

RIS Cisco: Esempio di configurazione ESA Virtual, Hosted e Hardware

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Provisioning account Cisco RES per ESA virtuale e ospitata](#)

[Cisco RES Account Provisioning per Hardware ESA](#)

[Notifica all'amministratore dell'account e verifica dell'account](#)

[Creazione numero account Cisco RES](#)

[Verifica della versione Cisco RES](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come creare un profilo di crittografia e completare il provisioning di un account per Cisco Email Security Appliance (ESA) con la creazione di un account Cisco Registered Envelope Service (RES).

Nota: Esistono differenze correnti tra Virtual e Hosted ESA e Hardware ESA. Queste sono descritte nel documento.

In questo articolo viene inoltre descritto come correggere il problema relativo all'impossibilità di effettuare il provisioning del profilo <nome_profilo> per il seguente motivo: "Unable find account" ("Impossibile trovare account"), poiché questo errore viene normalmente presentato da ESA virtuale e ospitata quando si tenta di aggiungere un profilo di crittografia. Se viene visualizzato questo errore, completare la procedura descritta nella sezione ESA virtuale e ospitata.

Prerequisiti

Verificare che la chiave della funzione *IronPort Email Encryption* sia installata sull'ESA. Verificare questa condizione dalla GUI ESA, da **System Administration > Feature Keys** o dalla CLI ESA con **feature key**.

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Configurazione

Provisioning account Cisco RES per ESA virtuale e ospitata

L'ESA virtuale e quella ospitata rilevano questo errore quando tentano di effettuare il provisioning di un profilo di crittografia:

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.

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

[Edit Settings...](#)

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

Cisco deve assistere e completare l'account di provisioning RES. Inviare una richiesta via e-mail a stg-cres-provisioning@cisco.com con queste informazioni:

- Nome dell'account (specificare il nome esatto della società, in quanto è necessario che venga elencato).

Se si tratta di un account cliente ospitato, indicare che il nome dell'account deve terminare con "<Nome account> HOSTED".

- Indirizzi di posta elettronica da utilizzare per l'account amministratore (specificare gli indirizzi di posta elettronica dell'amministratore corrispondenti).
- Il numero di serie completo (*) della o delle UEE

- Qualsiasi/tutti i domini del conto cliente da associare al conto RES a fini amministrativi

(*) I numeri di serie degli accessori possono essere richiamati da **GUI System Administration > Feature Keys** (Amministrazione sistema GUI > Chiavi funzione) o da CLI dell'accessorio se si esegue la versione del comando.

Nota: se esiste già un conto RES con provisioning, fornire il nome della società o il numero del conto RES utilizzato in precedenza. In questo modo si garantisce che i nuovi numeri di serie degli accessori vengano aggiunti al conto corretto ed evita la duplicazione delle informazioni aziendali e del provisioning.

Nota: un numero di serie di accessorio può essere registrato in un solo account in RES. In un account RES possono essere registrati più accessori per la società.

Le richieste inviate a stg-cres-provisioning@cisco.com vengono gestite entro un giorno lavorativo, se non prima. Dopo la registrazione dei numeri di serie o il completamento del provisioning di un nuovo account RES, viene inviato un messaggio di posta elettronica di conferma. L'indirizzo di posta elettronica utilizzato per l'account admin riceve una notifica quando viene elencato come amministratore per l'account associato.

Se si è già provato a creare il profilo di crittografia sull'ESA, attenersi alla seguente procedura:

1. Dalla GUI dell'ESA, selezionare **Security Services > Cisco IronPort Email Encryption > Email Encryption Profiles**.
2. Fare clic su **Riesegui provisioning**. L'operazione viene quindi completata come **provisioning**.
3. In caso contrario, continuare con i passaggi della sezione successiva per creare il profilo di crittografia sull'ESA.

Cisco RES Account Provisioning per Hardware ESA

A partire dalla versione 4.2 di Cisco RES, l'ESA hardware può effettuare il provisioning automatico, pertanto non è più necessario richiedere la creazione dell'account tramite e-mail.

Per l'ESA hardware, attenersi alla seguente procedura per completare il provisioning del profilo di crittografia.

1. Dalla GUI dell'ESA, selezionare **Security Services > Cisco IronPort Email Encryption**, abilitare la funzione e accettare il Contratto di Licenza con l'Utente Finale (EULA), se non è già stato completato:

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. Fare clic su **Modifica impostazioni**:

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](#)

Immettere un indirizzo di posta elettronica amministrativo per l'indirizzo di posta elettronica del campo Amministratore account di crittografia e fare clic su **Invia**:

Edit Cisco IronPort Email Encryption Global Settings

Cisco IronPort Email Encryption Settings

Enable Cisco IronPort Email Encryption

Maximum Message Size to Encrypt: Maximum
Add a trailing K or M to indicate units. Recommended setting is 10M or less.

Increasing the message size over the suggested value may result in decreased performance. Please consult documentation for size recommendations based on your environment.

Email address of the encryption account administrator:

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:

3. Creare un profilo di crittografia utilizzando il pulsante **Add Encryption Profile**:


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

4. Durante la creazione del profilo, assicurarsi di fornire un nome di profilo significativo in modo da poterlo correlare in seguito ai filtri messaggi o contenuti creati per utilizzare la crittografia:

Add Encryption Envelope Profile

Encryption Profile Settings

Profile Name:

Key Server Settings

Key Service Type:

Proxy: *A proxy server is not currently configured.*

Cisco Registered Envelope Service URL:

Advanced *Advanced key server settings*

Envelope Settings Example Envelope

Envelope Message Security:

- High Security**
Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).
- Medium Security**
No password entry required if recipient credentials are cached ("Remember Me" selected).
- No Password Required**
The recipient does not need a password to open the encrypted message.

5. Al termine, fare clic su **Submit** (Invia).

L'opzione **Non attivato** è elencata per il profilo appena creato. È necessario eseguire il commit delle modifiche prima di procedere:

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:	<input type="text" value=""/>
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. Dopo aver eseguito il commit delle modifiche, fare clic su **Provisioning** per completare il processo di provisioning:

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. Al termine del provisioning, si riceve una notifica banner e il pulsante di attivazione del profilo cambia in **Riesegui provisioning**:

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](#)

Profilo di crittografia completato. È ora possibile crittografare correttamente i messaggi provenienti dagli accessori tramite RES.

Notifica all'amministratore dell'account e verifica dell'account

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

L'indirizzo di posta elettronica specificato in precedenza per l'indirizzo di posta elettronica dell'amministratore dell'account di crittografia riceve notifica dello stato dell'amministratore dell'account:

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

Dopo aver ricevuto la notifica relativa all'amministrazione dell'account, accedere al sito [Amministrazione risorse umane](#) e verificare l'account. Una volta eseguito l'accesso, il numero di account verrà visualizzato nel riepilogo account. Inviare una richiesta via e-mail a stg-cres-provisioning@cisco.com con queste informazioni:

- Numero conto
- Nome account
- Qualsiasi/tutti i domini del conto che devono essere mappati al conto RES a fini amministrativi

In questo modo si garantisce la piena visibilità dell'account per TUTTI gli account di dominio

registrati tramite Servizi di ripristino.

Creazione numero account Cisco RES

Il numero di conto RES viene creato in base alle informazioni sul contratto associate all'accessorio. Il numero di conto viene generato in base all'ID Global Ultimate (GU), mentre il nome di conto viene generato in base al **nome della sede di installazione**. Per procedere alla revisione, accertarsi di disporre del corretto Cisco Connection Online (CCO) e dei relativi diritti, quindi controllare il [Cisco Service Contract Center](#) (CSCC).

Verifica della versione Cisco RES

Da <http://res.cisco.com/admin>, nell'angolo in alto a destra, selezionare il collegamento ipertestuale [Informazioni su](#). La versione Cisco RES corrente viene visualizzata nel popup.

Esempio:

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per verificare che l'ESA sia in grado di comunicare con i server Cisco RES, immettere questo comando:

```
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.
```

Informazioni correlate

- [Esempio di configurazione di ESA Email Encryption](#)
- [Quali sono gli IP e i nomi host dei server chiave Cisco RES?](#)
- [Cisco Email Security Appliance - Guide per l'utente](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)