Configurare il componente aggiuntivo Crittografia e-mail utilizzando Microsoft O365

Sommario

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:

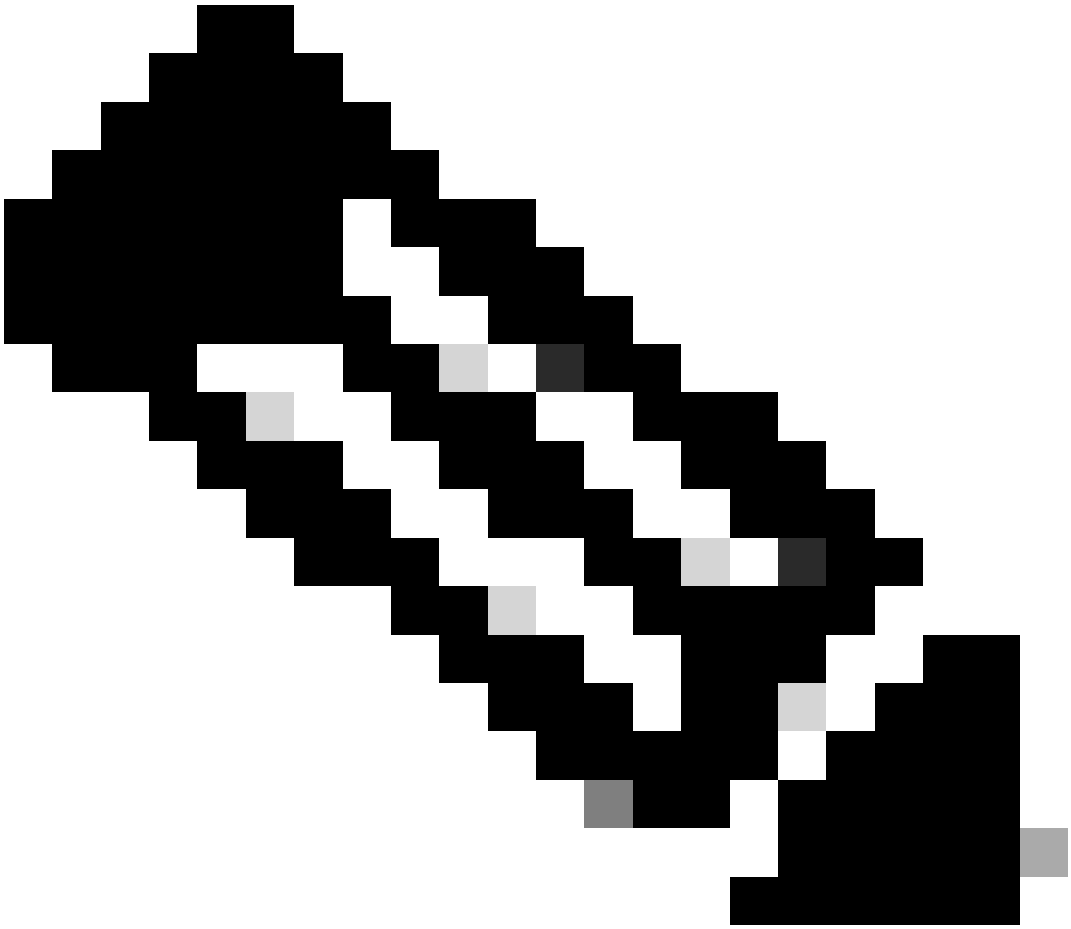
- Cisco Email Encryption Add-in 10.0.0

- 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.

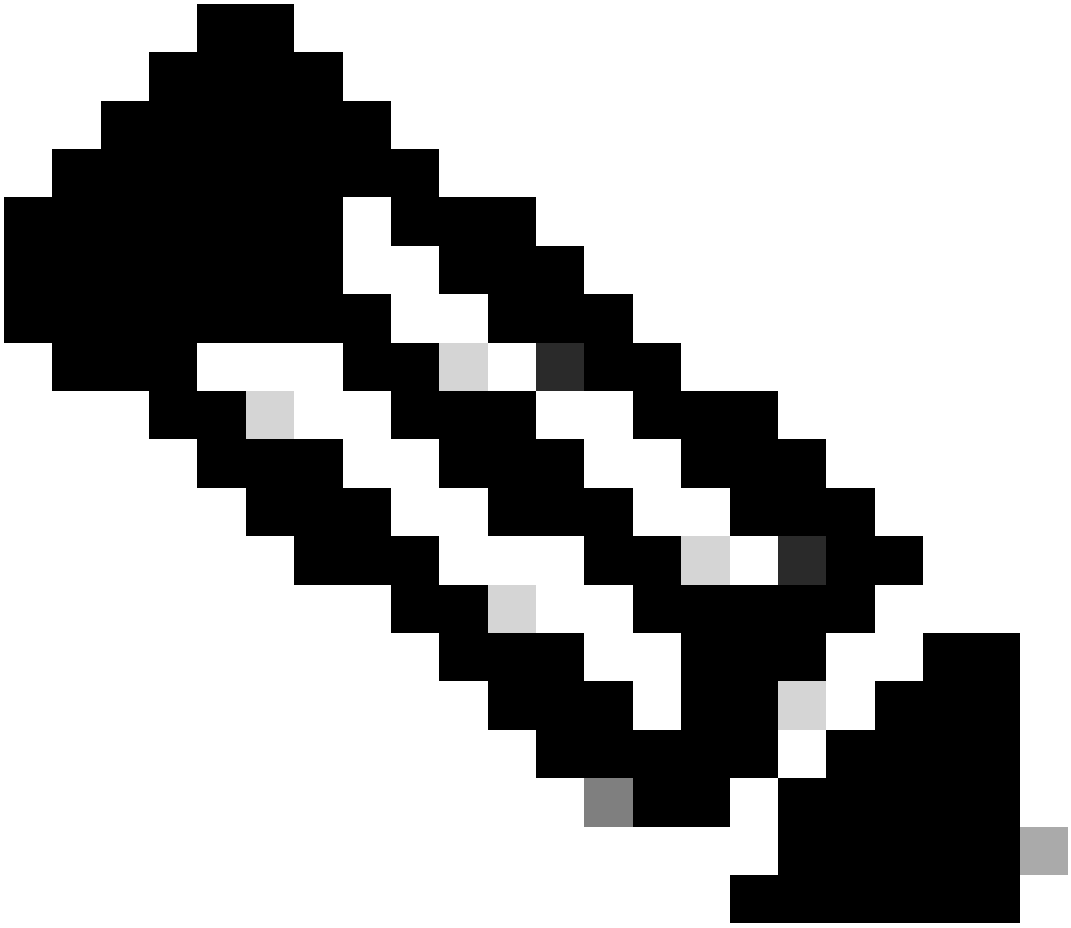
Configurazione

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).

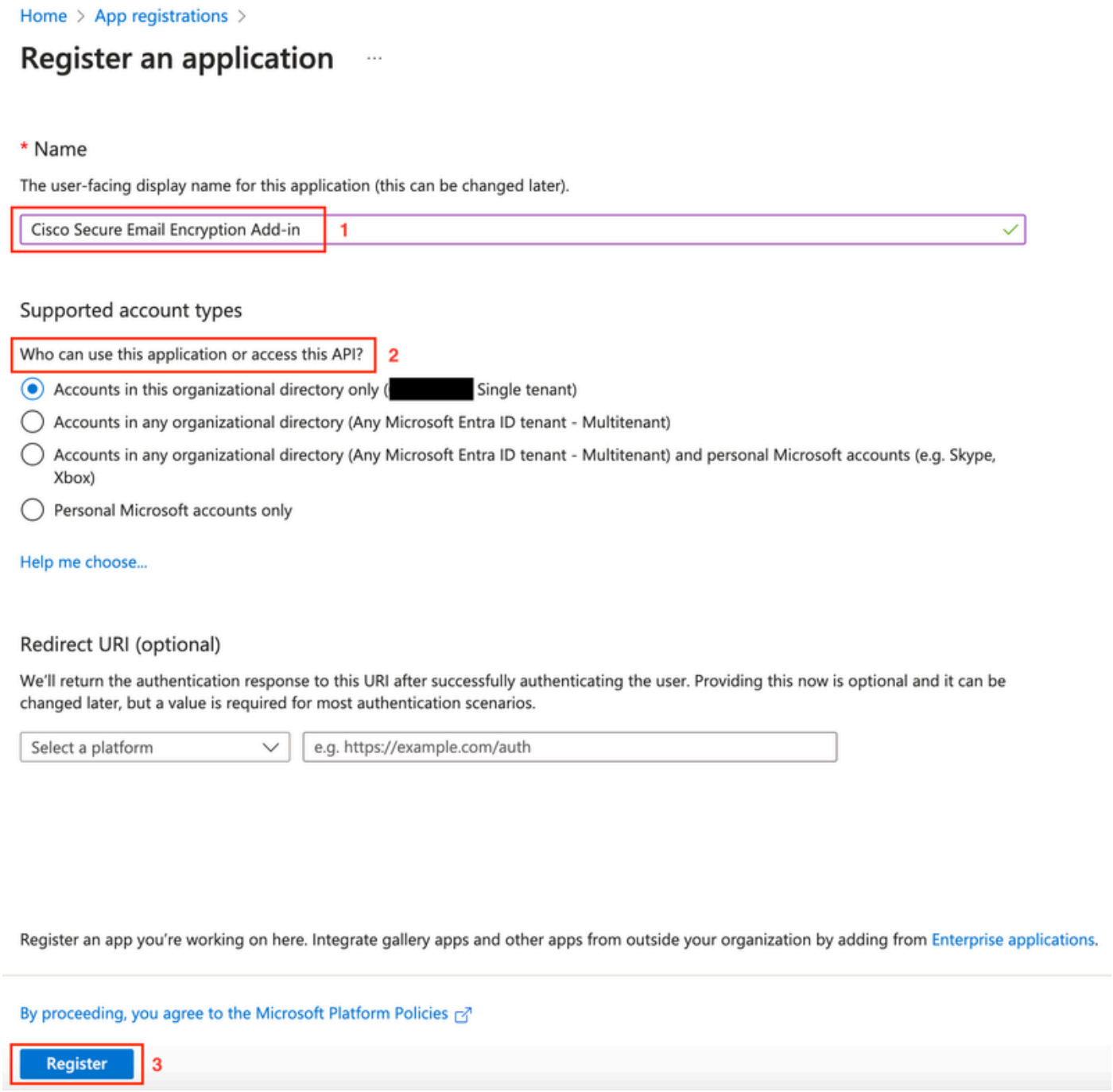
2. Nel menu a sinistra, espandere Admin Centerse fare clic su Identity.

3. Passare a Identity > Applications > App registrationse selezionare New registration.



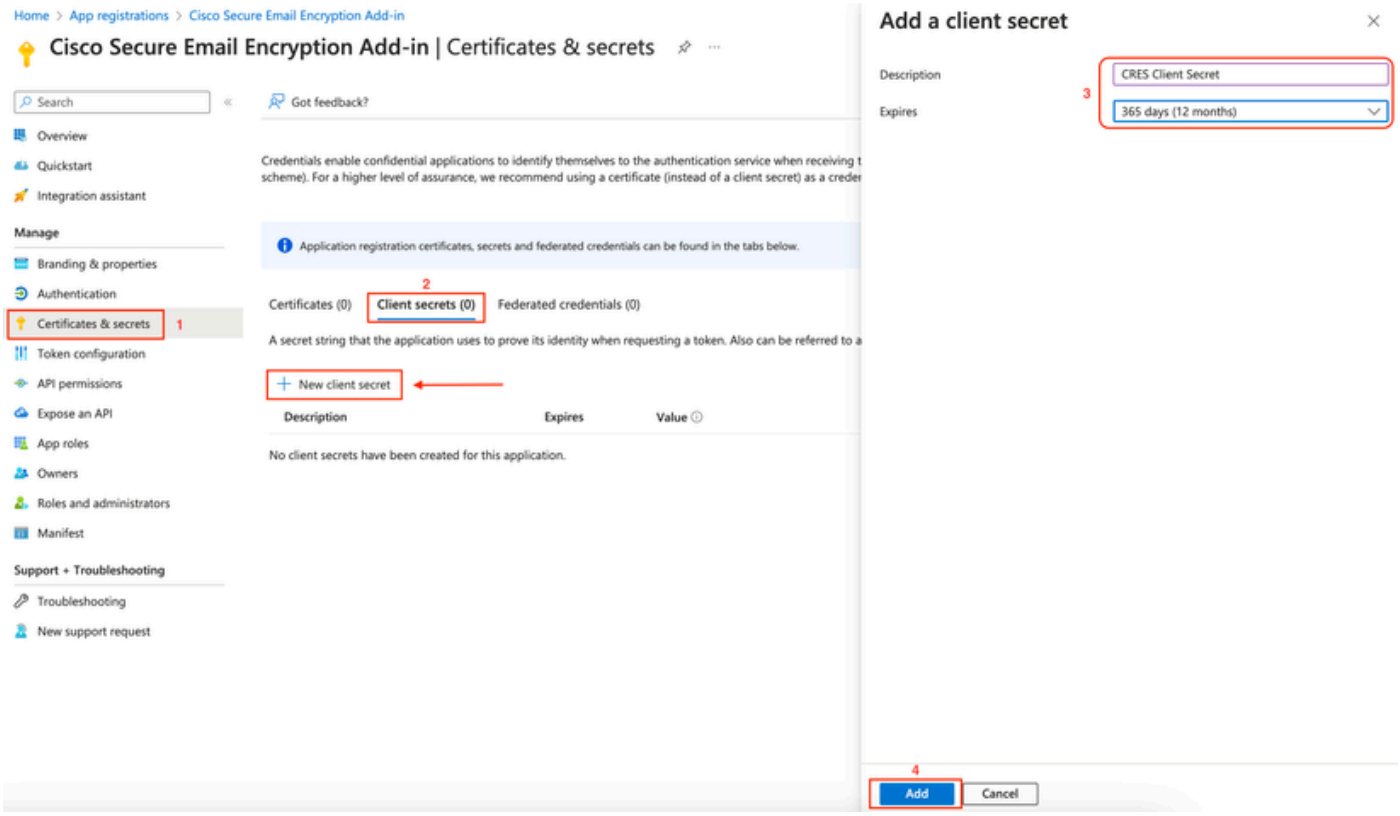
Nota: se si dispone dell'accesso a più tenant, utilizzare l'icona Impostazioni nel menu in alto a destra per passare al tenant in cui si desidera registrare l'applicazione dal menu Directory + Sottoscrizioni.

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



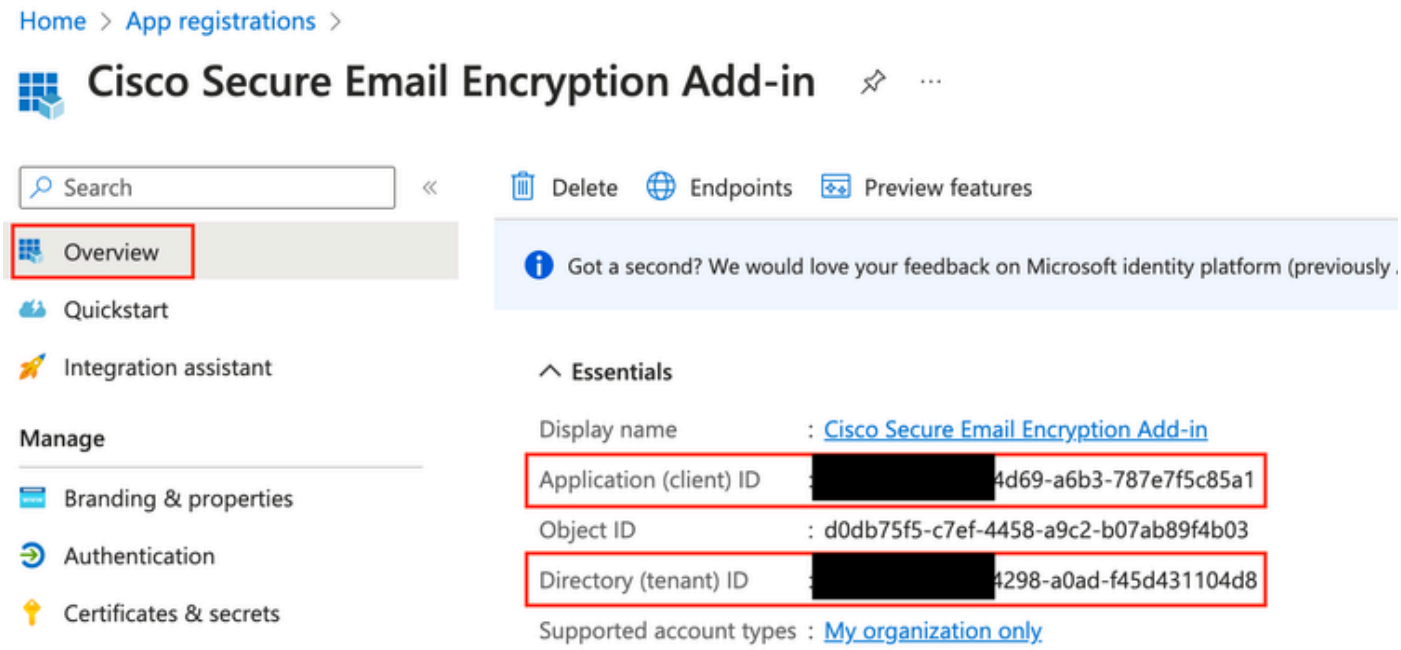
Registra applicazione

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.

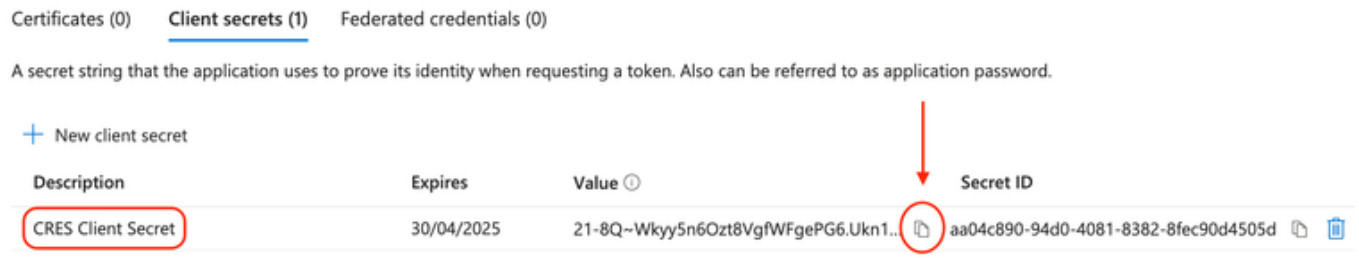


Configura segreto client

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.



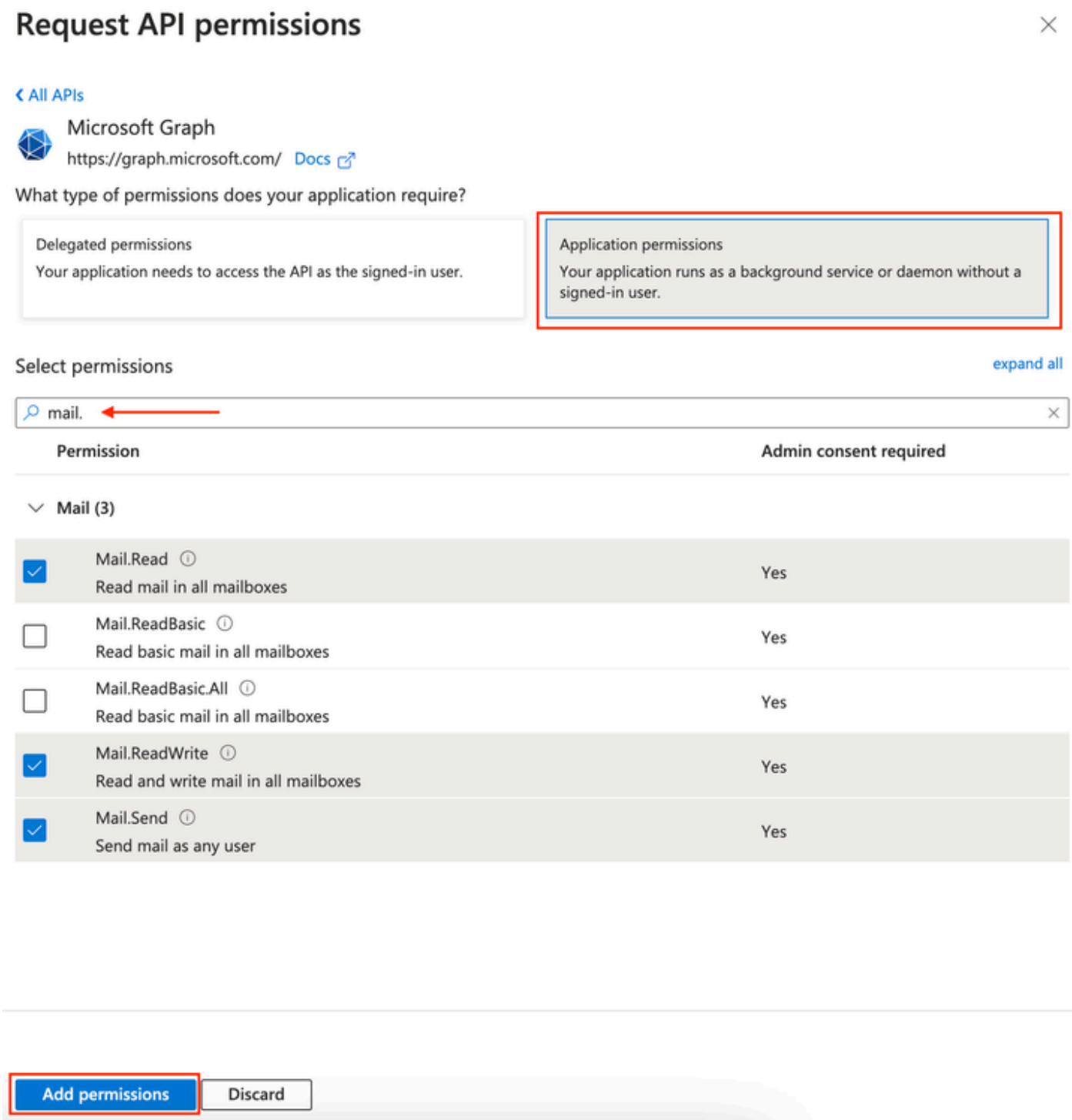
Panoramica dell'applicazione Entra ID



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



Configurazione autorizzazioni di Microsoft Graph

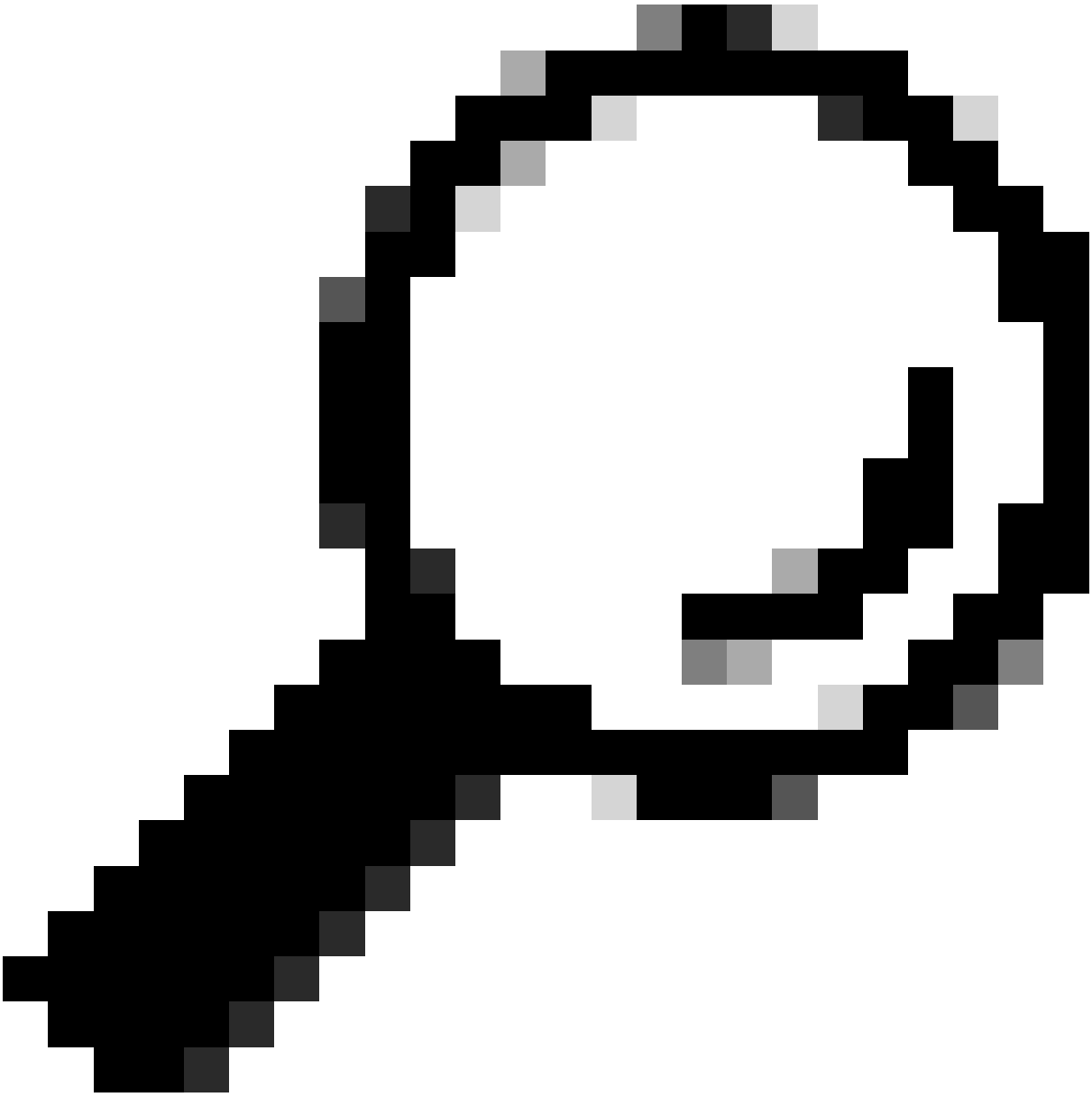
7. Fare clic su Grant Admin Consent for <tenant-name> per concedere all'applicazione l'accesso alle autorizzazioni per conto dell'organizzazione.

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

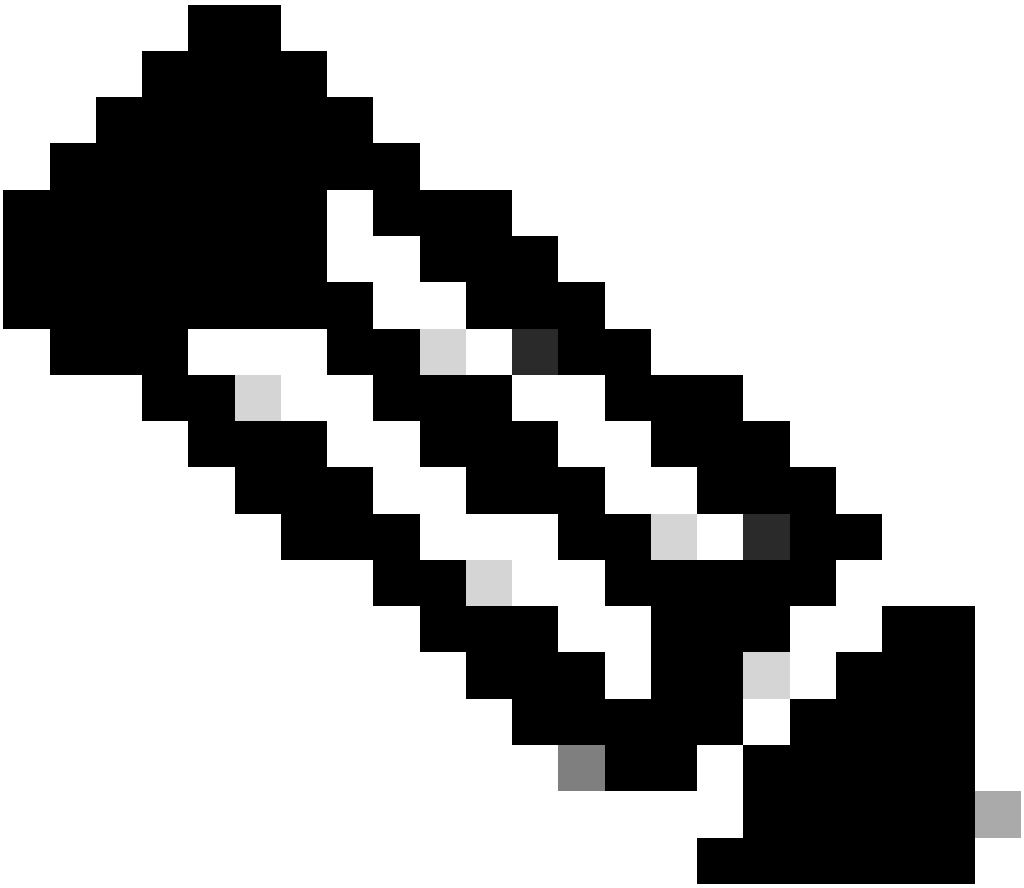
1. Accedere al portale di amministrazione di Cisco Secure Email Encryption Service (CRES) come amministratore di account. (https://res.cisco.com/admin)

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.

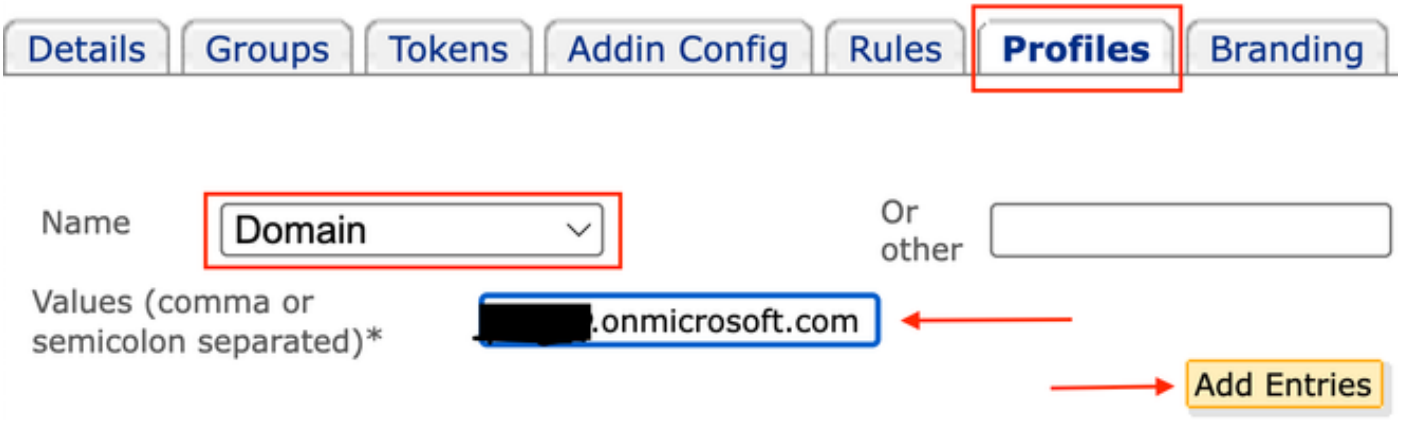
3. PassareProfiles a, selezionare il tipo Nome come Dominio e immettere il nome del dominio e-mail in Valori. Fare clic su **Add Entries** e attendere 5-10 secondi. Non aggiornare la pagina del browser o passare a un'altra pagina finché non viene aggiunta correttamente.



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.

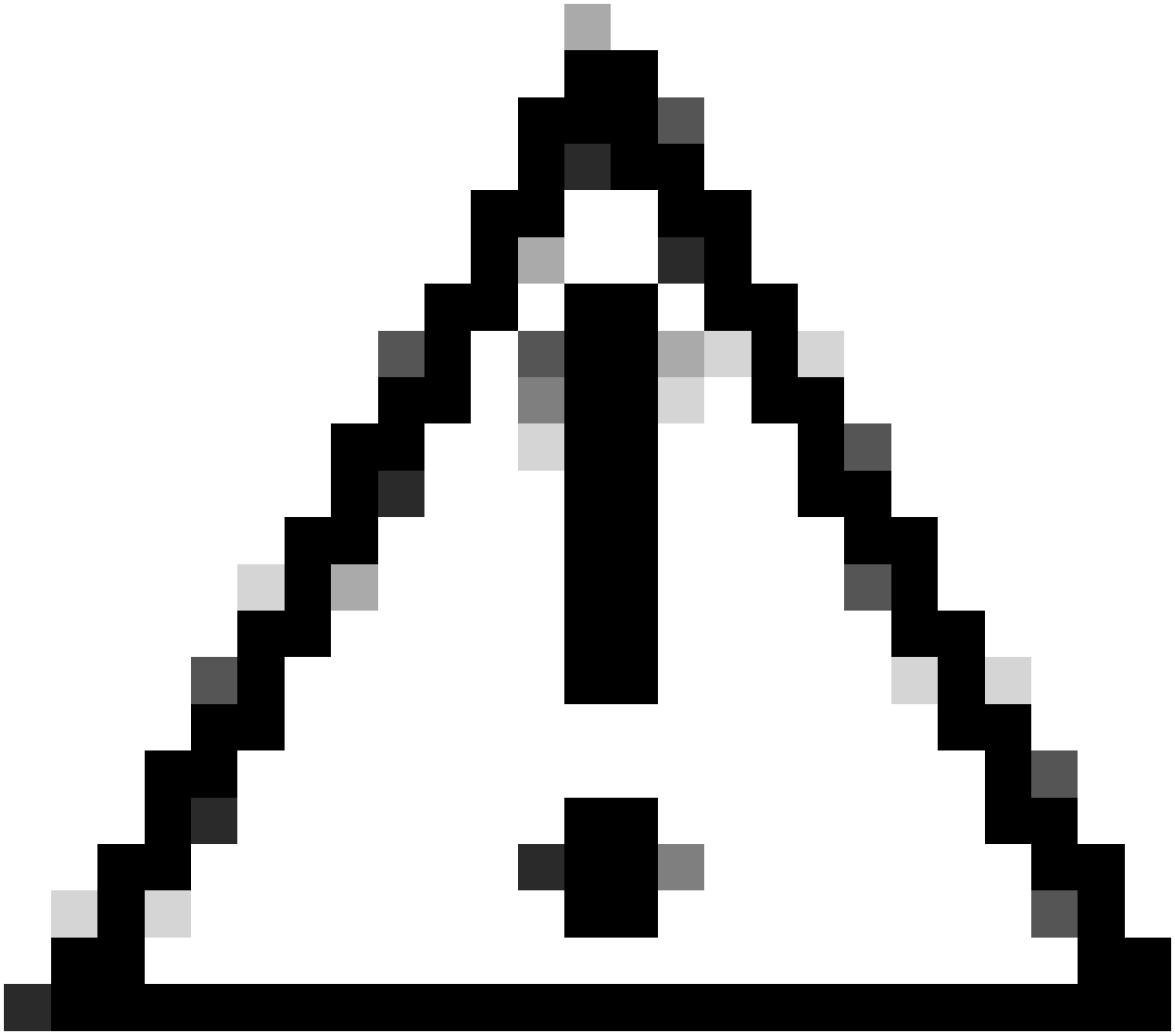


Profili portale di amministrazione CRES

4. Passare alla Add-in Configscheda.

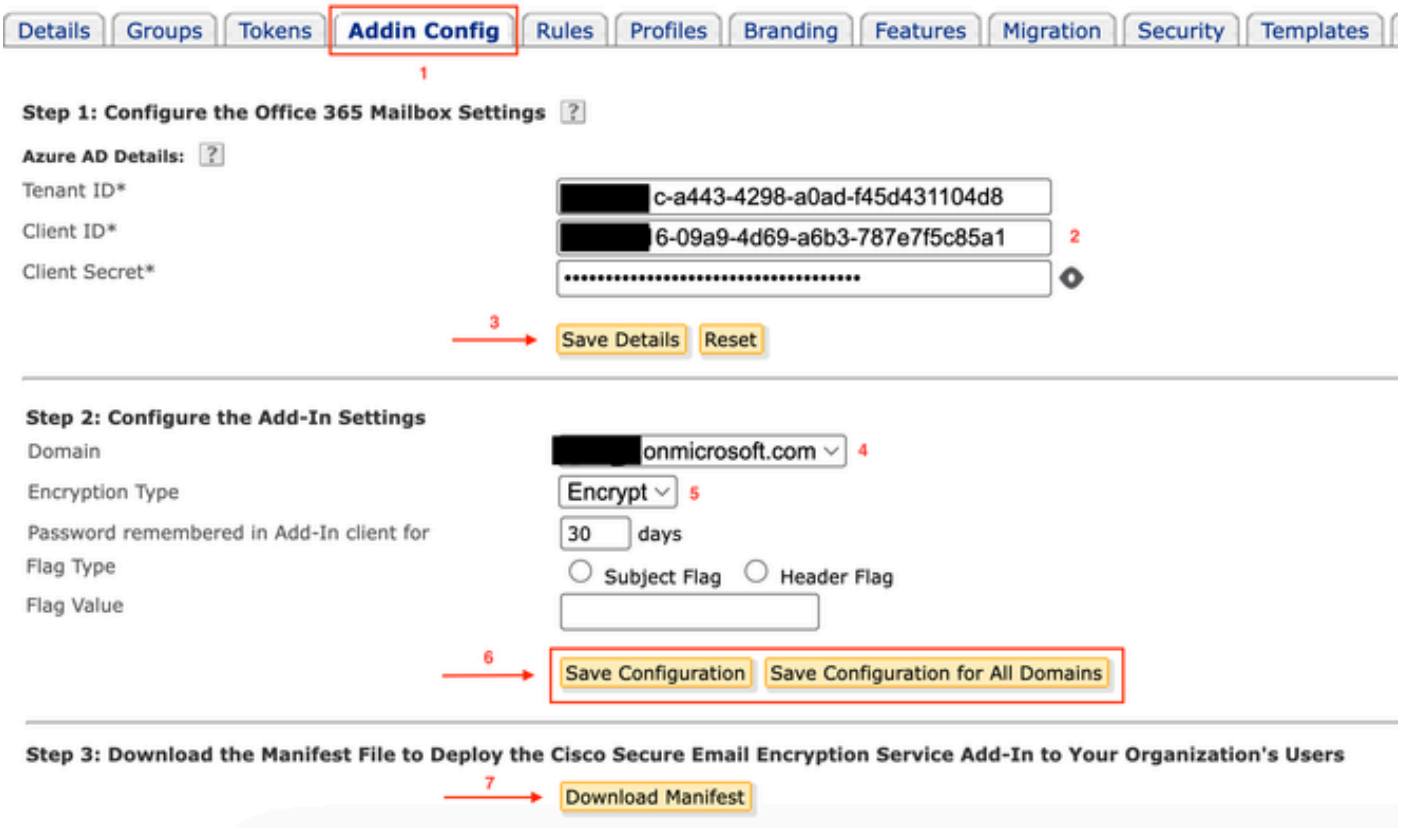
Passaggio 1: immettere il tenant, l'ID client e il segreto ottenuti dall'ID Entra in Dettagli di Azure AD. Fare clic su .Save Details

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.

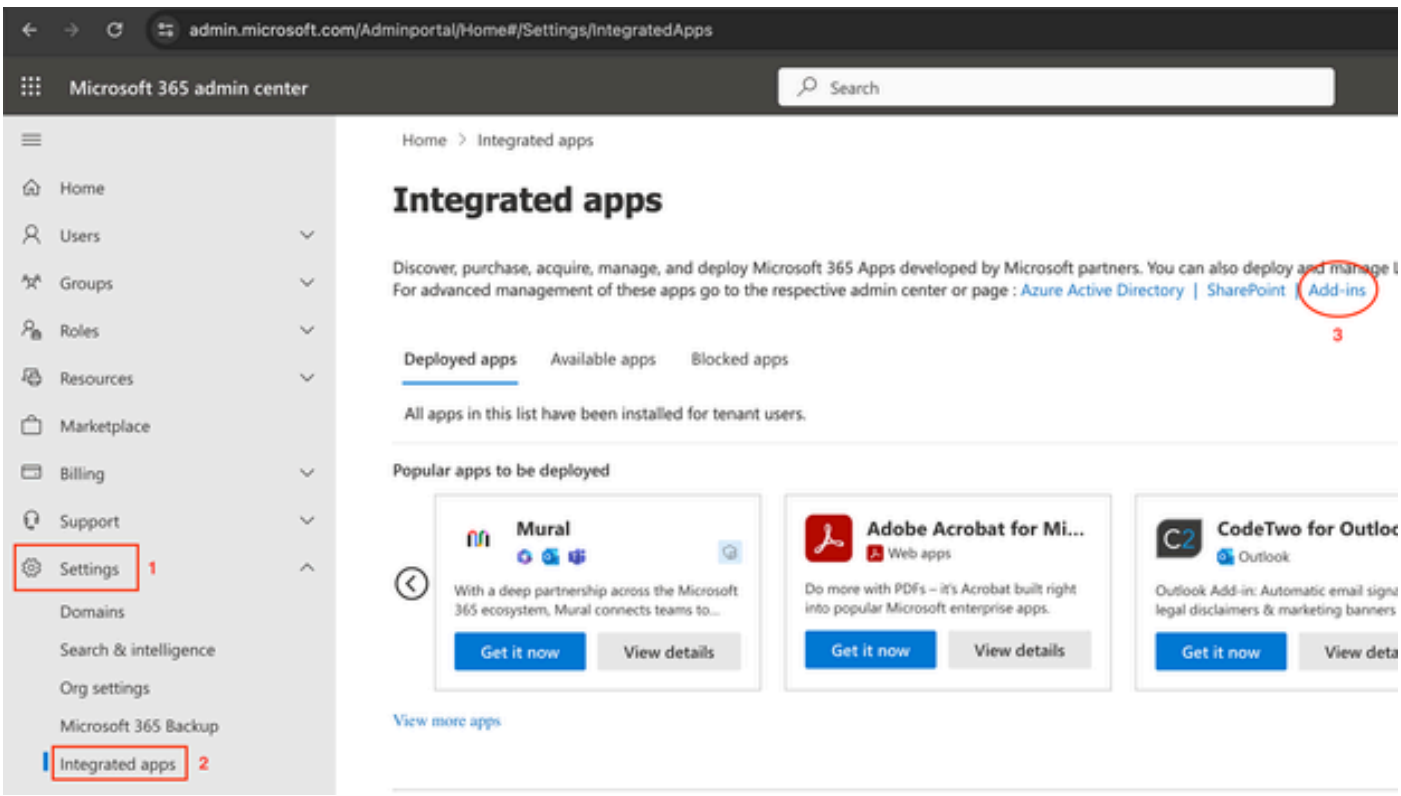


Configurazione del componente aggiuntivo del portale di amministrazione CRES

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

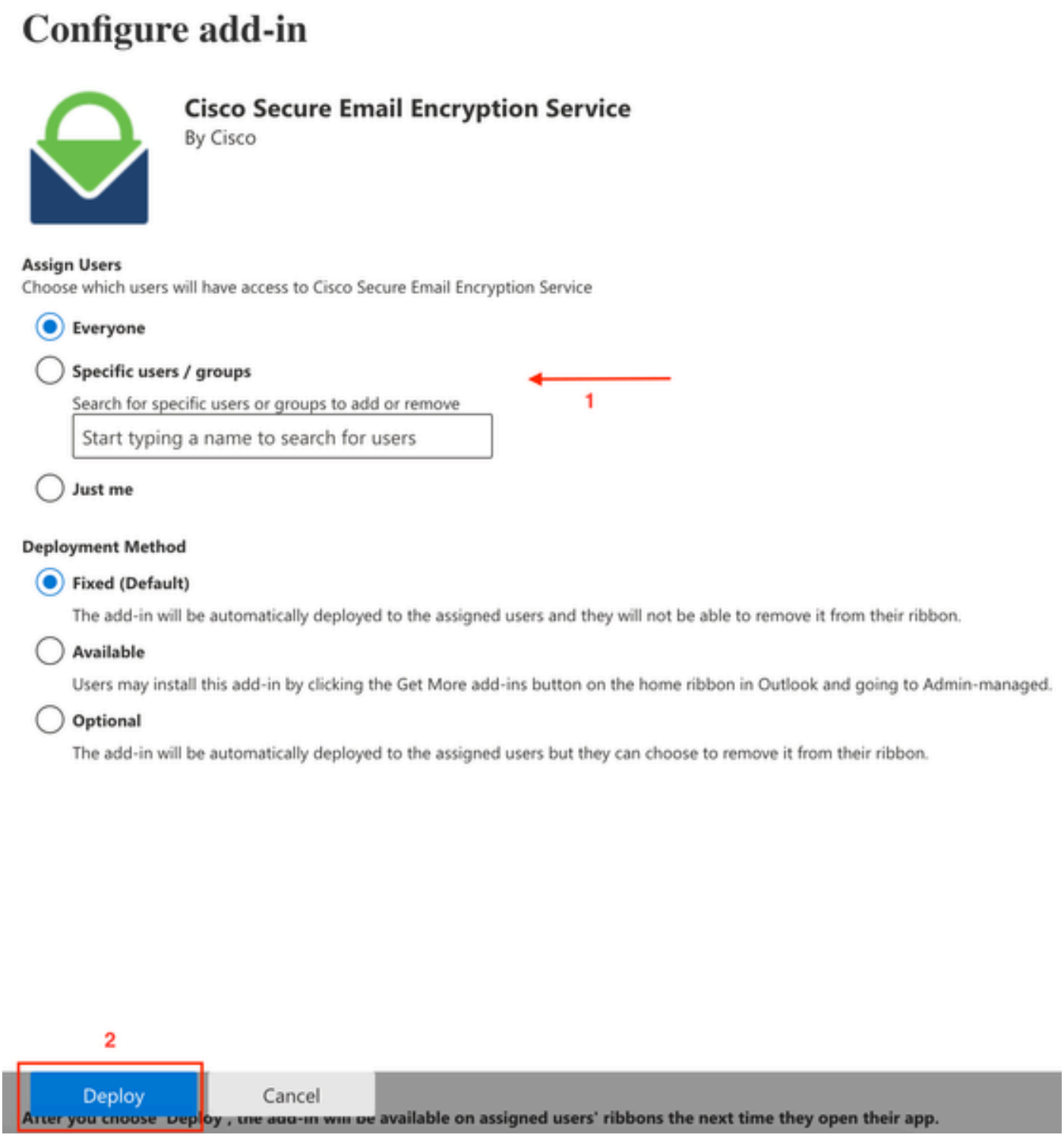
1. Accedere a Microsoft 365 Admin Center come amministratore. (Microsoft 365 Admin Center).

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



3. Fare clic su Deploy Add-ine 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 Specifc Users/groupse fare clic su Deploy.



Configurazione del componente aggiuntivo Microsoft Office 365

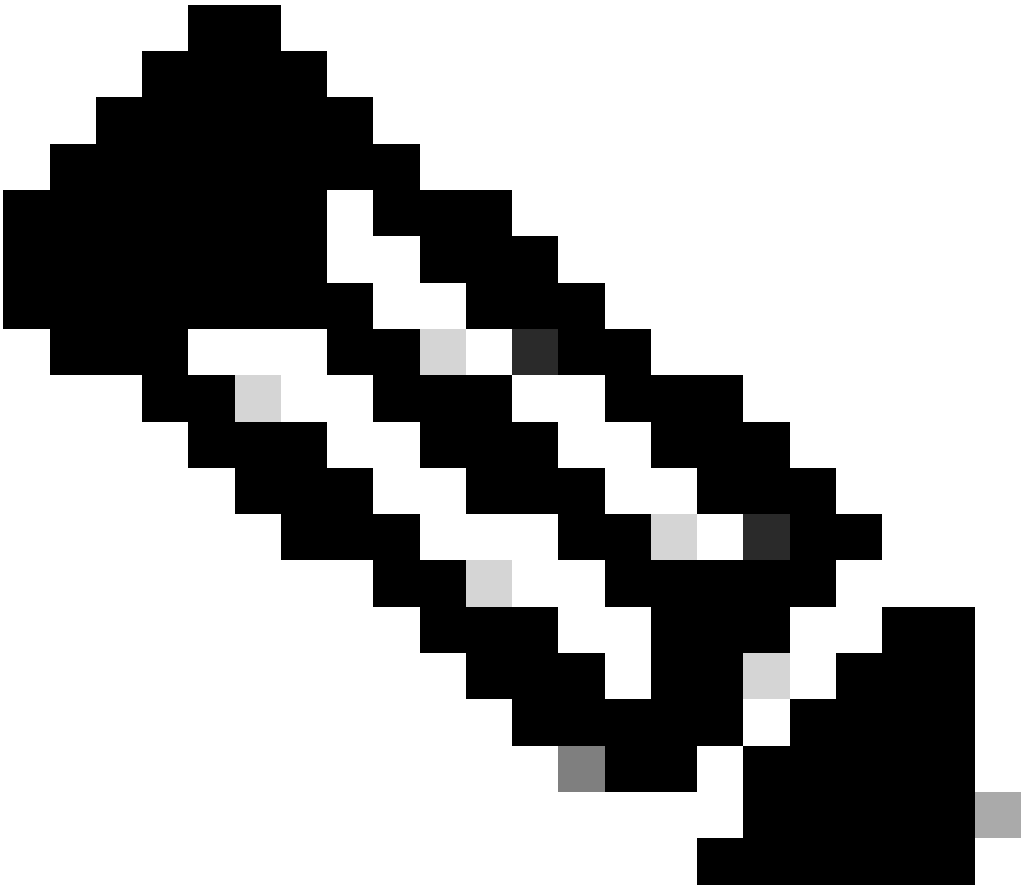
5. Una volta distribuito correttamente, il componente aggiuntivo può impiegare fino a 12 ore per essere visualizzato sulle barre multifunzione

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.



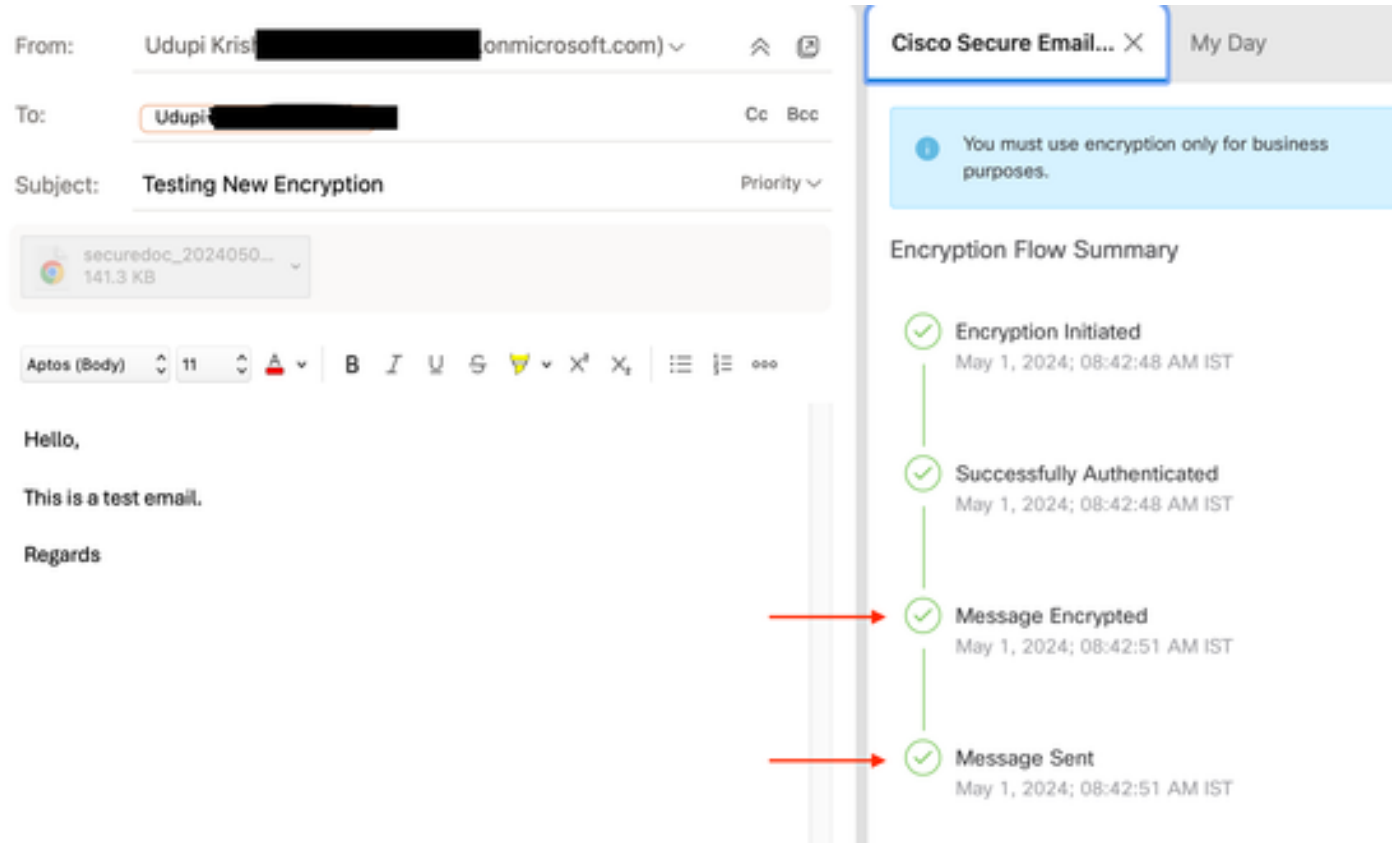
Nota: se il tipo di crittografia (impostato dall'amministratore) è Crittografa, accertarsi di aver completato il messaggio e di aver aggiunto destinatari validi prima di procedere al passaggio successivo. Dopo il passaggio 3, il messaggio viene crittografato e inviato immediatamente.

---

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 Crittografa 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).



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).