IBM DataPower

Integration Guide

gemalto
security to be free

Document Part Number: 007-013512-001, Rev. A

Release Date: June 2016

Contents

Preface

This document is intended to guide security administrators through the steps for IBM DataPower Virtual Appliance and SafeNet Network HSM integration, and also covers the necessary information to install, configure and integrate IBM DataPower Virtual appliance with SafeNet Network Hardware Security Modules (HSMs).

Scope

This document outlines the steps to integrate IBM DataPower Virtual Appliance with SafeNet Network HSM.

Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

Old product name	New product name
Luna SA HSM	SafeNet Network HSM
Luna PCI-E HSM	SafeNet PCI-E HSM
Luna G5 HSM	SafeNet USB HSM
Luna Client	SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts and code examples.

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 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 Gemalto Knowledge Base.	

1
Introduction

Overview

DataPower Gateway appliances help quickly secure, integrate, control and optimize access to a range of workloads through a single, extensible, DMZ-ready gateway. These appliances act as security and integration gateways for a full range of mobile, cloud, application programming interface (API), web, service-oriented architecture (SOA) and B2B workloads.

Hardware security model (HSM) is a factory-installed feature that is available on DataPower appliances. An HSM provides secure storage for RSA keys and accelerates RSA operations.

An HSM-equipped appliance supports the following operations.

- Accelerate synchronous and asynchronous RSA operations: Sign, verify, encrypt, and decrypt.
- Encrypted password-based login.
- Generate and store RSA private keys on the HSM.
- Export and import key material among HSM-equipped appliances. Appliances must share a key-wrapping key and belong to the same key-sharing domain.
- Delete RSA private keys from the HSM.

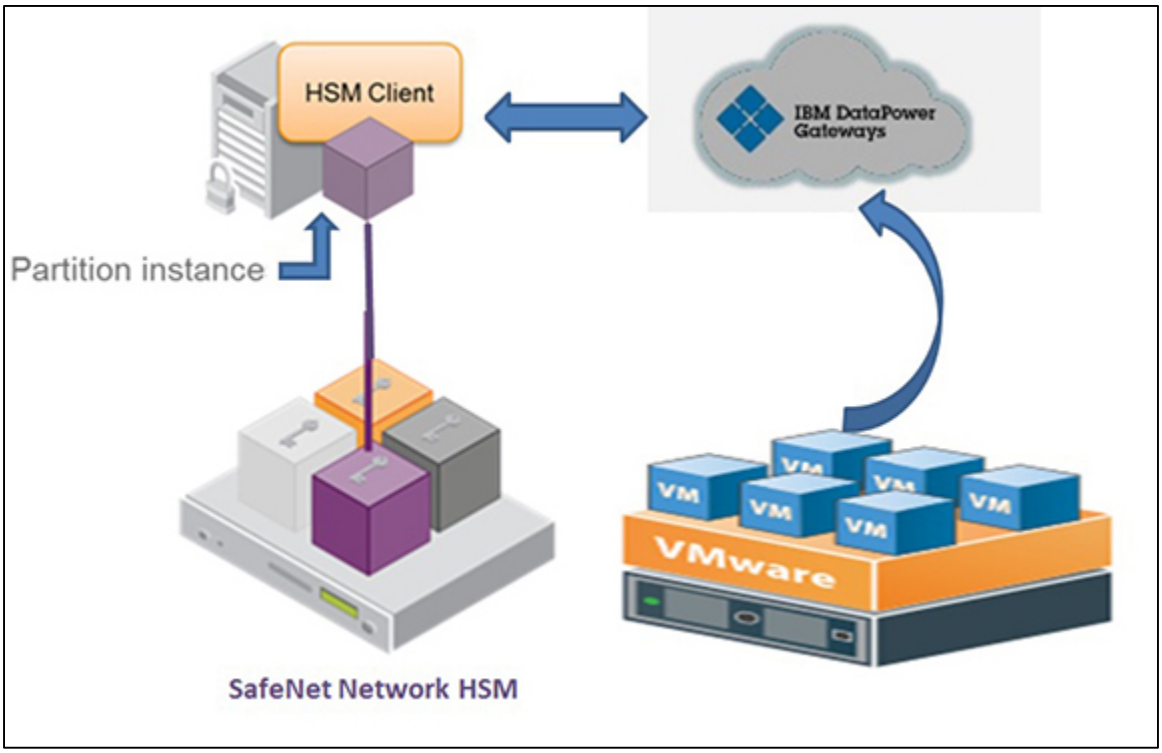
The DataPower (virtual or container) instances have no secure storage for keys. Cloud should have a physical HSM appliance to protect these keys.

You can use a network-based SafeNet Network HSM appliance as an HSM for secure key storage and cryptographic operations.

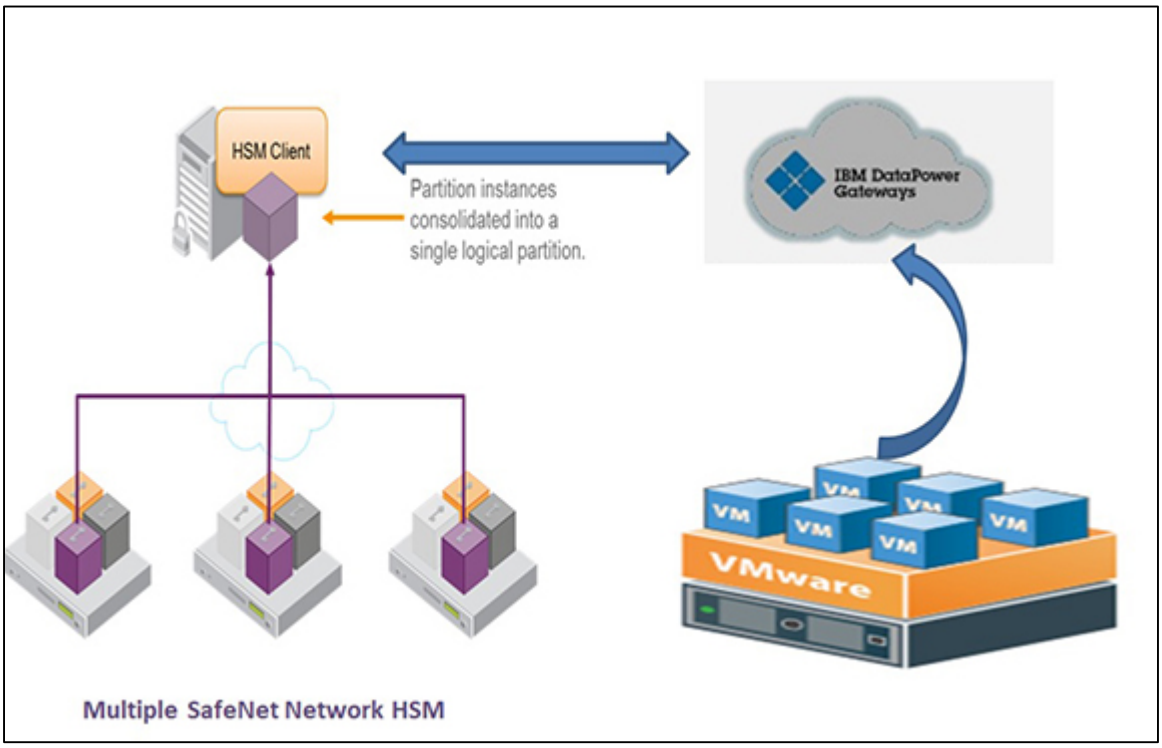
In the integration between the DataPower Gateway and the SafeNet Network HSM, the Network HSM is the server, and the DataPower Gateway is the client. Cryptographic requests are sent over a network trust link.

The SafeNet Network HSM stores the keys in the HSM partitions. One DataPower Gateway can integrate with multiple Network HSMs and use multiple partitions on each SafeNet Network HSM. The following figure illustrates the connection between the DataPower Gateway and the SafeNet Network HSM.

DataPower Gateway with Single partition on SafeNet Network HSM:



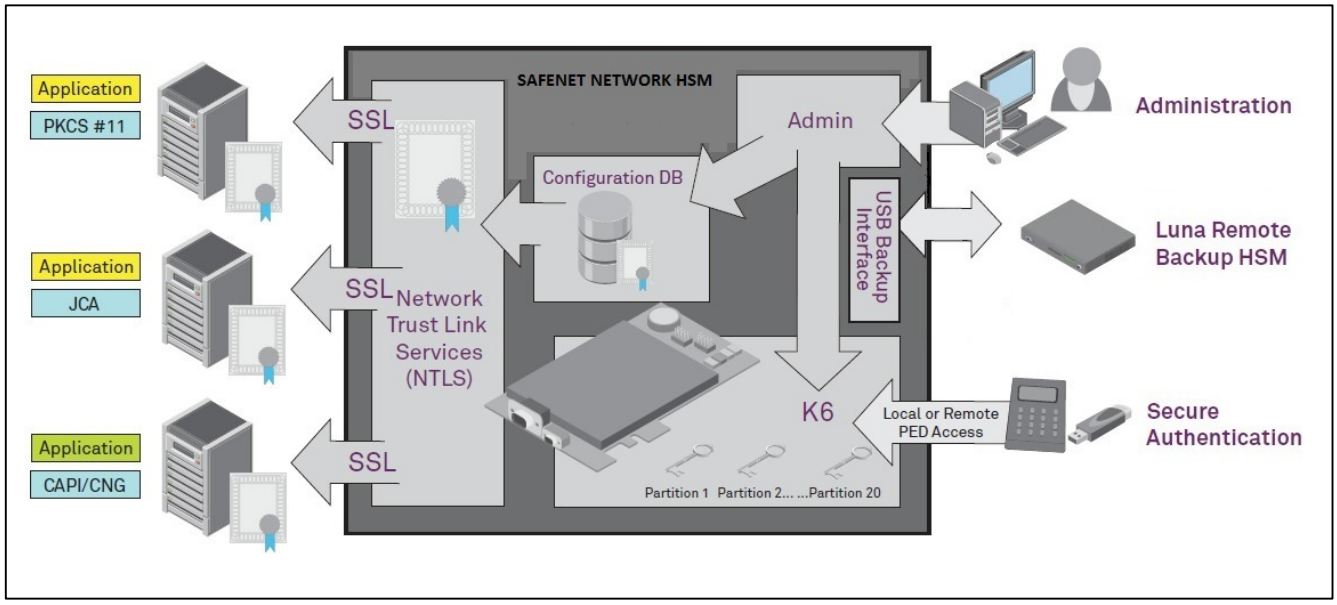
DataPower Gateway with HA configuration on SafeNet Network HSM:



SafeNet Network HSM (Luna-SA)

- Provides PKCS#11 Cryptoki opaque library for clients.
- Client command line tool cmu is used to create keys and certs.

The following block diagram is a conceptual overview of the SafeNet Network HSM Server depicting internal systems, communications, and interaction with application servers.



3rd Party Application Details

- IBM Data Power (Virtual Appliance)

Supported Platforms

Platforms Tested	SafeNet Luna Client Software version	Firmware Version
IBM Data Power (Virtual Appliance) 7.5.0.0	Luna Client 5.4.1-2 SA Appliance Version-5.4.7-1	6.10.9

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Linux systems. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password
- SafeNet Network HSM, and a hostname, suitable for your network
- SafeNet Network HSM parameters are set to work with your network
- Initialize the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and Client system.
- Create a partition on the HSM and remember the partition password that will be later used by IBM DataPower. Register the Client with the partition. Run the "vtl verify" command on the client system to verify the NTLS
- Enable Partition "Activation" and "Auto Activation" policies 22 and 23 respectively (applies to SafeNet Network HSM with Trusted Path Authentication).

IBM DataPower Virtual Appliance Setup

Use the appropriate virtual image file to deploy the virtual appliance on the VMware. For more information, see the IBM DataPower Gateways documentation in IBM Knowledge Center.

http://ibm.com/support/knowledgecenter/SS9H2Y

When your virtual appliance is on a VMware,complete the following steps:

- Access the WebGUI through the URL that you defined when you initialized the web management service. For example: <https://IP-Address:9090>
- Accept the license agreements.

2

Integrating IBM DataPower Virtual Appliance with SafeNet Network HSM

Creating Key on SafeNet Network HSM

Before creating key on HSM, make sure you have already established the NTLS connection with SafeNet Network HSM on RHEL machine.

Traverse to the LunaClient installation directory Path (/usr/safenet/lunaclient/bin) and execute the following command using Certificate Management utility

1. Generate the key pair using the below commands.

```
./cmu generatekeypair -modulusBits=1024 -publicExponent=65537 -labelPublic=joe_public -
labelPrivate=joe_private -encrypt=1 -decrypt=1 -sign=1 -verify=1
```

2. Cmu list to list the generated key pair.

```
./cmu list

Please enter password for token in slot 1 : ********

handle=29       label=joe_private

handle=26       label=joe_public
```

3. Generate a self-sign certificate.

```
./cmu selfsigncertificate -publichandle=1578 -privatehandle=2701 -startDate=20151017 -
endDate=20291017 -serialNumber=ADDEDFEE –label joe_cert
```

4. Export the certificate.

```
./cmu export -handle=<handle id of the certificate created in step 3> -outputfile joe_cert.pem
```

Configuring SafeNet Network HSM in DataPower

To configure the DataPower Gateway Virtual Appliance with the SafeNet Network HSM, perform the following steps:

1. Create or import the client key and certificate pair for the DataPower Gateway.

> **NOTE:** A DataPower Gateway can use only one client key-certificate pair to connect to the SafeNet Network HSM. If you have multiple Luna key-certificate pairs on the DataPower Gateway, the DataPower Gateway uses the most recent pair that you create or import

2. Copy the client certificate to the SafeNet Network HSM.
3. On the SafeNet Network HSM, register the DataPower Gateway as an authorized client and assign the HSM partitions that the DataPower Gateway can access.
4. On the DataPower Gateway, register the SafeNet Network HSM as a trusted server and configure the connection to the SafeNet Network HSM. This configuration is available in only the default domain.
5. On the DataPower Gateway, specify the SafeNet Network HSM partitions that DataPower Gateway accesses.

Creating Client Key-Certificate Pair

Create a private key and a certificate for the DataPower Gateway to establish NTLS connection to the SafeNet Network HSM.

You must know the IP address or host name of the DataPower Gateway. Open the WebGUI link of DataPower Appliance and follow the steps

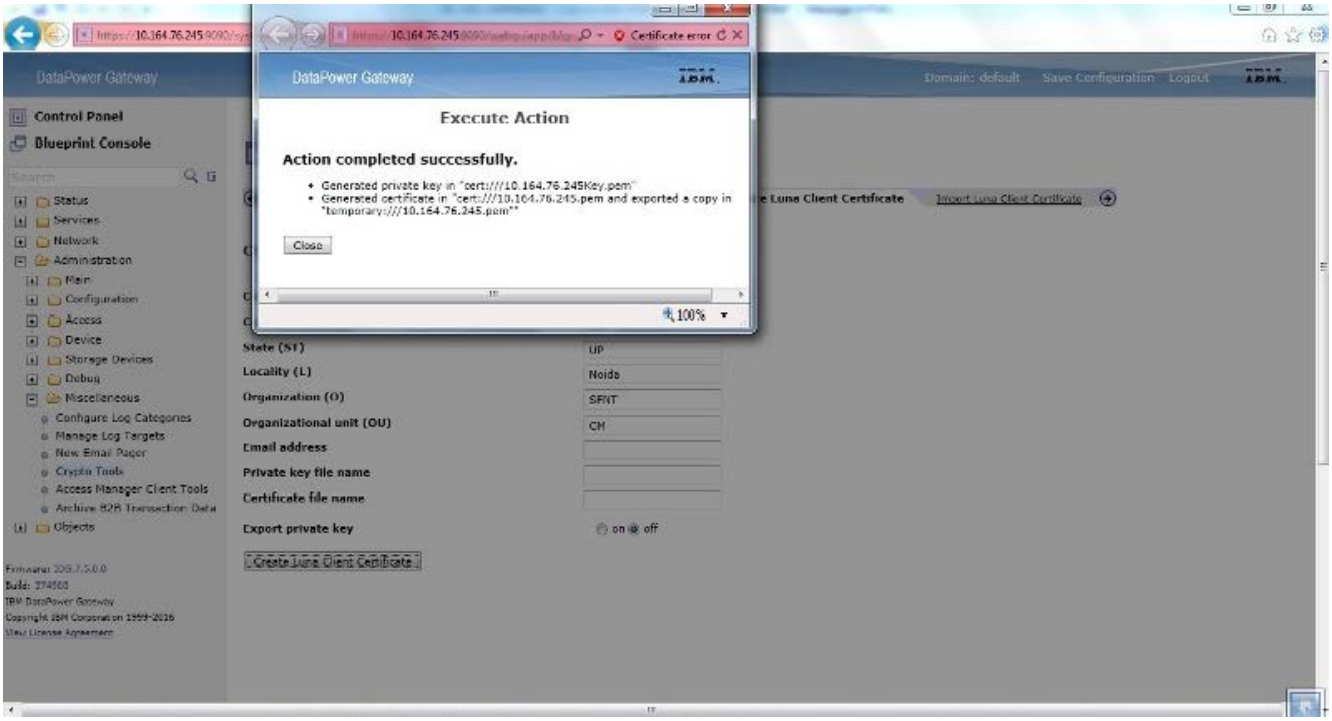
1. In the search field, type Crypto.
2. From the search results, click **Crypto Tools**.
3. Click the **Create Luna Client Certificate** tab.
4. Specify the common name.

> **NOTE:** The common name must be the IP address or the host name of the DataPower Gateway. The Luna HSM registers the DataPower Gateway by the common name. The NTL connection breaks when the provided common name is incorrect

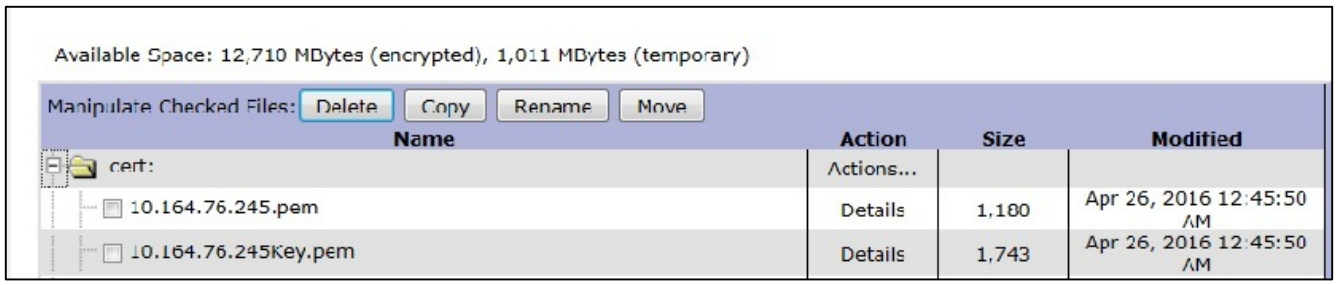
5. Optional: Specify the two-character country code.
6. Optional: Specify the unabbreviated name of the state or province.
7. Optional: Specify the name of the city or town.
8. Optional: Specify the organization name.
9. Optional: Specify the organizational unit name.
10. Optional: Specify the email address.

11. Optional: Specify the file name for the generated private key. If you do not specify, the private key file takes the format of common_nameKey.pem.
12. Optional: Specify the file name for the generated certificate. If you do not specify, the certificate takes the format of common_name.pem.
13. Optional: Specify whether to export the private key to the temporary: directory.
14. Click Create Luna Client Certificate. The key-certificate pair is created in the cert: directory. The certificate is exported to the temporary: directory. The private key is exported to the temporary: directory when you enable the export private key option.

After key-certificate pair is created successfully, the below screen displays.



Key-certificate pair is created at the below location.



NOTE: You can use Import Luna Client Certificate option in Crypto Tool if you want to use the existing client certificate.

Next step is to copy the certificate to the SafeNet Network HSM using DataPower CLI. You need to execute the below command from DataPower Virtual Appliance

```
idg(config) copy temporary:///<Client certificate.pem file> scp://<Safenet Network HSM>:
```

```
For Example-copy temporary:///10.164.76.245.pem scp://admin@10.164.76.114:
```

It prompts to enter the password for the SafeNet Network HSM.

Register DataPower Gateway on HSM

After Successful copy next step is to register the DataPower Gateway as an authorized client and assign the HSM partitions that the DataPower Gateway can access

Access the SafeNet Network HSM, through Putty utility and execute the Client register and client assign partition commands.

```
Client register –c <IP of the client machine> -h <Hostname of the machine>

Client assignpartition –c <IP of the client machine> -par <Partition Name>
```

Configure connection to SafeNet Network HSM

Register a SafeNet Network HSM as a trusted server to the DataPower Gateway and set the secure option for the connection between the DataPower Gateway and the HSM.

- Obtain the server certificate from the SafeNet Network HSM that the DataPower Gateway connects to using PSCP command on windows or scp command on Linux system.

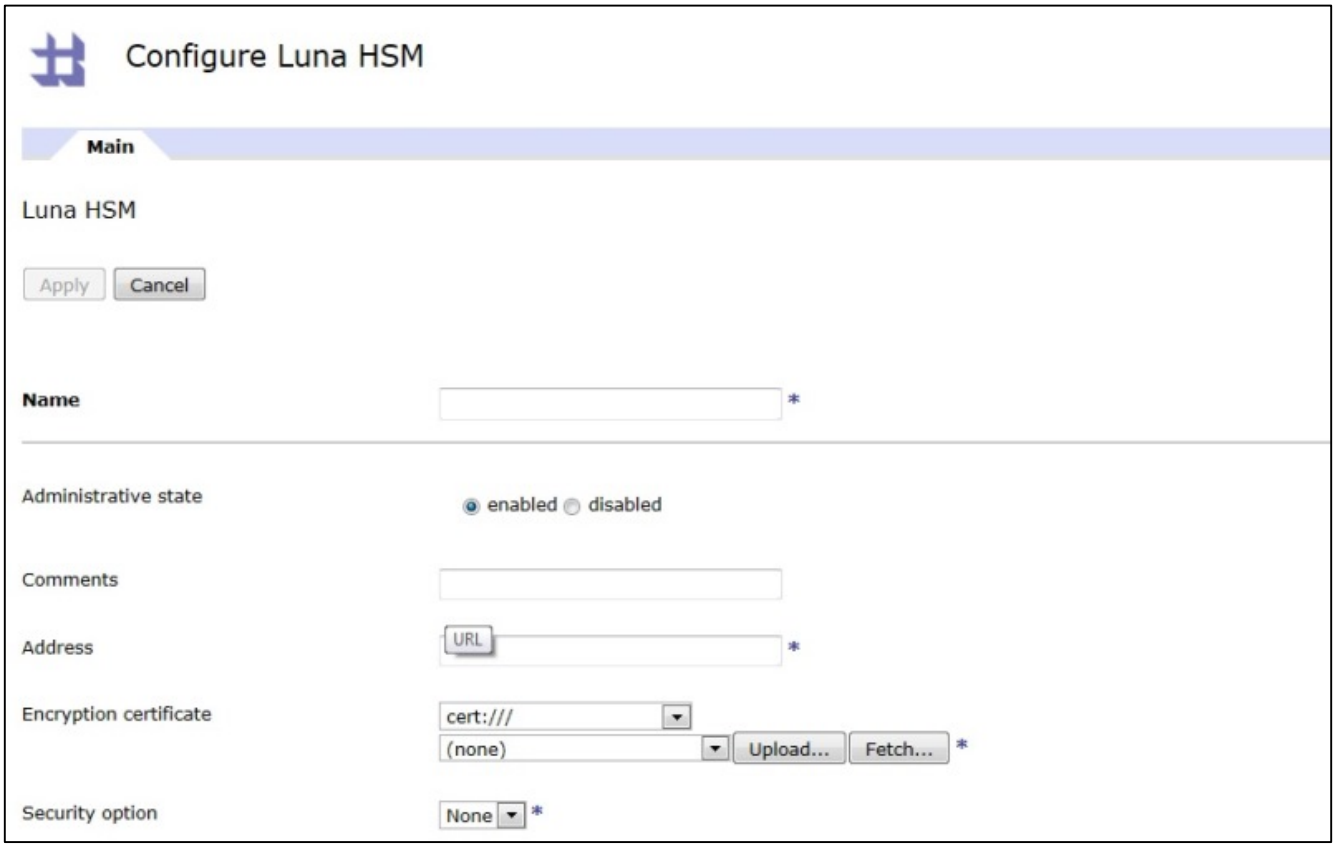
  Command format:

  RHEL: scp admin@<SafeNet Network HSM IP Address>:server.pem <Destination Folder)

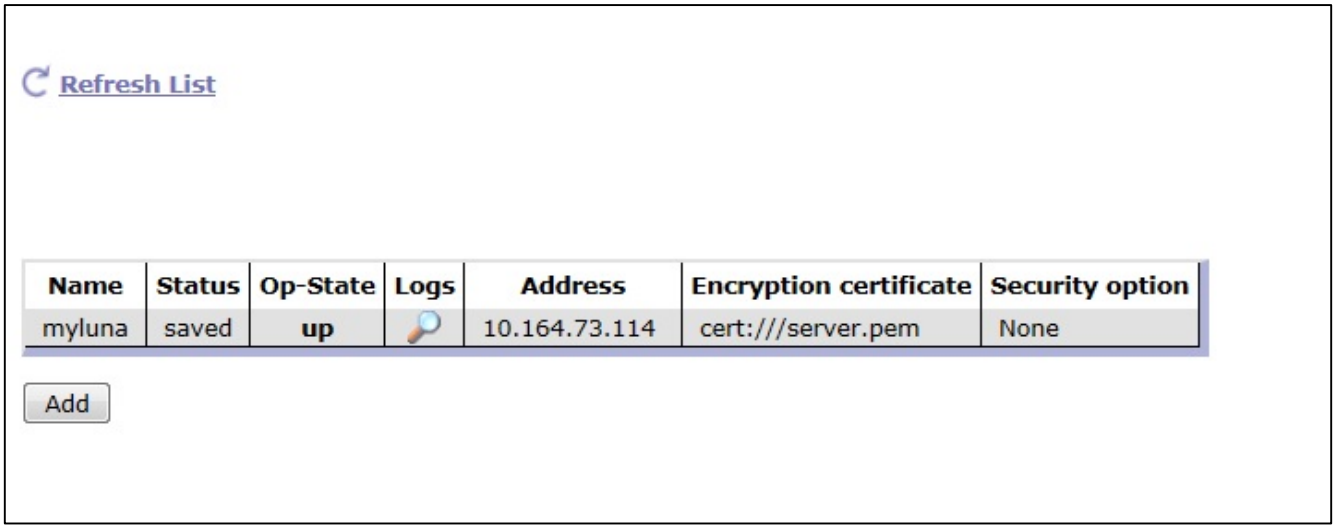
  Windows: PSCP.EXE admin@<SafeNet Network HSM IP Address>:server.pem <Destination Folder)

- Copy the certificate to machine from where you are accessing IBM DataPower GUI so that you can upload it.

- In the DataPower WebGUI In the search field, enter Luna HSM. Click on the Luna HSM.



- You can upload the server certificate using the **upload** button. Enter all the details in the above screen and click the **Apply** button. Check the op- state of the HSM, it should be **up**.



Specifying SafeNet Network HSM Partitions on DataPower

The HSM partition defines which HSM partition to use for secure storage on the SafeNet Network HSM.

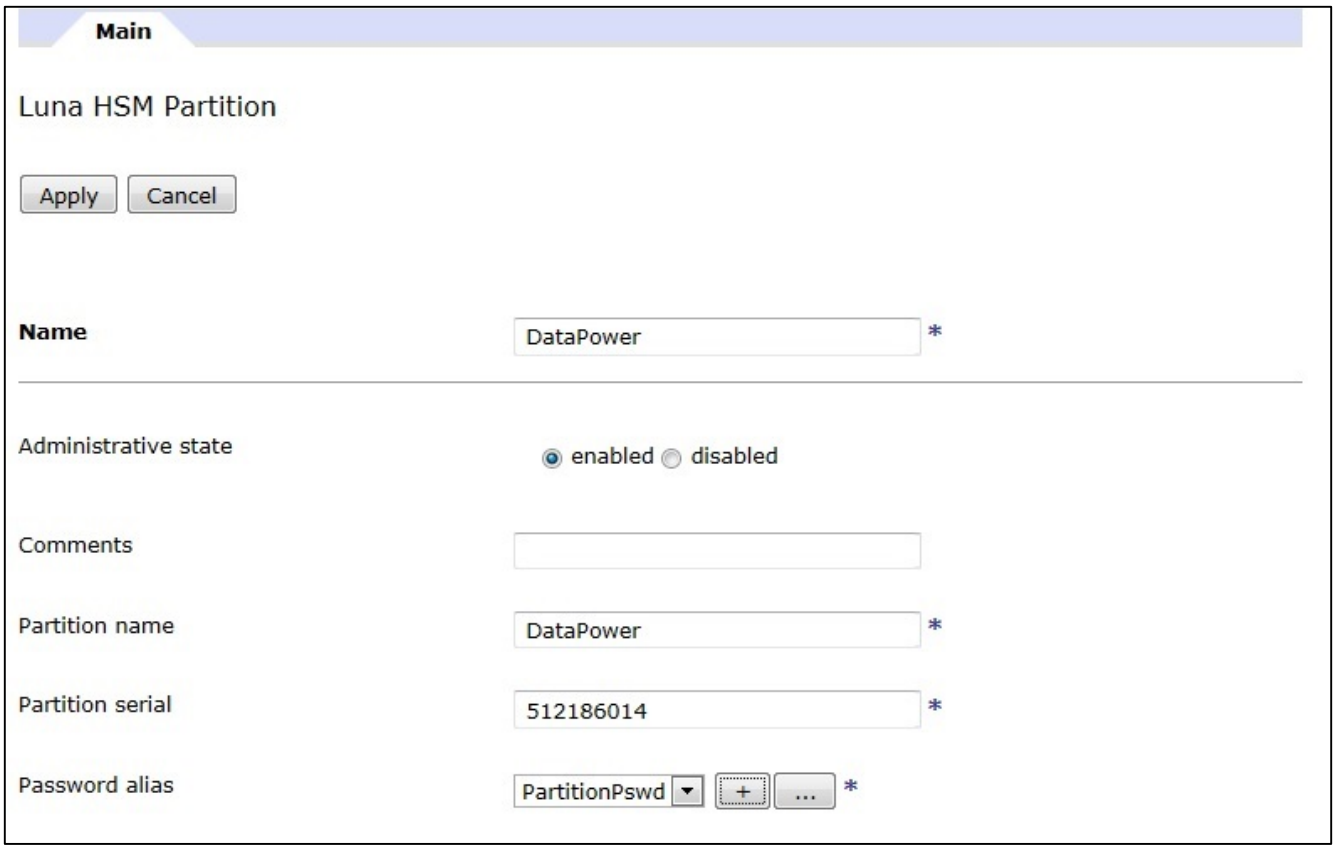
Before configuring partition, you are required to validate the following:

- Configure the connection to the SafeNet Network HSM where the partition locates and ensure that the operation state of the configuration is up.
- Assign the partition that the DataPower Gateway can access on the SafeNet Network HSM.
- Know the password to access the assigned partition.
- Use the partition show command on the SafeNet Network HSM to obtain the serial number of the partition.

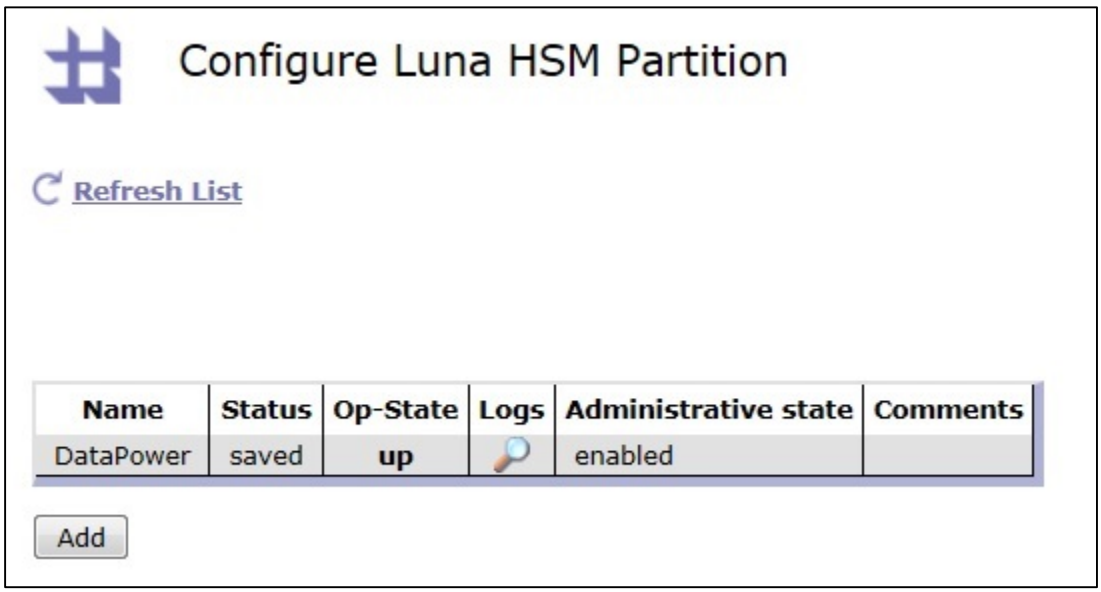
Perform the below steps once you have all the details.

1. In the search field, enter Luna.
2. From the search results, click Luna HSM Partition.
3. Click **Add**.
4. Define the basic properties: Name, administrative state, and descriptive summary.
5. Enter the name that identifies the partition on the Luna HSM.
6. Enter the serial number of the partition.
7. Select the password alias for the partition password.
8. Click on the '**+**' button to Configure Password Map Alias and enter the details of the Partition Password.
9. Click **Apply** to save the changes to the running configuration.

10. Click Save Configuration or Save changes to save the changes to the persisted configuration



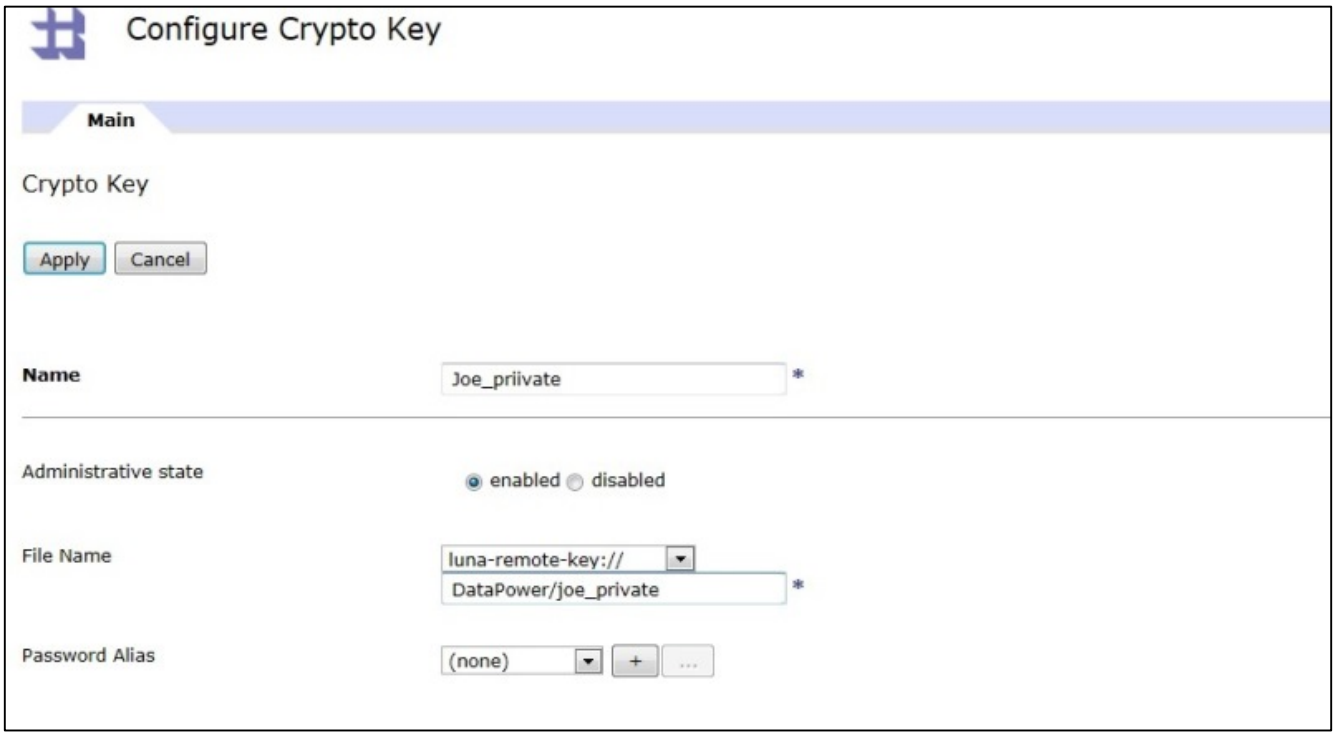
After Partition is configured you successfully, the below screen displays. Check the Op-state of the partition. It should be **up.**



Add Crypto Key object located on SafeNet Network HSM

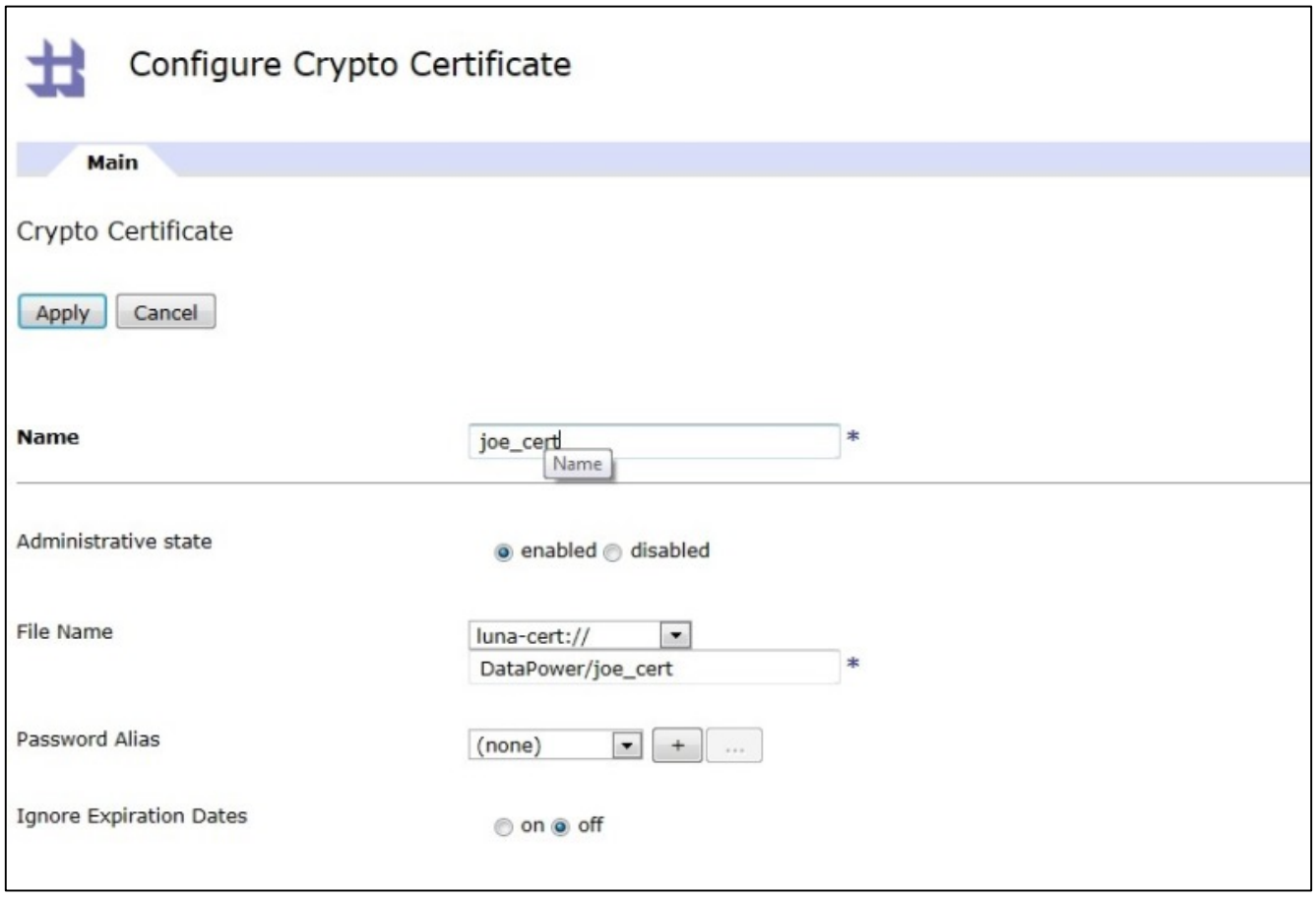
Once the HSM is configured with DataPower and Partition is successfully registered, add key objects located on SafeNet Network HSM to the DataPower.

1. In the search field, enter Crypto Key.
2. From the search results, click **Crypto Key**.
3. Click **Add**.
4. Enter the details as mentioned in the below screen.
5. Click **Apply**.



NOTE: Key format: luna-remote-key://<partition obj name>/<key label name>

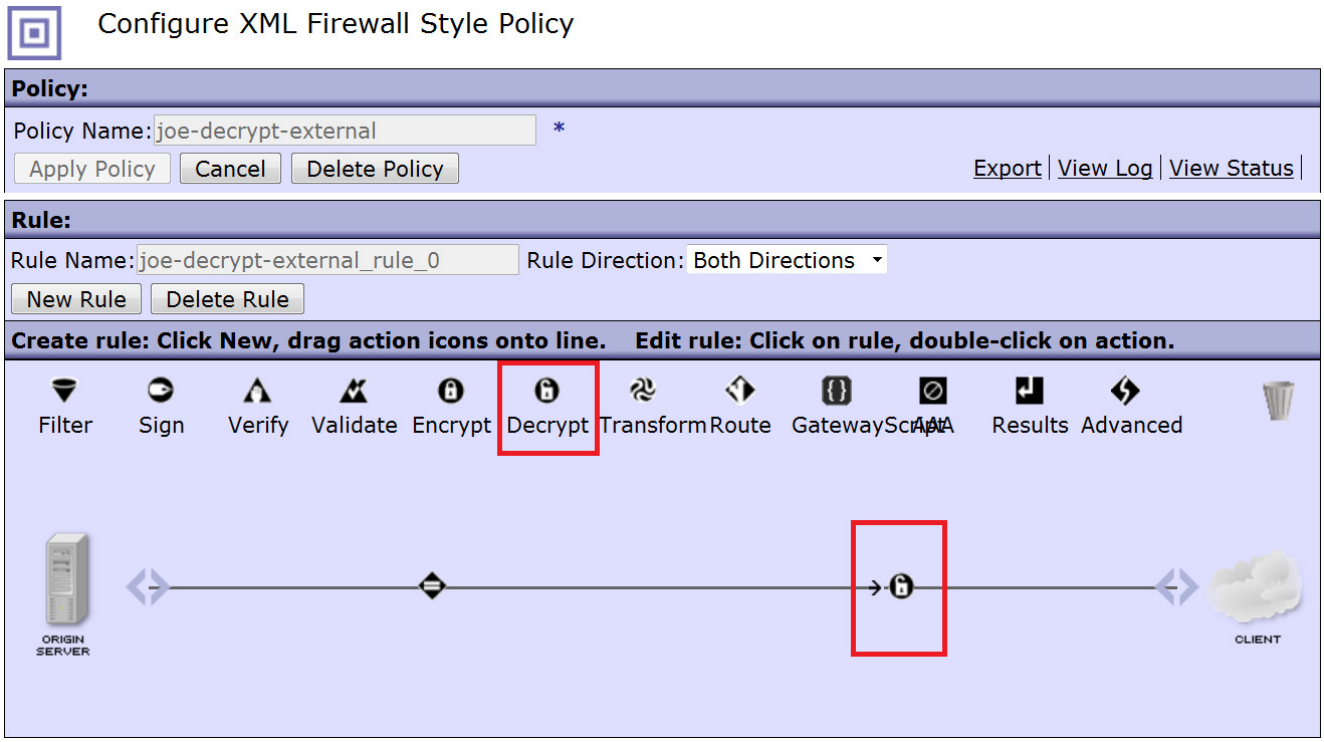
Configure the Crypto Certificate in similar way.



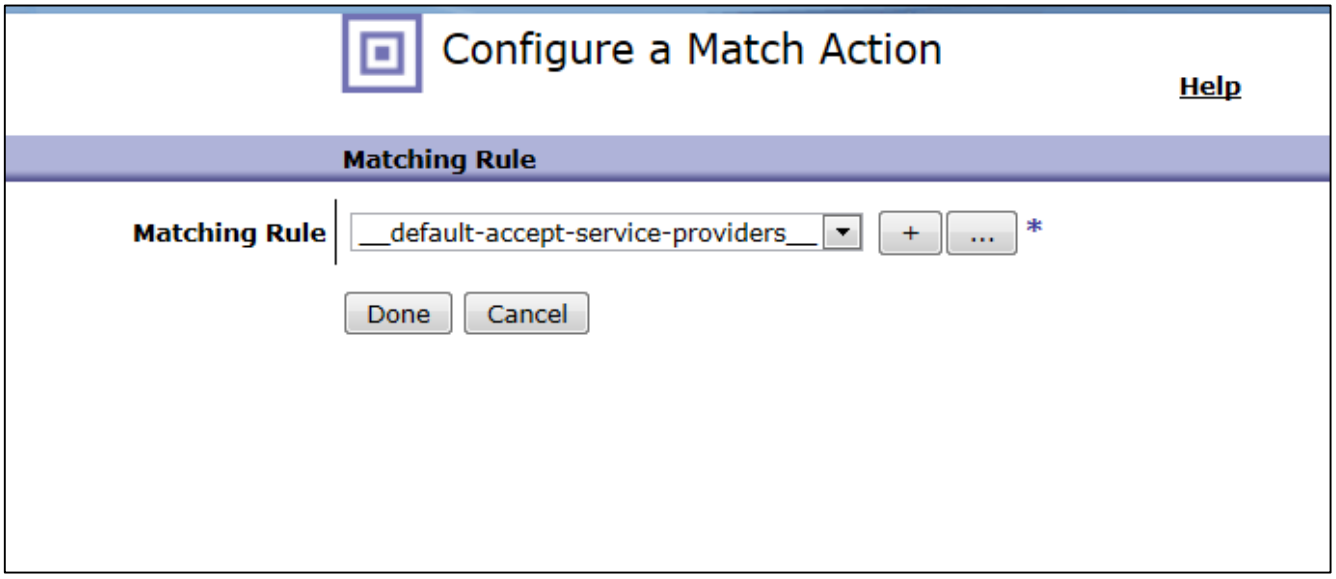
Supported Operations

Decrypt Operation

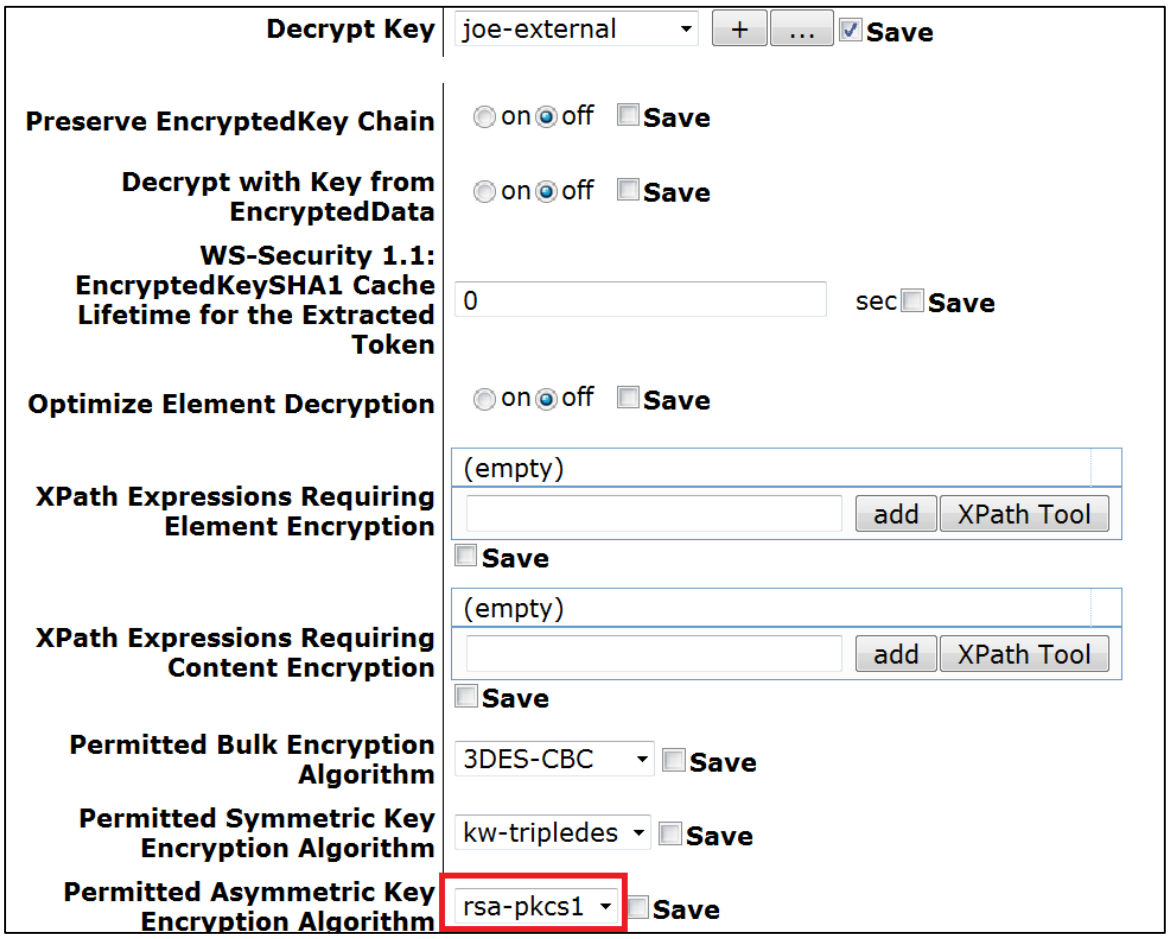
1. In the search field, enter XML Firewall Policy
2. From the search results, click XML Firewall Policy.
3. Click Add New Policy
4. Drag the Decrypt icon to the configuration path.
5. Double-click the Decrypt icon.
6. Enter the details as mentioned in the below screen.



7. Double-click on the Action icon to configure a Match Action. From the drop-down menu, select the matching rule.



8. Click on the Decrypt icon to configure Decrypt action and select the configuration as below.

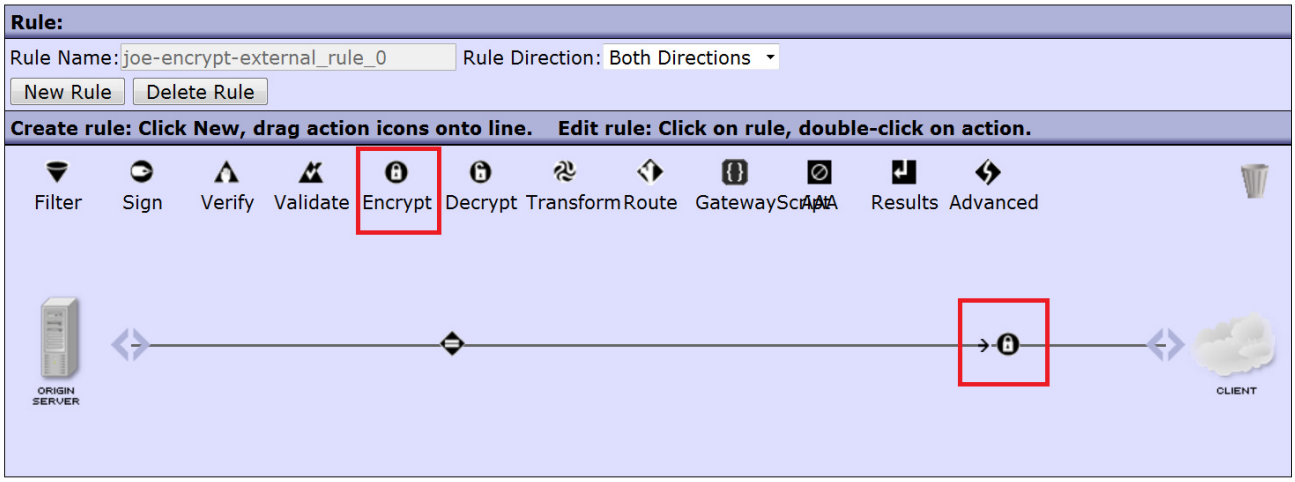


9. Click on the **Apply Policy** button after all settings are configured.

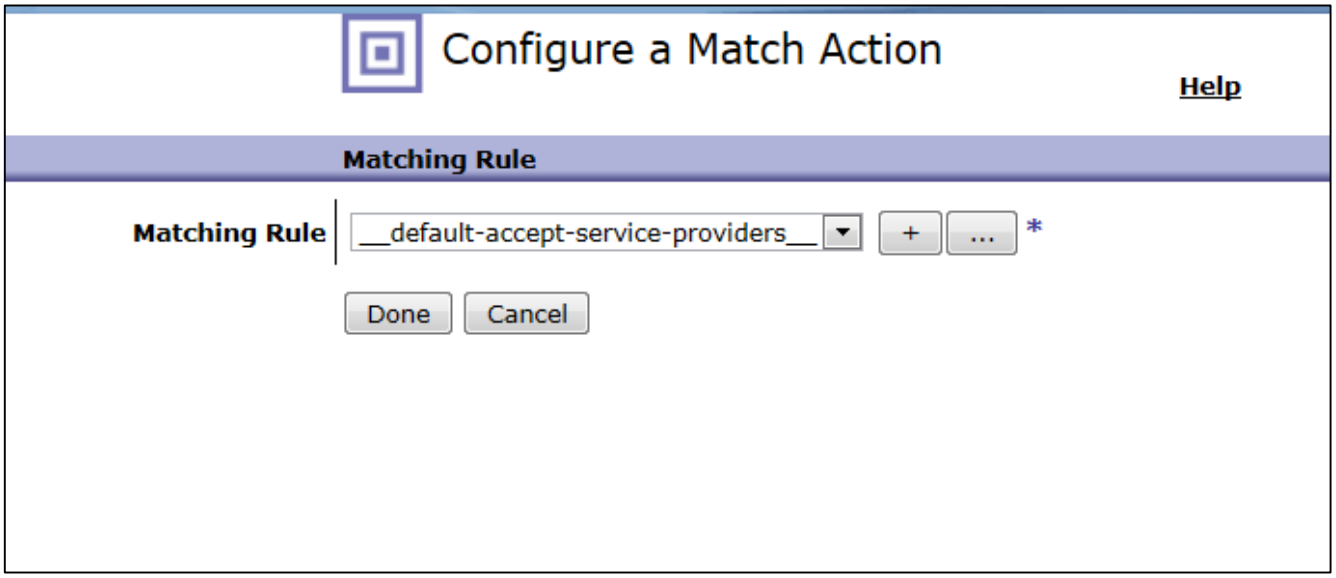
Encrypt Operation

1. In the search field, enter XML Firewall Policy.
2. From the search results, click XML Firewall Policy.
3. Click Add New Policy.
4. Drag the Encrypt icon to the configuration path.
5. Double-click the Encrypt icon.

6. Enter the details as mentioned in the below screen.



7. Double-click on Action to configure a Match Action. From the drop-down menu, select the matching rule.



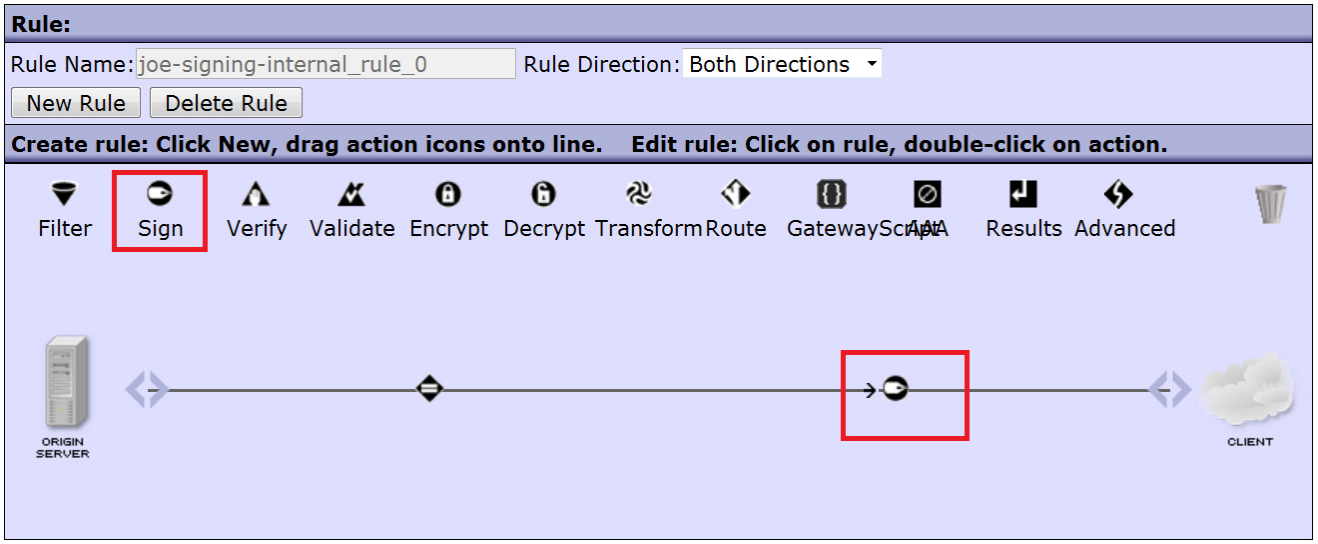
8. Click on Encrypt Action to configure Encrypt action and select the configuration as below.

9. Click on the **Apply Policy** button after all settings are configured

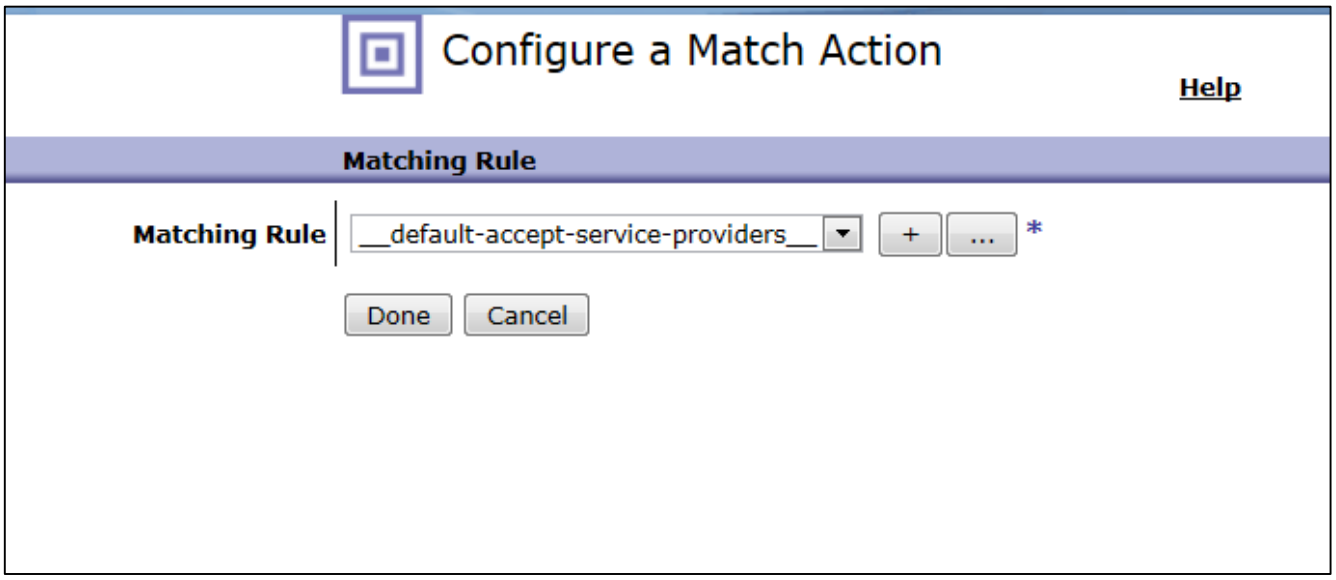
Sign Operation

1. In the search field, enter XML Firewall Policy.
2. From the search results, click XML Firewall Policy.
3. Click Add New Policy.
4. Drag the Sign icon to the configuration path.
5. Double-click the Sign icon.

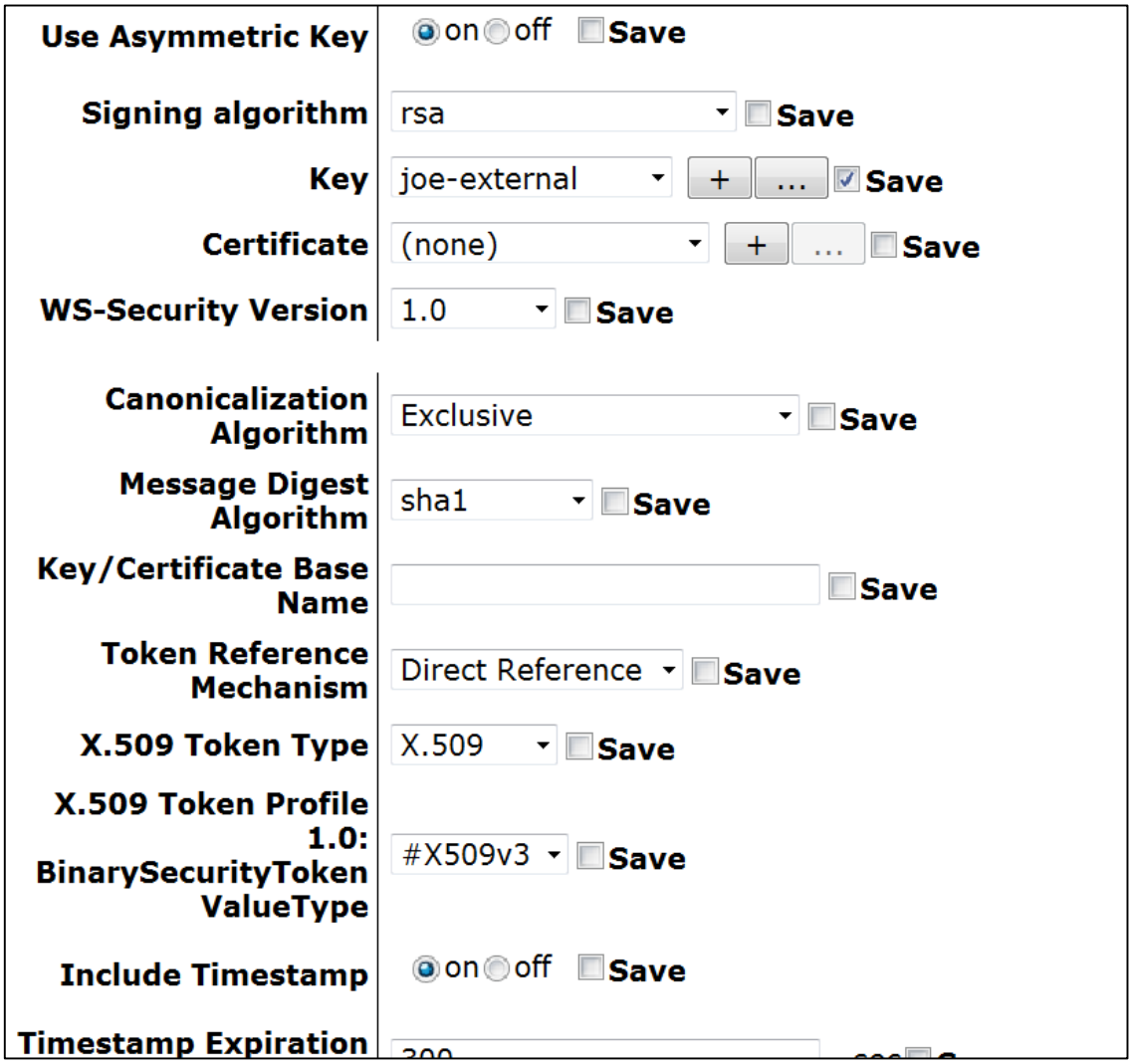
6. Enter the details as mentioned in the below screen.



7. Double-click on Action to configure a Match Action. From the drop-down menu, select the matching rule.



8. Click on Sign Action to configure Sign action and select the configuration as below. Select the matching rule as mentioned in Decrypt section.

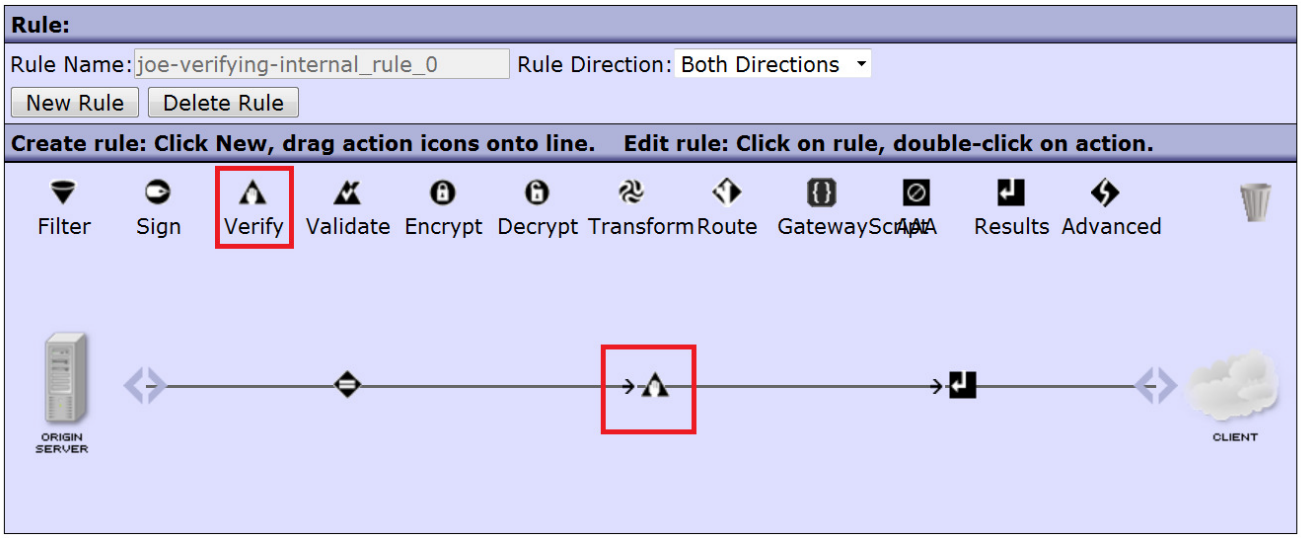


9. Click on the **Apply Policy** button after all settings are configured.

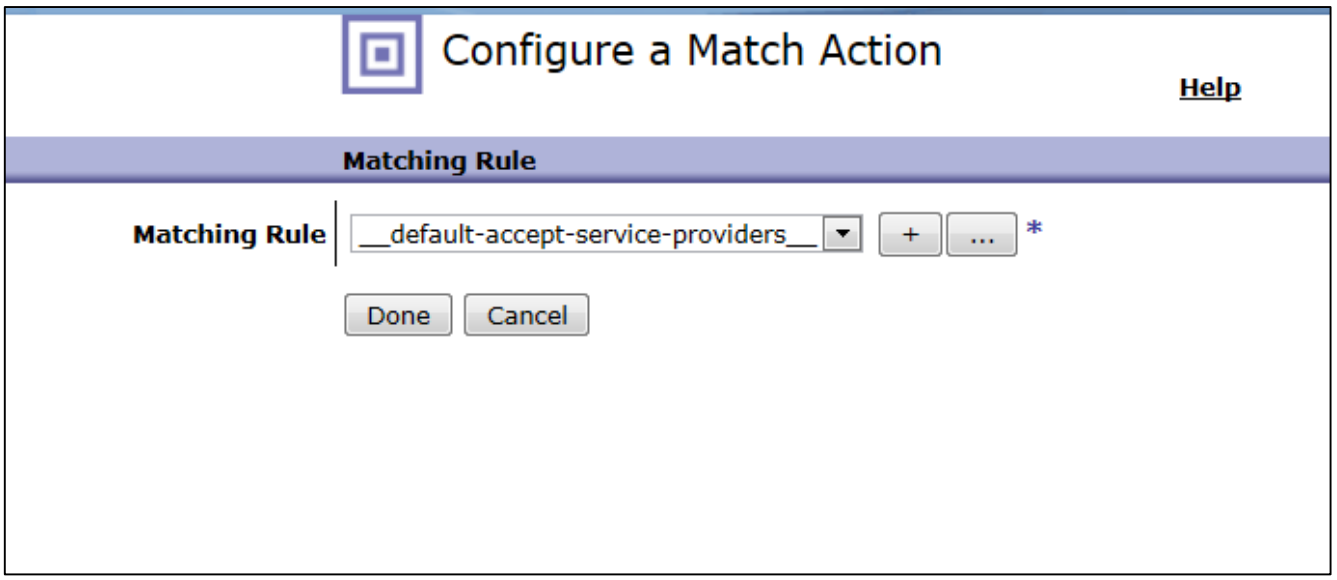
Verify Operation

1. In the search field, enter XML Firewall Policy.
2. From the search results, click XML Firewall Policy.
3. Click Add New Policy.
4. Drag the Verify icon to the configuration path.
5. Double-click the Verify icon.

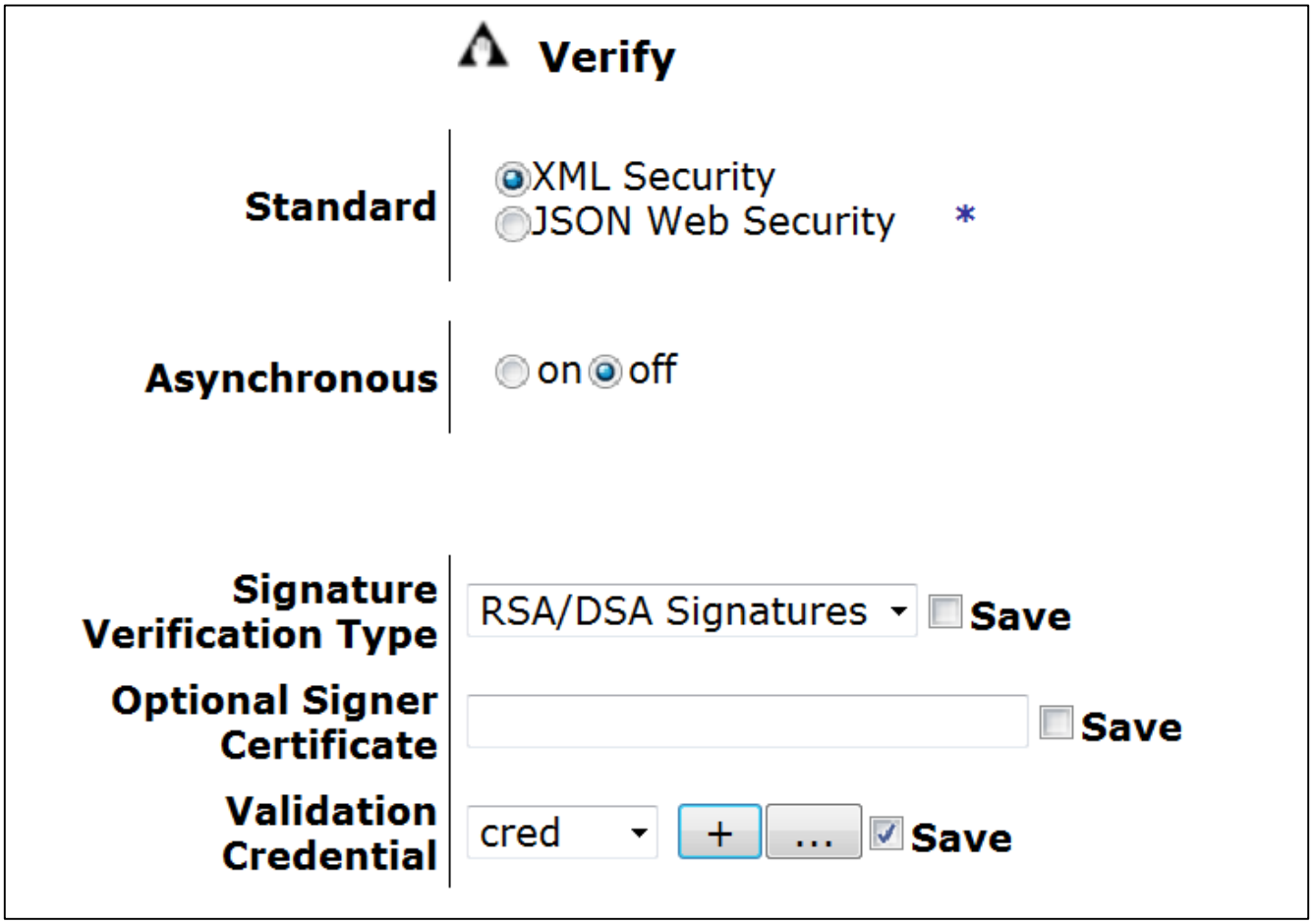
6. Enter the details as mentioned in the below screen.



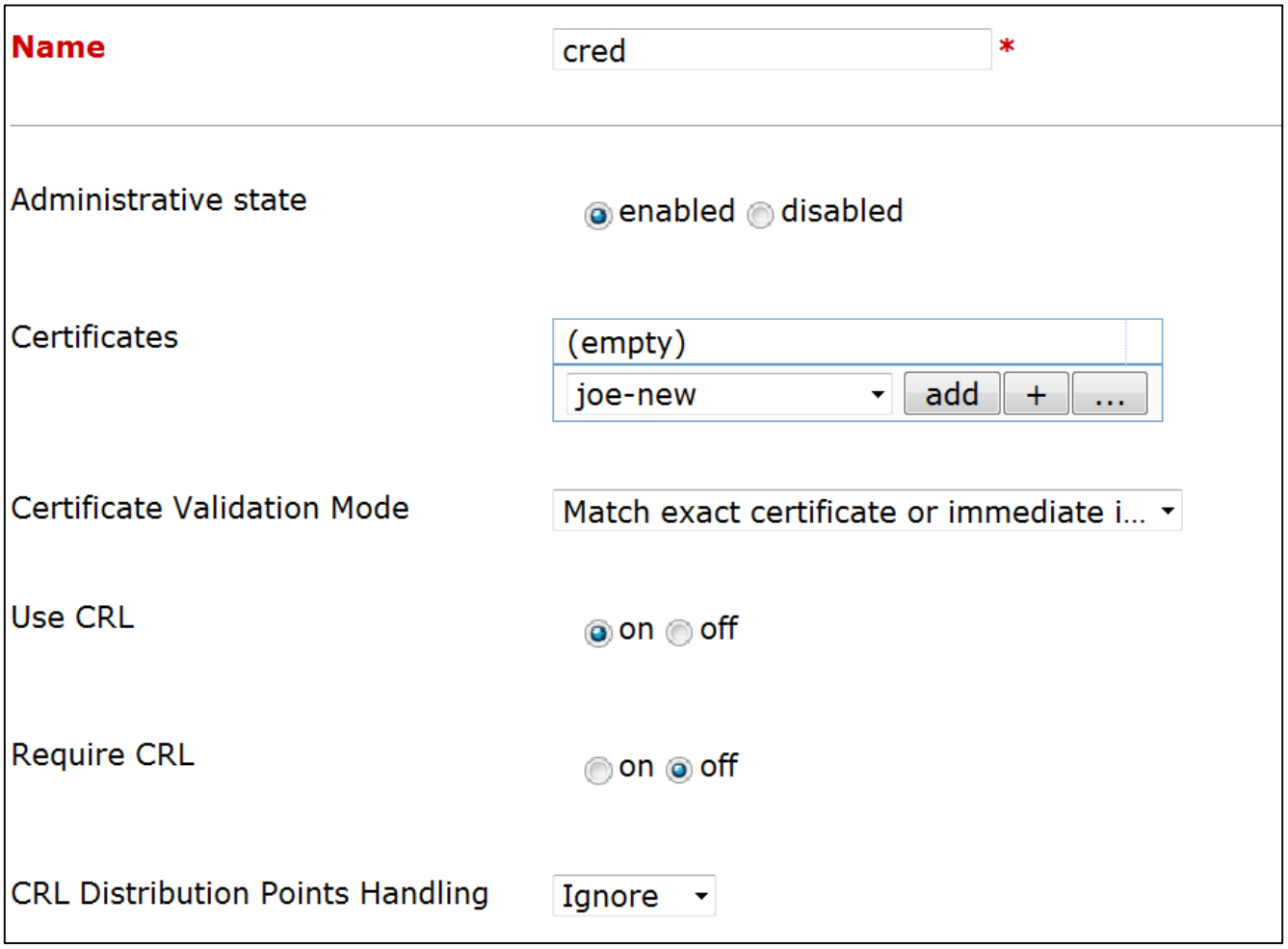
7. Double-click on Action to configure a Match Action. From the drop-down menu, select the matching rule.



8. Click on the Verify icon to configure verify action and select the configuration as below. Select the matching rule as mentioned in the Decrypt section.



9. Click on the '+' button in the **Validation Credential** field to configure the credentials. Enter the details as mentioned below.

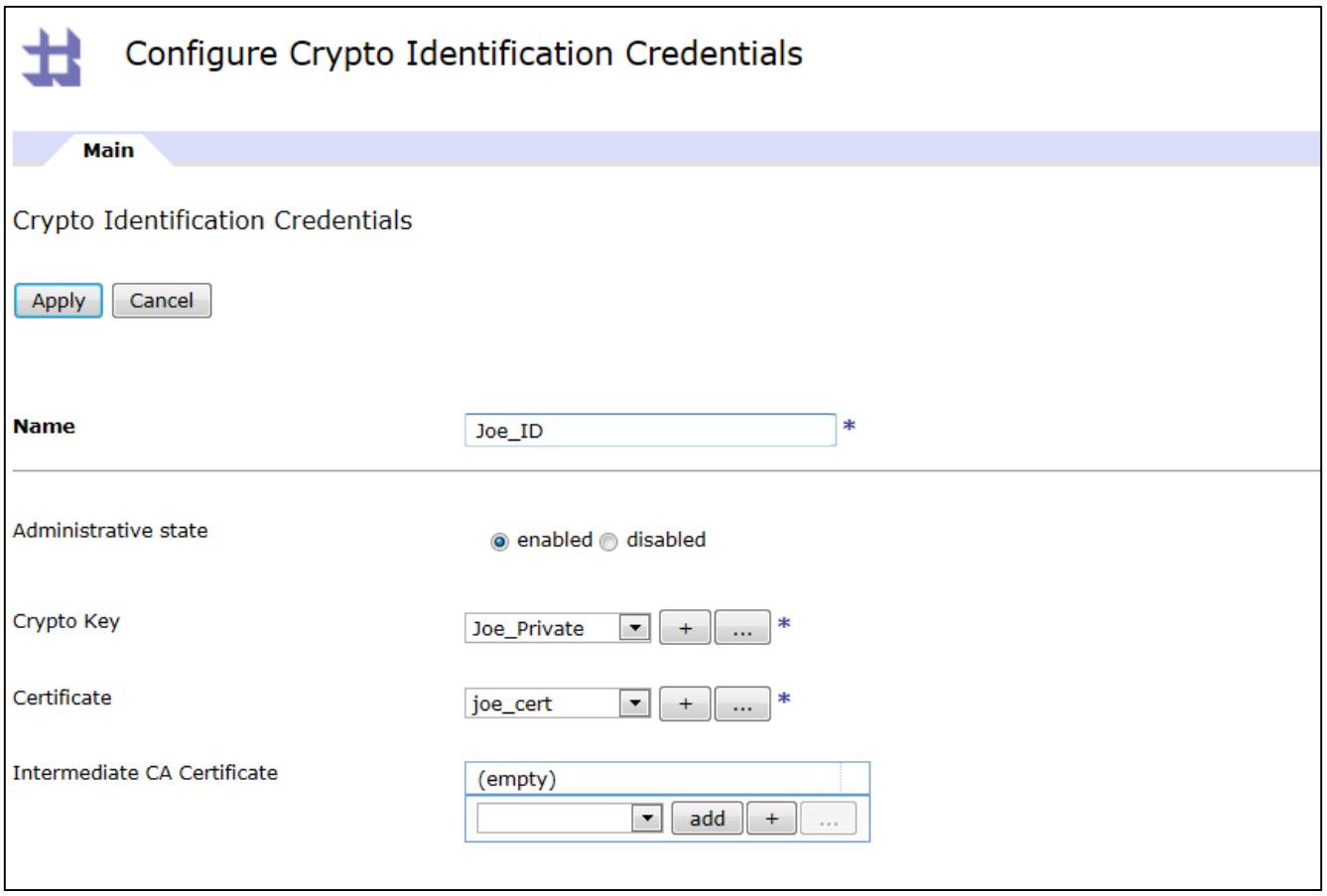


10. Click on the **Apply Policy** button after all settings are configured

Crypto Identification Credentials

1. In the search field, enter Crypto Identification Credentials.
2. From the search results, click Crypto Identification Credentials.
3. Click **Add**.

4. Enter the details as mentioned in the below screen.



After applying the above changes verify op-state should be up.

Luna HSM Transaction Latency

You can view the following information about the HSM partitions that the DataPower Gateway uses:

The latency of the last transaction in milliseconds.

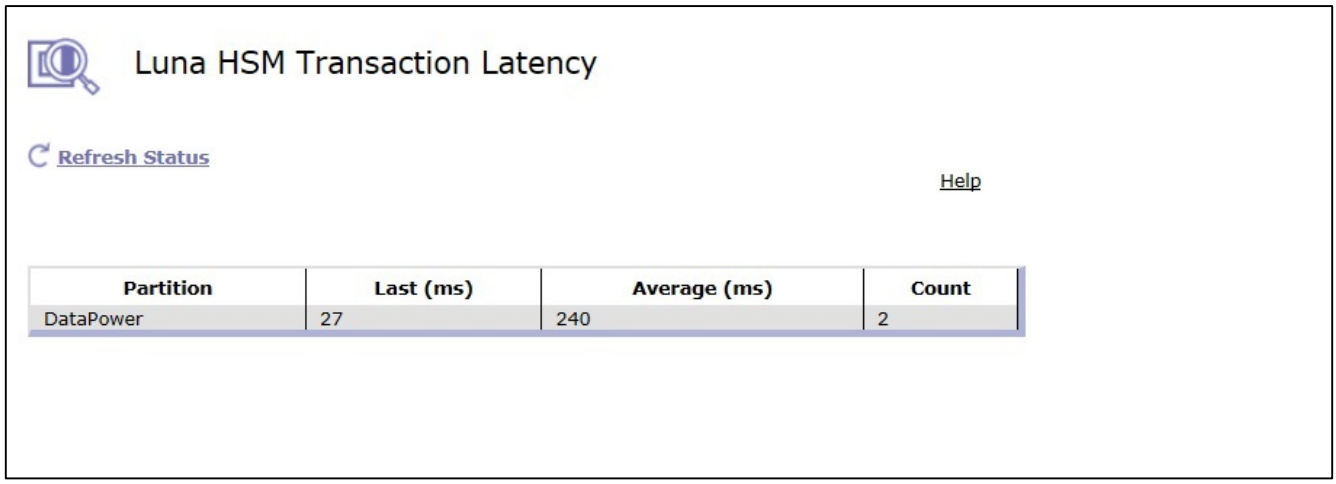
The decayed average latency of the last 10 transactions in milliseconds where more weight is applied to the newest transaction. The decayed average is calculated as 10% for the newest transaction plus 90% for the last average:

Decayed average = latency of the newest transaction *0.1 + last average*0.9

The number of transactions that the partition has processed for the DataPower Gateway

Procedure

1. In the search field, enter Luna.
2. From the search results, click Luna HSM Transaction Latency. The GUI displays the transaction information for each partition that the DataPower Gateway can access



You can use below commands on DataPower CLI to verify the Loads and to see the slot information.

```
idg(diag)# luna-list-slots
```

```
idg(diag)# luna-list-slots
Number of slots: 4

The following slots were found:

Slot #    Description          Label                           Serial #   Status
========= ==================== =============================== ========== ======
slot #1   LunaNet Slot         DataPower                       512186014  Presen
t
slot #2    -                    -                               -         Not pr
esent
slot #3    -                    -                               -         Not pr
esent
slot #4    -                    -                               -         Not pr
esent
idg(diag)#
idg(diag)#
idg(diag)# _
```

```
idg(diag)# luna-list-servers
```

```
idg(diag)# luna-list-servers
Server: 10.164.73.114   HTL required: no
idg(diag)# _
```

```
idg# show load
```

```
idg# show load

 Task ID Task name  Load Work list CPU Memory File count
 ------- ---------- ---- --------- --- ------ ----------
 1       main       1    0         0   22     89
 3       lunaClient 0    0         0   1      13
 4       luna       0    0         0   1      14

idg#
idg# _
```