Blue Coat SSL Visibility Appliance
Luna SP

Integration Guide

THE
DATA
PROTECTION
COMPANY

Document Information

Product Version	3.0
Document Part Number	007-012787-001 Rev. A
Release Date	October 2014

Revision History (*optional)

Remove this section if it will not be used.

Revision	Date	Reason

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction 4
Third-Party Software Acknowledgement 4
Overview 4
Audience 4
Working with a Luna SP HSM 5
Adding an HSM 6
Writing HSM Configuration in Policy 10
Support Contacts 13

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Blue Coat SSL Visibility Appliance. Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

SafeNet Luna SP hardware security modules (HSMs) integrate with Blue Coat's SSL Visibility Appliance to enhance the security of SSL traffic in enterprise networks while maintaining the privacy needs of the organization. Luna SP stores CA certificates and private keys used by the SSL Visibility Appliance to carry out SSL inspection using certificate re-sign. The CA certificate and key are stored in the Luna SP's secure, tamper-proof hardware appliance to make them inaccessible to unauthorized users, as well as easy to manage and scale as the capacity needs grow. The SSL Visibility Appliance identifies and manages all SSL-encrypted traffic to effectively enable protected communications based on acceptable use policies.

Audience

All products manufactured and distributed by SafeNet, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

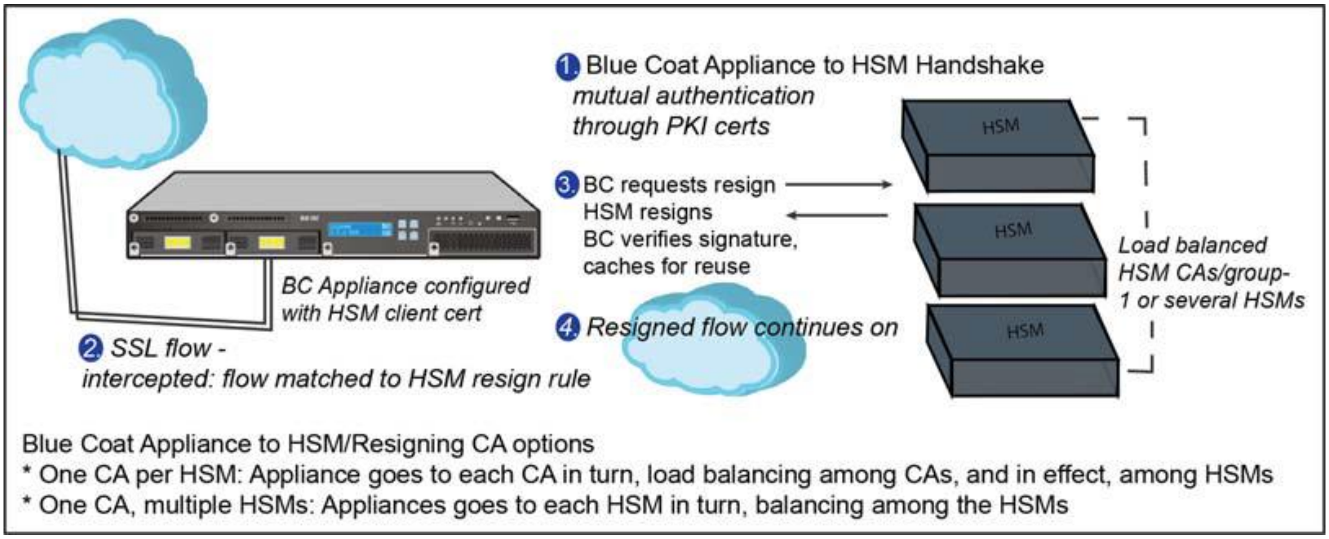
Working with a Luna SP HSM

A Hardware Security Module (HSM) provides additional security for storing cryptographic keys and certificates. The SSL Visibility Appliance is able to use a network-attached HSM appliance to store resigning CA keys, and to perform digital signature operations.

The SSL Visibility Appliance interacts with an HSM on its management interface. It exchanges signing requests and responses with the attached HSM appliance, over HTTPS. When mutually authenticated during the SSL handshake, the SSL Visibility Appliance sends resigning CAs data to the HSM; the HSM signs the data and returns the signature to the SSL Visibility Appliance.

An SSL Visibility Appliance can work with multiple HSM appliances, and multiple SSLV appliances can work with the same HSM.

In the event that policy a rule using an HSM to sign cannot work due to lack of response from the HSM, the attempt is logged, and the applicable policy action configured for HSM failure (for example, cut through, drop, or reject) occurs.



1 Blue Coat Appliance to HSM Handshake
mutual authentication
through PKI certs
3 BC requests resign
HSM resigns
BC verifies signature,
caches for reuse
4 Resigned flow continues on
BC Appliance configured
with HSM client cert
2 SSL flow -
intercepted: flow matched to HSM resign rule
HSM
HSM
HSM
Load balanced
HSM CAs/group-
1 or several HSMs
Blue Coat Appliance to HSM/Resigning CA options
* One CA per HSM: Appliance goes to each CA in turn, load balancing among CAs, and in effect, among HSMs
* One CA, multiple HSMs: Appliances goes to each HSM in turn, balancing among the HSMs

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

Blue Coat provides a Blue Coat HSM Agent and CLI to install on the Luna SP, which will be used to interact with Blue Coat appliances.

An SSL Visibility Appliance/HSM configuration has these steps, assuming the HSM is properly configured:

1. Configure the client certificate(s) used to authenticate with the HSM (or HSMs).
2. Configure an External CA(s) list used to authenticate the HSM.
3. Configure the HSM, using the client certificate(s) and External CA List(s) configured above.
4. Configure HSM resigning CA(s) using the HSM appliance configured above.
5. (Optional) Add the HSM resigning CAs) configured above to HSM resigning CA load balancing group(s).
6. Configure resign rule(s) in SSL Visibility Appliance policy using the HSM resigning CA load balancing group(s) configured previously, or the default **All HSM Resigning Certificate Authorities** group. If the default group is used, step 5 is not required.

Adding an HSM

Before You Begin: PKI Basics

HSM validation requires an external certificate authority list on the SSL Visibility Appliance. The SSL Visibility Appliance will validate non-self-signed HSM certificates using the external CA list selected for that HSM in the **PKI > HSM** Appliances window. The appliance will validate the server certificate chain.

NOTE: The CN or SAN in the HSM certificate must match the HSM appliance hostname or IP address for validation to succeed.

Adding a Trusted Certificate

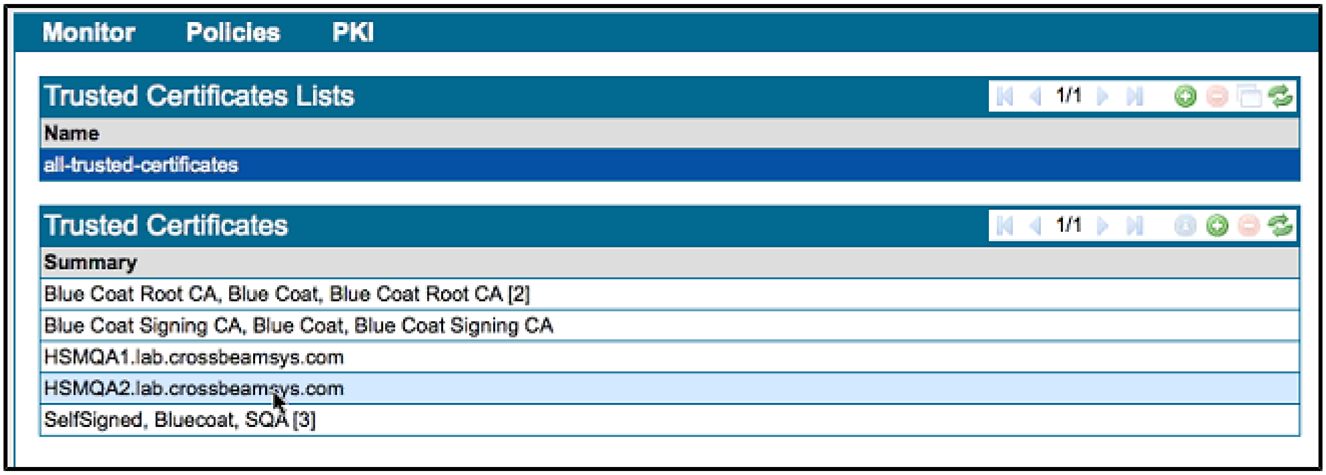
The SSL Visibility requires a trusted certificate for the communication channel with the HSM. The SSL Visibility Appliance will only validate a self-signed HSM certificate if it is a Trusted Certificate.

The communication channel certificate is the HSM server certificate which the SSL Visibility Appliance will use to verify and trust the HSM.

Highlight the **all-trusted-certificates** item in the **Trusted Certificates Lists** panel, then click the Add (plus sign tool) icon in the **Trusted Certificates** panel. The **Add Trusted Certificates** window pops up.

Upload the .pem or DER certificate file, or paste its text into the appropriate tab, then click Add. The new certificate will appear in the **Trusted Certificates** panel.

NOTE: Make note of the identifying details such as the DN and the key alias.



Name
all-trusted-certificates

Summary
Blue Coat Root CA, Blue Coat, Blue Coat Root CA [2]
Blue Coat Signing CA, Blue Coat, Blue Coat Signing CA
HSMQA1.lab.crossbeamsys.com
HSMQA2.lab.crossbeamsys.com
SelfSigned, Bluecoat, SQA [3]

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

Adding a Client Certificate

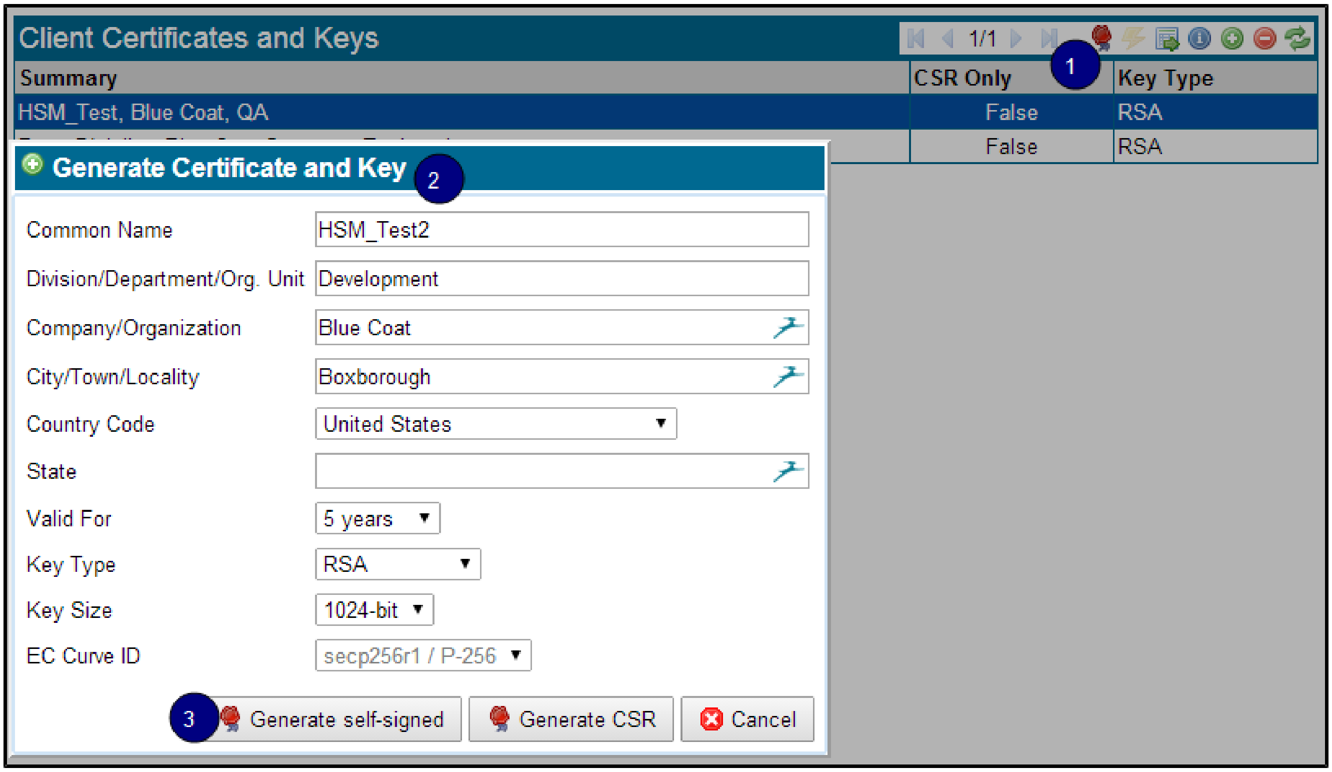
The SSL Visibility Appliance is a client to an HSM server, so the HSM must have a client certificate to authenticate the SSL Visibility Appliance. The SSL Visibility Appliance must have a client certificate for each

HSM it interacts with. The client certificates must be available to create policy. The “Manage PKI” role is required.

An authorized user can

Generate a client key and self signed certificate:

1. Generate a client key and self signed certificate; press the Generate (rose) icon.
2. Fill out the **Generate Certificate and Key** form.
3. Click **Generate self-signed**.



Client Certificates and Keys

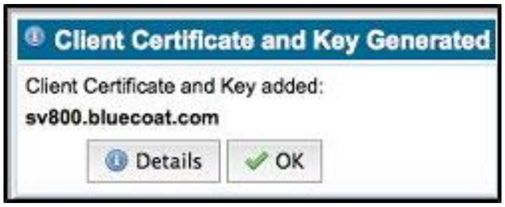
Summary	CSR Only	Key Type
HSM_Test, Blue Coat, QA	False	RSA
	False	RSA

Generate Certificate and Key

Common Name	HSM_Test2
Division/Department/Org. Unit	Development
Company/Organization	Blue Coat
City/Town/Locality	Boxborough
Country Code	United States
State	
Valid For	5 years
Key Type	RSA
Key Size	1024-bit
EC Curve ID	secp256r1 / P-256

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

When the certificate has been created, you will see a confirmation message:



Client Certificate and Key Generated

Client Certificate and Key added:
sv800.bluecoat.com

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

Generate a client key and a CSR, and get it signed by a third party resigning CA.

1. Press the Generate (rose) icon,
2. Fill out the **Generate Certificate and Key** form.

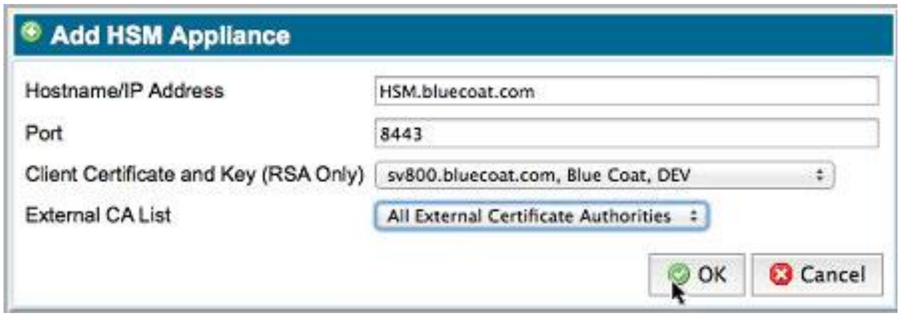
3. Click **Generate CSR**.
4. Send the CSR to your third-party CA, and have it signed.
5. Upload or copy in the signed certificate using the Install Certificate icon (lightning bolt).

Import a client key and already signed certificate.

1. Press Add (the plus icon).
2. Upload or Paste in the already signed certificate.

Add an HSM

Use the **PKI > HSM Appliances** window to manage attached HSM appliance connections. A user must have a Manage PKI role to add, remove, and edit HSM appliances. Users with Manage PKI and Manage Policy roles can view configured HSM appliances.



Add HSM Appliance

Hostname/IP Address: HSM.bluecoat.com

Port: 8443

Client Certificate and Key (RSA Only): sv800.bluecoat.com, Blue Coat, DEV

External CA List: All External Certificate Authorities

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

- **Hostname/IP Address**: Enter the hostname that appears in the HSM-created certificates.
- **Port**: Use the default 8443 port.
- **Client Certificate and Key (RSA Only)**: Select the client certificate created for the specific HSM.
- **External CA List**: Select the External CA List to used to authenticate this HSM appliance.

Adding Resigning Certificates

The SSL Visibility has a **HSM Certificate Authorities Groups** list of load-balancing groups on the **PKI > Resigning Certificate Authorities** window. The **all-hsm-certificate-authorities** list must contain all resigning certificates used by connected HSMs. The keys are stored remotely on the HSMs.

Creating, editing, and deleting HSM resigning CAs, and running self-tests, requires the Manage PKI authorization role.

A resigning certificate can be generated on the HSM with Blue Coat CLI. You can also create a CSR with the CLI, then sign the certificate off of the HSM.

Add HSM resigning CAs to the **PKI** store; they are initially added to the **all-hsm-certificate-authorities** list.

Adding a new HSM resigning certificate authority

1. Highlight the HSM Resigning Certificate Authorities Groups you want to add an authority to, then click Add in the HSM Resigning Certificate Authorities panel.

The Add HSM Resigning Certificate Authority window opens.

2. You may upload or paste in the certificate on the appropriate tab.

   - ○ **HSM Appliance:** Select the HSM this resigning CA uses (created at **PKI > AddHSM**).
   - ○ **HSM Key Alias**: Enter the key alias configured for that resigning CA on the HSM appliance.
   - ○ **CRL URL**: Applies when a resigning CA CRL is published at a public URL.

3. Click Add.

4. Click Apply near the footer to save your changes.

NOTE: Immediately after adding a new HSM resigning CA to the PKI store, the new CA will appear in yellow in the list. Make sure to Apply the changes, and then use the Refresh tool in the header in order for the new CA to appear in green

NOTE: HSM Resigning CA Status Colors

The color of the resigning CA in the list gives you the status of that CA.

- Green color = HSM CA is in OK/active state
- Yellow color = HSM CA status has not been checked
- Red color = HSM CA is in failed state

Load Balancing Groups

The SSL Visibility Appliance uses round robin load balancing, distributing connections evenly across the array of HSM resigning CAs in the group, when the configuration includes a HSM resigning CA group, and an inspected SSL flow matches a policy HSM group rule. If each resigning CA uses a separate HSM appliance, the load balancing occurs over the HSM appliances. You can create a new subset group, if required. The SSL Visibility Appliance will load balance between the HSM resigning CAs in the group.

If an HSM in a group, fails, the SSL Visibility Appliance automatically adjusts the load balancing in the group, excluding the failed HSM.The SSL Visibility Appliance periodically checks the failed appliance, and when a check succeeds, the HSM is restored and returned to the load balancing group.

Create a new HSM authorities load balancing group

1. On the PKI > Resigning Certificate Authorities window, select Add in the HSM Resigning Certificate Authorities Groups panel header.

2. On the resultant Add Resigning Certificate Authority List window, provide a name for the list, then click OK.

3. Highlight the new group in the HSM Resigning Certificate Authorities Groups panel SV800 & SV1800 Administration & Deployment Guide

4. Click Add in the HSM Resigning Certificate Authorities panel. The Manage PKI Custom List Items window opens.

5. Use the Add to Custom List and Remove from Custom List buttons to create your list.

6. Click OK.

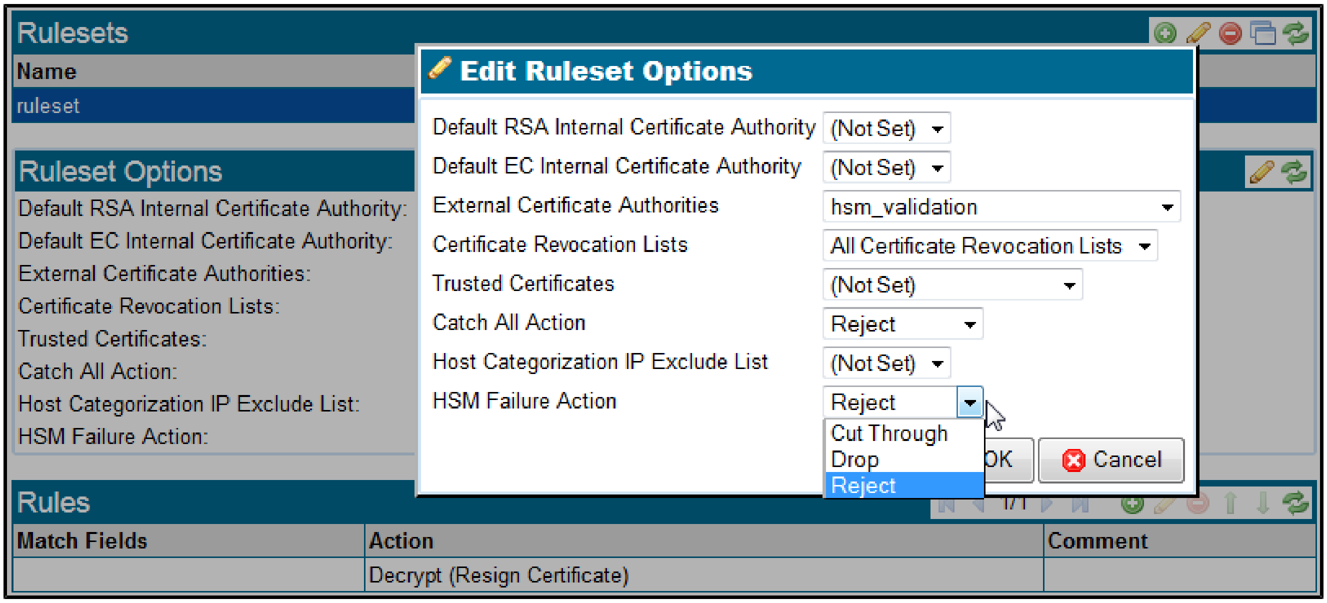
7. Click Apply near the footer to save your changes.

Running a Self-Test

Once you have the HSM connection configured, resigning certificates established, and a policy (ruleset) in place, you can manually run a self-test to verify resigning. Click the Play icon in the **HSM Resigning Certificate Authorities** header. In the self-test, the appliance sends a signing request to the HSM, and then validates the returned signature. To pass the test, the HSM must have been contacted, the HSM resign operation succeeded, and the returned signature verified as valid.

Writing HSM Configuration in Policy

The Ruleset Options panel (Policies > Rulesets) includes a HSM Failure Option. which defines what action the SSL Visibility Appliance will take when an HSM resign operation fails.



Rulesets
Name
ruleset
Ruleset Options
Default RSA Internal Certificate Authority:
Default EC Internal Certificate Authority:
External Certificate Authorities:
Certificate Revocation Lists:
Trusted Certificates:
Catch All Action:
Host Categorization IP Exclude List:
HSM Failure Action:
Edit Ruleset Options
Cut Through
Drop
Reject
OK
Cancel
Rules
1/1

Default RSA Internal Certificate Authority: (Not Set)
Default EC Internal Certificate Authority: (Not Set)
External Certificate Authorities: hsm_validation
Certificate Revocation Lists: All Certificate Revocation Lists
Trusted Certificates: (Not Set)
Catch All Action: Reject
Host Categorization IP Exclude List: (Not Set)
HSM Failure Action: Reject

Match Fields	Action	Comment
	Decrypt (Resign Certificate)	

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

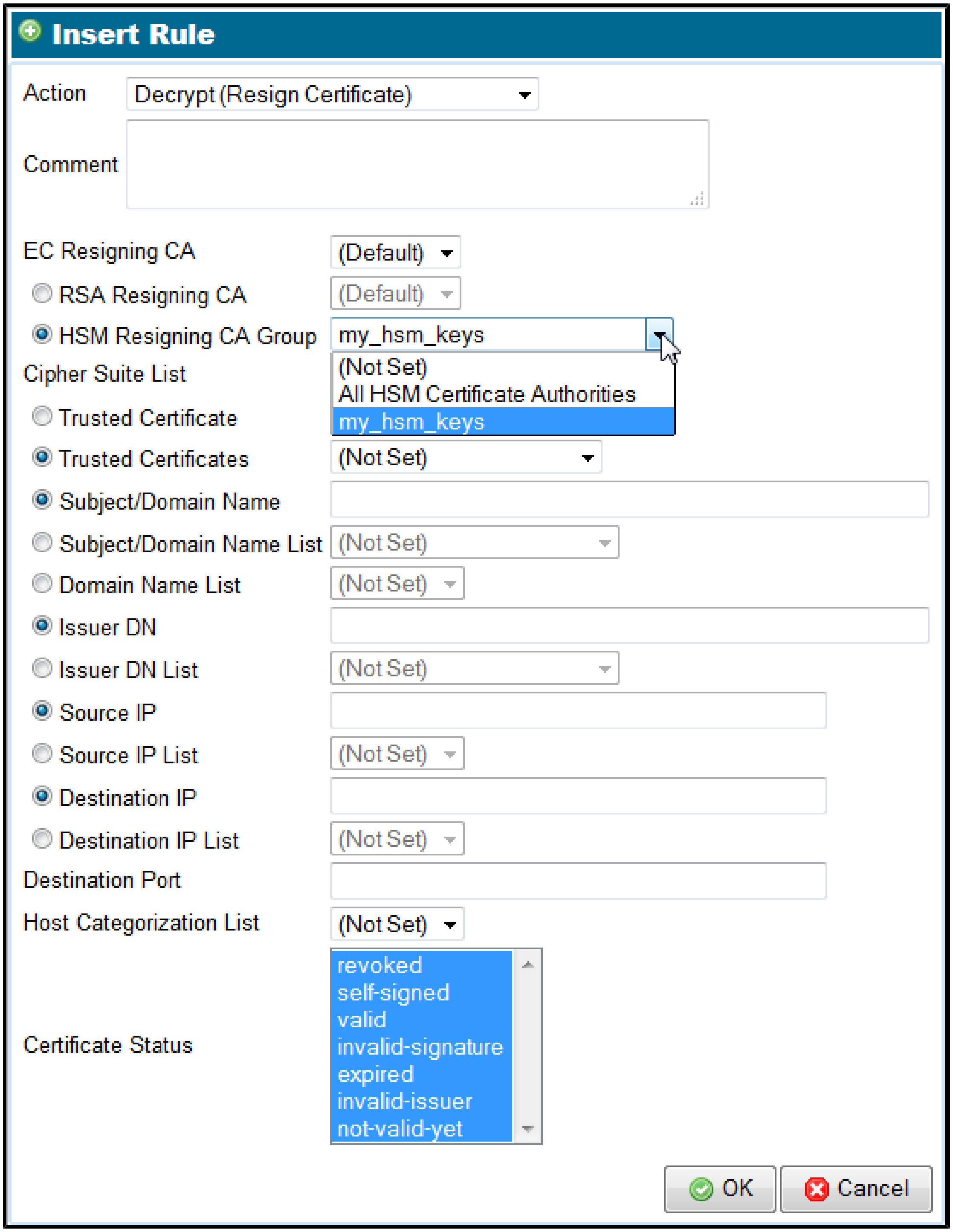
1. Create and name a ruleset: click Add in the **Rulesets** panel header and name the ruleset.

2. Click Edit (pencil tool) in the **Ruleset Options** panel header; the **Edit Ruleset Options** window displays, as shown in the figure. Here is the HSM selection to note:

- **HSM Failure Action:** Typically, you will Cut Through an SSL flow where the HSM resign operation has failed; you may also Reject or Drop the flows.

3. Click OK.

4. In the **Rules** panel, click Add. The **Insert Rule** window opens.



Insert Rule

Action: Decrypt (Resign Certificate)

Comment:

EC Resigning CA: (Default)

○ RSA Resigning CA: (Default)

● HSM Resigning CA Group: my_hsm_keys
- (Not Set)
- All HSM Certificate Authorities
- my_hsm_keys

Cipher Suite List

○ Trusted Certificate

● Trusted Certificates: (Not Set)

● Subject/Domain Name:

○ Subject/Domain Name List: (Not Set)

○ Domain Name List: (Not Set)

● Issuer DN:

○ Issuer DN List: (Not Set)

● Source IP:

○ Source IP List: (Not Set)

● Destination IP:

○ Destination IP List: (Not Set)

Destination Port:

Host Categorization List: (Not Set)

Certificate Status:
- revoked
- self-signed
- valid
- invalid-signature
- expired
- invalid-issuer
- not-valid-yet

(The screen image above is from Blue Coat. Trademarks are the property of their respective owners.)

- **Action:** Select **Decrypt (Resign Certificate)**
- **EC Resigning CA:** Select the CA to resign flows signed with EC certificate authorities.
- **RSA Resigning CA:** Select the CA to resign flows signed with RSA certificate authorities.

HSM Resigning CA Group: Select the HSM Resigning CA Group, then the HSM CA group which will resign HSM SSL traffic. Resigning traffic is load balanced across the CAs.

5. Click OK. The window closes.

6. On the **Rulesets** window, click Apply at **Policy Changes** in the footer. When everything is setup, the SSL Visibility Appliance will inspect traffic which matches an inspection rule, resign it with the verified HSM resigning signature, and send the flow on to its destination.

HSM Logs

HSM interaction information is available in the logs (under the **Monitor** menu item).

System Log: View HSM failures as follows:

- HSM appliance failure
- HSM appliance recovery

SSL Session Log: View HSM signature failures and other errors as follows:

HSM network connectivity failure:	HSM or Agent can't be reached
HSM secure connection failure:	SSL connection failure between the SSL Visibility Appliance and the HSM
Invalid HSM response:	HSM response is corrupt, or can't be verified
Invalid HSM request:	HSM returned a HTTP 400 response
HSM operation internal error:	HSM returned an HTTP 404 or 500 response

HSM Diagnostics

The Policy section of a diagnostics report will contain the resigning CA fields and HSM Failure options in the rulesets, as well as the user-defined HSM resigning CA groups. The PKI section will include the HSM configuration, HSM resigning CAs, and the client certificates.

NOTE: No diagnostic CLI is available for HSM connections for the SSL Visibility Appliance.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	