

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 IronPort Email Encryption Settings

Error — Unable to provision profile "ESA_C170_ENCRYPTION" for reason: Cannot find account. Please make sure that you have correctly registered your appliance with the hosted service and try again, or contact customer support for assistance.

The screenshot shows two configuration pages. The top page is titled "Email Encryption Global Settings" and contains the following information:

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	[Redacted]
Proxy Server (optional):	Not Configured

An "Edit Settings..." button is located at the bottom right of this section.

The bottom page is titled "Email Encryption Profiles" and contains a table of profiles:

Profile	Key Service	Provision Status	Delete
ESA_C170_ENCRYPTION	Cisco Registered Envelope Service	Not Provisioned Provision	[Delete Icon]

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:

Cisco IronPort Email Encryption Settings



Edit Cisco IronPort Email Encryption Global Settings

Cisco IronPort Email Encryption License Agreement

To enable Cisco IronPort Email Encryption, please review and accept the license agreement below.

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL

[Decline](#) [Accept](#)

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

Cisco IronPort Email Encryption Settings

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	Not Configured
Proxy Server (optional):	Not Configured

[Edit Settings...](#)

Email Encryption Profiles

[Add Encryption Profile...](#)

No Encryption Profiles Configured.

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

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

Edit Cisco IronPort Email Encryption Global Settings

Cisco IronPort Email Encryption Settings

Enable Cisco IronPort Email Encryption

Maximum Message Size to Encrypt:	<input type="text" value="10M"/> Maximum <small>Add a trailing K or M to indicate units. Recommended setting is 10M or less.</small>
Email address of the encryption account administrator:	<input type="text"/>

Proxy Server (optional)

Proxy Settings: Configure proxy for use in encryption profiles.

Proxy Type

HTTP
 SOCKS 4
 SOCKS 5

Host Name or IP Address

Port:

Authentication (Optional):

Username:

Password:

Retype Password:

- Erstellen Sie ein Verschlüsselungsprofil mit der Schaltfläche **Verschlüsselungsprofil** hinzufügen:

Cisco IronPort Email Encryption Settings

Success — Settings have been saved.

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	<input type="text"/>
Proxy Server (optional):	Not Configured

Email Encryption Profiles



No Encryption Profiles Configured.

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0

- 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:

Add Encryption Envelope Profile

Encryption Profile Settings	
Profile Name:	ESA_C170_ENCRYPTION
Key Server Settings	
Key Service Type:	Cisco Registered Envelope Service
Proxy:	A proxy server is not currently configured.
Cisco Registered Envelope Service URL:	https://res.cisco.com
Advanced	Advanced key server settings
Envelope Settings	
Example Envelope	
Envelope Message Security:	<input checked="" type="radio"/> High Security <small>Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).</small> <input type="radio"/> Medium Security <small>No password entry required if recipient credentials are cached ("Remember Me" selected).</small> <input type="radio"/> No Password Required <small>The recipient does not need a password to open the encrypted message.</small>

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.

Cisco IronPort Email Encryption Settings

Success — A Cisco Registered Envelope Service profile "ESA_C170_ENCRYPTION" was saved.

1. Commit this configuration change before continuing.
2. Return to provision the hosted service.

Email Encryption Global Settings	
Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	
Proxy Server (optional):	Not Configured
Edit Settings...	

Email Encryption Profiles			
Add Encryption Profile...			
Profile	Key Service	Provision Status	Delete
ESA_C170_ENCRYPTION	Cisco Registered Envelope Service	Not Provisioned	

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0
Update Now		

Cisco IronPort Email Encryption Settings

Success — Your changes have been committed.

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	[REDACTED]
Proxy Server (optional):	Not Configured

[Edit Settings...](#)

Email Encryption Profiles

[Add Encryption Profile...](#)

Profile	Key Service	Provision Status	Delete
ESA_C170_ENCRYPTION	Cisco Registered Envelope Service	Not Provisioned Provision	

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

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

Cisco IronPort Email Encryption Settings

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	[REDACTED]
Proxy Server (optional):	Not Configured

[Edit Settings...](#)

Email Encryption Profiles

[Add Encryption Profile...](#)

Profile	Key Service	Provision Status	Delete
ESA_C170_ENCRYPTION	Cisco Registered Envelope Service	Provisioning...	

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

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

Cisco IronPort Email Encryption Settings

Info — Cisco Registered Envelope Service "ESA_C170_ENCRYPTION" was successfully provisioned.

Email Encryption Global Settings

Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	[REDACTED]
Proxy Server (optional):	[REDACTED]

[Edit Settings...](#)

Email Encryption Profiles

[Add Encryption Profile...](#)

Profile	Key Service	Provision Status	Delete
ESA_C170_ENCRYPTION	Cisco Registered Envelope Service	Provisioned Re-provision	

PXE Engine Updates

Type	Last Update	Current Version
PXE Engine	Never updated	6.9.4-120
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

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 Verschlüsselungskontoadministrators** angegeben wurde, erhält eine Benachrichtigung über den Status des Kontoadministrators:

You are now an account administrator for the '~~XXXXXXXXXXXXXXXXXXXX~~' 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/pwdForgot.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:

Cisco Registered Envelope Service

Version 4.3.0

Copyright © 2001-2014 Cisco Systems, Inc. All rights reserved.

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://tools.cisco.com/legal/export/pepd/Search.do>

Close

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-Schlüsselsever?](#)
- [Cisco Email Security Appliance - Benutzerhandbücher](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)