Cisco RES: Konfigurationsbeispiel für die Kontobereitstellung für virtuelle, gehostete und Hardware-ESA

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Cisco RES-Kontobereitstellung für virtuelle und gehostete ESA
Cisco RES-Kontobereitstellung für Hardware-ESA
Benachrichtigung des Kontoadministrators und Kontoüberprüfung
Erstellen von Cisco RES-Kontonummern
Ermitteln Sie die Cisco RES-Version.
Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Verschlüsselungsprofil erstellen und die Kontobereitstellung für eine Cisco E-Mail Security Appliance (ESA) mit der Erstellung eines Cisco Registered Envelope Service (RES)-Kontos abschließen.

> **Hinweis**: Derzeit bestehen Unterschiede zwischen virtueller und gehosteter ESA und Hardware-ESA. Diese werden im Dokument beschrieben.

In diesem Artikel wird auch erläutert, wie Sie das "Profil <*profile_name*> nicht bereitstellen können: Konto-Fehler kann nicht gefunden werden", da dieser Fehler in der Regel von der virtuellen und gehosteten ESA angezeigt wird, wenn Sie versuchen, ein Verschlüsselungsprofil hinzuzufügen. Wenn Sie diesen Fehler erhalten, gehen Sie wie im Abschnitt "Virtuelle und gehostete ESA" beschrieben vor.

Voraussetzungen

Stellen Sie sicher, dass der *IronPort*-Feature-Schlüssel für *E-Mail-Verschlüsselung* auf der ESA installiert ist. Überprüfen Sie dies über die ESA-GUI, **Systemverwaltung > Feature Keys** oder die ESA-CLI mit **Feature**.

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Cisco RES-Kontobereitstellung für virtuelle und gehostete ESA

Virtuelle und gehostete ESA erhalten diesen Fehler, wenn sie versuchen, ein Verschlüsselungsprofil bereitzustellen:

Cisco muss Ihnen beim Erstellen des RES-Bereitstellungskontos behilflich sein. Senden Sie eine E-Mail-Anfrage an stg-cres-provisioning@cisco.com mit folgenden Informationen:

- Name des Kontos (Geben Sie den genauen Firmennamen an, wie dies erforderlich ist.)

  Wenn es sich um ein gehostetes Kundenkonto handelt, notieren Sie den Kontonamen, der enden soll als *"<Kontoname> GEHOSTET"*.

- E-Mail-Adresse(n) für den Account-Administrator (Geben Sie eine oder mehrere Admin-E-Mail-Adressen an.)

- Die vollständige Seriennummer (*) der EUB(s)

- Alle Domänen für das Kundenkonto, die zu Administrationszwecken dem RES-Konto zugeordnet werden sollten

(*) Die Seriennummern der Appliance können Sie über die **GUI Systemverwaltung > Feature Keys** oder die Appliance-CLI aufrufen, wenn Sie die Befehlsversion ausführen.

Hinweis: Wenn bereits ein RES-Konto bereitgestellt wurde, geben Sie den Firmennamen oder die zuvor verwendete RES-Kontonummer an. Dadurch wird sichergestellt, dass alle neuen Seriennummern der Geräte dem richtigen Konto hinzugefügt werden, und es werden doppelte Firmeninformationen und doppelte Bereitstellung vermieden.

Hinweis: Eine Geräte-Seriennummer kann nur für ein Konto in RES registriert werden. Bei einem RES-Konto sind möglicherweise mehrere Appliances für Ihr Unternehmen registriert.

Anfragen an stg-cres-provisioning@cisco.com werden innerhalb eines Werktags, wenn nicht früher, bearbeitet. Sobald die Seriennummern registriert oder die Bereitstellung eines neuen RES-Kontos abgeschlossen ist, wird eine Bestätigungs-E-Mail gesendet. Die E-Mail-Adresse, die für das Administratorkonto verwendet wird, erhält eine Benachrichtigung, sobald sie als Administrator für das zugehörige Konto aufgeführt ist.

Wenn Sie bereits versucht haben, das Verschlüsselungsprofil auf der ESA zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie in der ESA-GUI zu **Security Services > Cisco IronPort Email Encryption > Email Encryption Profiles**.

2. Klicken Sie auf **Erneute Bereitstellung**. Dieser Vorgang wird dann wie **bereitgestellt** abgeschlossen.

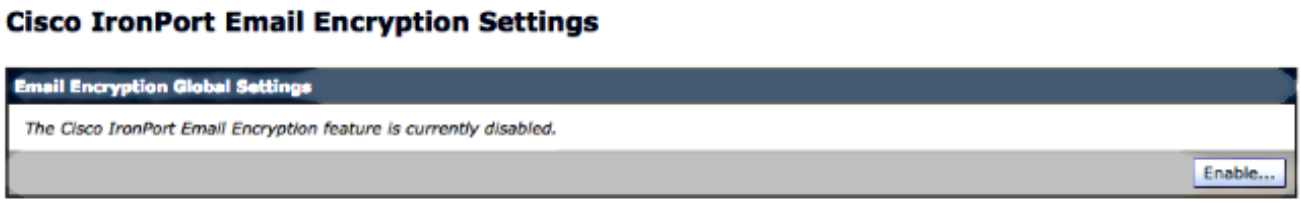
3. Falls nicht, fahren Sie mit den Schritten im nächsten Abschnitt fort, um das Verschlüsselungsprofil auf der ESA zu erstellen.

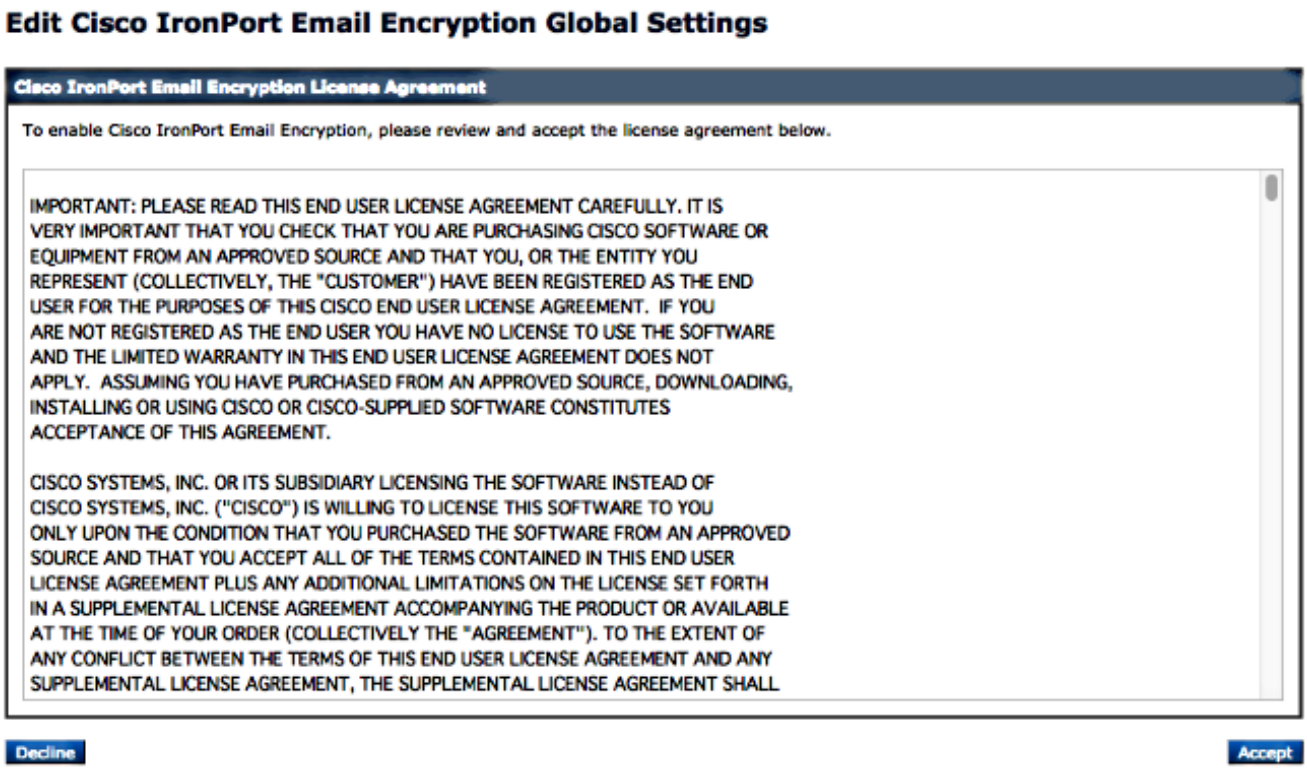
Cisco RES-Kontobereitstellung für Hardware-ESA

Ab Cisco RES Version 4.2 kann die Hardware-ESA automatisch bereitgestellt werden, d. h. es ist nicht mehr erforderlich, die Kontoerstellung per E-Mail anzufordern.

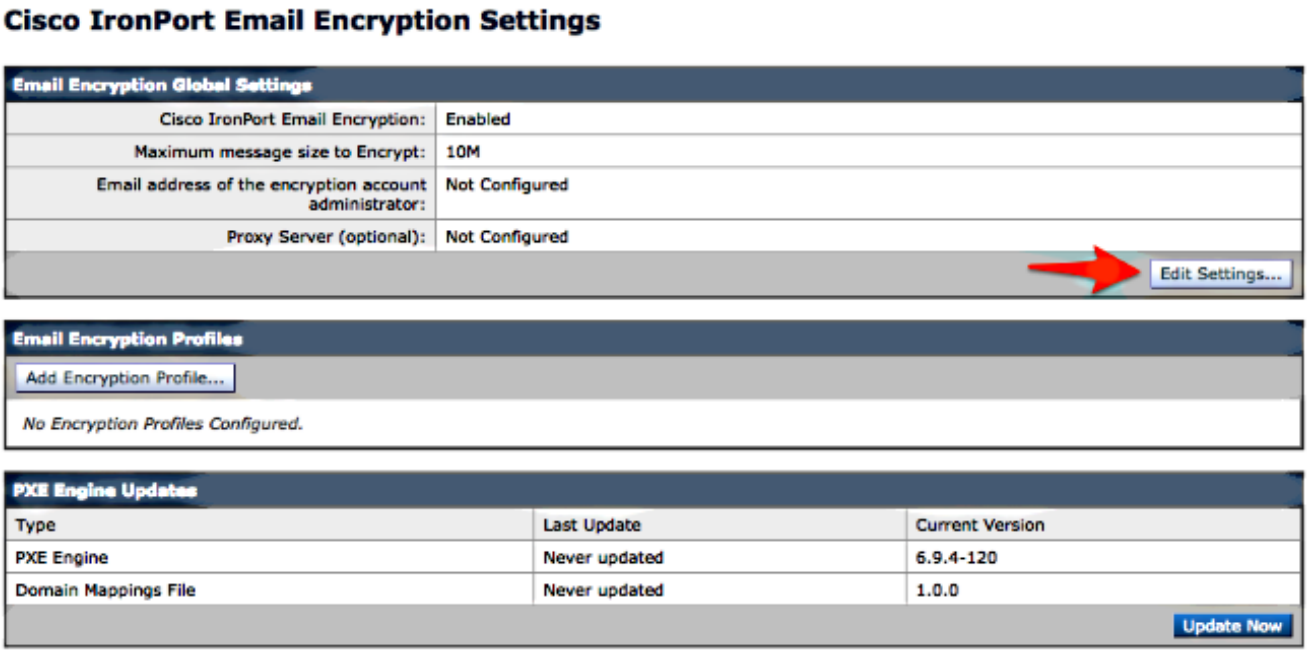
Für Hardware-ESA führen Sie die folgenden Schritte aus, um die Bereitstellung des Verschlüsselungsprofils abzuschließen.

1. Navigieren Sie in der ESA-GUI zu **Security Services > Cisco IronPort Email Encryption**, aktivieren Sie die Funktion, und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), sofern sie noch nicht abgeschlossen ist:

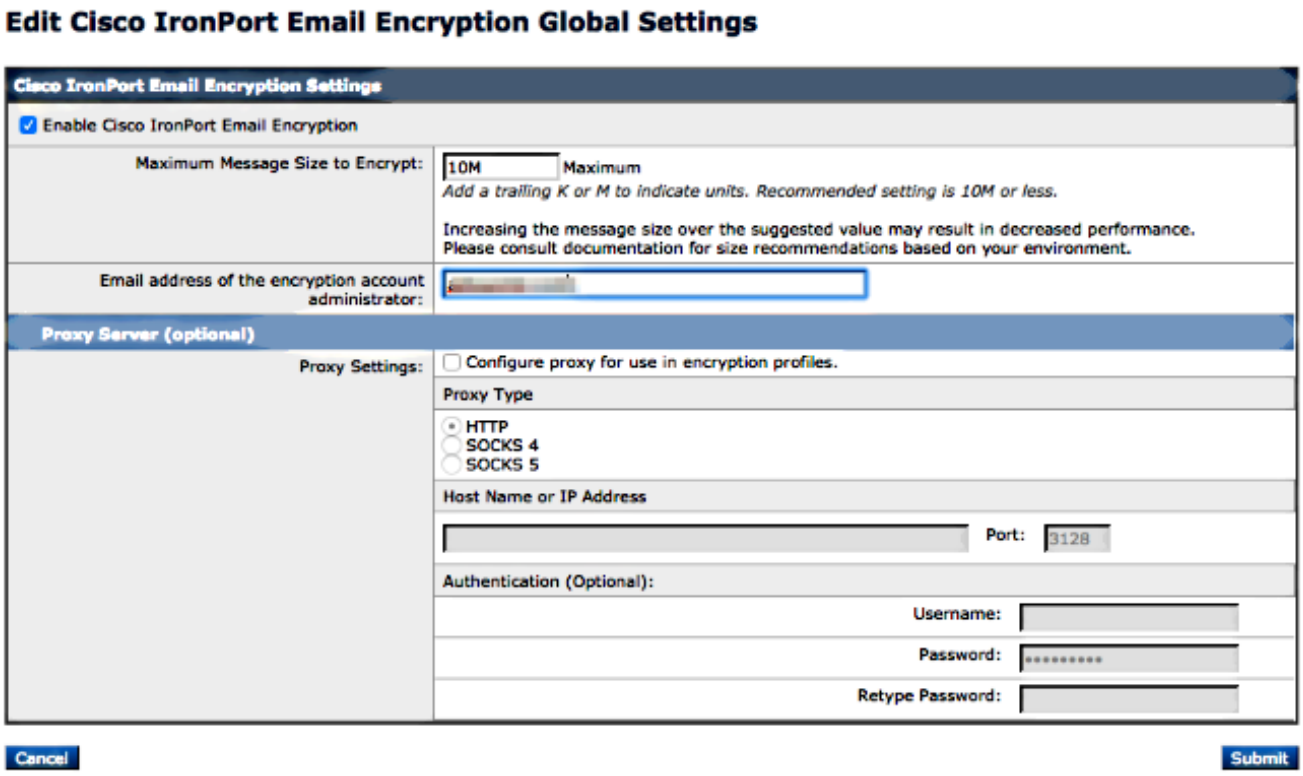




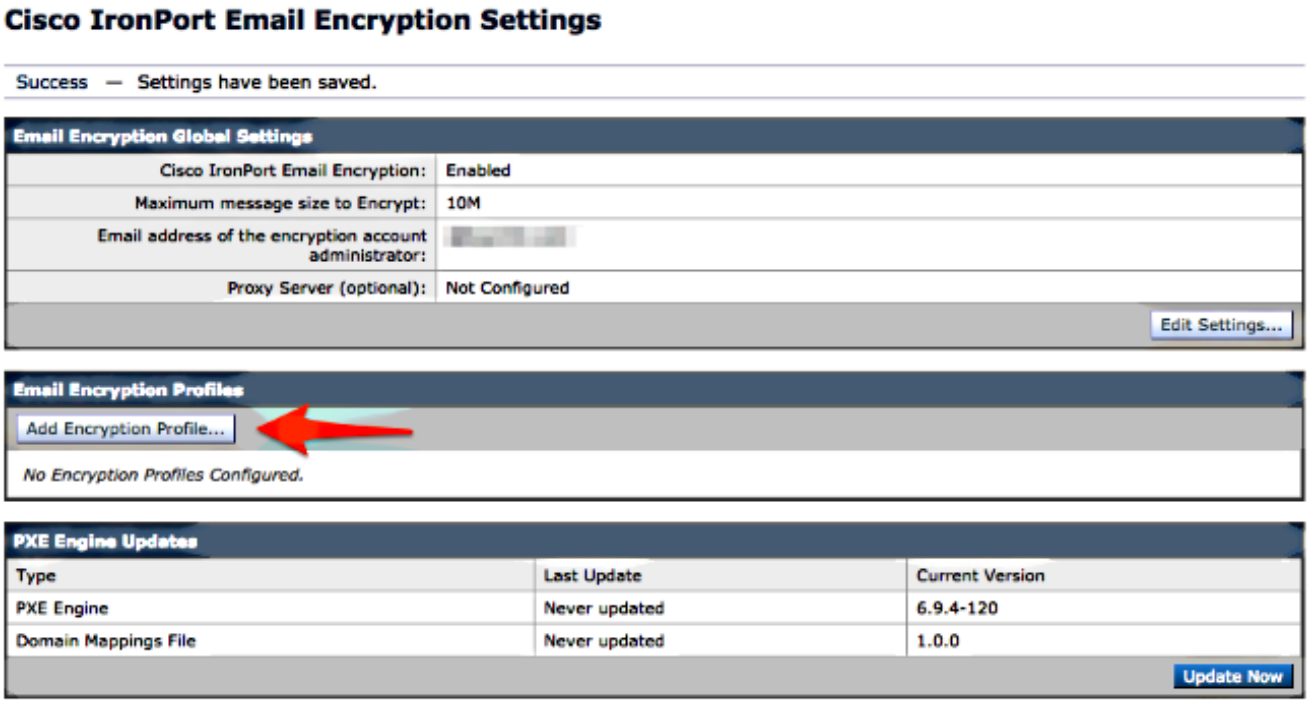
2. Klicken Sie auf **Einstellungen bearbeiten**:



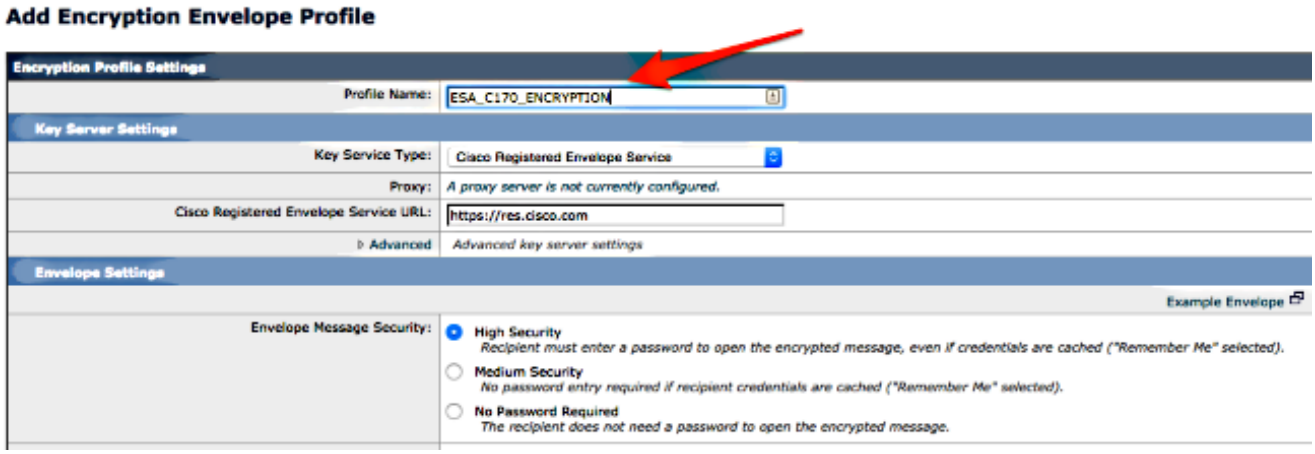
Geben Sie eine E-Mail-Adresse für die E-Mail-Adresse im Feld für den Administrator des Verschlüsselungskontos ein, und klicken Sie auf **Senden**:



3. Erstellen Sie ein Verschlüsselungsprofil mit der Schaltfläche **Verschlüsselungsprofil hinzufügen**:

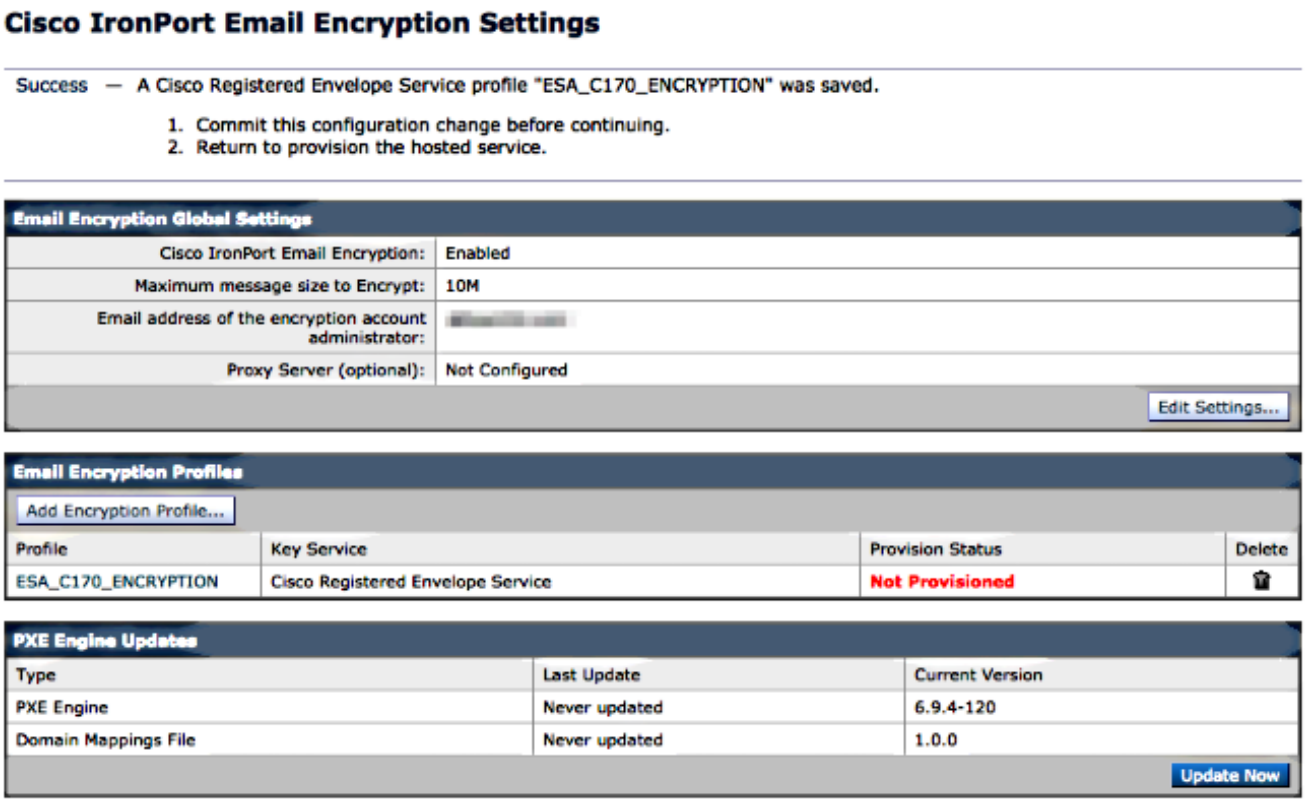


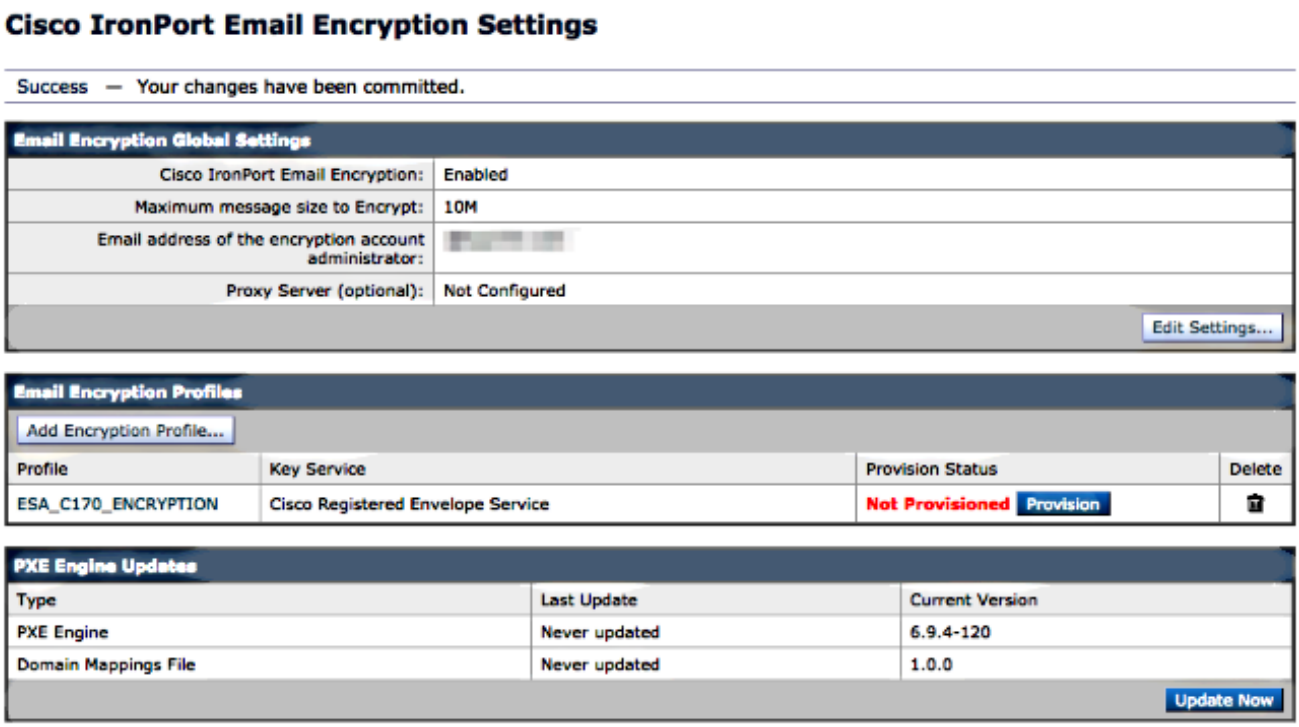
4. Stellen Sie bei der Profilerstellung sicher, dass Sie einen aussagekräftigen Profilnamen angeben, damit Sie diesen später mit Nachrichten- oder Inhaltsfiltern verknüpfen können, die zur Verschlüsselung erstellt wurden:



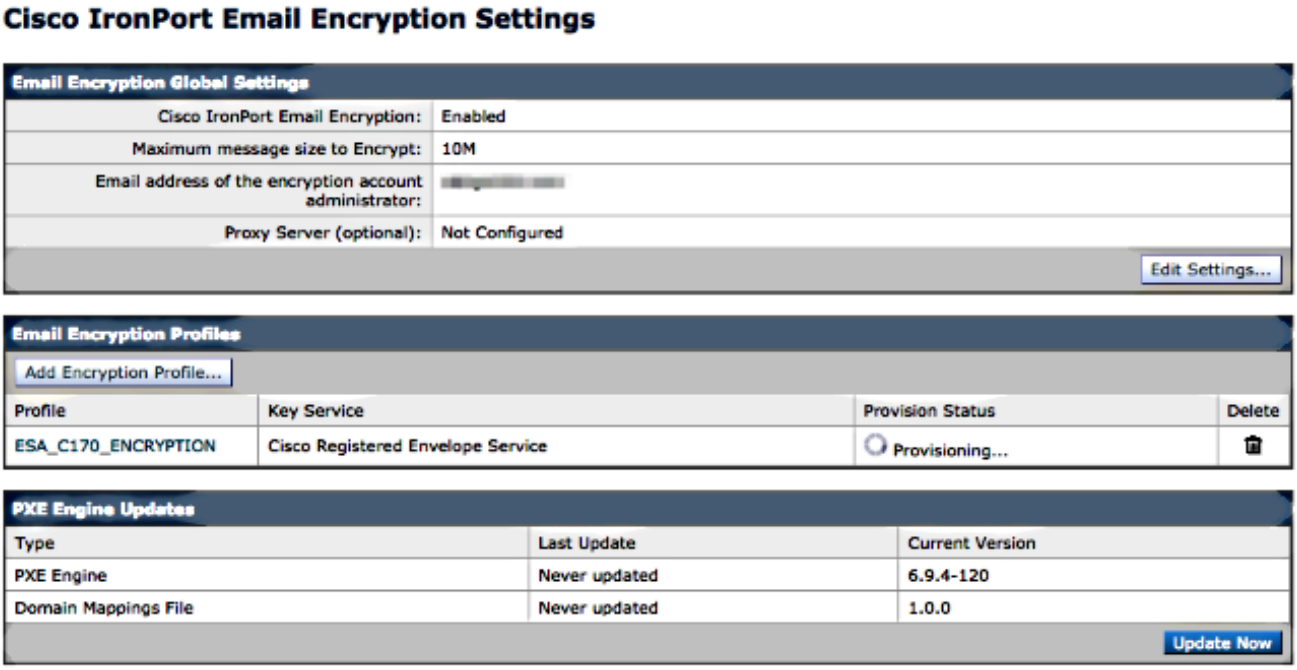
5. Klicken Sie abschließend auf **Senden**.

Not Provisioned (Nicht bereitgestellt) wird für Ihr neu erstelltes Profil aufgelistet. Sie müssen Ihre Änderungen bestätigen, bevor Sie fortfahren.

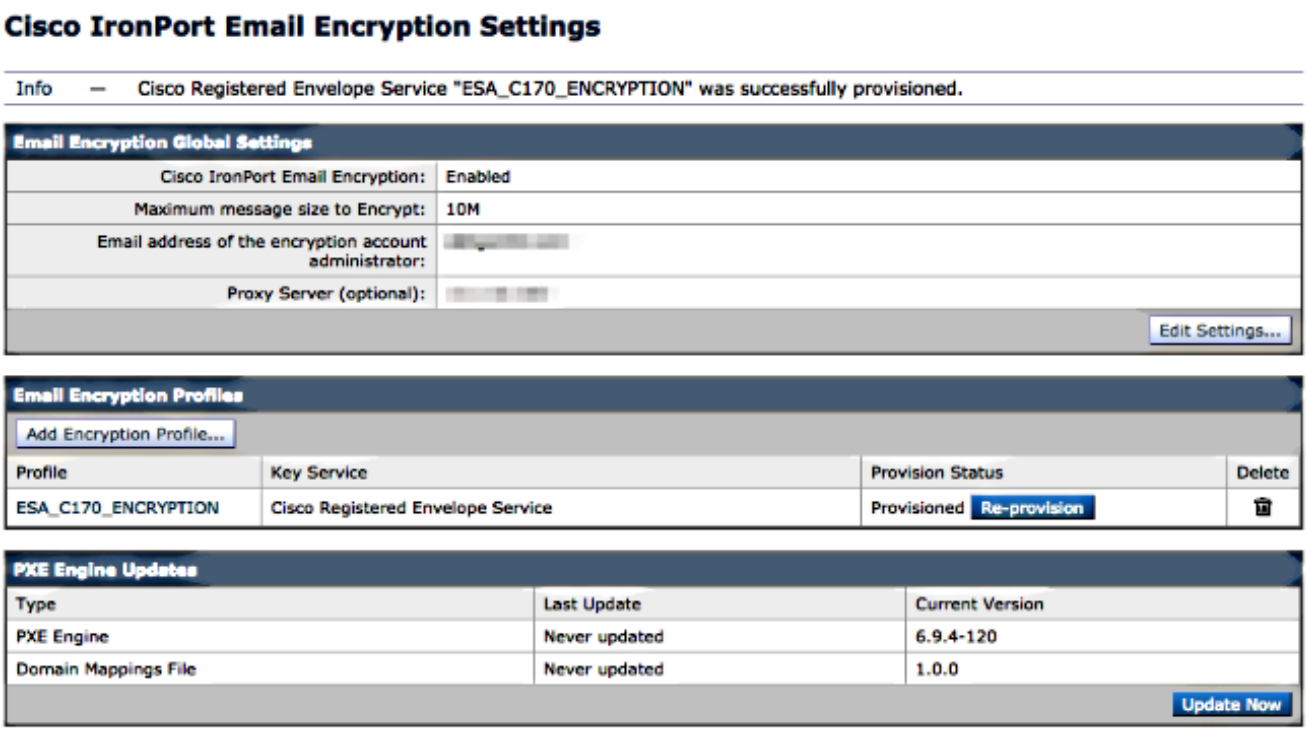




6. Wenn Ihre Änderungen übernommen wurden, klicken Sie auf **Provisioning (Bereitstellung)**, um den Bereitstellungsprozess abzuschließen:



7. Nach Abschluss der Bereitstellung erhalten Sie eine Bannerbenachrichtigung, und die Schaltfläche zur Profilbereitstellung ändert sich in **Erneute Bereitstellung**:



Das Verschlüsselungsprofil ist abgeschlossen. Sie können nun E-Mails von Ihrer(n) Appliance(n) über RES erfolgreich verschlüsseln.

Benachrichtigung des Kontoadministrators und Kontoüberprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die E-Mail-Adresse, die zuvor für die **E-Mail-Adresse des Verschlüsselungskontenadministrators** angegeben wurde, erhält eine Benachrichtigung über den Status des Kontoadministrators:

You are now an account administrator for the '[redacted]' account. This account is currently Active.

As an account administrator, you can perform various tasks such as locking or expiring Registered Envelopes and viewing usage statistics for the account.

If you were not previously registered, a user name (email address) and password has been automatically generated for you. You will need to reset this password in order to access your account. Click here https://res.cisco.com/websafe/pswdForgot.action to set your new password.

If you have already registered and have a password please go to https://res.cisco.com/admin and log in.

IMPORTANT
To help keep your personal information safe, Cisco recommends that you never give your Cisco Registered Envelope Service password to anyone, including Cisco employees.

Thank you,
Cisco Registered Envelope Service Customer Support

Sobald Sie die Kontoverwaltungsbenachrichtigung erhalten haben, melden Sie sich bei der RES-Admin-Website an und überprüfen Sie Ihr Konto. Nach der Anmeldung sehen Sie die in der Kontenübersicht erstellte Kontonummer. Senden Sie eine E-Mail-Anfrage an stg-cres-provisioning@cisco.com mit folgenden Informationen:

- Kontonummer
- Kontoname
- Alle Domänen für das Konto, die dem RES-Konto zu Administrationszwecken zugeordnet werden sollten

Dadurch wird sichergestellt, dass Ihr Konto volle Transparenz für ALLE Domänenkonten erhält,

die über RES registriert sind.

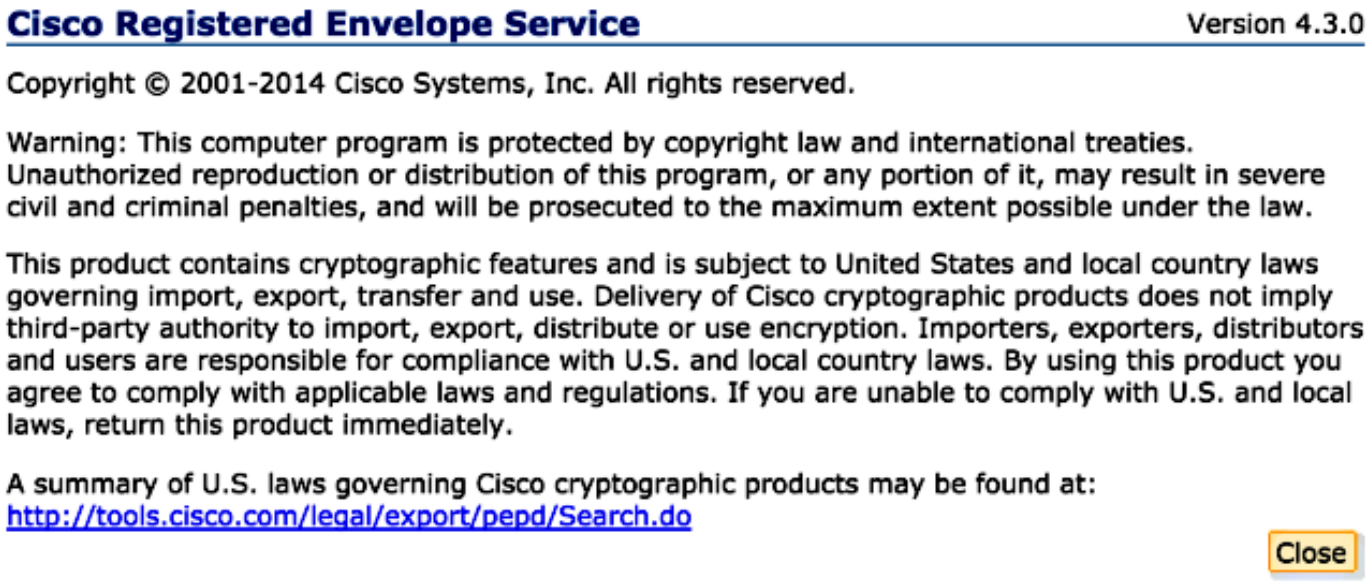
Erstellen von Cisco RES-Kontonummern

Die RES-Kontonummer wird basierend auf den an die Appliance gebundenen Vertragsinformationen erstellt. Die Kontonummer wird basierend auf der Global Ultimate (GU) ID und ein Kontoname basierend auf dem **Namen** des **installierten Standorts** generiert. Prüfen Sie, ob Sie über die richtige Cisco Connection Online (CCO) und die entsprechenden Berechtigungen verfügen, und überprüfen Sie das Cisco Service Contract Center (CSCC).

Ermitteln Sie die Cisco RES-Version.

Wählen Sie in der rechten oberen Ecke des Hyperlinks Info aus. Die aktuelle Version von Cisco RES wird im Popup-Fenster angezeigt.

Beispiel:



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Geben Sie den folgenden Befehl ein, um zu bestätigen, dass die ESA erfolgreich mit den Cisco RES-Servern kommunizieren kann:

```
myesa.local> telnet res.cisco.com 443

Trying 184.94.241.74...
Connected to 184.94.241.74.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Zugehörige Informationen

- Konfigurationsbeispiel für E-Mail-Verschlüsselung der ESA
- Wie lauten die IPs und Hostnamen der Cisco RES-Schlüsselserver?
- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems