E-Mail-Verschlüsselungs-Add-In mit Microsoft O365 konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Cisco Email Encryption Service Add-in für die zentrale Bereitstellung über Microsoft Office 365 konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Email Gateway
- Cisco Secure Email Encryption Service (ehemals Cisco Registered Envelope Service)
- Microsoft O365 Suites (Exchange, Entra ID, Outlook)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

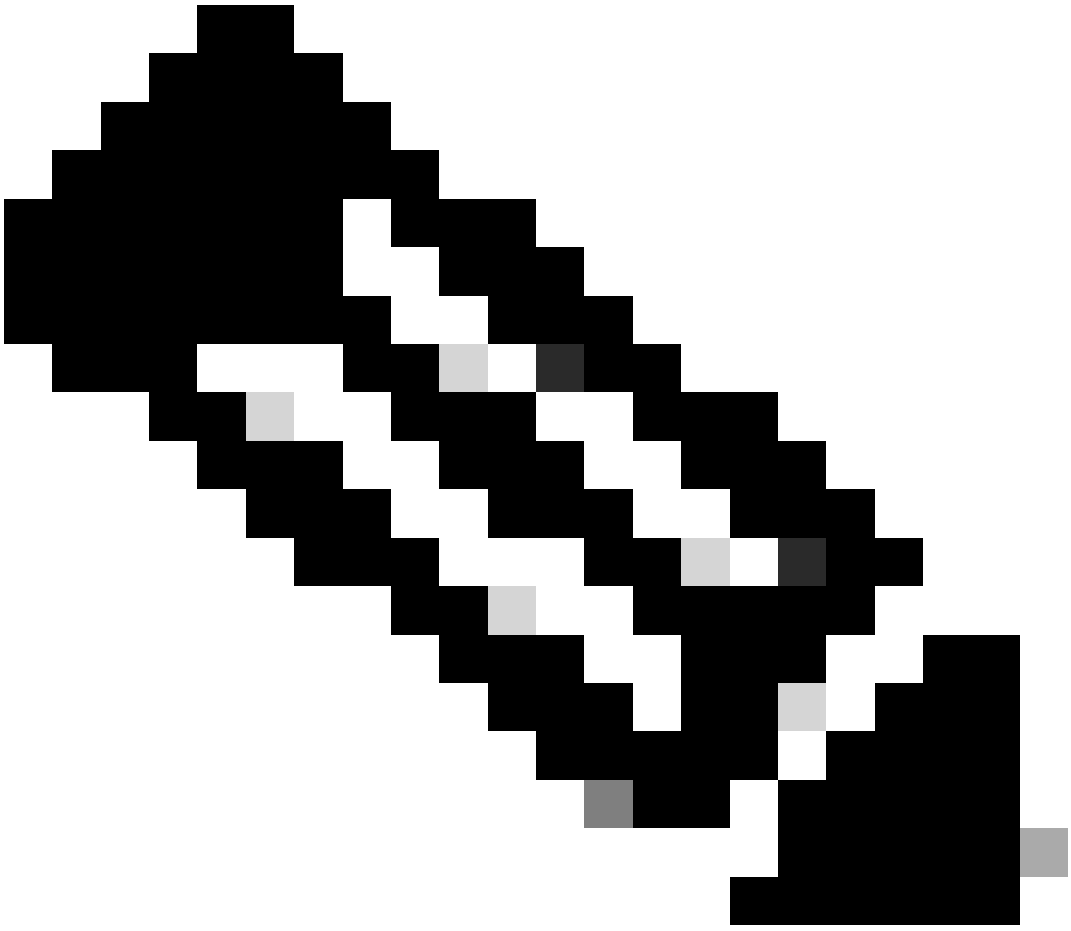
- Cisco Email Encryption Add-in 10.0.0

- Microsoft Exchange Online
- Microsoft Entra ID (ehemals Azure AD)
- Outlook für O365 (MacOS, Windows)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Mit dem Cisco Secure Email Encryption Service Add-in können Ihre Endbenutzer ihre Nachrichten direkt in Microsoft Outlook mit einem einzigen Mausklick verschlüsseln. Dieses Add-In kann in Microsoft Outlook (für Windows und MacOS) und Outlook Web App bereitgestellt werden.



Hinweis: Dieses Dokument ist ideal für alle Endbenutzer, die das Add-In verwenden möchten, Office 365/Microsoft 365-Abonnement verwenden möchten, und alle

---

Endbenutzer, die das Add-In verwenden möchten, sind registrierte Benutzer des Cisco Secure Email Encryption Service.

Best Practices für die Bereitstellung des Add-Ins für den Cisco Secure Email Encryption Service

- Testphase: Bereitstellung des Add-Ins für eine kleine Gruppe von Endbenutzern in einer Abteilung oder einem Bereich. Evaluieren Sie die Ergebnisse, und gehen Sie bei Erfolg zur nächsten Phase über.
- Pilotphase: Bereitstellung des Add-Ins für mehr Endbenutzer aus verschiedenen Abteilungen und Funktionen Evaluieren Sie die Ergebnisse, und gehen Sie bei Erfolg zur nächsten Phase über.
- Produktionsphase: Bereitstellung des Add-Ins für alle Benutzer

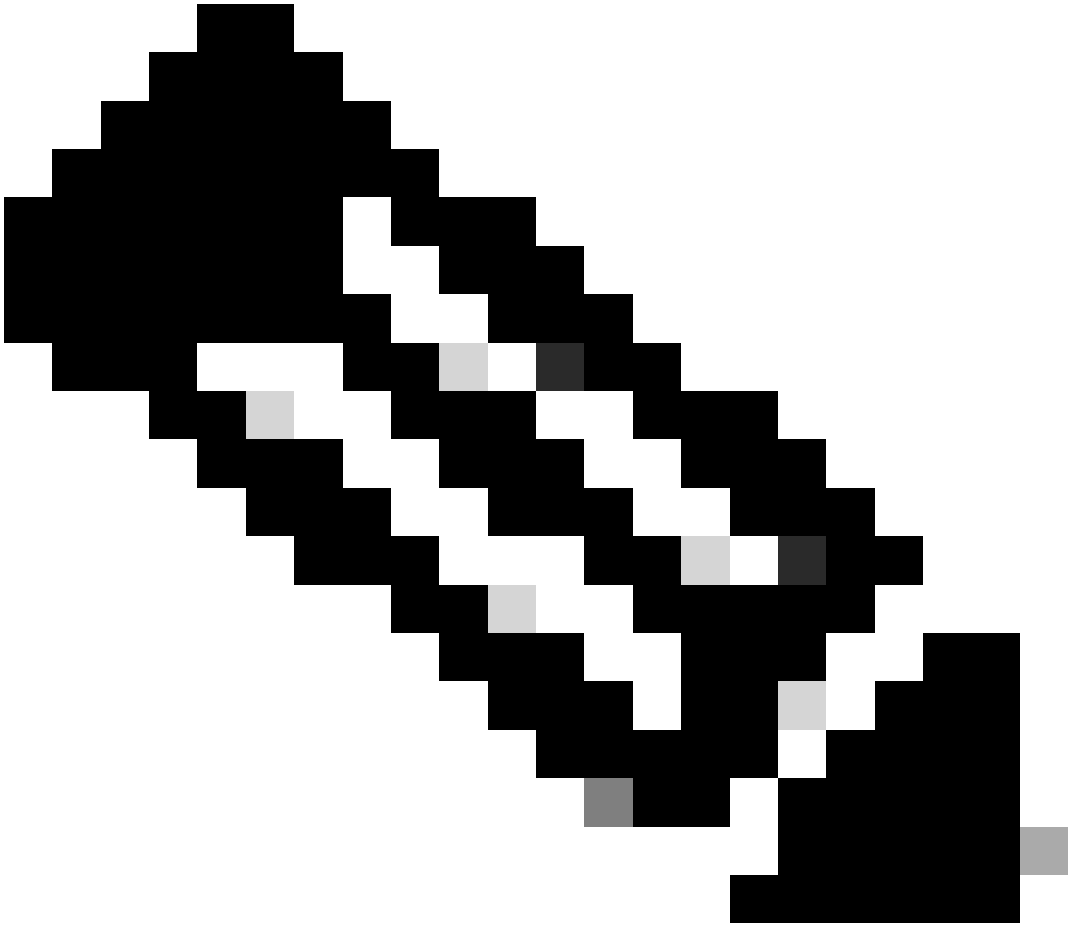
Konfigurieren

Registrierung der Add-In-Anwendung für den Cisco Secure Email Encryption Service

1. Melden Sie sich beim Microsoft 365 Admin Center als mindestens Cloud Application Administrator (Microsoft 365 Admin Center) an.

2. Erweitern Sie das Menü auf der linken Seite, Admin Centersund klicken Sie auf Identity.

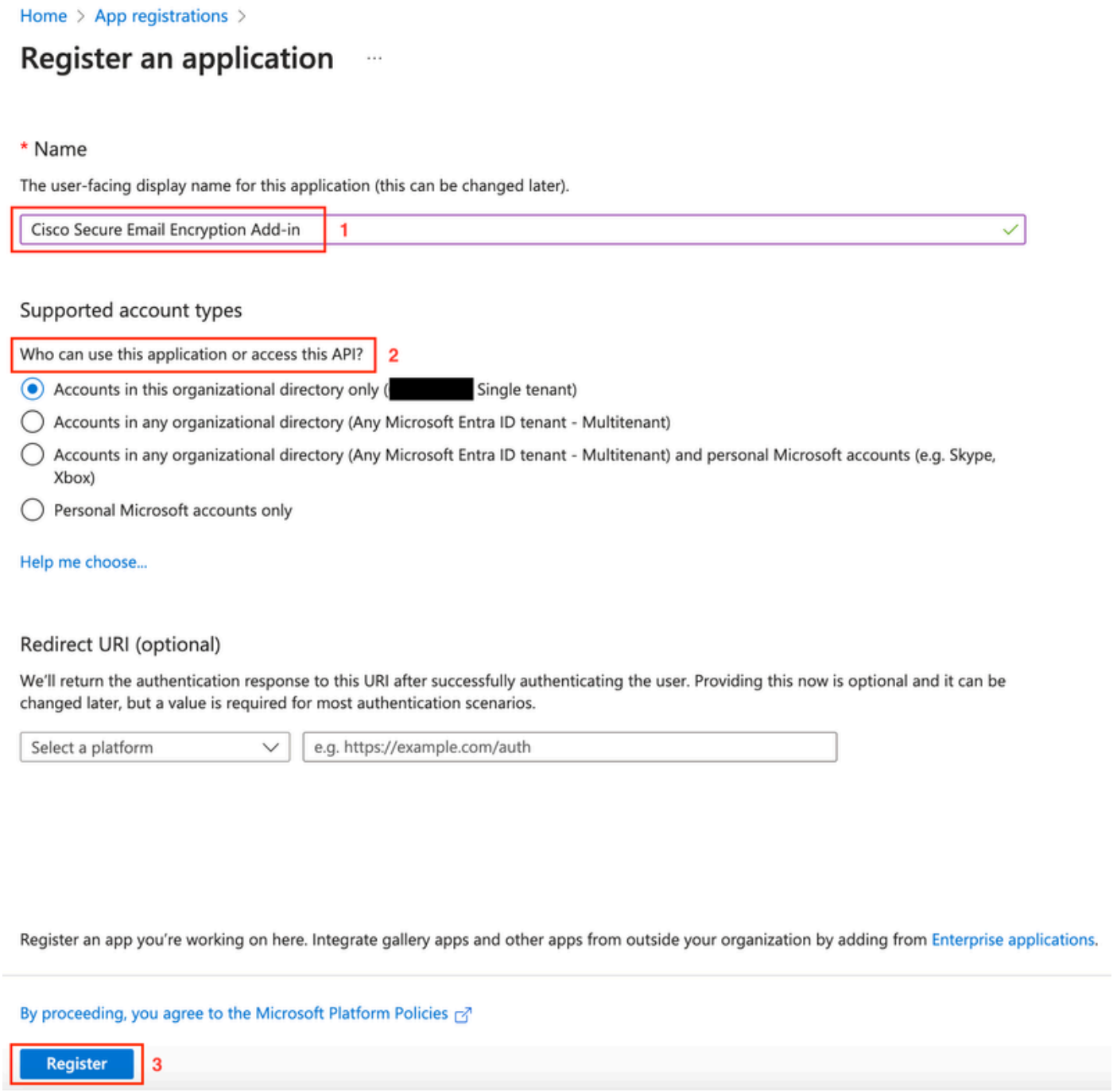
3. Navigieren Sie zu , Identity > Applications > App registrationsund wählen Sie New registration.



Hinweis: Wenn Sie Zugriff auf mehrere Tenants haben, wechseln Sie über das Einstellungssymbol oben rechts zum Tenant, in dem Sie die Anwendung registrieren möchten. Dies geschieht über das Menü Verzeichnisse + Abonnements.

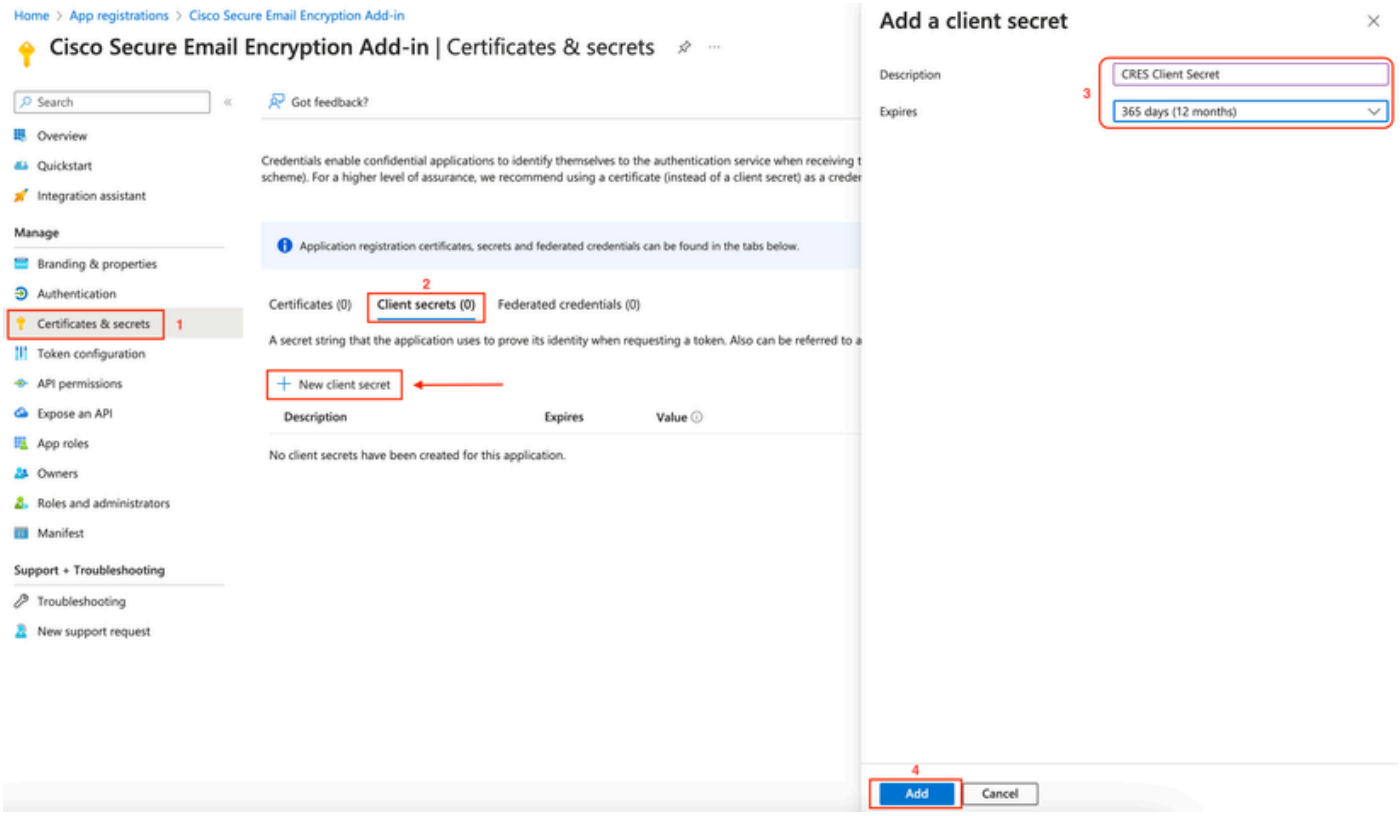
---

4. Geben Sie einen Anzeigenamen für die Anwendung ein, wählen Sie Konten aus, die die Anwendung verwenden können, und klicken Sie auf Register.



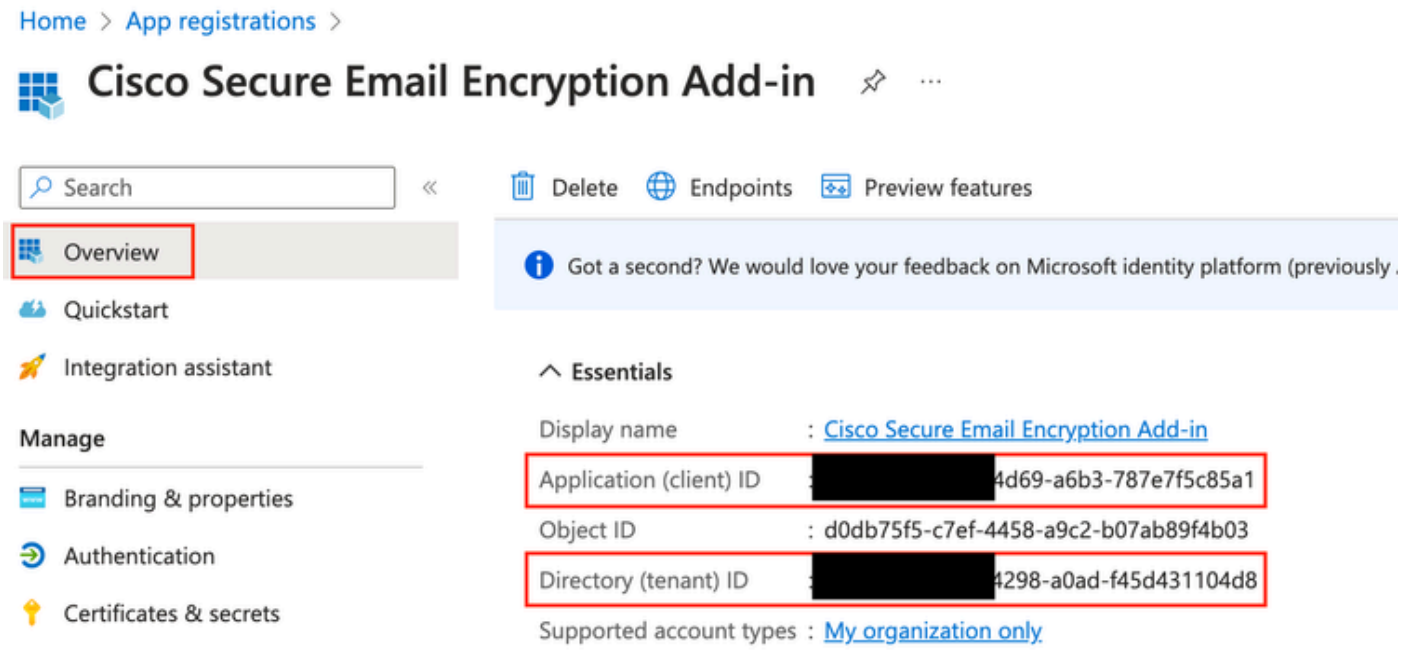
Anwendung registrieren

5. Navigieren Sie nach erfolgreicher Registrierung zur Anwendung, um den Clientschlüssel zu konfigurieren unter Certificates & Secrets. Wählen Sie den Ablauftermin gemäß den gesetzlichen Vorschriften des Unternehmens aus.

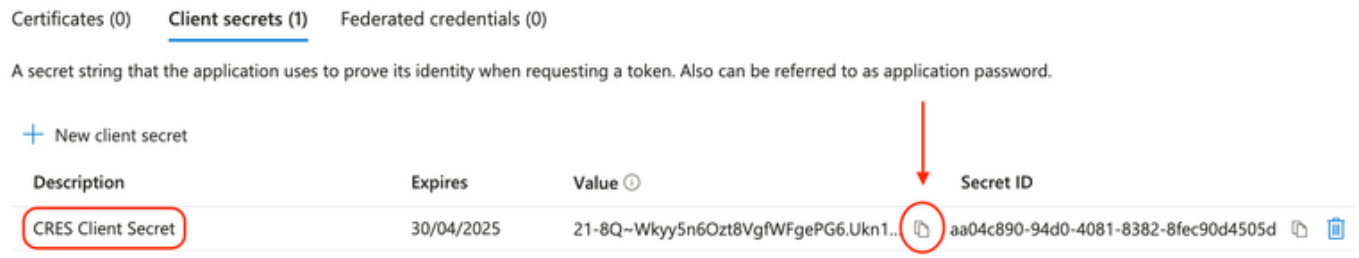


Client-Schlüssel konfigurieren

6. Kopieren Sie auf der Seite "Übersicht" der registrierten Anwendung das Application (client) ID und Directory (tenant) ID. Kopieren Sie die **Client Secret** aus den im vorherigen Schritt generierten Zertifikaten und Schlüsseln.



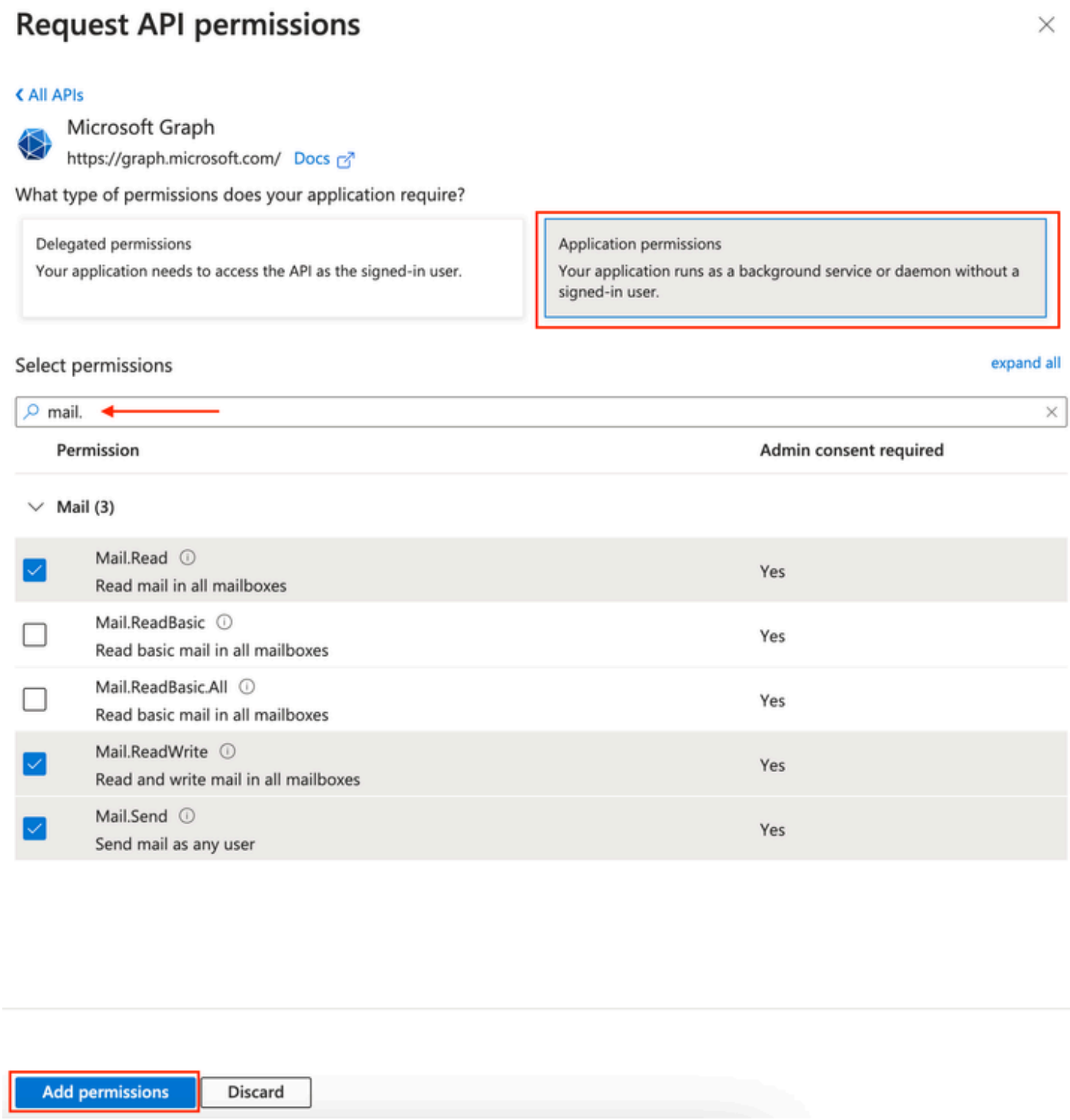
Übersicht über die Entra-ID-Anwendung



Client-Schlüssel kopieren

7. Navigieren Sie zur **registrierten E-Mail-Verschlüsselungsanwendung**, und navigieren Sie dann zu API permissions. Klicken Sie auf Add a permission, und wählen Sie die erforderlichen Microsoft Graph Application Permissions:

- Mail.Read
- Mail.ReadWrite
- E-Mail senden
- Benutzer.Lesen.Alle



Microsoft Graph-Berechtigungskonfiguration

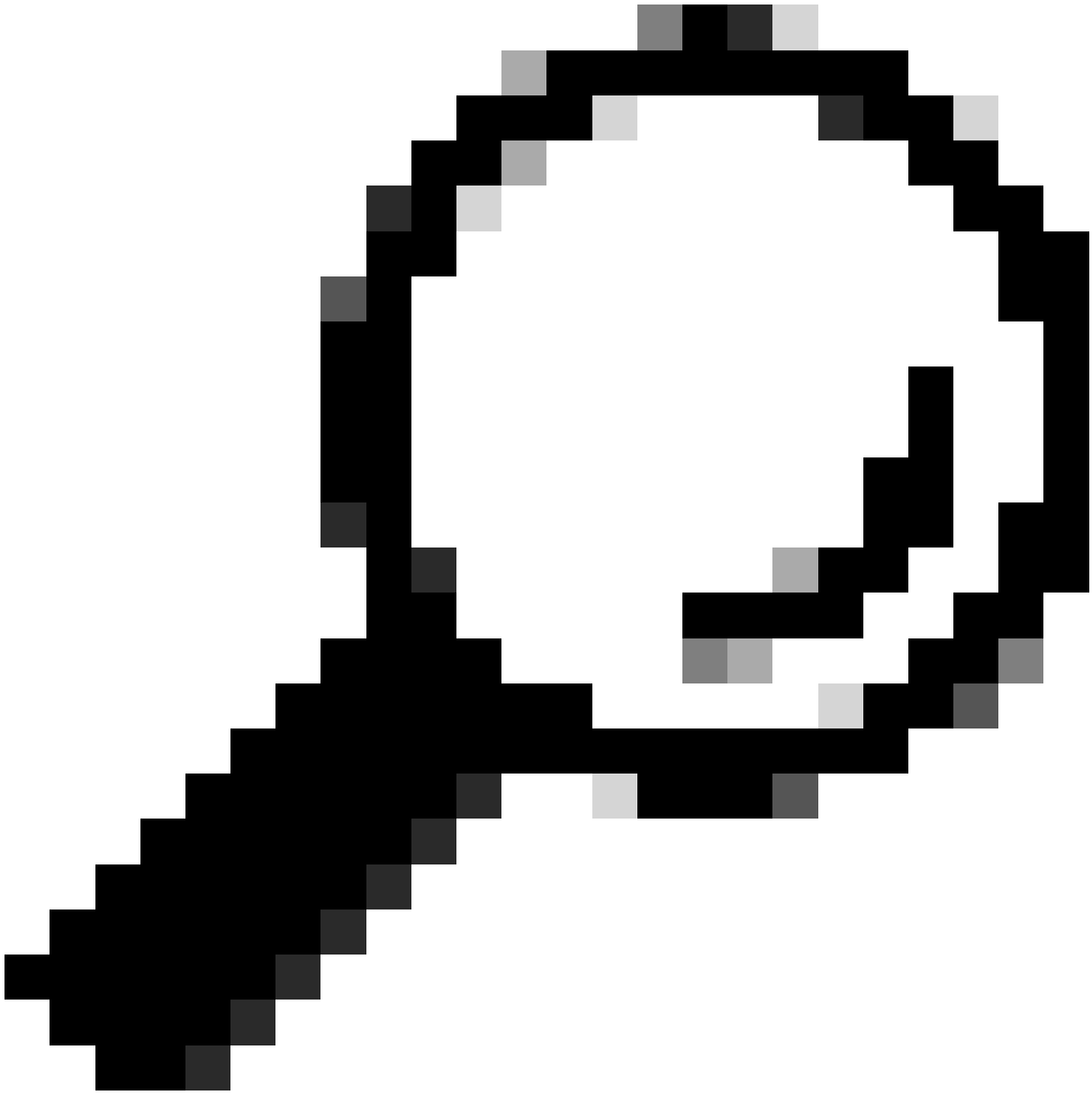
7. Klicken Sie Grant Admin Consent for <tenant-name> hier, um der Anwendung im Namen der Organisation Zugriff auf Berechtigungen zu gewähren.

Konfigurieren der Domänen- und Add-In-Einstellungen im Cisco Secure Email Encryption (CRES)-Administratorportal

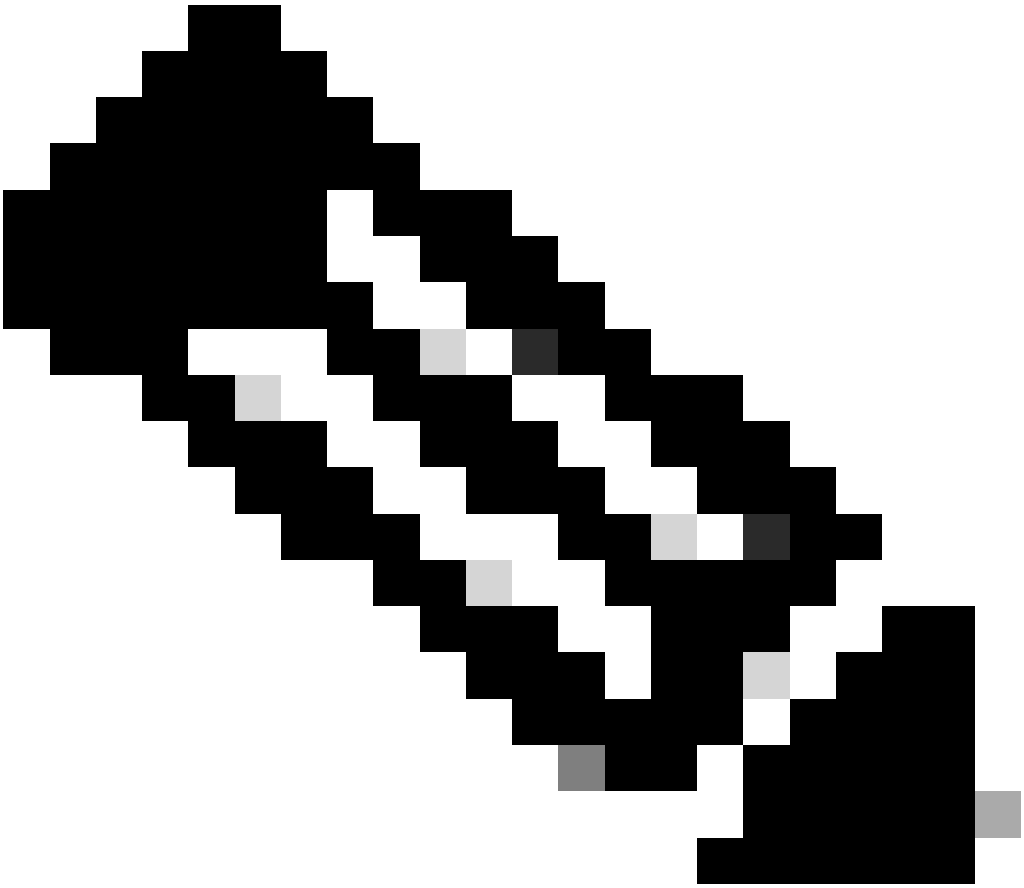
1. Melden Sie sich als Kontoadministrator beim Administratorportal des Cisco Secure Email Encryption Service (CRES) an. (Sicherer E-Mail-Verschlüsselungsservice)

2. Navigieren Sie zu Accounts > Manage Accounts. Klicken Sie auf die Kontonummer, die Ihrer Organisation zugewiesen ist, oder auf das Konto, für das Sie das E-Mail-Verschlüsselungs-Add-In konfigurieren möchten.

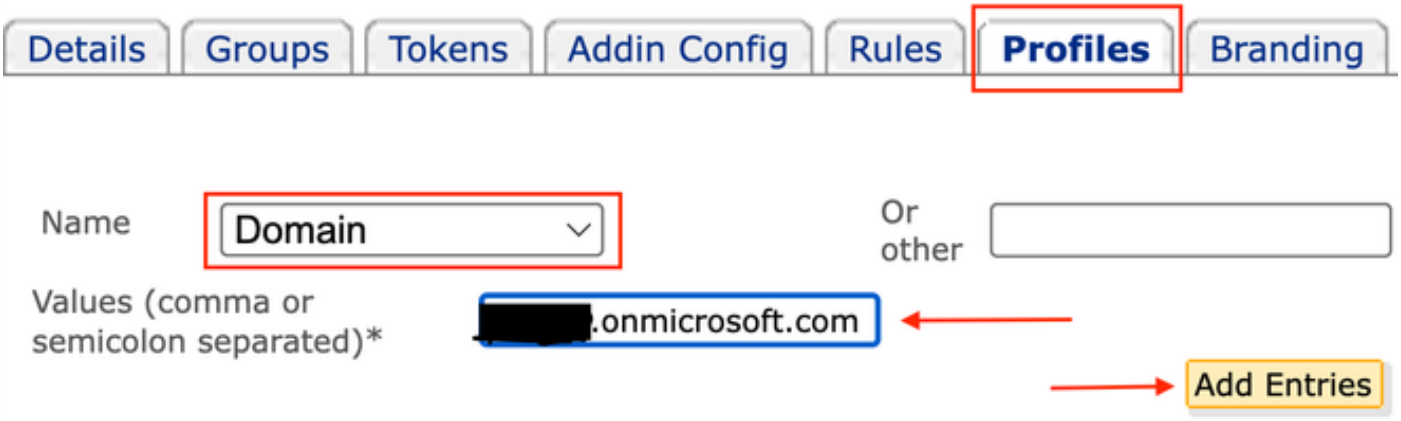
3. Navigieren Sie zu Profiles, wählen Sie den **Namenstyp** als Domäne und geben Sie Ihren **E-Mail-Domänennamen** unter Werte ein. Klicken Sie, **Add Entries** und warten Sie 5 bis 10 Sekunden. (Aktualisieren Sie die Browserseite nicht, und navigieren Sie erst zu einer anderen Seite, wenn die Seite erfolgreich hinzugefügt wurde.)



Tipp: Wiederholen Sie die gleichen Schritte, um weitere E-Mail-Domänen hinzuzufügen, die den E-Mail-Verschlüsselungsdienst in Ihrer Organisation nutzen werden.



Hinweis: Wenden Sie sich an das Cisco Technical Assistance Center, um die E-Mail-Domänen im CRES-Admin-Portal hinzuzufügen.

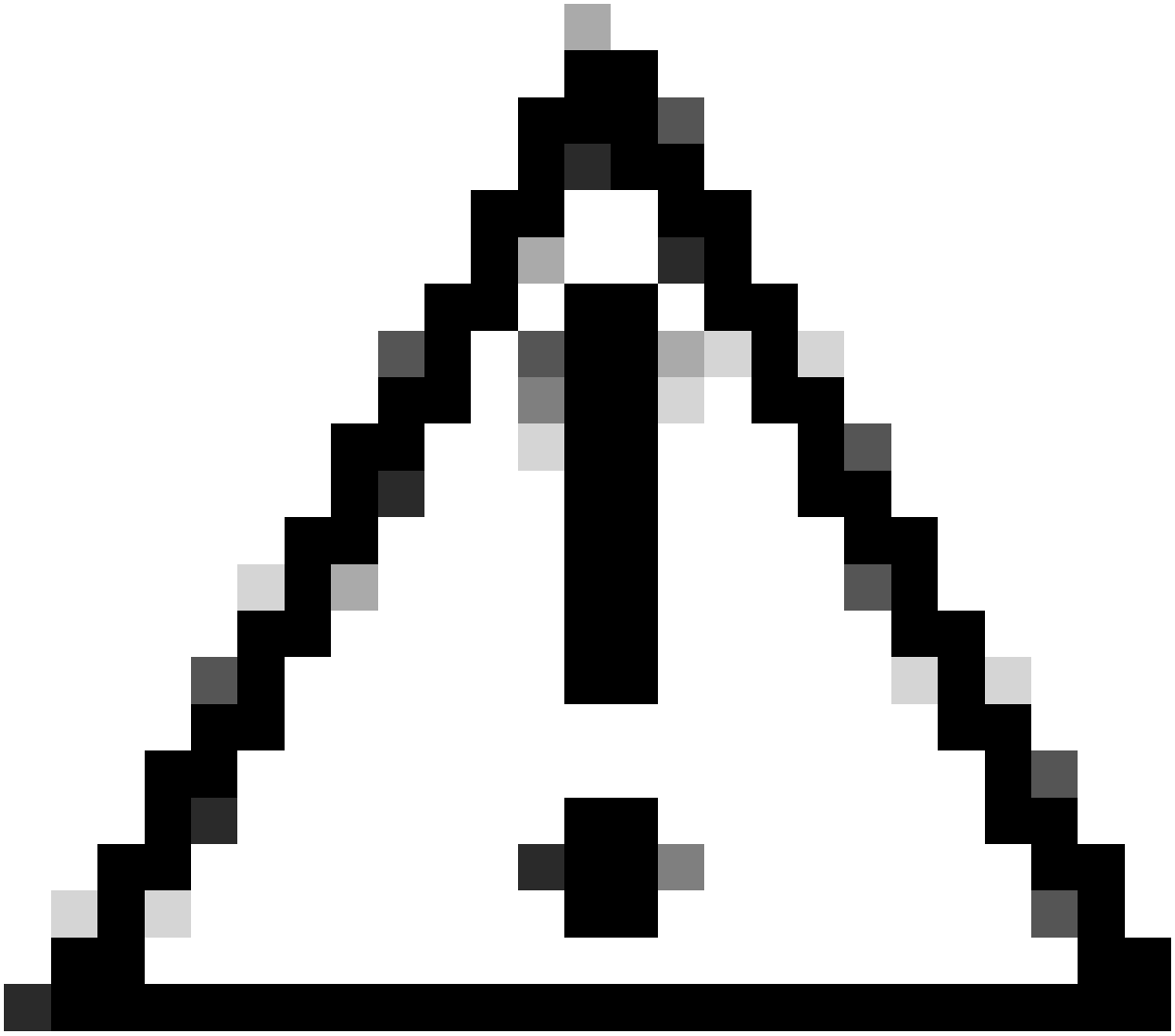


CRES-Administratorportalprofile

4. Navigieren Sie zur Add-in Config Registerkarte.

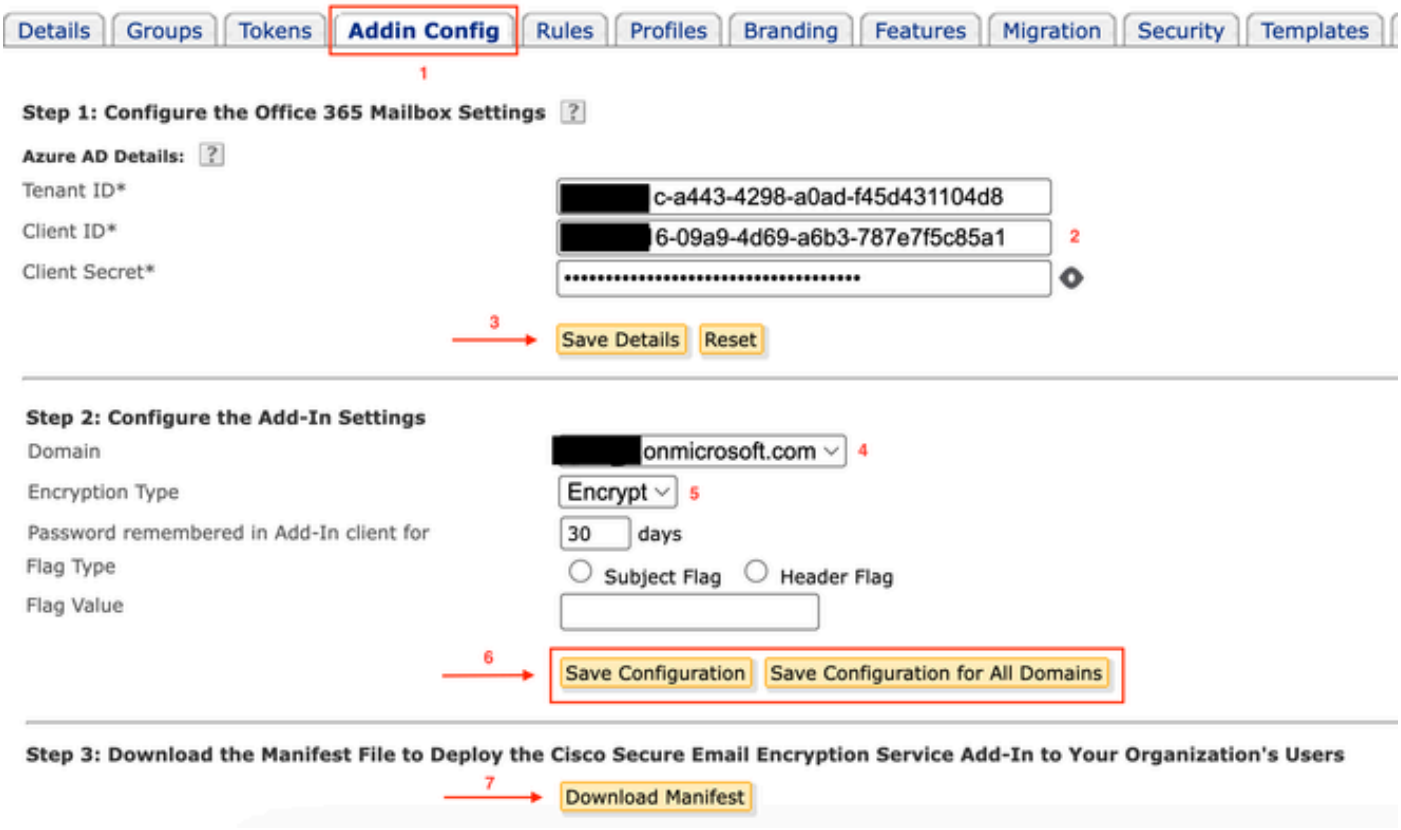
Schritt 1: Geben Sie den Tenant, die Client-ID und den Schlüssel ein, die Sie von der Entra-ID unter Azure AD-Details erhalten haben. Klicken Sie auf .Save Details

Schritt 2: Wählen Sie die Domäne, Verschlüsselungstyp, und klicken Sie auf Save Configuration. Verwenden Sie Save Configuration diese Option für alle Domänen, um die gleichen Einstellungen auf alle hinzugefügten Domänen anzuwenden.



Vorsicht: Navigieren Sie nicht zu einer anderen Seite, ohne die Schritte 1. und 2. gemeinsam auszuführen. Wenn Schritt 2. nicht gleichzeitig abgeschlossen wird, werden Azure AD-Details nicht gespeichert.

Schritt 3: Klicken Sie auf Download Manifest.

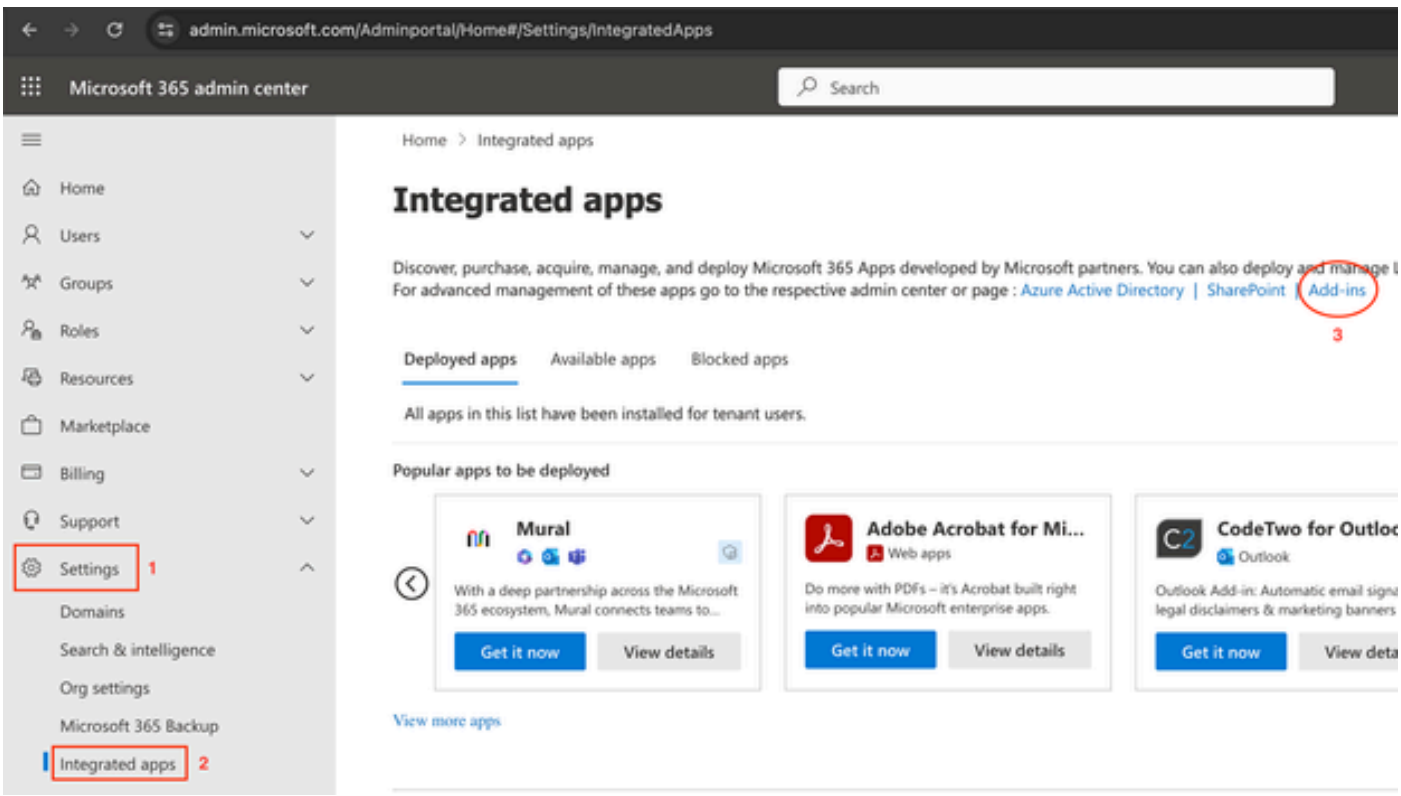


CRES-Admin-Portal - ADDIN-Konfiguration

Manifestdatei in Microsoft 365 hochladen, um das Add-In für den E-Mail-Verschlüsselungsdienst bereitzustellen

1. Melden Sie sich als Administrator beim Microsoft 365 Admin Center an. (Microsoft 365 Admin Center).

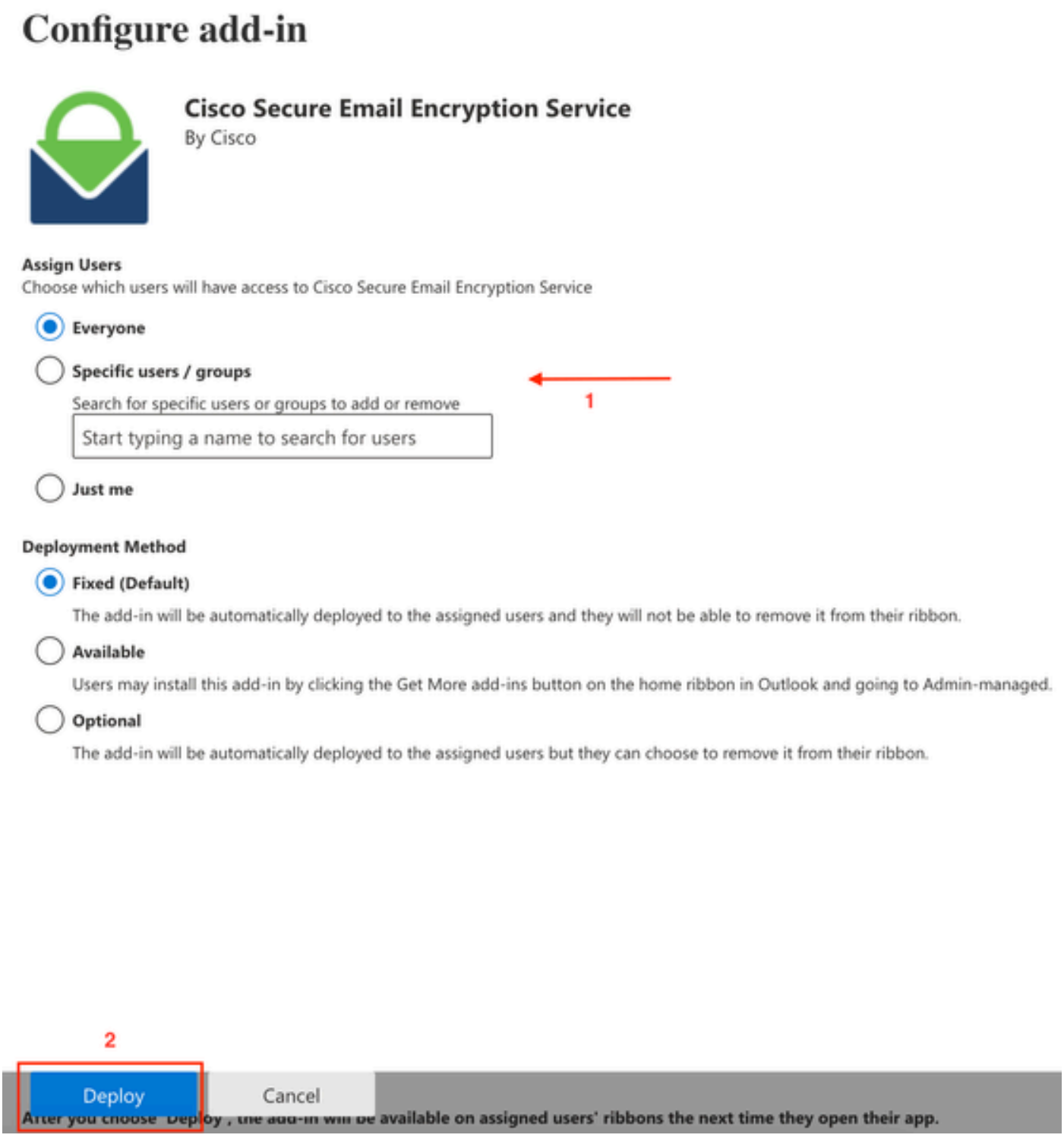
2. Navigieren Sie zu Settings > Integrated apps und klicken Sie auf **Add-Ins**.



Microsoft O365-Addin-Einstellungen

3. Klicken Sie Deploy Add-inund wählen Sie Upload Custom Apps. Wählen Sie die Datei aus, die Sie aus dem Cisco Email Encryption Service-Administratorportal heruntergeladen haben, I have the manifest file (.xml) on this deviceund laden Sie sie hoch. Klicken Sie auf .Upload

4. Weisen Sie im nächsten Schritt Benutzer zu, die Zugriff auf den Cisco Secure Email Encryption Service benötigen. Um die Bereitstellung schrittweise umzusetzen, wählen Sie Specifc Users/groupsund klicken Sie auf Deploy.



Microsoft O365-Zusatzkonfiguration

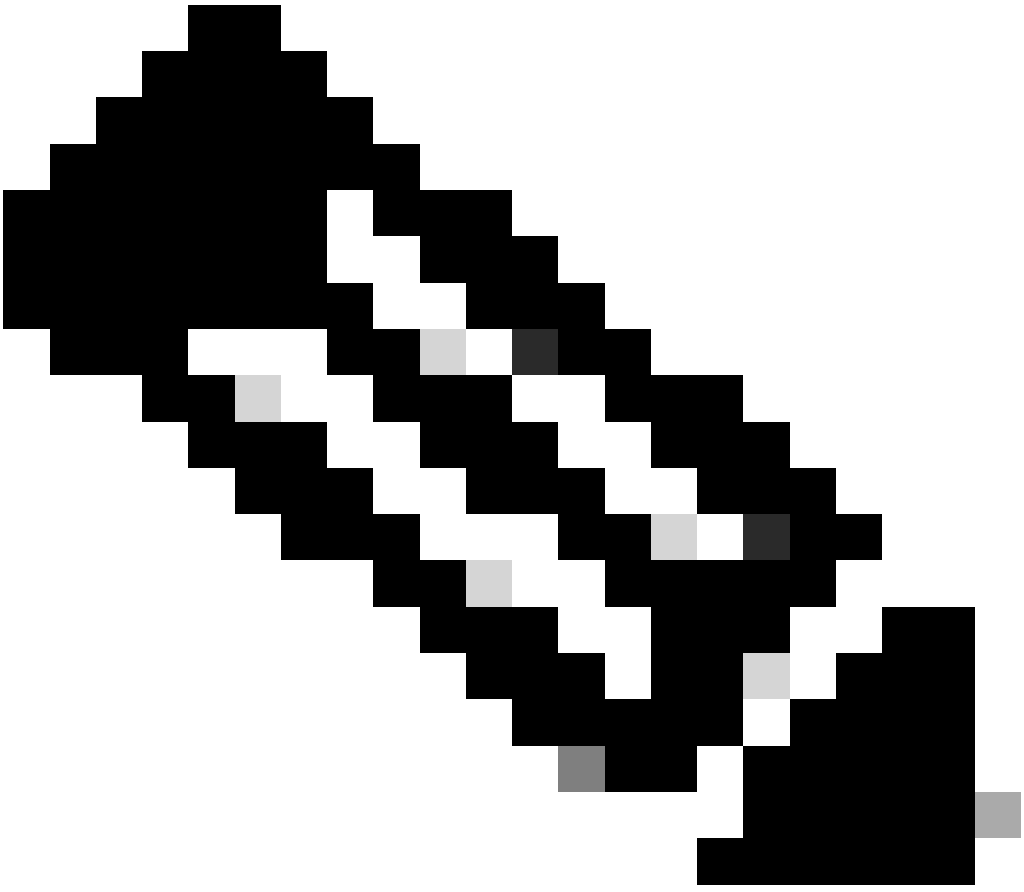
5. Nach der erfolgreichen Bereitstellung des Add-Ins kann es bis zu 12 Stunden dauern, bis es auf den Multifunktionsleisten des Endbenutzers

(Outlook-Client) angezeigt wird.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Starten Sie Outlook für Office 365/Microsoft 365 oder Outlook Web App, erstellen Sie die Nachricht, die Sie verschlüsseln möchten, und fügen Sie mindestens einen gültigen Empfänger hinzu.



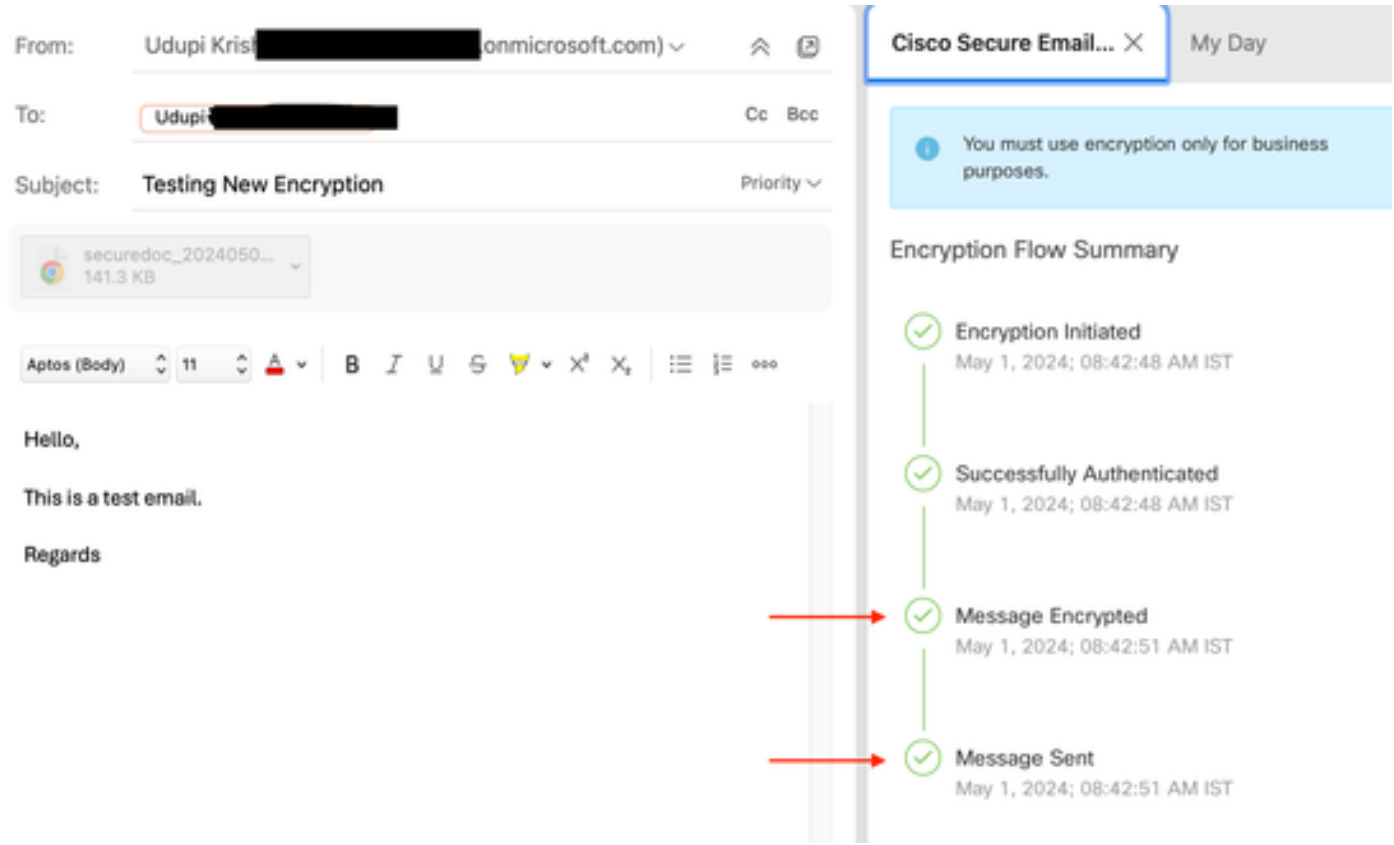
Hinweis: Wenn der vom Administrator festgelegte Verschlüsselungstyp "Verschlüsseln" lautet, stellen Sie sicher, dass die Nachricht vervollständigt und gültige Empfänger hinzugefügt wurden, bevor Sie mit dem nächsten Schritt fortfahren. Nach Schritt 3 wird die Nachricht verschlüsselt und sofort gesendet.

---

2. Öffnen Sie das Add-In Cisco Secure Email Encryption Service, und klicken Sie darauf.

- Klicken Sie in Outlook Web App auf das Auslassungszeichen (neben den Schaltflächen Senden und Verwerfen), und klicken Sie auf Cisco Secure Email Encryption Service.
- Klicken Sie in Outlook für Windows oder MacOS in der Multifunktionsleiste oder Symbolleiste auf **Verschlüsseln**.
- Wenn Sie Outlook für MacOS Version 16.42 oder höher verwenden und die neue Outlook-Schnittstelle verwenden, klicken Sie in der Symbolleiste auf klickenCisco Secure Email Encryption Service.

3. Geben Sie Ihre Anmeldeinformationen ein, und klicken Sie auf Sign in. (Nur wenn der Verschlüsselungstyp Flag ist, klicken Sie auf Send).



Microsoft Outlook-Verschlüsselungsstatus

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Benutzerleitfaden für Kontoadministratoren zum Cisco Secure Email Encryption Service
- Cisco Secure Email Encryption Service Add-in - Benutzerhandbuch
- Microsoft Entra Application Registration Guide
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.