IBM Security Access Manager Integration Guide



THE DATA PROTECTION COMPANY 4

Document Information

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

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.

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	5
Scope	e e e e e e e e e e e e e e e e e e e	5
Prerequisites		7
CHAPTER 2	Integrating IBM Security Access Manager with Luna HSM	3
Configuring the	Security Access Manager for Luna HSM	3

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.

BM Security Access Manag	jer			admin Kelp Language I
Home Appliance Dashboard	Monitor Analysis and Diagnostics	Secure Web Setting	ps Secure Mobile Setting	gs System Settings
Updates and Licensing	Network Settings	System	Settings	Secure Settings
Overview	∎ General	∎ Date/Tir	ne	SSL Certificates
Application Database Settings	I DNS	Adminis	trator Settings	⊯ File Downloads
Available Updates	Interfaces	∎ Manage	ment Authentication	■ Silent Configuration
Scheduled Security Updates	Static Routes	∎ Manage	ment Authorization	
Update Servers	Front End Load Balancer	∎ Manage	ment SSL Certificate	
Update History	Hosts File	 Account 	Management	
Licensing and Activation	Packet Tracing Churten Configuration	Advance Casash	d Tuning Parameters	
Firmware Settings	Cluster Configuration	= Snapsno	Files	
Geolocation Database		= System	Δlerts	
		SNMP M	onitoring	
		Restart	or Shut down	
		Applicat	on Locale	
× *				rinn patri in a tracki di di anno para si interna a di ancienti
📥 <u>1.4</u>	▲ <u>1.2</u>			Flow Data is not enabled for any Reverse Proxy instances on this appliance. Enable Flow Data in one or more Reverse Proxy instances to use this widget.
n				
ut January	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
4 1.3	4 1.1			
n				
ut Juine	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
dated: Apr 15, 2015 5:30:41 PM		Defeash	 Security Actions 	
aacan npi 15/2010 0100111111		Kerresii		PAM Statistics recording is not enabled for any Reverse Proxy instances on this appliance.
everse Proxy Health				Enable PAM Statistics in one or more Reverse Proxy instances to use this widget.

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.

		admin Help Language 預設
iltor ysis and Diagnostics	ecure Secure Manage leb Settings Manage	
	-	
Replicate with Cluster	Create SSL Certificate Database	X
Туре	Main SafeNet	
	Name *	
Local	lunastore	services. Do NOT delete.
Local	Tune *	NOT delete.
Local	Network	T delete.
	Passcode * •••••• HSM Type O Thales nShield Connect @ SafeNet Luna SA	
	ittor International Constraints of Second Se	Itor Secure Manage Veb Settings Mobile Settings System Settings Replicate with Cluster Main SafeNet Type Main SafeNet Local Type * Network: Local Token Label * Parti Parti Parti Parti

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

Idia Security Access Manager Admin * Help * Langu Monice Appliance Dashboard Monitor Manalysis and Diagnostics Secure Web Settings Manage Mobile Settings SSL Certificates Image Manage Mobile Settings Secure Mobile Settings Secure Mobile Settings SSL Certificates Image Manage Mobile Settings Image Manage Mobile Settings Secure Mobile Settings Secure Mode Manager Image Manager Image Manager Secure Mobile Settings Secure Mode Manager Image Manager Secure Mobile Settings Secure Mobile Settings Imager Imager Main SafeNet Secure Manager Secure Manager Imager Imager Imager Secure Secure Manager	Language IR				
Home Appliance Dashboard Ana	nitor Iysis and Diagnostics	ecure Secure Manage eb Settings Mobile Settings System Settings			
SL Certificates				1	
🖟 New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 🚽	Access Manager admin Help Language IBM. Dashboard Monitor Web Settings Secure System Settings Lette Refresh Replicate with Cluster Main Safelitet Secure Secure Secure System Settings Idete Refresh Replicate with Cluster Main Safelitet Secure Secure				
Certificate Database Name					
No filter applied	isambeta/isam/ssl_certificates				
rt_profile_keys	Local	10.164.64.67		services. Do NOT delete.	
imi_trust_store	Local	Administrator Password *		NOT delete.	
embedded_ldap_keys	Local	••••••		T delete.	
		Previous	Nevt Save Carrel		
				J	

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.

 Martps://isdifibeta/ 	isany ssi_cerunedtes#				 		223
IBM Security Access Manager			Abbie Settings System Settings es or apply them to the system, ge T. Last M. Dodar a		IBM.		
Home Appliance Dashboard Anal	litor ysis and Diagnostics	admin * Help *					
IBM Security Access Manager admin Heip Language IBM. IBM Security Access Manager IBM. IBM.<							
	IdM Security Access Manager IdM Security Access Manager Manage Secure Manage System Settings Model and Desphoard Manages and Diagnostics Secure Web Settings Secure System Settings SSL Certificates SSL Certificates Secure To provide thange or apply them to the system. Secure To provide thange or apply them to the system. Image There is currently one undeployed change. Click here to review the changes or apply them to the system. Secure To provide thange or apply them to the system. Image There is currently one undeployed change. Click here to review the changes or apply them to the system. Image To provide them to the system. Image Type To provide thange Type Click here to review the changes or apply them to the system. Image Type Type Click here to review the changes or apply them to the system. Image Type Type Click here to review the changes or apply them to the system. Image Type Type Click here to review the changes or apply them to the system. Image Type Type Click here to review the changes require the runtime server to runtime server to be restarted, the restart will happen automatically as part of the deploy process. This will result in the runtime server being unavailable for a period of time while the restart takes place. Image Type Type Type Type Type Type Type Typ						
Home Appliance Dashboard Monitor Analysis and Diagnostics Secure Web Settings Manage System Settings SSL Certificates Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: There is currently one undeployed change. Click here to review the changes or apply them to the system. Image: The imag							
IBM Security Access Manager admin Heip Language Monitor Appliance Dashboard Monitor Monitor Appliance Dashboard Analysis and Diagnostics Secure Web Settings System Settings St Certificates Secure Monitor Monage System Settings There is currently one undeployed change. Click here to review the changes or apply them to the system. Secure Secure Image: Provide a policide Refresh Repricate with Cluster Manage Image: Provide a policide of the applied Refresh Repricate with Cluster Manage Image: Provide a policide detabase Name Type Least Deloy Pending Changes X Module Date Modified Secure or babase Name Type Securitizate Database Name Y Securitizate Database Name Type Least Apr 13, 2015 6:00:16 PM FM double services. Do NOT delete. FM double detabase Name Imastore Network Apr 13, 2015 6:00:16 PM FM double detabase Name FM do							
rt_profile_keys	Local	Secure Web Settings Secure Mobile Settings Secure System Settings Instruction of the system settings System Settings Instruction of the system settings State System settings Instruction of the set set set set set set set set set se					
Imi_trust_store	Local						
embedded_ldap_keys	Local						
) lunastore	Network	Apr 15,	Pettings Mobile Settings LastM Deploy Pending Changes LastM Deploy Pending Changes X Module SSL Certificates Apr 13, Date Modified Apr 13, Please note that if any of the changes require the runtime server to be restarted, the restart will happen automatically as part of the deploy process. This will result in the runtime server being unavailable for a period of time while the restart takes place.				
			the deploy process. unavailable for a pe	Secture Mobile Settings Manage System Settings upby them to the system. log Pending Changes bdule SL Certificates Date Modified Apr 15, 2015 6:00:16 PM Vease note that if any of the changes require the runtime serve bei unavailable for a period of time while the restart takes place Icancel Roll Back			
		admm Help Language Secure System Settings System Settings eview the chances or apply them to the system. System Settings Manage ¬ Last M Last M Deploy Pending Changes X Apr 13 Apr 13 Apr 15 Please note that if any of the changes require the runtime server being unavailable for a period of time while the restart takes place. In Mol Manage T Cancell Roll Back Deploy					

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.

C Kettps://isambeta/isam/ssl_certificates		
M Security Access Manager		admin Help Language
Home Monitor George Sect Appliance Dashboard Analysis and Diagnostics Web Edit SSL Certificate Database - lunastore	re Secure Manage Jettings Mobile Settings System Settings	
🖶 New 🕲 Edit 🗙 Delete 🗞 Refresh Manage 🔻		Hel
Signer Certificates Personal Certificates Certificate Requests		
Label	Subject	Key Size
0 Rem	Certificate Request Distinguished Name * CN=ISAMBETA, O=SafeNet, Key Size 2048 v Save Cancel	
, o norm		

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.

a secul	ity Access Manager				admin Help	Language		and a
Edit SSL	Certificate Database - lunastore							2
	🛛 🖗 Edit 🗍 🗙 Delete 🗍 🖑 Refresh 🗍	Manage 🔻					Help	?
Signer (Certificates Personal Certificates Cer	View	sts					
Lab	bel	Import		Subject		Key Size		
1	No filter applied	Export				0040		
ISA	MBETA	Extract		CN=ISAMBETA,O=SafeNet,C=IN		2048		
		Land						
1 - 1 of 1	i item			5 10 25 50 100 All		(4 - 4 -))
							Clo	se

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.

a security Access manager						
Home Mo Edit SSL Certificate Database -	nitor Secure	Secure Manage				
🔹 New 🕲 Edit 🗙 Delete	🛷 Refresh 🛛 Manage 👻					Help
Signer Certificates Personal C	ertificates Certificate Requests					
Label	Issuer	Subject	Not Before	Not After	Version	Key Size
No filter applied						
		Import Signer Certificate	x			
me Monitor Secure Manage It SSL Certificate Database - Lunastore Making Certificate Certificate Requests I tobel Refresh Manage * Signer Certificates Certificate Requests Import Signer Certificate Label Issuer Subject Not Before Not After Version 20- No fifter appled Import Signer Certificate Certificate File * ContosoCA.cer Envise						
		Contosocation				
	ify Access Manager admin * Help * Langua Monitor Secure Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Monitor Certificate Database - lunastore Certificates Personal Certificates Certificates Mer appled Not Before Import Signer Certificate Not After Version Certificate File * Contoso CA.cer Envoyse Certificate Label * Contoso CA.cer Contoso CA.cer Envoyse Certificate Label * Contoso CA.cer Import Cancel Monitor					
		Certificate Label *				
		ContosoCA				
		Import Car	ncel			
		N				
0.8						
Vitem						
						Clo

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

I Security Acce	ss Manager							
Home	Monitor	Secure Secure	Manage					
Edit SSL Certifica	te Database - lunastore	mastice W Mish Cottings W Mahile Co	Hinne - 25 Curtan Caltinan					1
🝦 New 🛛 🗐 Ed	t 🛛 🗙 Delete 🛛 🦑 Refresi	n Manage ▼					Help	-
Signer Certificate	s Personal Certificates	Certificate Requests						
Label	<u>.</u>	Issuer	Subject	Not Before	Not After	Version	Key Size	
No filter app	lied		ON suction DO suction DO sum	Dec 4, 2014 2:31:51	Dec 4, 2019 2:41:49	VEROLUR	20.40	
1 - 1 of 1 item		5 10 25	1 50 100 AU				4 1):	H

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

Home Appliance Dashboard Appliance Dashboard	(march)						
Edit SSL Certificate Database - lunastore	Appliance Dashboard Anal	itor Secure ysis and Diagnostics Web Settings	Secure Mobile Settings				
New Stelt X belete Refresh Manage Help. Signer Certificate Personal Certificate Requests Label Default No filter applied Receive Personal Certificate File * ISAMBETA.cer Browse Default Receive Cancel	Edit SSL Certificate Database - I	unastore					
Signer Certificates Personal Certificate Requests Label Default Issuer Subject Not Before Not After Version Key Size 20 No filter applied Receive Personal Certificate File * ISAMBETA.cer Browse Default Receive Cancel	🐠 New 🛛 😒 Edit 🛛 🗙 Delete	🗬 Refresh 🛛 Manage 🔻					Help
Label Default Issuer Subject Not Before Not After Version Key Size 200 No filter applied Certificate X Certificate File ISAMBETA.cer Browse Default Receive Cancel	Signer Certificates Personal Co	ertificates Certificate Requests					
Receive Personal Certificate X Certificate File * ISAMBETA.cer Browse Default Receive Cancel	Label	Default Issuer	Subject	Not Before	Not After	Version	Key Size
Receive Personal Certificate X Certificate File * ISAMBETA.cer Browse Default Receive Cancel							
			Default	Cancel			
0 item	0 item						
0 item	0 item						Clo

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

	cess manager							
Home	Monitor	Secure	Secure	Manage				
Edit SSL Certifi	icate Database - lunakey	agnostics web Setting:	s Mobile Settings	System Settings				
🗣 New 🛛 😰	Edit 🛛 🗙 Delete 🛛 🖑 Refre	esh 🛛 Manage 🔻						Help
Signer Certific	ates Personal Certificates	Certificate Requests						
Label	Defau	it Issuer		Subject	Not Before	Not After	Version	Key Size
😒 No filter	applied						8	
O ISAMBETA	false	CN=contosoCA,DC=contoso	b,DC=com	CN=ISAMBETA,O=SafeNet,C=IN	Apr 16, 2015 10:02:55 AM	Apr 15, 2017 10:02:55 AM	×509 √3	2048
1 - 1 of 1 item			5 10 25 50	100 [All			14	4 1 +

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

	ager				
-	Monitor	Cocuro 🗖	Eacura 🕅	Managa	
verse Proxy Basic Confi	guration - isam_rp				
					Hel
Server SSL	Junction Authenticatio	n Session Response	SSO Loggir	g Interfaces	
Client Connection				Threads and Connections	
				Persistent Connection Timeout *	
HTTPS Port *				5	
444				Worker Threads *	
HTTP				300	
HTTP Port *					
81					
Primary Interface					
0.0.0.0	v				
Cluster					
Cluster is Master					
Master Instance Name					
	•				

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.

C C C C C C C C C C C C C C C C C C C	Meverseproxy#			X
BM Security Access Manager				Language IB)
Home Appliance Dashboard Monitor	and Diagnostics	Secure Mobile Settings		
erse Proxy				
There is currently one undeployed cha	inge. <u>Click here to review the change</u>	s or apply them to the system.		
 New 🕲 Edit 🗙 Delete 🕨 Start	Stop Restart Refresh	Manage 💌		
Instance Name	State	Deploy Pending Changes	x d	
No filter applied				
isam_rp	🖾 st		5 3:30:45 PM	
1 of 1 item				N 9011

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.

IBM Security Access Mana ×	Britan Area	Streep Stephine Sold, Locald, Mr.	the Manhood Star	Meizannad 🗖 🖉 📈
← → C	erseproxy#			* =
IBM Security Access Manager				admin Help Language IBM .
Home Monitor Appliance Dashboard	iagnostics	ettings Manage System Settings		
Reverse Proxy				
🜗 New 🕲 Edit 🗙 Delete 🕨 Start 🥘 S	Stop 🛛 🖸 Restart 🛛 🖑 Refresh 🔹 Manage 🔻			?
Instance Name	State	Changes are Active	Last Modified	
No filter applied			A 04 0045 0.00.04 DM	
lisam_rp	Started	Irue Irue	Apr 24, 2015 3:32:34 PM	1. 1840 S. 18

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.

