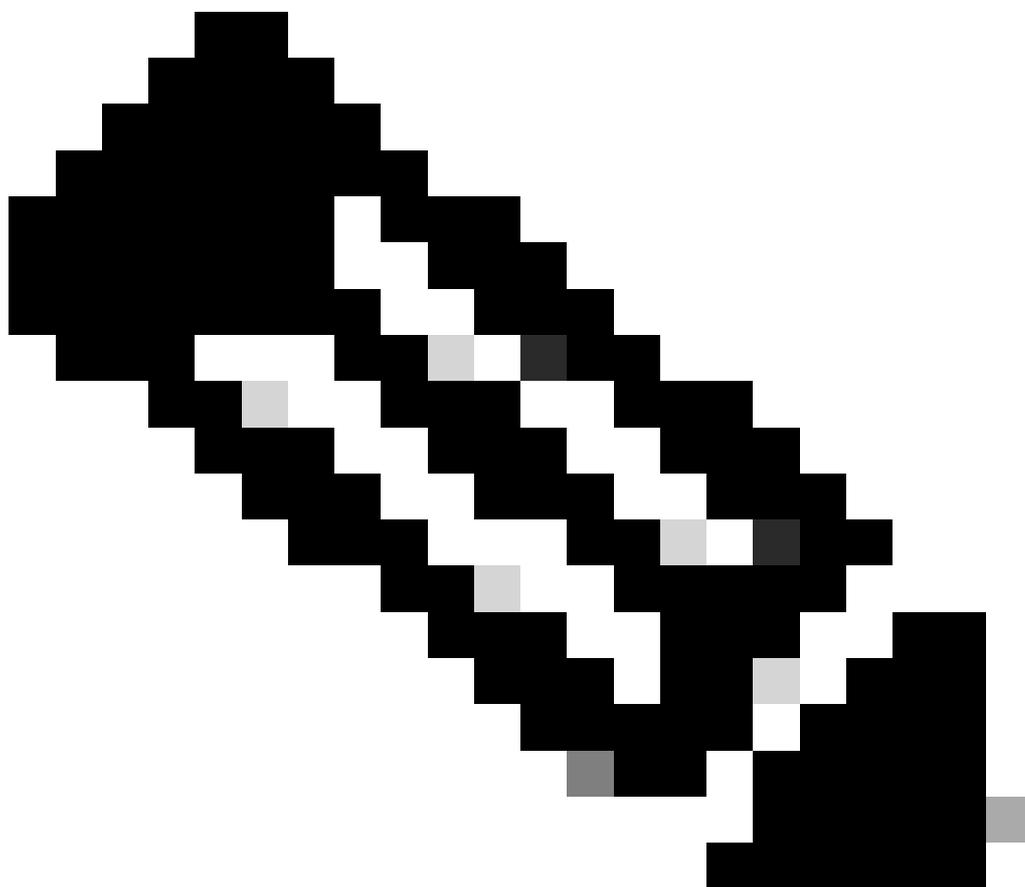
5. Una volta distribuito correttamente, il componente aggiuntivo può impiegare fino a 12 ore per essere visualizzato sulle barre multifunzione

degli utenti finali (client Outlook).

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Avviare Outlook per Office 365/Microsoft 365 o Outlook Web App, comporre il messaggio che si desidera crittografare e aggiungere almeno un destinatario valido.



Nota: se il tipo di crittografia (impostato dall'amministratore) è Crittografia, accertarsi di aver completato il messaggio e di aver aggiunto destinatari validi prima di procedere al passaggio successivo. Dopo il passaggio 3, il messaggio viene crittografato e inviato immediatamente.

2. Aprire/fare clic sul componente aggiuntivo Servizio Cisco Secure Email Encryption.

- In Outlook Web App, fare clic sull'icona con i puntini di sospensione (accanto ai pulsanti Invia e Ignora), quindi fare clic su Cisco Secure Email Encryption Service.
- In Outlook per Windows o MacOS, fare clic su Crittografia dalla barra multifunzione o dalla barra degli strumenti.
- Se si utilizza Outlook per MacOS versione 16.42 o successiva e si utilizza la nuova interfaccia di Outlook, fare clic Cisco Secure Email Encryption Service su dalla barra degli strumenti.

3. Immettere le credenziali e fare clic su Sign in. (Solo se il tipo di crittografia è Contrassegno, fare clic su Send).

The screenshot displays the Outlook interface for an email titled "Testing New Encryption". The sender is "Udupi Kris" and the recipient is "Udupi". A file named "securedoc_2024050..." (141.3 KB) is attached. The email body contains the text: "Hello, This is a test email. Regards". On the right side, the "Cisco Secure Email Encryption" pane is open, showing a notification: "You must use encryption only for business purposes." Below this, the "Encryption Flow Summary" is displayed as a vertical timeline with four steps, each marked with a green checkmark: "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), and "Message Sent" (May 1, 2024; 08:42:51 AM IST). Red arrows point to the "Message Encrypted" and "Message Sent" steps.

Stato crittografia di Microsoft Outlook

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni sulla relazione

- [Guida dell'utente per l'amministratore dell'account del servizio Cisco Secure Email Encryption](#)
- [Guida per l'utente del componente aggiuntivo del servizio Cisco Secure Email Encryption](#)
- [Guida alla registrazione di Microsoft Entra Application](#)
- **[Supporto tecnico Cisco e download](#)**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).