

Cisco RES: Account Provisioning for Virtual, Hosted, and Hardware ESA Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Cisco RES Account Provisioning for Virtual and Hosted ESA](#)

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

[Account Administrator Notification and Account Verification](#)

[Cisco RES Account Number Creation](#)

[Determine the Cisco RES Version](#)

[Troubleshooting](#)

[Related Information](#)

Introduction

This document describes how to create an encryption profile and complete account provisioning for a Cisco Email Security Appliance (ESA) with the creation of a Cisco Registered Envelope Service (RES) account.

Note: There are current differences between Virtual and Hosted ESA and Hardware ESA. These are described in the document.

This article also discusses how to correct the "Unable to provision profile <profile_name> for reason: Cannot find account" error, as this error is normally presented from Virtual and Hosted ESA when you attempt to add an encryption profile. If you receive this error, complete the steps provided in the Virtual and Hosted ESA section.

Prerequisites

Ensure that you have the *IronPort Email Encryption* feature key installed on your ESA. Verify this from the ESA GUI, **System Administration > Feature Keys**, or on the ESA CLI with **featurekey**.

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Cisco RES Account Provisioning for Virtual and Hosted ESA

Virtual and Hosted ESA encounter this error when they attempt to provision an encryption profile:

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 must assist and complete the RES provisioning account for you. Initiate an email request to stg-cres-provisioning@cisco.com with this information:

- Name of account (Specify the exact company name, as you require this to be listed.)

If this is for a Hosted customer account, notate the account name to end as "*<Account Name> HOSTED*".

- Email address(es) to be used for the Account Admin (Specify a corresponding admin email address(es).)
- The complete serial number (*) of ESA(s)
- Any/all domains for the customer account that should be mapped to the RES account for administration purposes

(*) Appliance serial numbers can be located from the **GUI System Administration > Feature Keys**, or appliance CLI if you run the command version.

Note: If there is an already provisioned RES account, provide the company name or RES account number previously used. This assures that any new appliance serial numbers are added to the correct account, and avoids any duplication of company information and

provisioning.

Note: An appliance serial number can be registered to only one account in RES. One RES account might have multiple appliances registered to your company.

Requests sent to stg-cres-provisioning@cisco.com are handled within one business day, if not sooner. A confirmation email is sent once the serial numbers are registered or new RES account provisioning is completed. The email address that is used for the admin account receives a notification once it is listed as an administrator for the associated account.

If you had already tried to create the encryption profile on the ESA, complete these steps:

1. From the ESA GUI, navigate to **Security Services > Cisco IronPort Email Encryption > Email Encryption Profiles**.
2. Click **Re-provision**. This then completes as **Provisioned**.
3. If it does not, continue to the steps in the next section in order to create the encryption profile on the ESA.

Cisco RES Account Provisioning for Hardware ESA

As of Cisco RES Version 4.2, the hardware ESA has the ability to auto-provision, which means it is no longer necessary to request account creation by email.

For hardware ESA, follow these steps to complete the encryption profile provisioning.

1. From the ESA GUI, navigate to **Security Services > Cisco IronPort Email Encryption**, enable the feature, and accept the End User License Agreement (EULA), if not completed already:

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. Click **Edit Settings**:

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](#)

Ensure that you enter an administrative email address for the email address of the encryption account administrator field, and click **Submit**:

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. Create an encryption profile with the **Add Encryption Profile** button:


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. During profile creation, ensure that you provide a meaningful Profile Name so that you can relate this later to message or content filter(s) created to use encryption:

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. Click **Submit** when completed.

Not Provisioned is listed for your newly-created profile. You must commit your changes before you proceed:

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. After your changes are committed, click **Provision** in order to complete the provisioning process:

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. Once the provisioning is completed, you receive a banner notification and the profile provision button changes to **Re-provision**:

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](#)

The Encryption Profile is complete. You are now able to successfully encrypt mail from your appliance(s) through RES.

Account Administrator Notification and Account Verification

Use this section in order to confirm that your configuration works properly.

The email address that was specified earlier for the **Email address of the encryption account administrator** receives notification of account administrator status:

You are now an account administrator for the 'Cisco Registered Envelope Service' 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

Once you have received the Account Administration notification, log into the [RES Admin](#) site and verify your account. After you log in, you see the account number created in the Account Summary. Initiate an email request to stg-cres-provisioning@cisco.com with this information:

- Account Number
- Account Name
- Any/all domains for the account that should be mapped to the RES account for administration purposes

This ensures that your account has full visibility to ALL domain accounts that are registered through RES.

Cisco RES Account Number Creation

The RES account number is created based on the contract information tied to the appliance. The account number is generated based on the Global Ultimate (GU) ID and an Account Name is generated based on the **Installed At Site Name**. In order to review, assure that you have proper Cisco Connection Online (CCO) and entitlement, and check the [Cisco Service Contract Center \(CSCC\)](#).

Determine the Cisco RES Version

From <http://res.cisco.com/admin>, in the upper right-hand corner, select the [About](#) hyperlink. The current Cisco RES version is displayed in the pop-up.

Example:

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

Troubleshooting

This section provides information you can use in order to troubleshoot your configuration.

In order to confirm that the ESA is able to successfully communicate with the Cisco RES servers, enter this command:

```
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.
```

Related Information

- [ESA Email Encryption Configuration Example](#)

- [What are the IPs and hostnames of the Cisco RES key servers?](#)
- [Cisco Email Security Appliance - End-User Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)