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	θ	5
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	er			admin 🔭 Help 🎽 Language 🎽 打
	fonitor nalysis and Diagnostics	Secure Web Settir	gs Secure Mobile Setting	gs The System Settings
Updates and Licensing	Network Settings	System	Settings	Secure Settings
Application Database Settings	General DNS		me strator Settings	SSL Certificates
Available Updates	Interfaces		ment Authentication	silent Configuration
Scheduled Security Updates	Static Routes		ment Authorization	
Update Servers	Front End Load Balancer	∎ Manage	ment SSL Certificate	
Update History	Hosts File	Account	t Management	
Licensing and Activation	Packet Tracing		ed Tuning Parameters	
Firmware Settings	 Cluster Configuration 	■ Snapsh		
Fix Packs Geolocation Database		 Suppor System 		
ocolocation batabase		SNMP N		
		■ Restart	or Shut down	
		Applica	tion Locale	
▲ 1.4	▲ 1.2			Flow Data is not enabled for any Reverse Proxy instances on this appliance.
n <u></u>	T <u>1.2</u>			Enable Flow Data in one or more Reverse Proxy instances to use this widget.
ut January				
A				
n <u>1.3</u>	<u>▲ 1.1</u>			
ut ,				
			Security Actions	
dated: Apr 15, 2015 5:30:41 PM		<u>Refresh</u>		
everse Proxy Health				PAM Statistics recording is not enabled for any Reverse Proxy instances on this appliance. Enable PAM Statistics in one or more Reverse Proxy instances to use this widget.
everse Floxy nediul				······································

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.

IBM Security Access Manager			admin Help Language]室所。
	nitor lysis and Diagnostics	ecure Secure Manage eb Settings Mobile Settings	
SL Certificates		Create SSL Certificate Database	x
🛊 New 🛛 🗙 Delete 🛛 💣 Refresh 🛛 🖣	Replicate with Cluster	M	
Certificate Database Name	Туре	Main SafeNet	
No filter applied		Name *	
rt_profile_keys	Local	lunastore	services, Do NOT delete.
Imi_trust_store	Local	Type *	NOT delete.
embedded_ldap_keys	Local	Network	T delete.
		Passcode * •••••• HSM Type ① Thales nShield Connect @ SafeNet Luna SA	

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

IBM Security Access Manager			admin Help Language IBM
	me Analysis and Diagnostics Secure Analysis and Diagnostics Web Settings Mobile Settings System Settings System Settings Create SSL Certificate Database Create SSL Certificate Database Main SafeNet HSM IP Address * 10.164.54.647 Administrator Password *	sound hop surgary 1518	
Appliance Dashboard Ana	lysis and Diagnostics	Neb Settings Mobile Settings System Settings	
SL Certificates		Create SEL Cartificate Database	Y
🥐 New 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 🚽	Replicate with Cluster	M	
Certificate Database Name	Туре	Main SafeNet	
IBM Security Access Manager Mome Monitor Secure Manage Appliance Dashboard Monitor Secure System Settings SSL Certificates Create SSL Certificate Database X Main SafeNet SafeNet Soc. No filter applied Local HSM IP Address * 10.164.64.67 Imimust_store Local Local Administrator Password * T delte.			
	Local	10.164.64.67	services, Do NOT delete.
		Administrator Password *	
embedded_ldap_keys	Local	••••••	T delete.
		Previous	Next Save Cancel

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.

Home Appliance Dashboard Monitor Analysis and Diagnostics Secure Web Settings Secure Mobile Settings Manage System Settings State Certificates Image: Secure Web Settings Secure Web Settings Secure Sec	Appendix Desired at any of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the system, Image of the provide any of the changes of apply them to the provide any of the changes require the runtime server to be restarted, the restart will happen automatically ap part of the provide apply the provide any of the changes require the runtime server to be restarted, the restart will happen automatically ap part of the provide any of the provide any of the provide apply the provide any of the provi	IBM Security Access Manager						admin Help	Language 1
SSL Certificates Image: Subsection base harmonic of the services of apply them to the system. Image: Structure base harmonic of the services of apply them to the system. Image: Structure base harmonic of the services of apply them to the system. Image: Structure base harmonic of the services of apply them to the system. Image: Structure base harmonic of the services of t	ertificates	Home Mo				Manage			
New X Delete Repficate with Cluster Manage ▼ Certificate Database Name Type Last M Deploy Pending Changes X No filter applied In cprofile_keys Local Apr 13, SSL Certificates Apr 15, 2015 6100:16 PM Int Use NOT delete. Im Usu t_store Local Apr 13, Nanatore Please note that if any of the changes require the runtime server to be restarted, the restart will happen automatically as part of the delploy process. This will restart takes place. From NoT delete.	Andle Replicate with Cluster Manage ew X Delete Replicate with Cluster Manage with replied Type Lost M Deploy Pending Changes X No filter applied Manage Module Date Modified Tor Mobile services. Do NOT delete. mit_trust_store Local Apr 13, SL Certificates Apr 15, 2015 6:00:16 PM unastore Network Apr 15, Please note that if any of the changes require the runtime server to be restarted, the restart value runtime server to be restarted, the restart value period of time while the restart takes place. er. Do NOT delete.	- Spinner Series and - Alle	Monitor Analysis and Diagnostics Secure Web Settings Secure Mobile Settings Manage System Settings currently one undeployed change. Slick here to review the changes or apply them to the system. Delete Refresh Replicate with Cluster Manage Delete Refresh Replicate with Cluster Manage Deloy Pending Changes applied Babase Name Type Last M Deloy Pending Changes applied Apr 13, Dire Local Apr 13, Network Apr 13, Apr 13, Network Please note that if any of the changes require the run to be restarted, the restart will happen automatically the deloy process. This will result in the runtime ser- unavailable for a period of time while the restart take		System Setungs				
New X Delete Repficate with Cluster Manage ▼ Certificate Database Name Type Last M Deploy Pending Changes X No filter applied In cprofile_keys Local Apr 13, SSL Certificates Apr 15, 2015 6100:16 PM Int Use NOT delete. Im Usu t_store Local Apr 13, Nanatore Please note that if any of the changes require the runtime server to be restarted, the restart will happen automatically as part of the delploy process. This will restart takes place. From NoT delete.	Andle Replicate with Cluster Manage ew X Delete Replicate with Cluster Manage with replied Type Lost M Deploy Pending Changes X No filter applied Manage Module Date Modified Tor Mobile services. Do NOT delete. mit_trust_store Local Apr 13, SL Certificates Apr 15, 2015 6:00:16 PM unastore Network Apr 15, Please note that if any of the changes require the runtime server to be restarted, the restart value runtime server to be restarted, the restart value period of time while the restart takes place. er. Do NOT delete.		Reference Monitor Secure Monitor Manage ance Dashboard Analysis and Diagnostics Web Settings Email Settings Email Settings tes is currently one undeployed change. Click here to review the changes or apply them to the system. X Delete Refresh Replicate with Cluster Manage X Delete Refresh Replicate with Cluster Manage Monage te Database Name Type Lost M Deploy Pending Changes ter applied Apr 13, Latore Lost A Date Modified Latore Local Apr 13, re SL Certificates Apr 15, 2015 6:00:16 PM Please note that if any of the changes require the runtime serve unavailable for a period of time while the restart takes Manage monage	aucham					
Certificate Delabases Name Type Last M Deploy Pending Changes X In Lyron flex applied	Certificate Database Name Type Last M Deploy Pending Changes X Notifier applied	<u> </u>	tes is currently one undeployed change. Click here to review the changes or apply them to the system. X Delete Refresh Refresh Replicate with Cluster K Delete Replicate Replicate with Cluster K Delete Replicate Replicat	system.					
Modile Date Modified Apr 13, Mi_strus_tstre Date Modified Apr 13, SLCerbificates To Modele services, Do NOT delete. Module SSLCerbificates Apr 15, 2015 6:00:16 PM Int U. Do NOT delete. Imastore Local Apr 13, Network Namastore Network Apr 13, Network	No filter applied Date Modified Apr 13, Imi_brust_store Date Modified Apr 13, SL Certificates Total Modified Apr 15, 2015 6:00:16 PM Total Models services: Do NOT delete. Imi_brust_store Local Apr 13, SL Certificates Pate Modified Apr 15, 2015 6:00:16 PM Int UL Do NOT delete. Imi_brust_store Network Apr 15, Please note that if any of the changes require the runtime server to be restarted, the restart takes place. Int UL Do NOT delete.							7	
Int_profile_keys Local Apr 13, SL Certificates Date Modified Apr 13, 2015 6:00:16 PM Int UL Do NOT delete. Imt_srus_store Local Apr 13, SL Certificates Date Modified Apr 15, 2015 6:00:16 PM Int UL Do NOT delete. Imt_srus_store Local Apr 13, Please note that if any of the changes require the runtime server being unavailable for a period of time while the restart takes place. Int UL Do NOT delete.	Ingroße_keys Local Apr 13, SL Certificates Date Modified Apr 15, 2015 6:00:16 PM for Mobile services. Do NOT delete. mit_trust_store Local Apr 13, Lonastore Local 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. for Mobile services. Do NOT delete.		Туре	Last Mo	Apr 13 Module Date Modified Apr 13 SSL Certificates Apr 15, 2015 6:00:16 PM Apr 13 Please note that if any of the changes require the runtime set to be restarted, the restart will happen automatically as part	х			
Imit trust_store Local Apr 13, embedded_ldap_keys Local Apr 13, kinastore Network Apr 15, Please note that if any of the changes require the runtime server bing unavailable for a period of time while the restart takes place.	Im_trust_store Local Apr 13, SSL Certificates Apr 15, 2015 6:00:16 PM Int UI. Do NOT delete. embedded_dsp_keys Local Apr 13, Please note that if any of the changes require the runtime server being unavailable for a period of time while the restart takes place. Int UI. Do NOT delete.		Local	Apr 13.	Deploy Pending Changes × pr 13. Module Date Modified SL Certificates Apr 15, 2015 6:00:16 PM pr 15. 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		for Mobile services. Do NOT delete.		
Numastore Network Apr 15, 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.	Network Apr 15 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.		Local				int UI. Do NOT delete.		
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.	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.	embedded_ldap_keys	Local	Apr 13,				er. Do NOT delete.	
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. This will result in the runtime server being unavailable for a period of time while the restart takes place.) Junastore	Network	Apr 15,					
	Cancel Roll Back Deploy				the deploy process.	Mobile Settings System Settings ar apply them to the system, beploy Pending Changes Module SSL Certificates Date Modified Apr 15, 2015 6:00:16 PM Please note that if any of the changes require the runtime sen to be restarted, the restart will happen automatically as part o the deploy process. This will result in the runtime server being unavailable for a period of time while the restart takes place.	ng		
Cancell Roll Back Deploy							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 Steps://isambeta/isam/ssl_certificates				
M Security Access Manager		admin 🔭 Help 👕 Langu	age 🔻	Ī
Home Monitor Appliance Dashboard Analysis and Diagnostics We Edit SSL Certificate Database - lunastore	settings Secure Manage Settings System Settings			×
🌵 New 🛛 🗐 Edit 🛛 🗙 Delete 🛛 🖑 Refresh 🛛 Manage 🔻			Help	?
Signer Certificates Personal Certificates Certificate Request				
Label	Subject	Key S	ize	
	Create Certificate Request X Certificate Request Label * ISAMBETA Certificate Request Distinguished Name * CN=ISAMBETA, O=SafeNet, Key Size 2048 ZO48 V			
0 žem			Clo	ose

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.

Edit SSL Certificate Database - lunastore			
💠 New 🛛 😰 Edit 🗍 🗙 Delete 🗍 🖑 Refre			Help
Signer Certificates Personal Certificates	Cer	5	
Label	Receive	Subject	Key Size
🗱 No filter applied	Import		
ISAMBETA	Export	CN=ISAMBETA,O=SafeNet,C=IN	2048
	Extract		
	Load		
1 - 1 of 1 item		5 10 25 50 100 All	(4 - 4 - 1 - 4 3
			Clos

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.

M Security Access Manager						
Home Andianae Dackhard Mo Edit SSL Certificate Database -	lusis and Diagnostics Mah Catting	Secure Manage				
🗣 New 🗐 Edit 🗎 🗙 Delete	🔗 Refresh 🛛 Manage 👻					Help
	ertificates Certificate Requests					
Label	Issuer	Subject	Not Before	Not After	Version	Key Size
No filter applied						
		Import Signer Certificate	x			
		Certificate File * ContosoCA.cer				
		Browse				
		Browse				
		Certificate Label * ContosoCA				
		Import Car	land			
			icer			
0 item						
						Clos

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

M Security Acc	ss Manager							
Home	Monitor	Secure Secure	Manage					
	te Database - lunastore	andstice - Mohile Cettinger - Mohile Ce	Hinar 25 Curtan Caltiner					1
New 🕅 Ed	it 🛛 🗙 Delete 🛛 🖑 Refres	h Manage 🔻					Help	
Signer Certificat	es Personal Certificates	Certificate Requests						
		Issuer	Subject	Not Before	Not After	Version	Key Size	
Label 10 No filter ap ContosoCA	blied	CN=contosoCA,DC=contoso,DC=com	CN=contosoCA,DC=contoso,DC=com	Dec 4, 2014 2:31:51 PM	Dec 4, 2019 2:41:49 PM	X509 V3	2048	
1 - 1 of 1 item		5 10 25	I 50 100 All			.96	4.1)	1

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

I Security Access Manag	jer					
Appliance Dashboard	Monitor Analysis and Diagnostics Web Settin	ngs Secure Manage Mobile Settings System Settings				
Edit SSL Certificate Databas	e - lunastore					
🖗 New 🛛 😒 Edit 🛛 🗙 Del	ete 🛷 Refresh 🛛 Manage 🔻					Help
Signer Certificates Person	al Certificates Certificate Requests					
Lahel		Subject	Not Before	Not After	Version	Key Size
No filter applied						
		Certificate File * ISAMBETA.cer Browse				
		ISAMBETA.cer	Cancel			
		ISAMBETA.cer Browse Default	Cancel			
0 item		ISAMBETA.cer Browse Default	Cancel			
0 item		ISAMBETA.cer Browse Default	Cancel			Cit

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

	ty Access	Manager								
Home		Moni		Secure Secure	Manage System Settings					
- inpprisition	Dashboard Certificate	Analys Database - Iu	is and Dia	anostics Web Settings Mobile Set	ttings System Settings					2
		X Delete		h Manage 🔻					Help	
									neip	1
		Personal Cer	00 (2000 A) II	Certificate Requests				l.	1	
Labe	el o filter applied		Default	Issuer	Subject	Not Before	Not After	Version	Key Size	
	IBETA		false	CN=contosoCA,DC=contoso,DC=com	CN=ISAMBETA,O=SafeNet,C=IN	Apr 16, 2015 10:02:55 AM	Apr 15, 2017 10:02:55 AM	X509 V3	2048	
				5 10 25	50 100 All			14	(1)	H
1 - 1 of 1	item									

 o) 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 🗖	Facura	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	
HTTPS				Persistent Connection Timeout *	
HTTPS Port *				5	
444				Worker Threads *	
HTTP				300	
HTTP Port *					
81					
Primary Interface Interface Address *					
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 States://isambeta/wga/	reverseproxy#			*
IBM Security Access Manager				Language IBM
Home Appliance Dashboard Analysis an	nd Diagnostics	Secure Mobile Settings		
verse Proxy				
There is currently one undeployed chan	ige. Click here to review the change	s or apply them to the system.		
New 🛛 🗐 Edit 🛛 🗙 Delete 🗍 🕨 Start 🗍				
Instance Name	State	Deploy Pending Changes	x d	
No filter applied				
isam_rp	🖾 S.		5 3:30:45 PM	
1 of 1 item				R = 0 ≤ 1 →

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 Start	Meizannad 🗖 🖉 📈
← → C 🕼 https://isambeta/wga/rev	erseproxy#			* =
IBM Security Access Manager				admin Help Language IIN.
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 isam_rp	Started	True	Apr 24, 2015 3:32:34 PM	
1 - 1 of 1 item	10 25 50		Apr 24, 2015 3:32:34 PM	H € 1 ⊨ H

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.

