IBM Security Access Manager
Integration Guide

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-013015-001 (Rev A)
Release Date	May 2015

Trademarks

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimer

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

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

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.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520

Contents

CHAPTER 1
Introduction

This document outlines the steps to configure and integrate IBM Security Access Manager with SafeNet HSM.

IBM® Security Access Manager, a new integrated appliance specifically designed to help:

- Protect web applications against fraudulent and unauthorized access.
- Safeguard mobile interactions across the enterprise.

IBM Security Access Manager Family includes two offerings:

- IBM Security Access Manager for Web
- IBM Security Access Manager for Mobile

IBM Security Access Manager for Web is an integrated access appliance that combines web reverse proxy with built-in web application protection.

Security Access Manager for Web is available as a virtual or hardware-based appliance and is a part of the IBM Security Access Manager Family.

IBM Security Access Manager for Web

Security Access Manager for Web helps secure user access and helps protect content against common web vulnerabilities. It is available as either a virtual appliance or hardware appliance. Security Access Manager for Web helps centrally secure internal and external user access points into the corporate network from web and mobile channels. Highly scalable and configurable, the solution is designed to provide a policy-based user authentication and authorization system that helps defends against the latest web-based security threats.

Web access and applications are subject to repeated attacks by external and internal attackers seeking to acquire valuable content. According to the Open Web Application Security Project (OWASP) top 10 list of web vulnerabilities, external hackers use SQL injections, broken authentication, and cross-site scripting (XSS) as common methods to gain unauthorized access into the web applications. An application risk management program that includes awareness training, application testing, and remediation using web access management systems can help protect against these attacks.

Security Access Manager for Web key capabilities:

- Provides an integrated access system with a web reverse proxy for use across the enterprise.
- Provides web single sign-on and access policy enforcement for multifactor authentication.
- Ability to help block known in-line preventable OWASP top 10 web vulnerabilities.
- Delivers highly scalable and available system with built-in Layer 7 load balancing and distributed session cache to provide shared session management across multiple appliances and application instances.

IBM Security Access Manager for Mobile

Security Access Manager for Mobile provides a modular solution to safeguard mobile, social, and business partner interactions using context-based access control.

Mobile access is becoming the preferred form of access for consumer interactions with corporate applications. According to the IBM X-Force® Security and Risk trend report, attackers use phishing attacks and social engineering to compromise end-user access to gain unauthorized access into corporate applications. Identity fraud and bring your own device (BYOD) are growing concerns for enterprises, as they expand their web application reach into mobile, business partner, and social collaborations.

Security Access Manager for Mobile key capabilities:

- Provides a risk scoring engine to enforce context-aware authorization using information about the users, their mobile devices, and other transactions-based information.
- Provides mobile sign-on, session management, and an authentication service for supporting multiple strong authentication schemes, for example, one-time password, SMS, RSA SecureID.
- Helps provide secure mobile transactions with a graded level of trust to allow and deny access using mobile device fingerprinting, geographic location awareness, and IP reputation. IBM Security Access Manager for Mobile also integrates with IBM Worklight.
- Helps improve mobile security intelligence with built-in integration with IBM Security QRadar SIEM.
- Provides a graphical policy management interface that supports authoring complex policies.
- Integrates with IBM Security Access Manager for Web.

With Security Access Manager Family of products, enterprises can address these web and mobile security challenges and simplify the deployment of access system in the DMZ.

IBM Security Access Manager provides inbuilt support for SafeNet HSM and it will use the SSL certificate keys stored on SafeNet HSM. The SafeNet Luna HSM (Hardware Security Module) secures the Security Access Manager SSL keys within an industry standard FIPS 140-2 level 3 validated HSM.

Scope

3rd Party Application Details

- IBM Security Access Manager 8.0.1.1 (Virtual Appliance)

HSMs and Firmware Version

IBM Security Access Manager has been tested with the following:

- Luna SA f/w 6.21.0 with s/w v5.4.7

Prerequisites

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the Luna SA box. Before you get started ensure the following:

- Luna SA appliance and a secure admin password.
- Luna SA, and a hostname, suitable for your network.
- Luna SA network parameters are set to work with your network.
- Initialize the HSM on the Luna SA appliance.
- Create a partition on the HSM and remember the partition password that will be use later.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

IBM Security Access Manager Setup

The installation of Security Access Manager virtual appliance is addressed in the Appliance Administration guide that can be downloaded from the documentation section on IBM Security Access Manager Website at:

https://www-304.ibm.com/connections/forums/html/topic?id=b630b7e2-c374-4e3f-ac19-cd3cfd0cf7ff

https://www14.software.ibm.com/webapp/iwm/web/reg/download.do?source=swerpiss-ascdpp-3&S_PKG=access&lang=en_US

The administration guide also covers requirements and supported host operating systems as well as the installation pre-requisites. Please follow the documentation to install and configure the virtual appliance.

CHAPTER 2
Integrating IBM Security Access Manager with Luna HSM

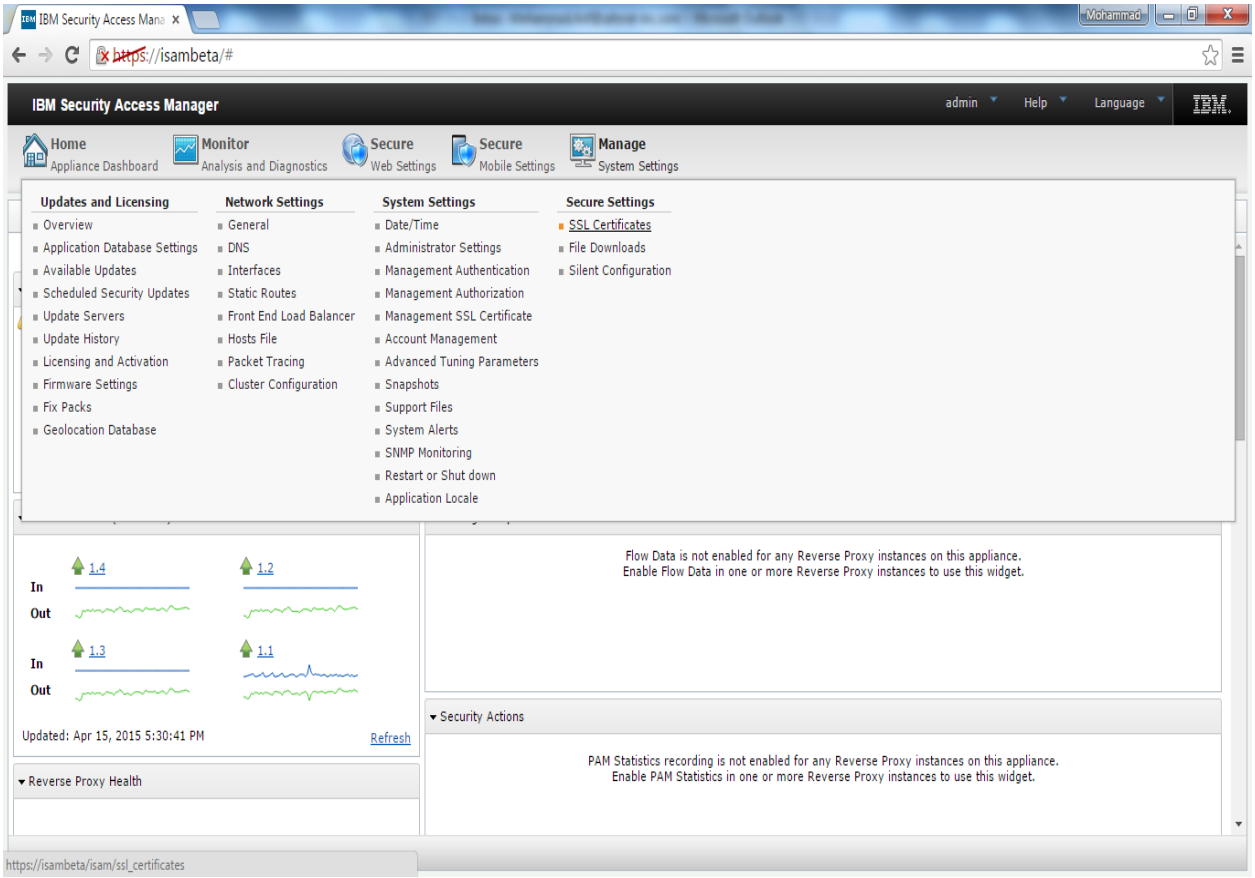
This chapter outlines the steps for configuring Luna HSM with Security Access Manager and generating the key/certificate for SSL profile.

Configuring the Security Access Manager for Luna HSM

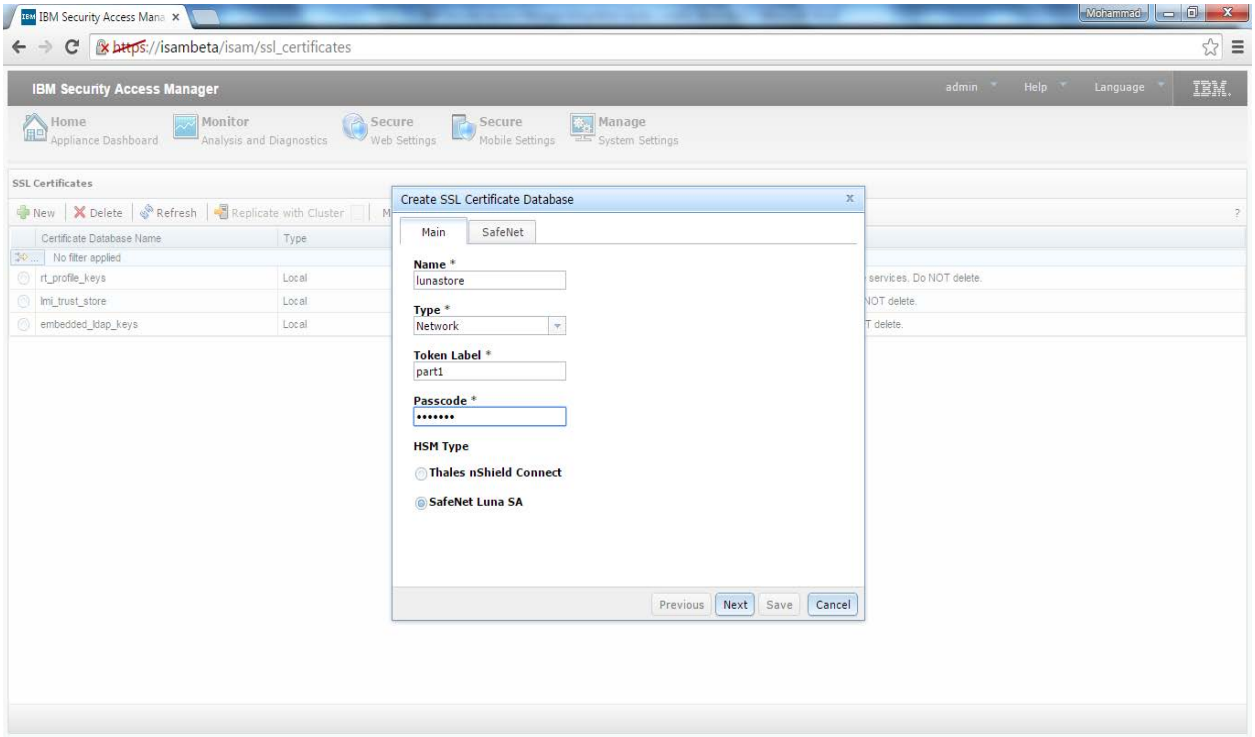
a) Open the browser, type https://hostname and enter.

b) Login to web console using username and password.

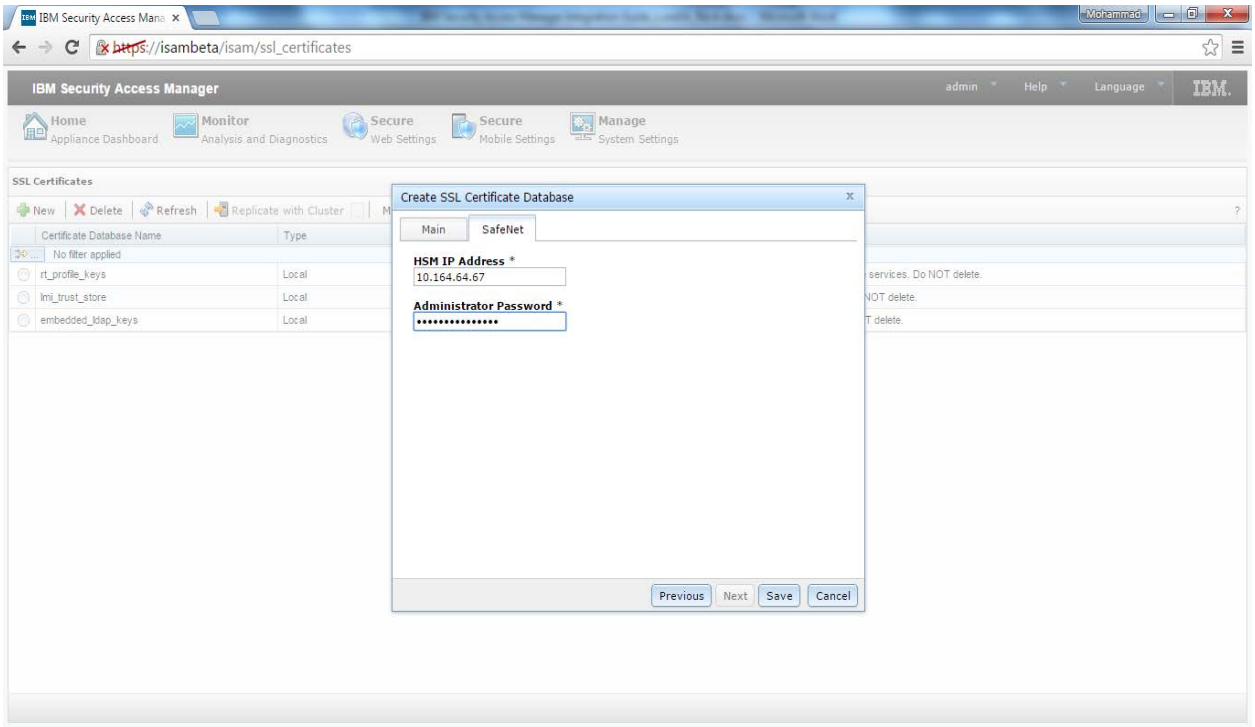
c) Click Manage -> Secure Settings -> SSL Certificates.



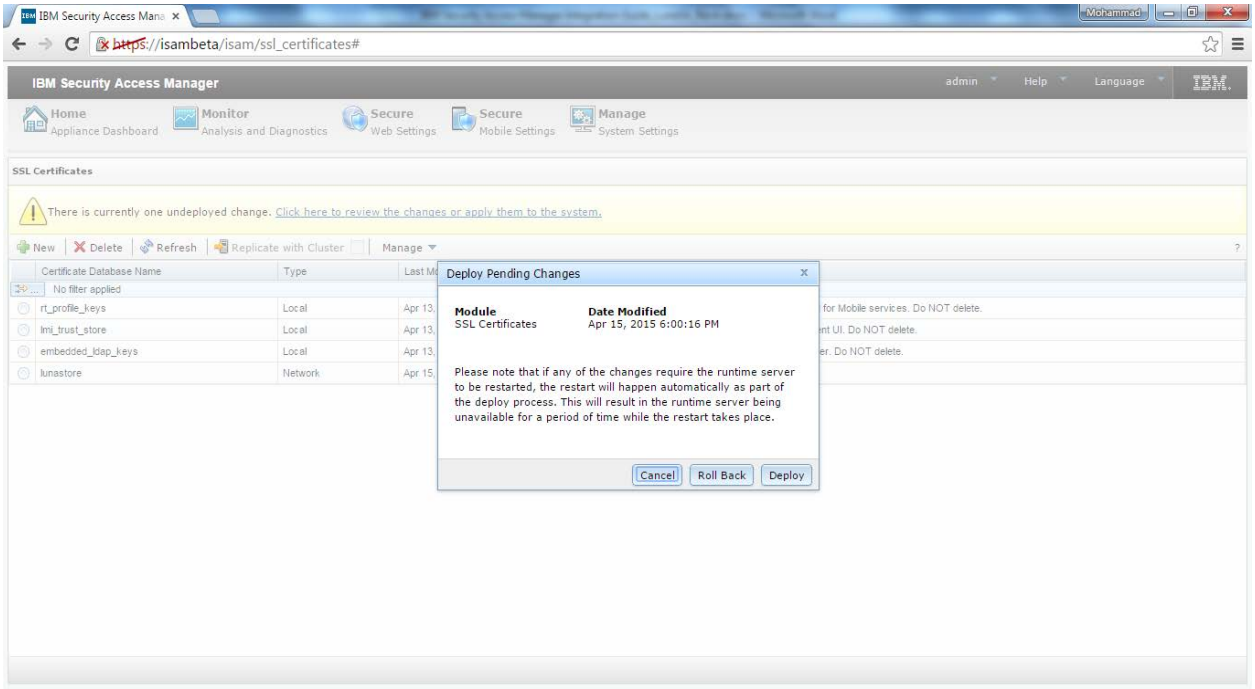
d) Click New to open Create SSL Certificate Database and provide Name of the database, select Type as Network. In HSM Type, select SafeNet Luna SA and enter HSM partition label in Token Label and partition password in Passcode. Click Next.



e) Enter HSM IP Address and Administrator Password and click Save.



f) Click the link “Click here to review the changes or apply them to the system.” and click Deploy and wait for the deployment to be completed.

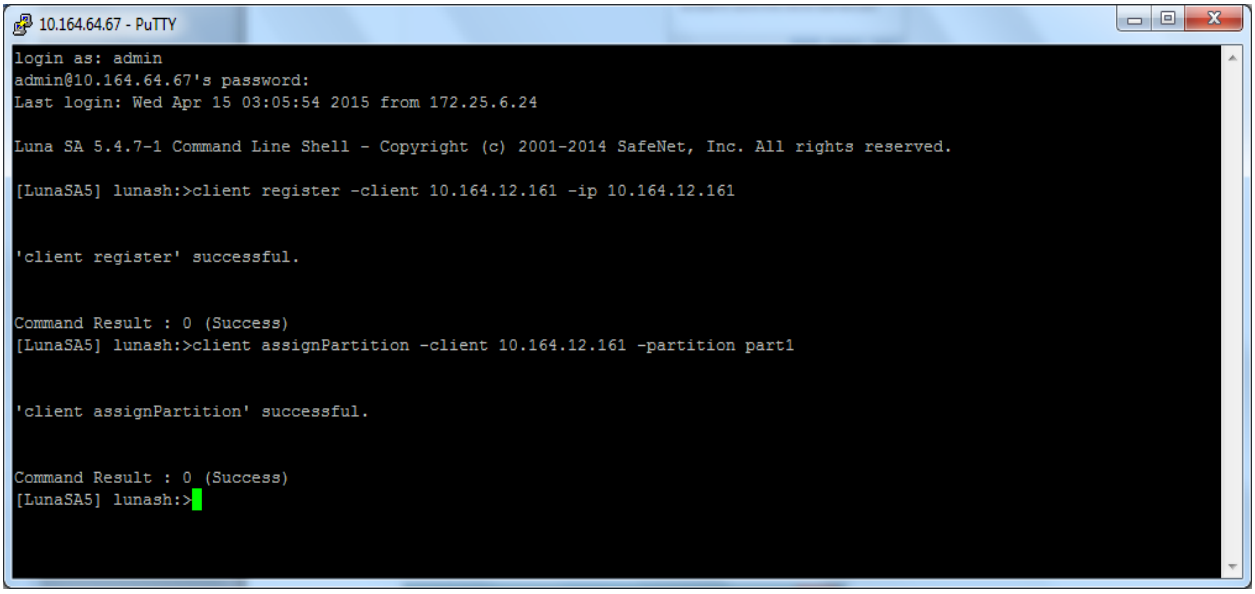


g) Now login to Luna SA console using putty or ssh and register the client on Luna SA and assign them the partition which you have registered with Security Access Manager web console. You need to execute below two commands:

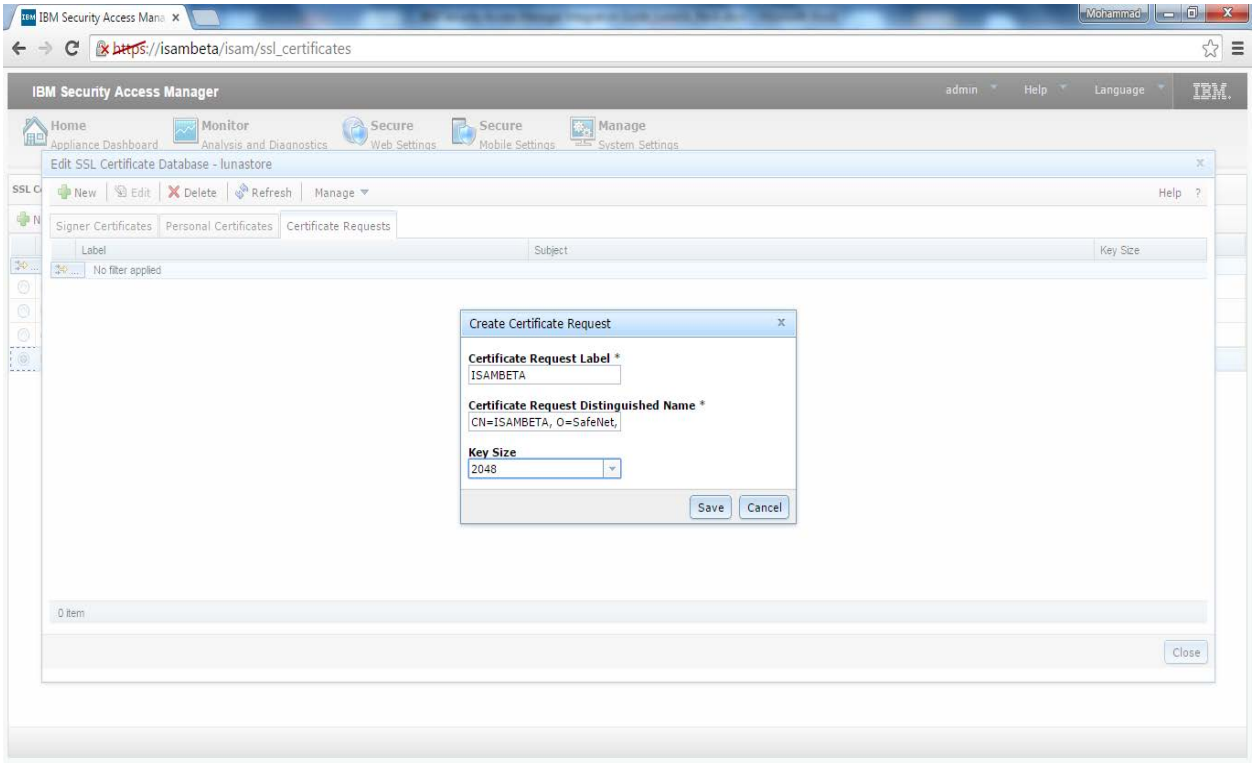
[LunaSA5] lunash:>client register -client <hostname or ip address> -ip <ip address>

[LunaSA5] lunash:>client assignPartition -client <hostname or ip address> -partition <partition name>

Partition name should be the same that you have provided at the time of database creation in web console.

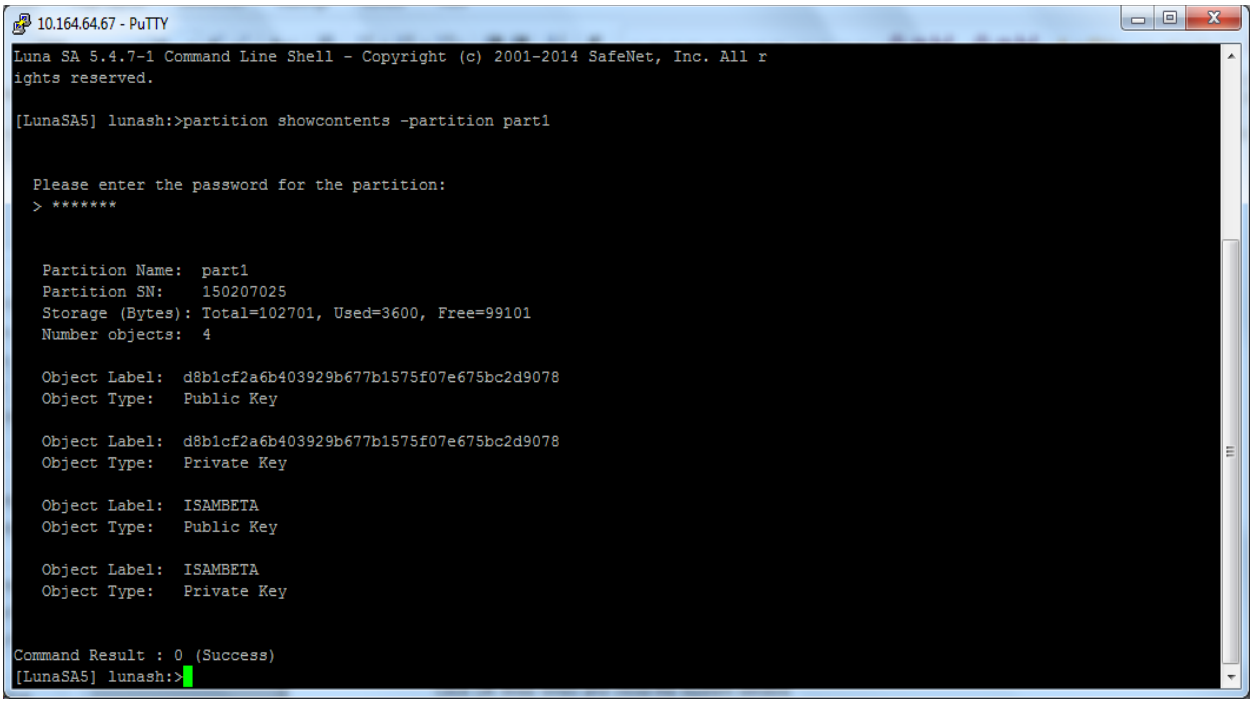


h) Now select the certificate database you have created. Click Manage -> Edit Certificate Database. A window will pops up, select Certificate Request tab and click New. In Create Certificate Request, enter the Certificate Request Label, Distinguished Name and Key Size. Click Save.

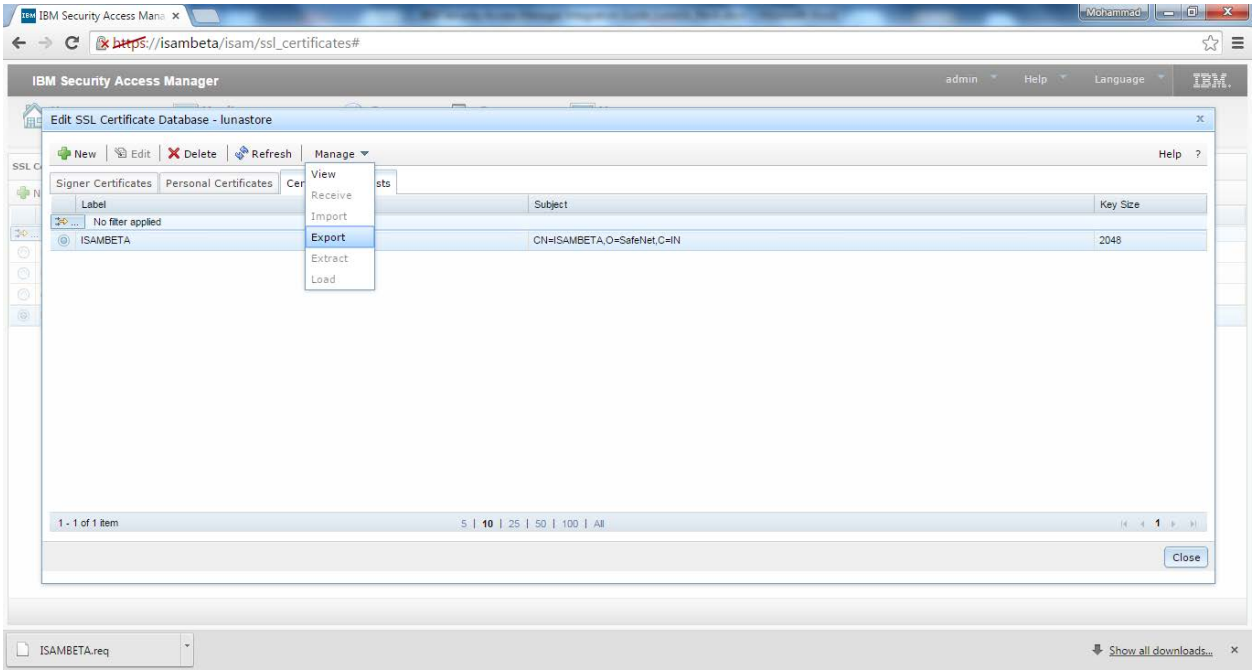


i) You can check the key pair generated on the Luna SA console using the command:

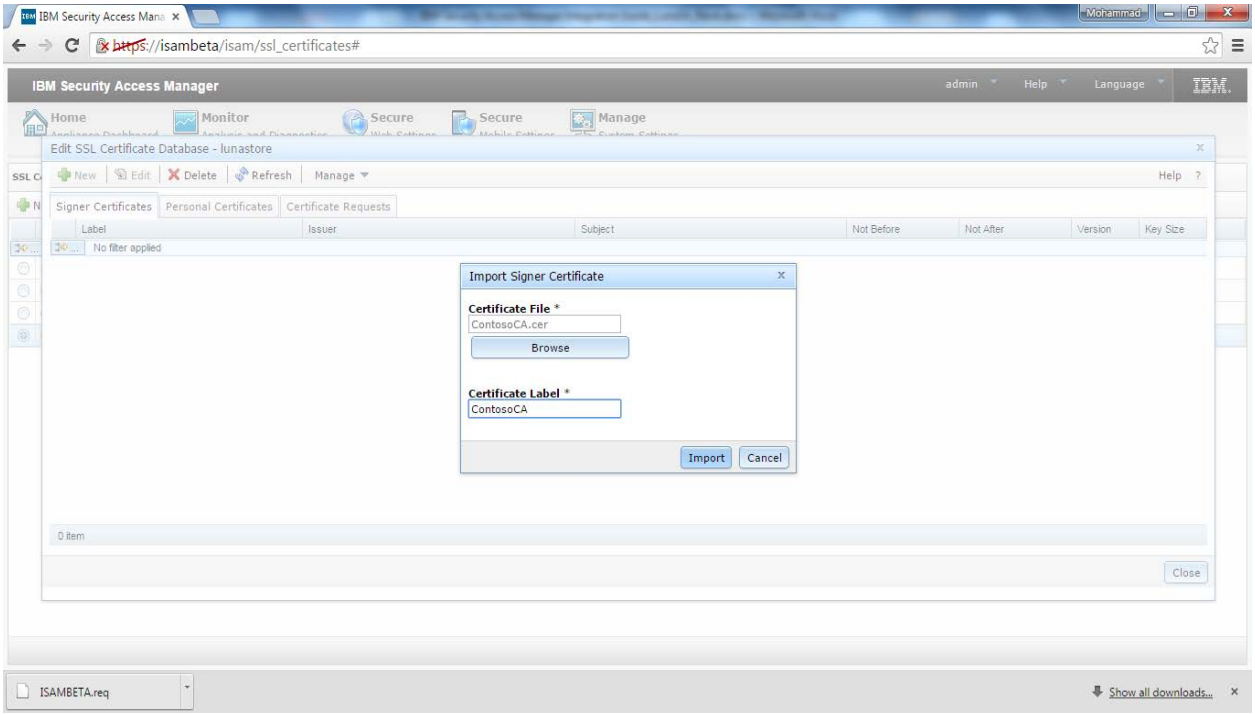
[LunaSA5] lunash:>partition showcontents -partition <partition name>



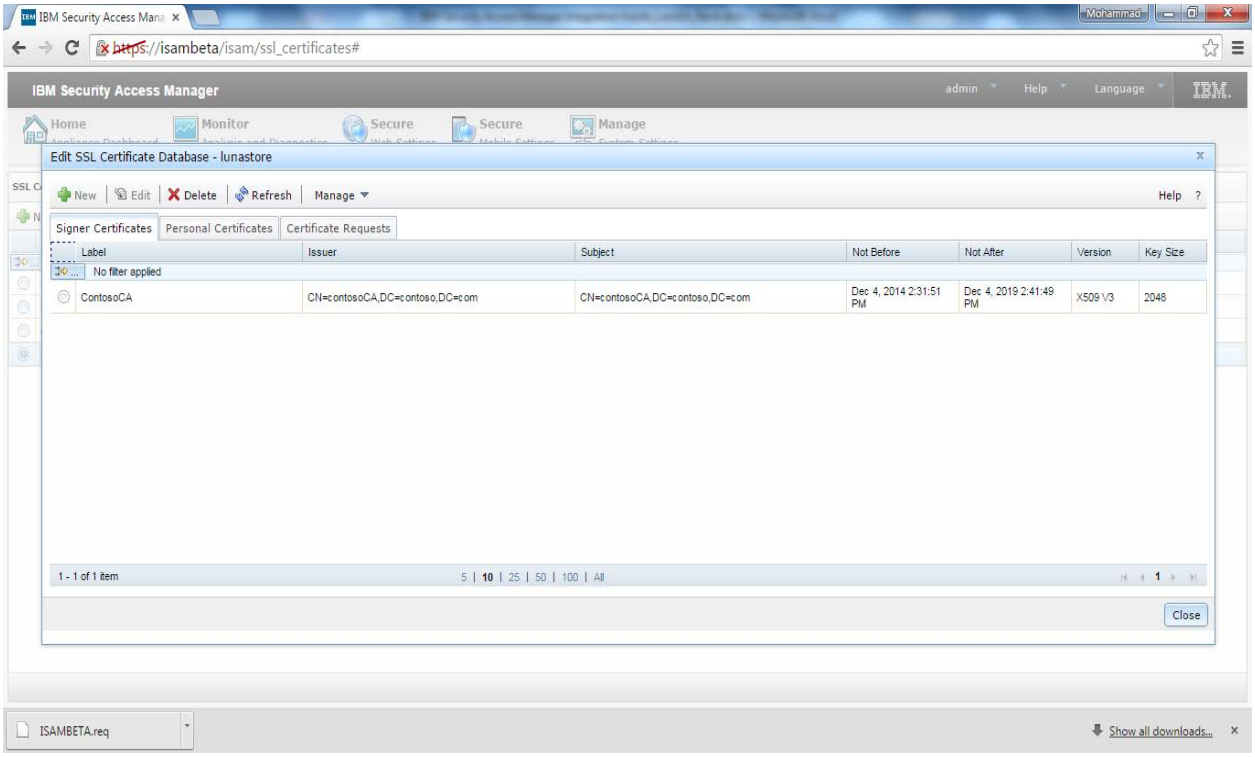
j) We need to submit this certificate request to the CA to obtain the signed certificate from CA. To do these please export the certificate request and send it to CA for signing. Open web console and select Certificate Request you have created and click Manage -> Export. A file containing the certificate request will be downloaded.



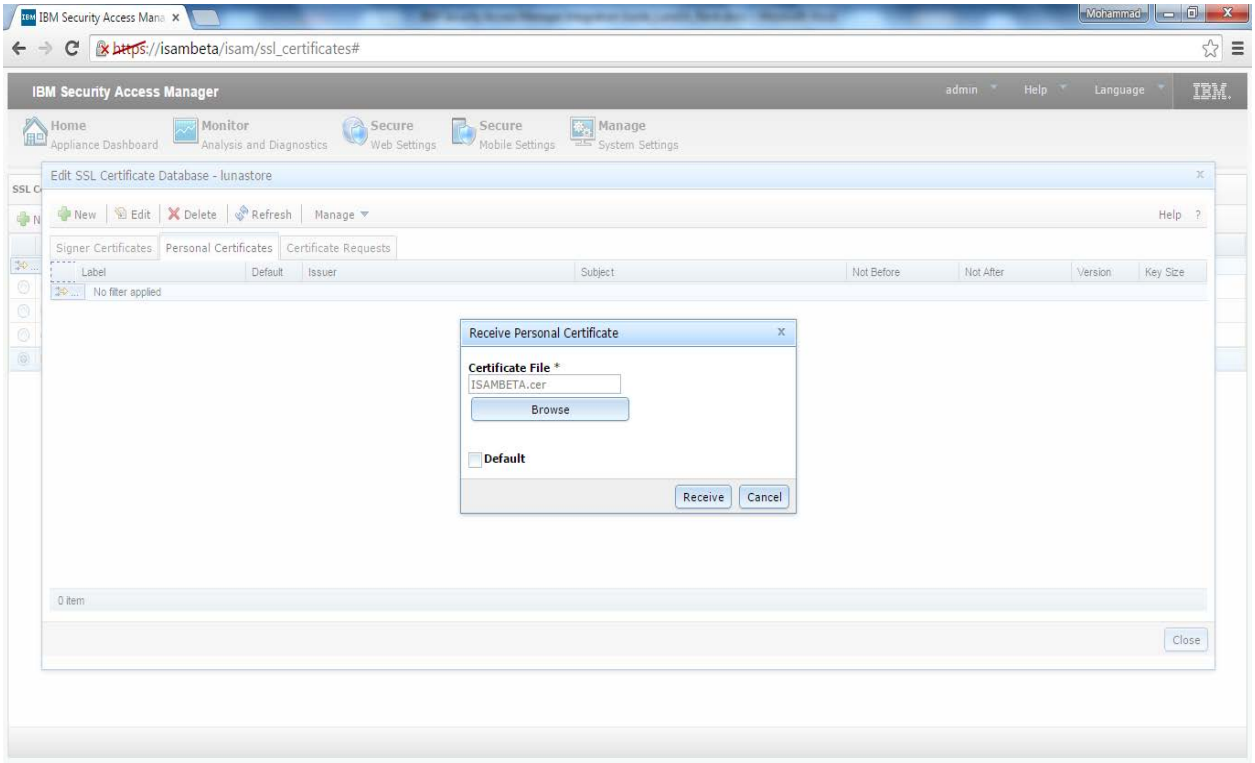
k) Send this certificate request to CA and obtain signed certificate request and CA signing certificate. Select certificate database and click Manage -> Edit Certificate Database. When window opens select Signer Certificate tab, click Manage -> Import. Browse and select signer certificate (CA that signed your certificate request), provide Certificate Label and click Import.



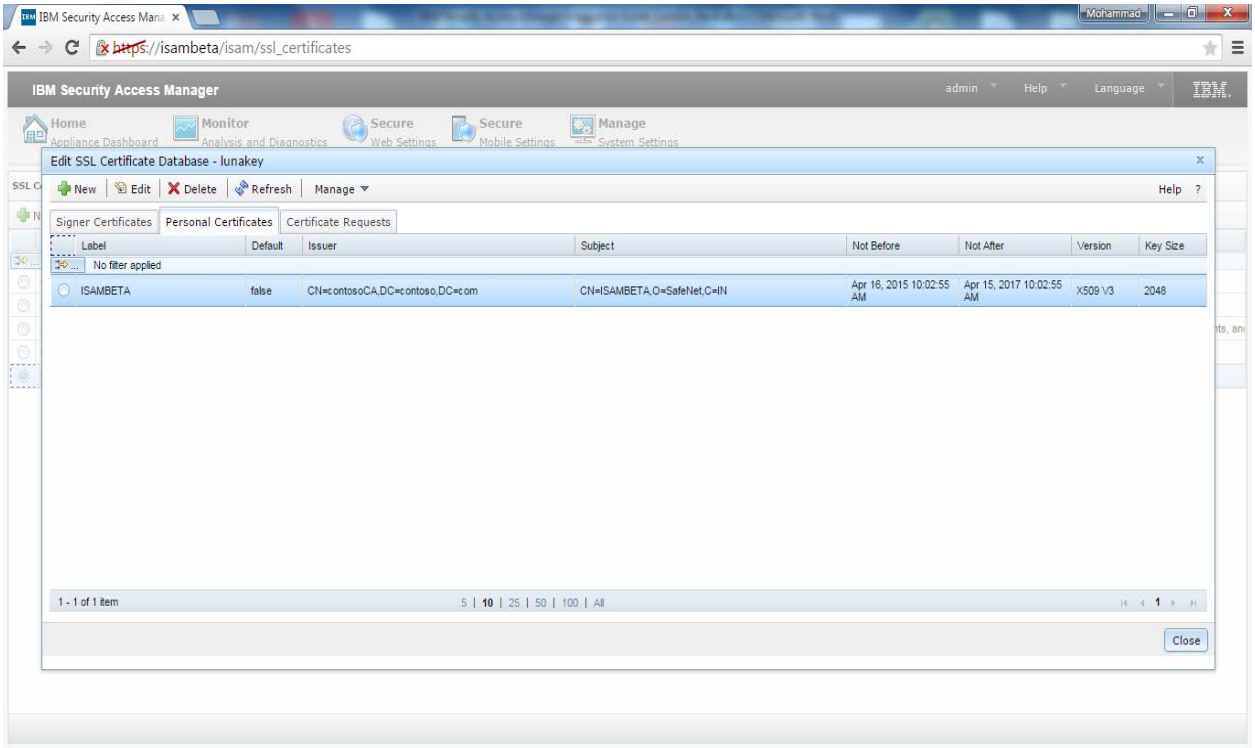
l) When the certificate import completed. CA certificate will be listed under Signer Certificate.



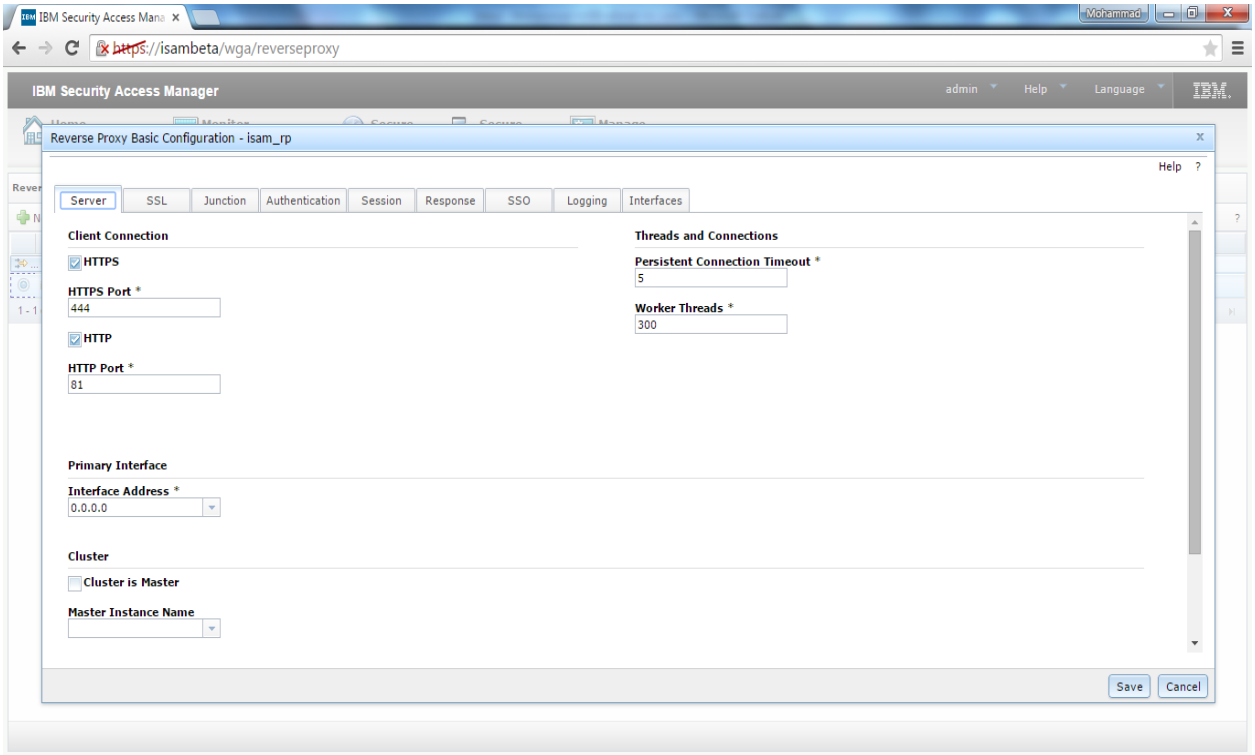
m) Select Personal Certificate tab, click Manage -> Receive. Browse and select the CA signed certificate and click Receive.



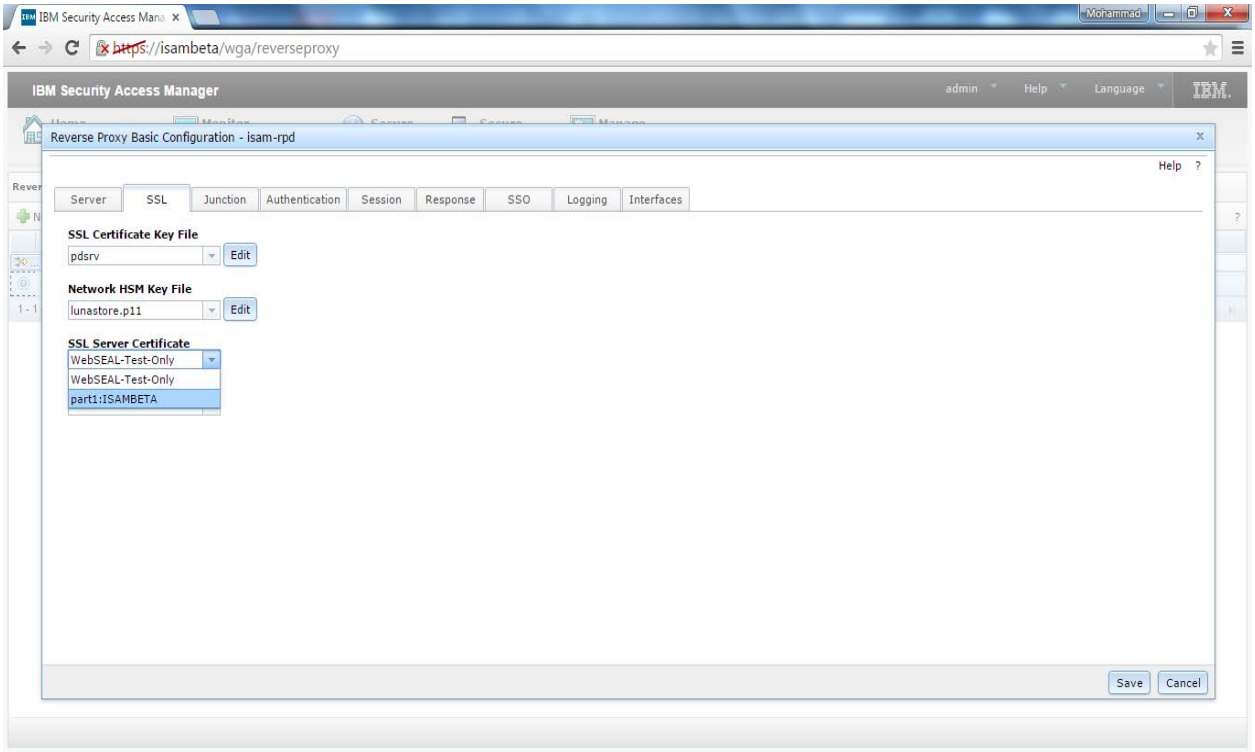
n) When the certificate received, it will be listed in the Personal Certificate tab. Click Close.



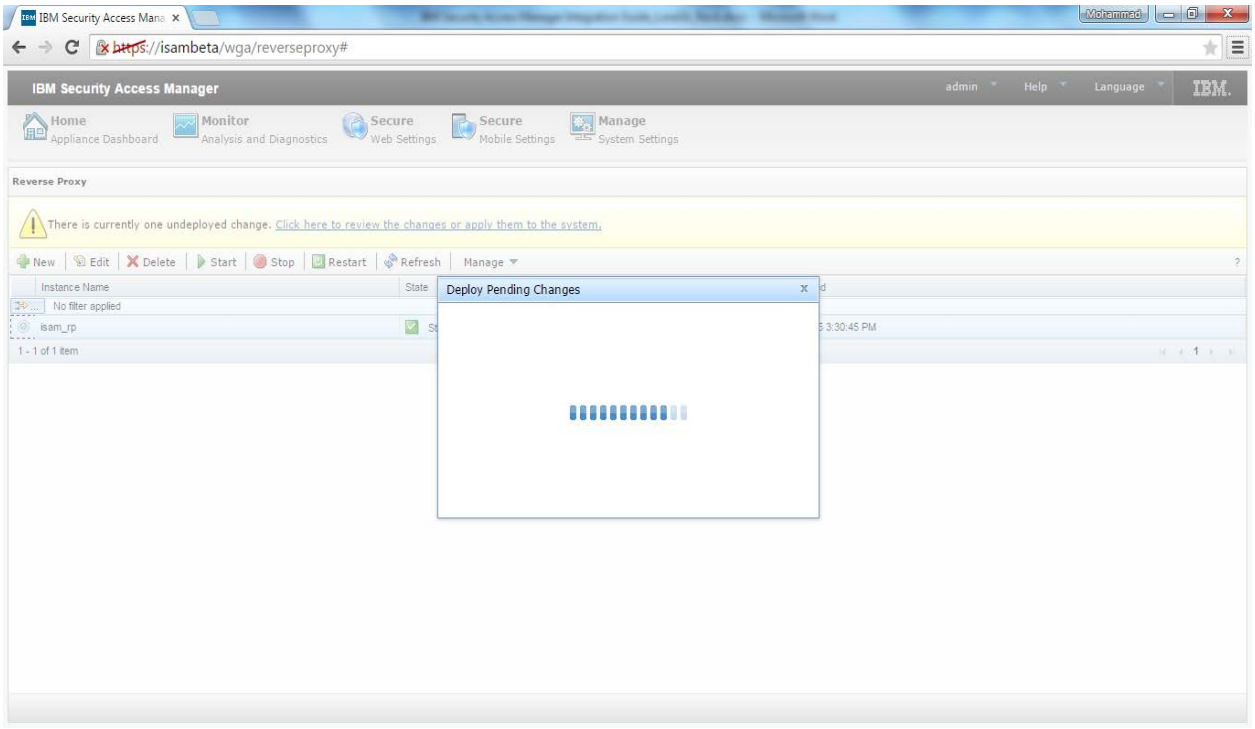
o) Click Secure Web Settings -> Reverse Proxy. Select Reverse Proxy instance name and click Edit. Select Server tab, under Client Connections select HTTPS.



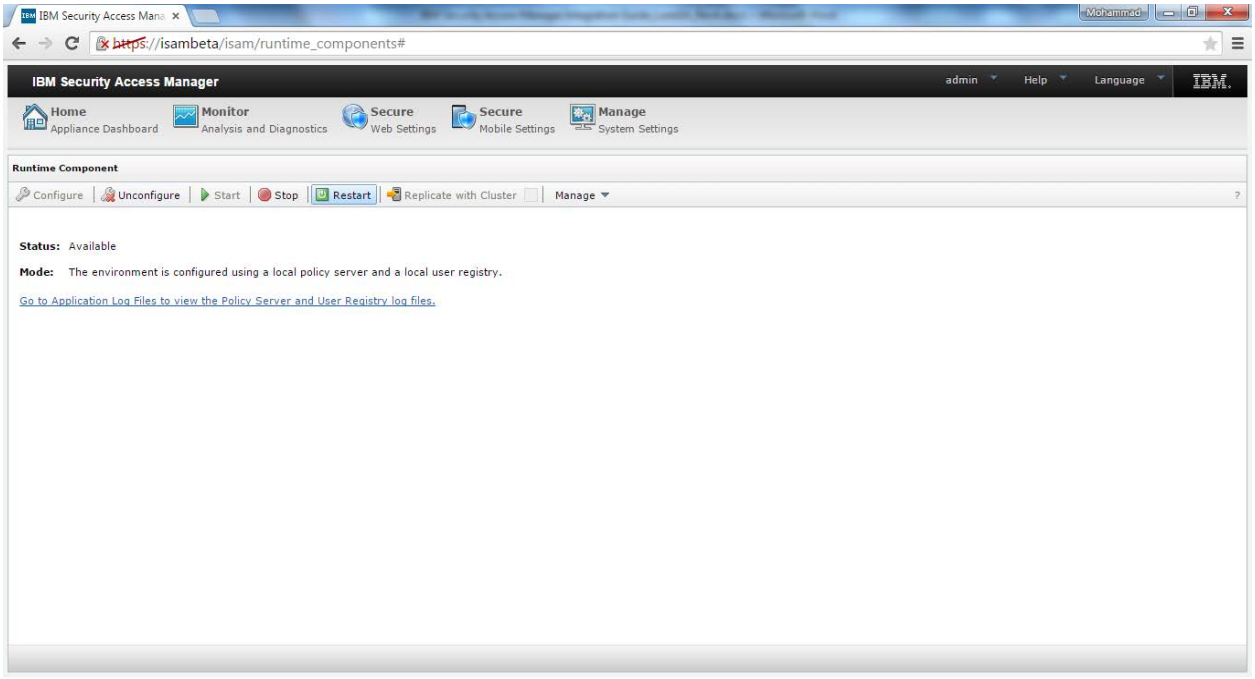
p) Click on SSL tab, select SSL Certificate Key File as pdsrv, select Network HSM Key File that you have created and select the SSL Server Certificate stored on the SafeNet HSM, the certificate name will be TokenLabel:CertificateName. Click Save.



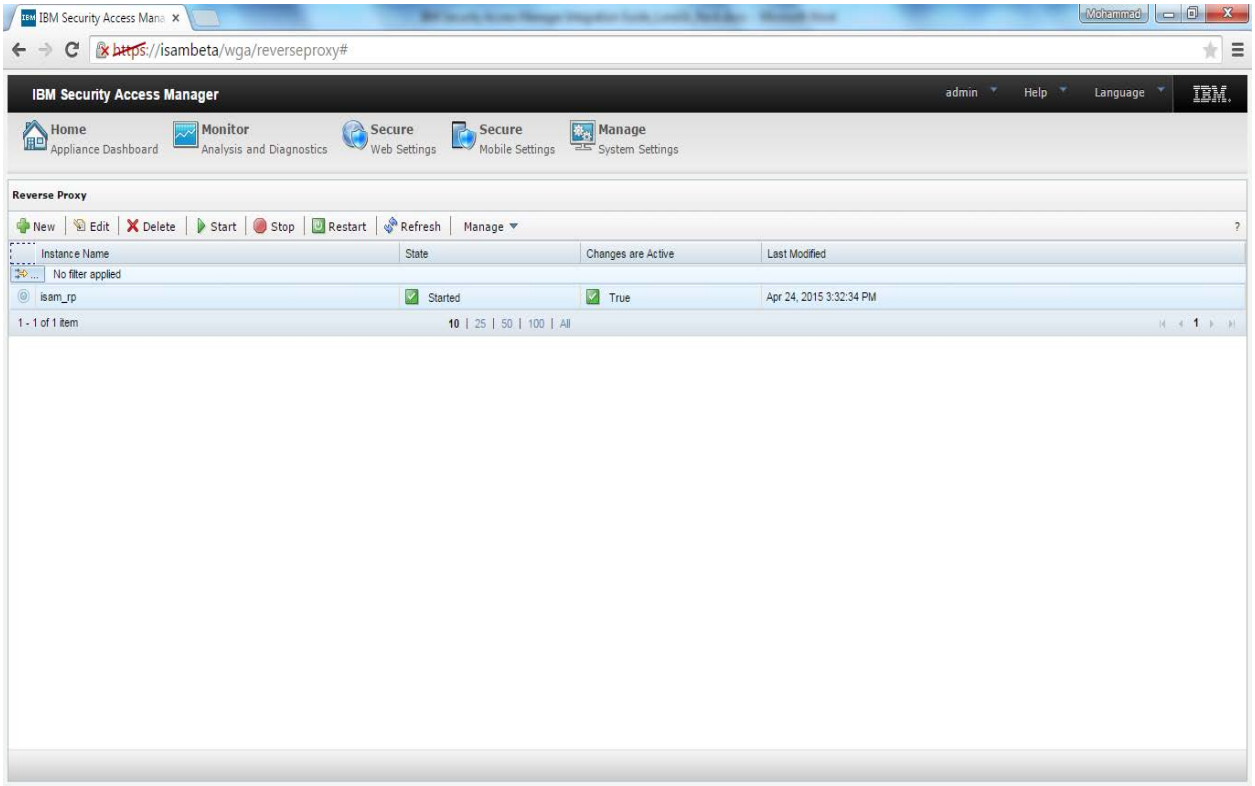
q) Click to the link Click here to review the changes or apply them to the system. Click Deploy and wait for the configuration to deploy successfully.



r) When the deployment complete. Click Secure Web Settings -> Runtime Component -> Restart.



s) Click Secure Web Settings -> Revere Proxy. Select Reverse Proxy Instance and click Restart. After restart State should be Started and Changes are Active should be true.



You have successfully configured the reverse proxy on HTTS using the SSL certificate stored on Luna HSM.

t) Now open the browser and enter the URL https://<ISAM Server Name>:444. For example: https://isambeta:444. When asked for authentication, provide username and password. Username will be sec_master and password that you have set.

Verify the SSL certificate, it will use the certificate that you have generated and stored on SafeNet HSM partition.