interopLab

Interoperability of Bloombase StoreSafe and HPE Enterprise Secure Key Manager (ESKM) for Data At-Rest Encryption

January, 2015

BLOOMBASE®

Executive Summary

HPE Enterprise Secure Key Manager (ESKM) KMIP-compliant key management server is validated by Bloombase InteropLab to run with Bloombase StoreSafe data at-rest encryption security solution. This document describes the steps carried out to test interoperability of HPE Enterprise Secure Key Manager (ESKM) KMIP-compliant key manager with Bloombase StoreSafe software appliance on VMware ESXi. Client host systems on Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) and HP-UX are validated against HPE Enterprise Secure Key Manager (ESKM) powered Bloombase StoreSafe with Microsoft Windows Server as backend storage.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase, Inc.

Bloombase, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, Inc, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase, Inc. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, Inc, and neither the document nor any such information may be released without the written consent of Bloombase, Inc.

Document No.: BLBS-TN-Bloombase-StoreSafe-HPEE-Enterprise-Secure-Key-Manager-(ESKM)-Interoperability-USLET-EN-R3

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate HPE Enterprise Security Key Manager (ESKM) with Bloombase StoreSafe to secure sensitive enterprise business persistent data managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with HPE Enterprise Security Key Manager (ESKM)
- Interoperability testing on client host systems including Linux, Windows and HP-UX

Assumptions

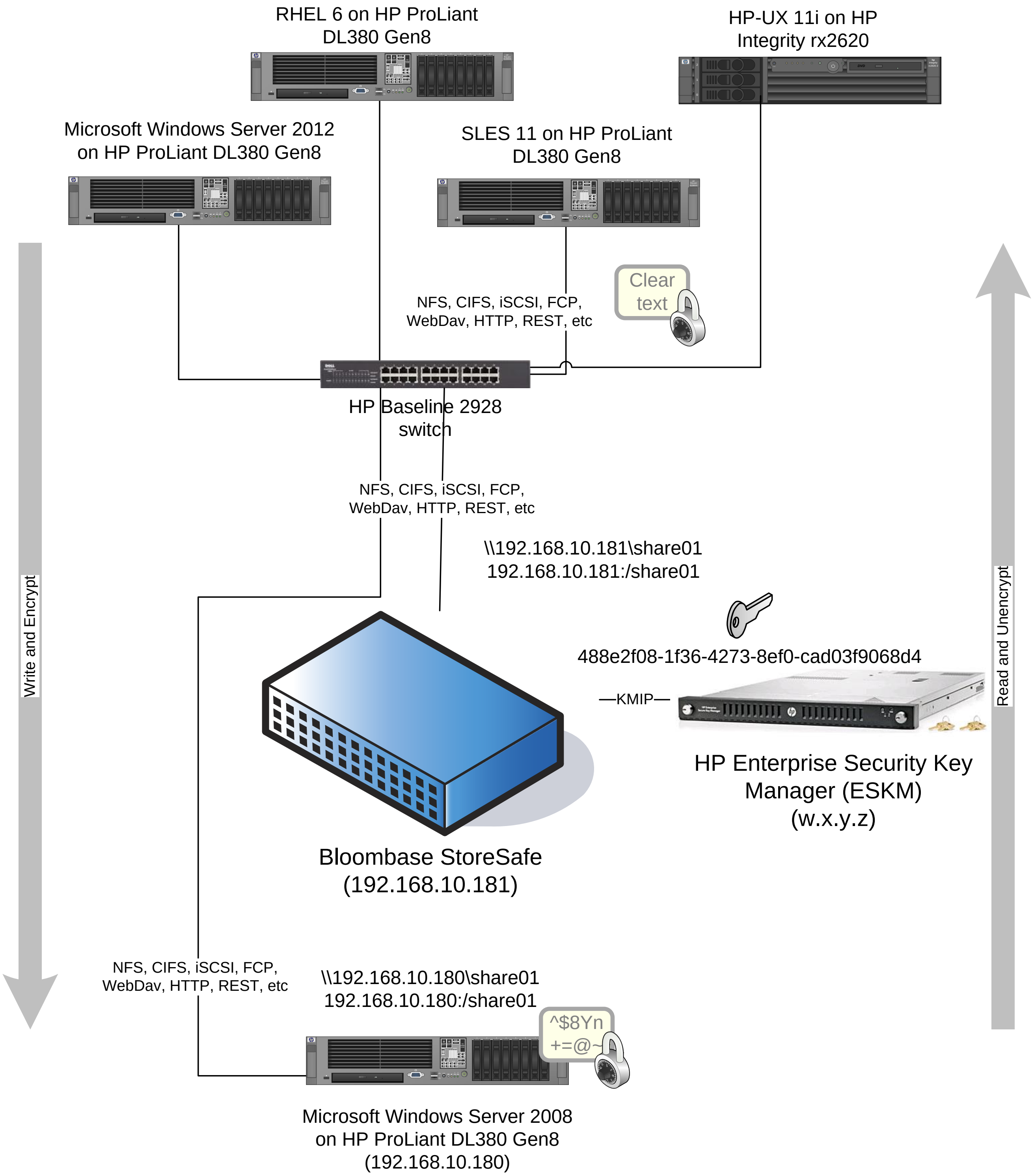
This document describes interoperability testing of HPE Enterprise Security Key Manager (ESKM) with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of HPE Enterprise Security Key Manager (ESKM), storage systems and major operating systems including Linux, Microsoft Windows and HP-UX. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of operating system.

As HPE Enterprise Security Key Manager (ESKM) is third party hardware option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of HPE Enterprise Security Key Manager (ESKM) for your actual use case. We assume you have basic knowledge of storage networking and information cryptography. For specific technical product information of Bloombase StoreSafe, please refer to our website at http://www.bloombase.com or Bloombase SupPortal http://supportal.bloombase.com.

Infrastructure

Setup

The validation testing environment is setup as in below figure


RHEL 6 on HP ProLiant DL380 Gen8
HP-UX 11i on HP Integrity rx2620
Microsoft Windows Server 2012 on HP ProLiant DL380 Gen8
SLES 11 on HP ProLiant DL380 Gen8
Clear text
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
HP Baseline 2928 switch
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
488e2f08-1f36-4273-8ef0-cad03f9068d4
—KMIP—
HP Enterprise Security Key Manager (ESKM) (w.x.y.z)
Bloombase StoreSafe (192.168.10.181)
Write and Encrypt
Read and Unencrypt
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn +=@~
Microsoft Windows Server 2008 on HP ProLiant DL380 Gen8 (192.168.10.180)

Key Manager

Key Manager	HPE Enterprise Security Key Manager (ESKM)

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.4 on Bloombase OS 5 (security hardened Linux OS kernel version 2.6)
Server	VMware Virtual Machine (VM) on VMware ESXi 5.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	Microsoft Windows Server 2008 on HPE ProLiant DL380 Gen8

Client Hosts

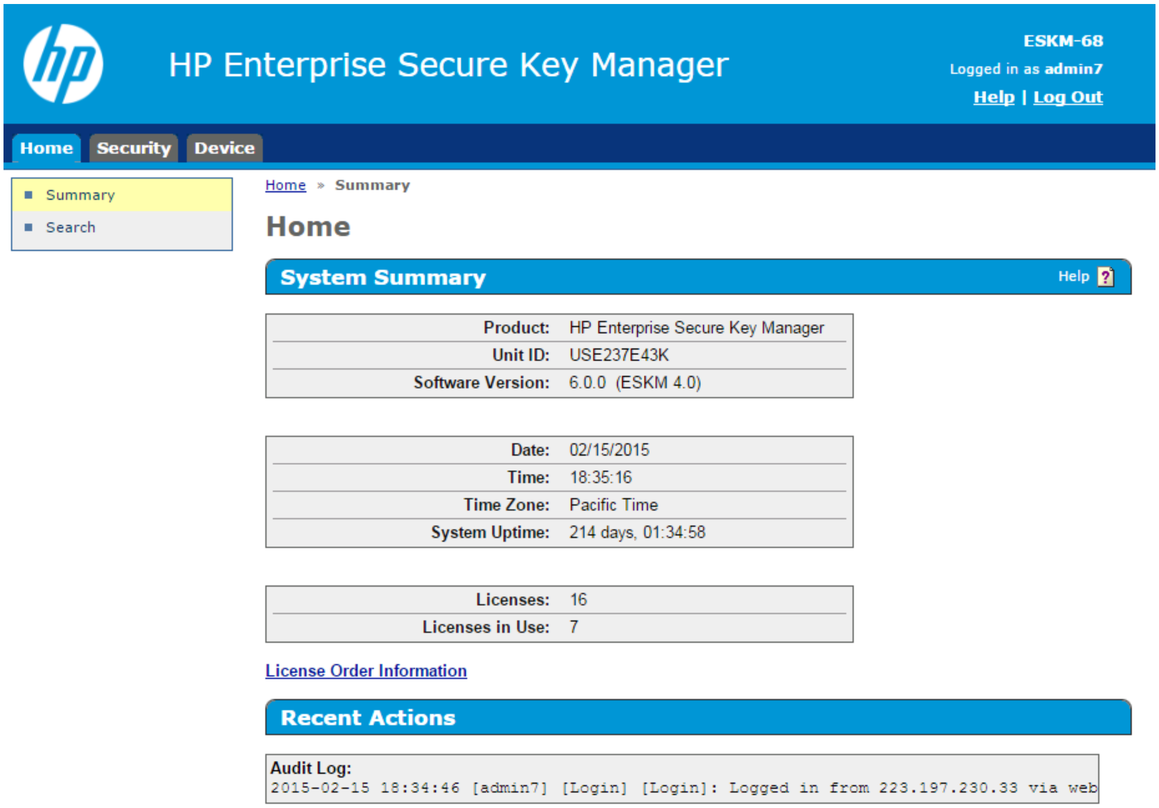
Model	HPE ProLiant DL380 Gen8	HPE ProLiant DL380 Gen8	HPE ProLiant DL380 Gen8	HPE Integrity rx2620
Operating System	Microsoft Windows Server 2012	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i

Configuration Overview

Key Server

HPE Enterprise Security Key Manager (ESKM) is installed and configured as a network attached appliance with IP address w.x.y.z assigned.

HPE ESKM can be managed remotely via web-based management console.



Product:	HP Enterprise Secure Key Manager
Unit ID:	USE237E43K
Software Version:	6.0.0 (ESKM 4.0)

Date:	02/15/2015
Time:	18:35:16
Time Zone:	Pacific Time
System Uptime:	214 days, 01:34:58

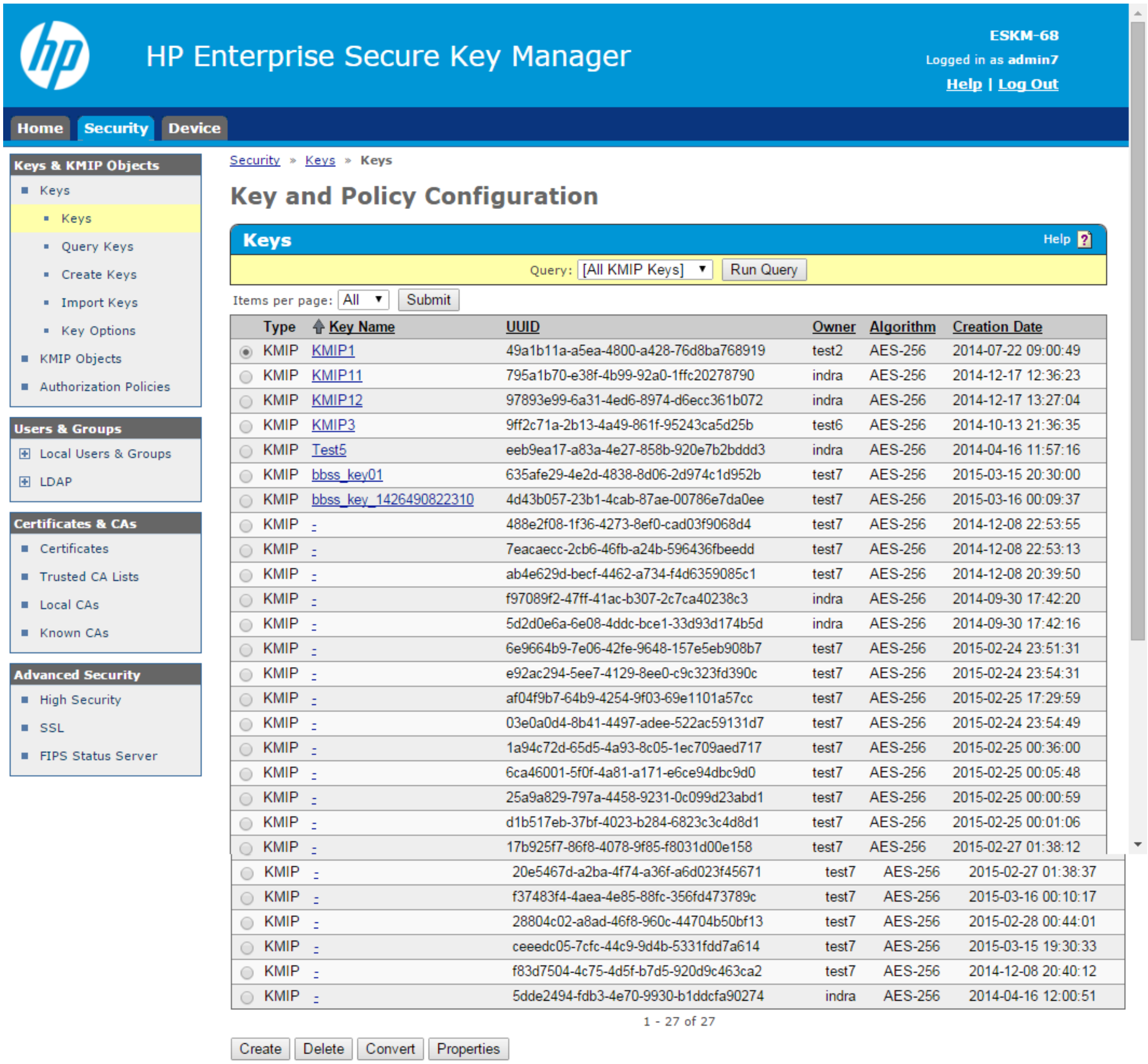
Licenses:	16
Licenses in Use:	7

Audit Log:

```
2015-02-15 18:34:46 [admin7] [Login] [Login]: Logged in from 223.197.230.33 via web
```

For the purpose of this interoperability testing, administrator "admin7" is provisioned and assigned for the Bloombase StoreSafe software appliance instance.

X.509 key pair "CN=test7, OU=Atalla, O=Bloombase, L=Sunnyvale, ST=CA, C=US" is created and assigned as the authentication key pair for Bloombase StoreSafe.



Key and Policy Configuration

Keys

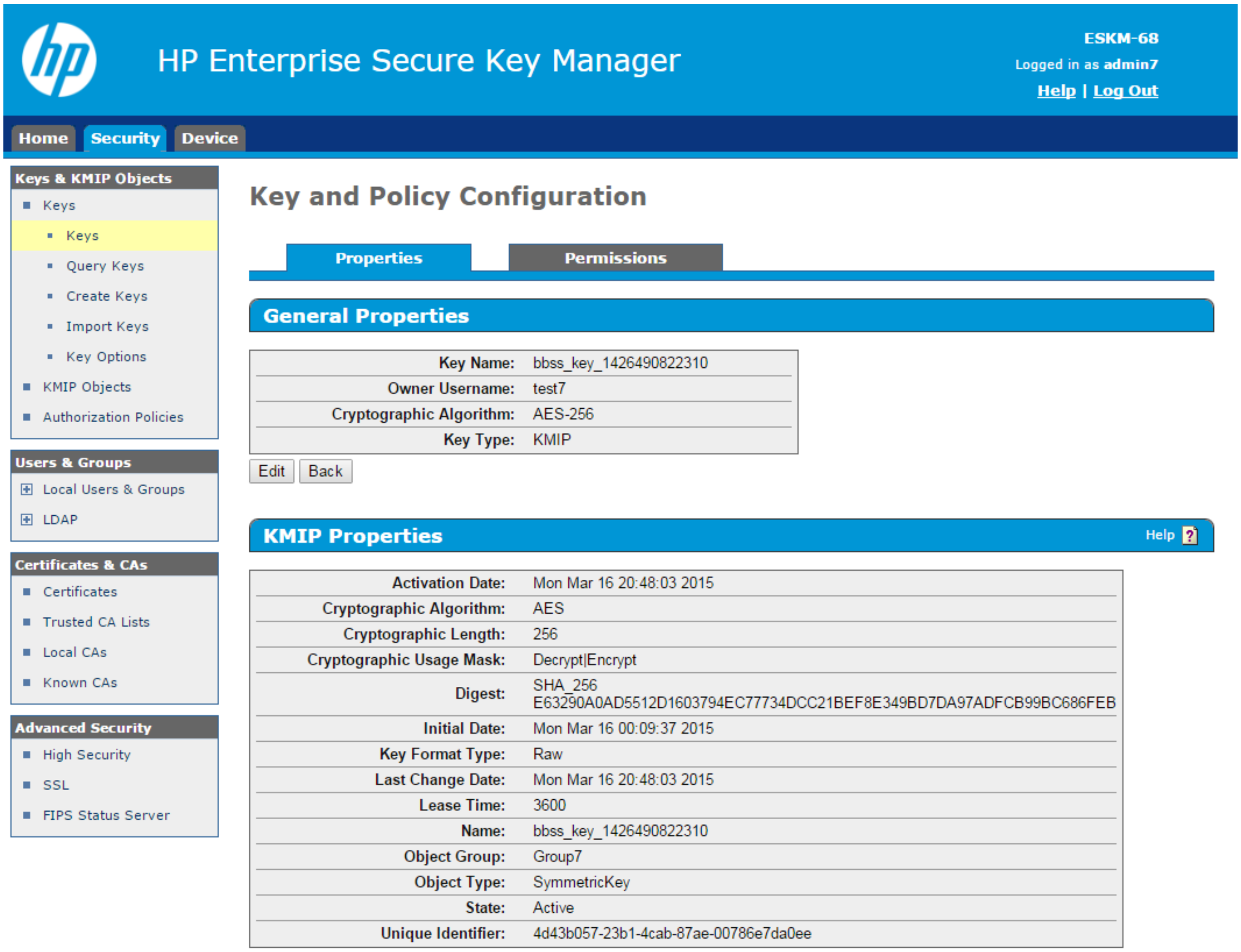
Query: [All KMIP Keys] Run Query

Items per page: All Submit

	Type	Key Name	UUID	Owner	Algorithm	Creation Date
●	KMIP	KMIP1	49a1b11a-a5ea-4800-a428-76d8ba768919	test2	AES-256	2014-07-22 09:00:49
○	KMIP	KMIP11	795a1b70-e38f-4b99-92a0-1ffc20278790	indra	AES-256	2014-12-17 12:36:23
○	KMIP	KMIP12	97893e99-6a31-4ed6-8974-d6ecc361b072	indra	AES-256	2014-12-17 13:27:04
○	KMIP	KMIP3	9ff2c71a-2b13-4a49-861f-95243ca5d25b	test6	AES-256	2014-10-13 21:36:35
○	KMIP	Test5	eeb9ea17-a83a-4e27-858b-920e7b2bddd3	indra	AES-256	2014-04-16 11:57:16
○	KMIP	bbss_key01	635afe29-4e2d-4838-8d06-2d974c1d952b	test7	AES-256	2015-03-15 20:30:00
○	KMIP	bbss_key_1426490822310	4d43b057-23b1-4cab-87ae-00786e7da0ee	test7	AES-256	2015-03-16 00:09:37
○	KMIP	-	488e2f08-1f36-4273-8ef0-cad03f9068d4	test7	AES-256	2014-12-08 22:53:55
○	KMIP	-	7eacaecc-2cb6-46fb-a24b-596436fbeedd	test7	AES-256	2014-12-08 22:53:13
○	KMIP	-	ab4e629d-becf-4462-a734-f4d6359085c1	test7	AES-256	2014-12-08 20:39:50
○	KMIP	-	f97089f2-47ff-41ac-b307-2c7ca40238c3	indra	AES-256	2014-09-30 17:42:20
○	KMIP	-	5d2d0e6a-6e08-4ddc-bce1-33d93d174b5d	indra	AES-256	2014-09-30 17:42:16
○	KMIP	-	6e9664b9-7e06-42fe-9648-157e5eb908b7	test7	AES-256	2015-02-24 23:51:31
○	KMIP	-	e92ac294-5ee7-4129-8ee0-c9c323fd390c	test7	AES-256	2015-02-24 23:54:31
○	KMIP	-	af04f9b7-64b9-4254-9f03-69e1101a57cc	test7	AES-256	2015-02-25 17:29:59
○	KMIP	-	03e0a0d4-8b41-4497-adee-522ac59131d7	test7	AES-256	2015-02-24 23:54:49
○	KMIP	-	1a94c72d-65d5-4a93-8c05-1ec709aed717	test7	AES-256	2015-02-25 00:36:00
○	KMIP	-	6ca46001-5f0f-4a81-a171-e6ce94dbc9d0	test7	AES-256	2015-02-25 00:05:48
○	KMIP	-	25a9a829-797a-4458-9231-0c099d23abd1	test7	AES-256	2015-02-25 00:00:59
○	KMIP	-	d1b517eb-37bf-4023-b284-6823c3c4d8d1	test7	AES-256	2015-02-25 00:01:06
○	KMIP	-	17b925f7-86f8-4078-9f85-f8031d00e158	test7	AES-256	2015-02-27 01:38:12
○	KMIP	-	20e5467d-a2ba-4f74-a36f-a6d023f45671	test7	AES-256	2015-02-27 01:38:37
○	KMIP	-	f37483f4-4aea-4e85-88fc-356fd473789c	test7	AES-256	2015-03-16 00:10:17
○	KMIP	-	28804c02-a8ad-46f8-960c-44704b50bf13	test7	AES-256	2015-02-28 00:44:01
○	KMIP	-	ceeedc05-7cfc-44c9-9d4b-5331fdd7a614	test7	AES-256	2015-03-15 19:30:33
○	KMIP	-	f83d7504-4c75-4d5f-b7d5-920d9c463ca2	test7	AES-256	2014-12-08 20:40:12
○	KMIP	-	5dde2494-fdb3-4e70-9930-b1ddcfa90274	indra	AES-256	2014-04-16 12:00:51

1 - 27 of 27

An AES-256 KMIP key object of UUID “488e2f08-1f36-4273-8ef0-cad03f9068d4” is generated and provisioned for Bloombase StoreSafe’s actual data at-rest encryption use.



Key and Policy Configuration

General Properties

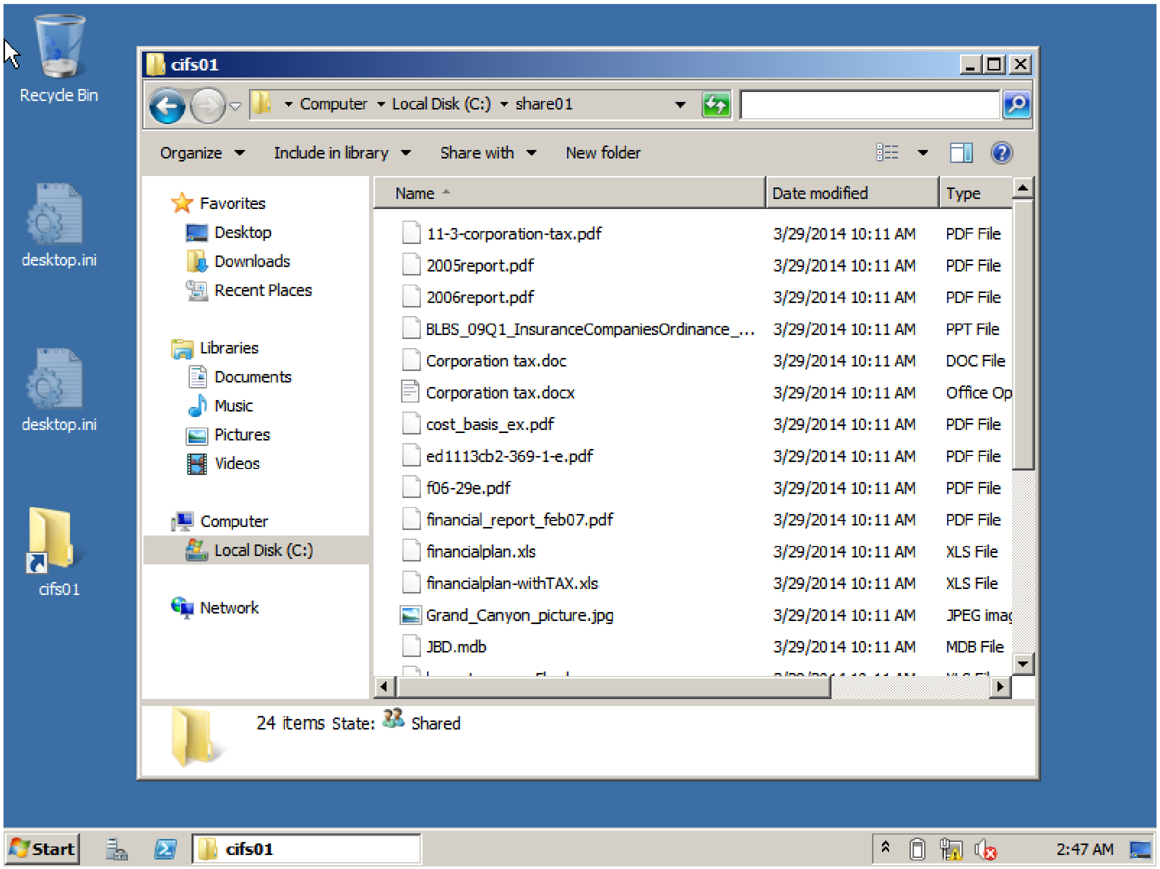
Key Name:	bbss_key_1426490822310
Owner Username:	test7
Cryptographic Algorithm:	AES-256
Key Type:	KMIP

KMIP Properties

Activation Date:	Mon Mar 16 20:48:03 2015
Cryptographic Algorithm:	AES
Cryptographic Length:	256
Cryptographic Usage Mask:	Decrypt|Encrypt
Digest:	SHA_256 E63290A0AD5512D1603794EC77734DCC21BEF8E349BD7DA97ADFCB99BC686FEB
Initial Date:	Mon Mar 16 00:09:37 2015
Key Format Type:	Raw
Last Change Date:	Mon Mar 16 20:48:03 2015
Lease Time:	3600
Name:	bbss_key_1426490822310
Object Group:	Group7
Object Type:	SymmetricKey
State:	Active
Unique Identifier:	4d43b057-23b1-4cab-87ae-00786e7da0ee

Storage

Microsoft Windows Server 2008 is used in this interoperability test which is able to provide storage services over network storage protocols including CIFS and iSCSI.



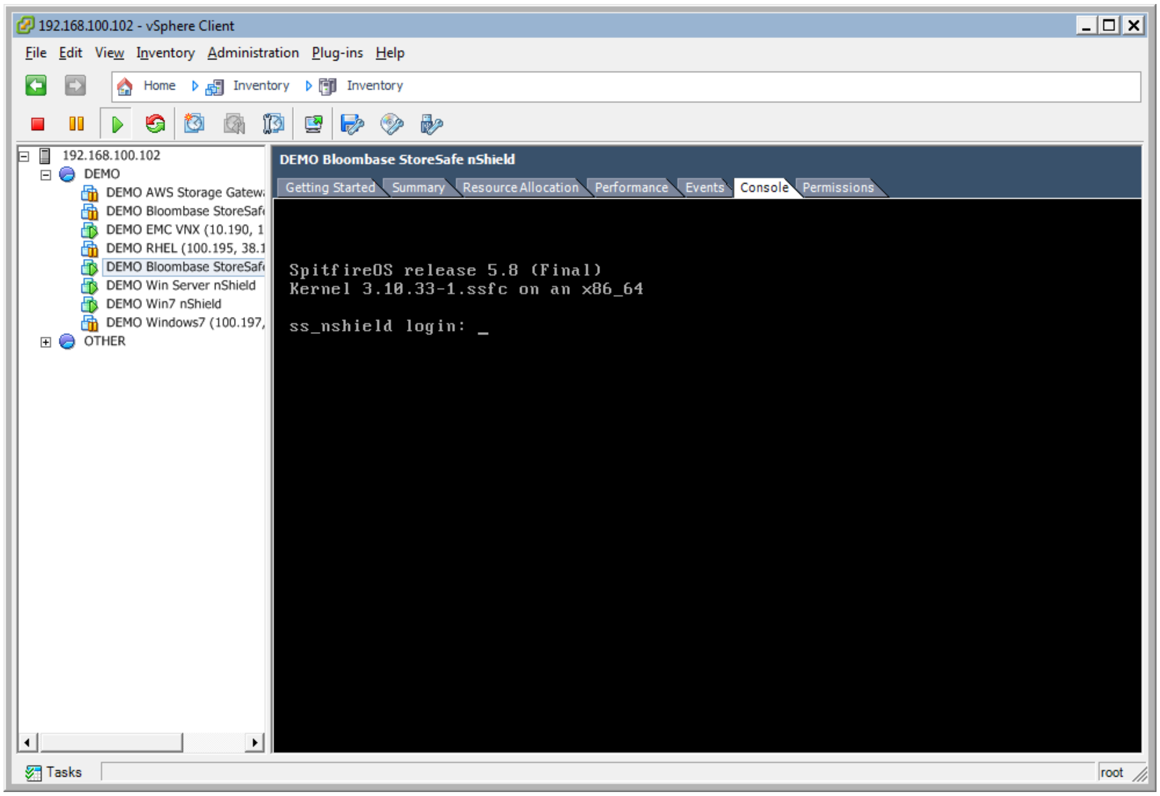
Name	Date modified	Type
11-3-corporation-tax.pdf	3/29/2014 10:11 AM	PDF File
2005report.pdf	3/29/2014 10:11 AM	PDF File
2006report.pdf	3/29/2014 10:11 AM	PDF File
BLBS_09Q1_InsuranceCompaniesOrdinance_...	3/29/2014 10:11 AM	PPT File
Corporation tax.doc	3/29/2014 10:11 AM	DOC File
Corporation tax.docx	3/29/2014 10:11 AM	Office Op
cost_basis_ex.pdf	3/29/2014 10:11 AM	PDF File
ed1113cb2-369-1-e.pdf	3/29/2014 10:11 AM	PDF File
f06-29e.pdf	3/29/2014 10:11 AM	PDF File
financial_report_feb07.pdf	3/29/2014 10:11 AM	PDF File
financialplan.xls	3/29/2014 10:11 AM	XLS File
financialplan-withTAX.xls	3/29/2014 10:11 AM	XLS File
Grand_Canyon_picture.jpg	3/29/2014 10:11 AM	JPEG imag
JBD.mdb	3/29/2014 10:11 AM	MDB File

Microsoft Windows Server delivers storage services supporting multiple network storage protocols including CIFS, HTTP, and iSCSI, etc.

Windows file sharing resource “share01” is provisioned at Microsoft Windows Server 2008 to be used in this testing.

Bloombase StoreSafe

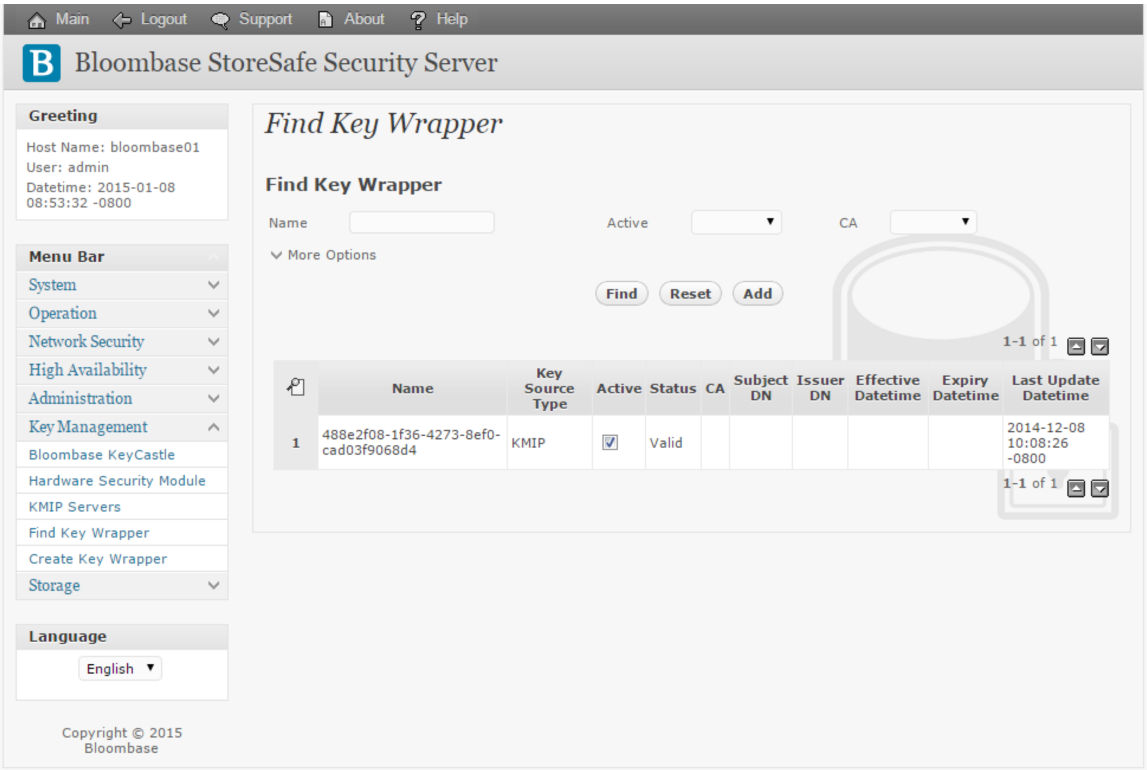
Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at HPE Enterprise Security Key Manager (ESKM).



```
SpitfireOS release 5.8 (Final)
Kernel 3.10.33-1.ssfc on an x86_64

ss_nshield login: _
```

Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware ESXi.



Greeting

Host Name: bloombase01
User: admin
Datetime: 2015-01-08 08:53:32 -0800

Find Key Wrapper

Find Key Wrapper

Name | Active | CA

1-1 of 1

	Name	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	488e2f08-1f36-4273-8ef0-cad03f9068d4	KMIP	☑	Valid						2014-12-08 10:08:26 -0800

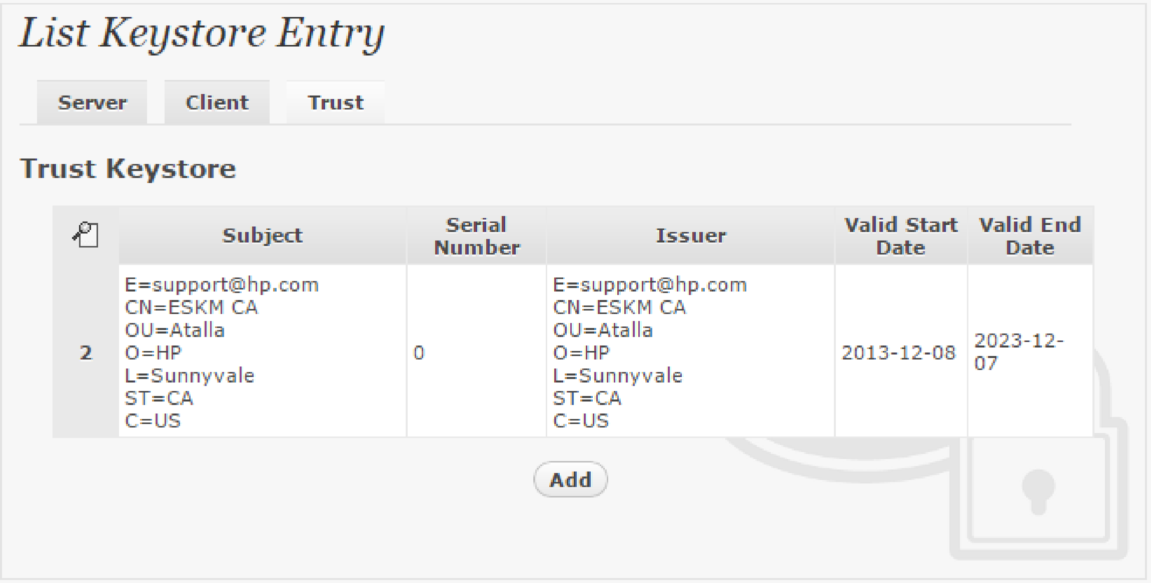
1-1 of 1

Network Security, Trust and Authentication Configuration

In this interoperability test effort, Bloombase StoreSafe serves as the client of HPE ESKM for encryption key access to deliver data at-rest encryption services.

HPE ESKM utilizes TLS for data in-flight security protecting privacy of data transmission over network with client applications.

HPE ESKM KMIP service is trusted by adding the certificate authority of KMIP server certificate to Bloombase StoreSafe's trust key store.



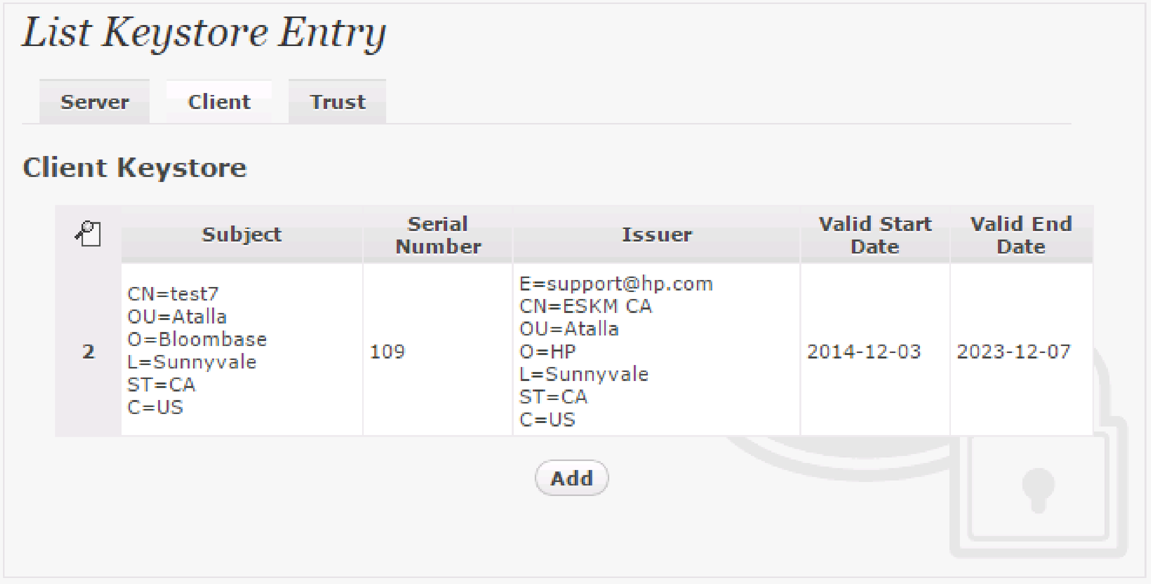
List Keystore Entry

Trust Keystore

	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
2	E=support@hp.com CN=ESKM CA OU=Atalla O=HP L=Sunnyvale ST=CA C=US	0	E=support@hp.com CN=ESKM CA OU=Atalla O=HP L=Sunnyvale ST=CA C=US	2013-12-08	2023-12-07

HPE ESKM utilizes certificate-based authentication for client access control. An X.509 compliant key pair is generated and installed at Bloombase StoreSafe's client key store.

The client certificate is also configured at HPE ESKM as a trusted credential which allows access of KMIP services by trusted Bloombase StoreSafe instance from over remote network.



List Keystore Entry

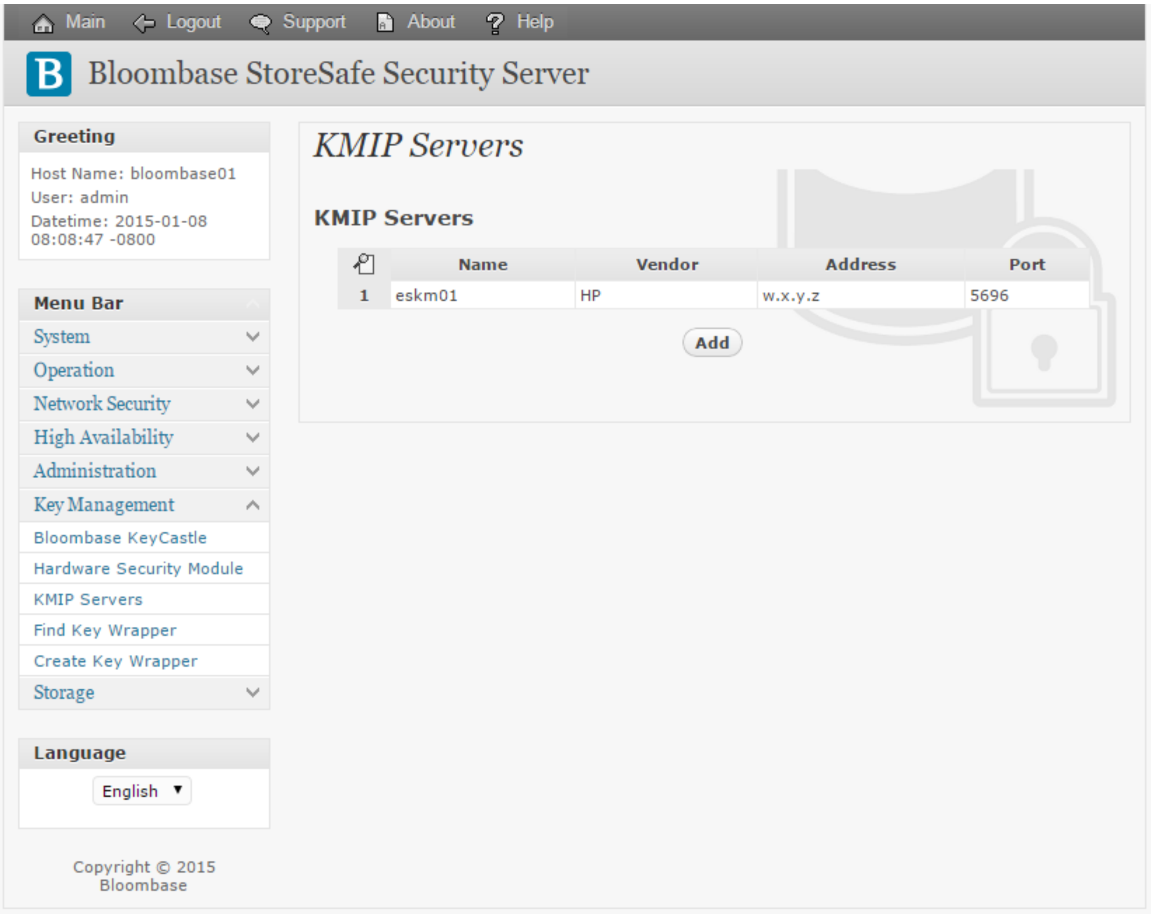
Client Keystore

	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
2	CN=test7 OU=Atalla O=Bloombase L=Sunnyvale ST=CA C=US	109	E=support@hp.com CN=ESKM CA OU=Atalla O=HP L=Sunnyvale ST=CA C=US	2014-12-03	2023-12-07

HPE Enterprise Security Key Manager (ESKM) and Bloombase KeyCastle Integration

To enable the built-in Bloombase KeyCastle to utilize keys managed in the network attached HPE ESKM KMIP-compliant key manager. The KMIP service configuration at Bloombase web management console has to be set up.

Bloombase supports HPE ESKM out of the box due to the fact that both support OASIS Key Management Interoperability Protocol (KMIP).



Greeting

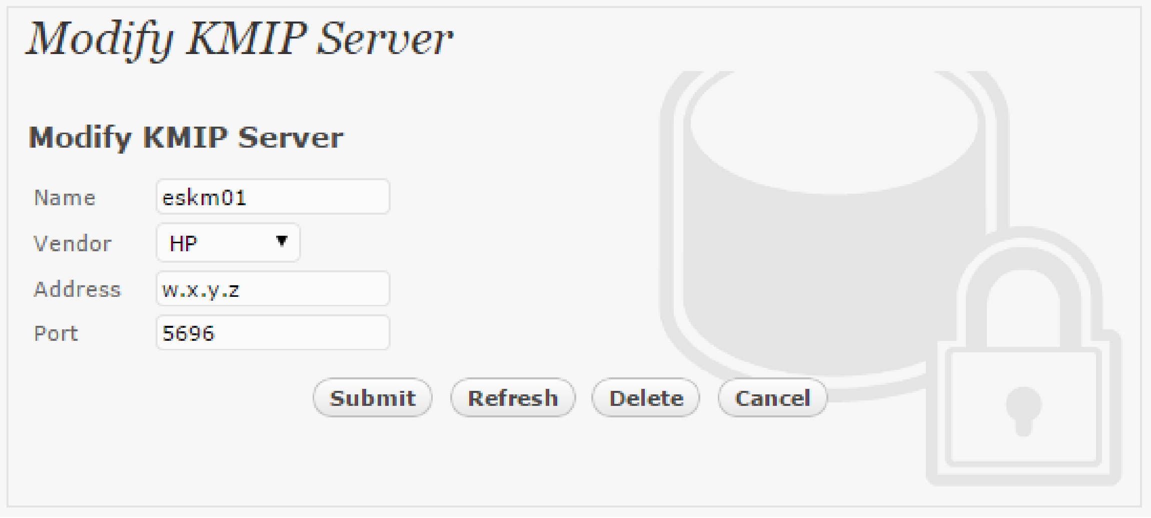
Host Name: bloombase01
User: admin
Datetime: 2015-01-08 08:08:47 -0800

KMIP Servers

KMIP Servers

	Name	Vendor	Address	Port
1	eskm01	HP	w.x.y.z	5696

HPE ESKM server setting is properly configured at Bloombase StoreSafe web management console and assigned the name ‘eskm01’.



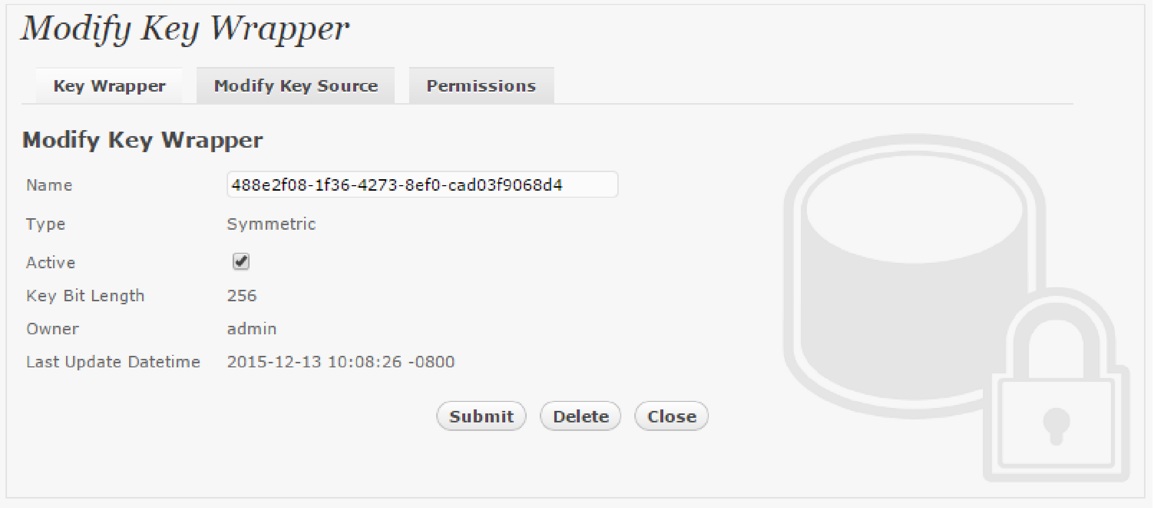
Modify KMIP Server

Modify KMIP Server

Name	eskm01
Vendor	HP
Address	w.x.y.z
Port	5696

Encryption Key Provisioning

Existing HPE ESKM KMIP key object “488e2f08-1f36-4273-8ef0-cad03f9068d4” has to be linked to Bloombase StoreSafe before it can be used for secure storage configuration delivering stored data encryption services.

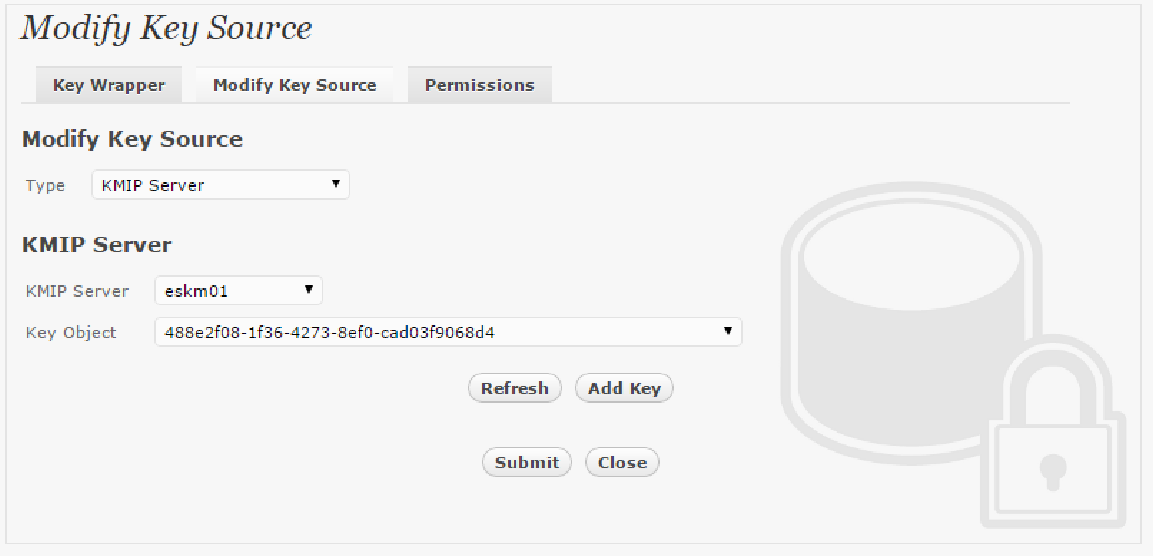


Modify Key Wrapper

Modify Key Wrapper

Name: 488e2f08-1f36-4273-8ef0-cad03f9068d4
Type: Symmetric
Active: ☑
Key Bit Length: 256
Owner: admin
Last Update Datetime: 2015-12-13 10:08:26 -0800

To properly associate an existing key object at HPE ESKM from built-in Bloombase KeyCastle, select Key Source Type as “KMIP Server”, KMIP Server as the identifier “eskm01” and select the encryption key to be used for data encryption, in this case “488e2f08-1f36-4273-8ef0-cad03f9068d4”.



Modify Key Source

Modify Key Source

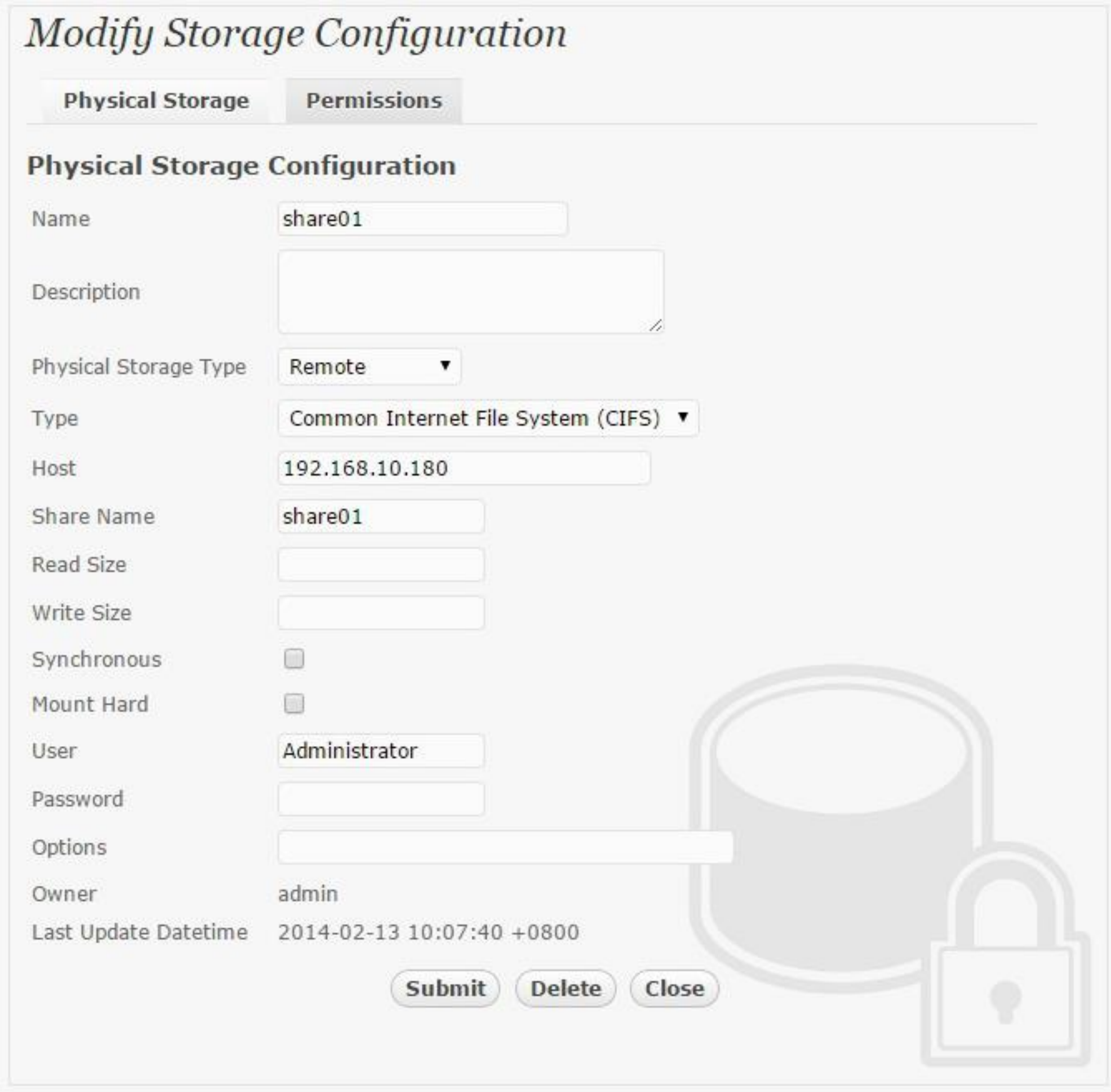
Type: KMIP Server

KMIP Server

KMIP Server: eskm01
Key Object: 488e2f08-1f36-4273-8ef0-cad03f9068d4

Backend Physical Storage Configuration

Physical storage namely ‘share01’ is configured to be secured by Bloombase StoreSafe using encryption.

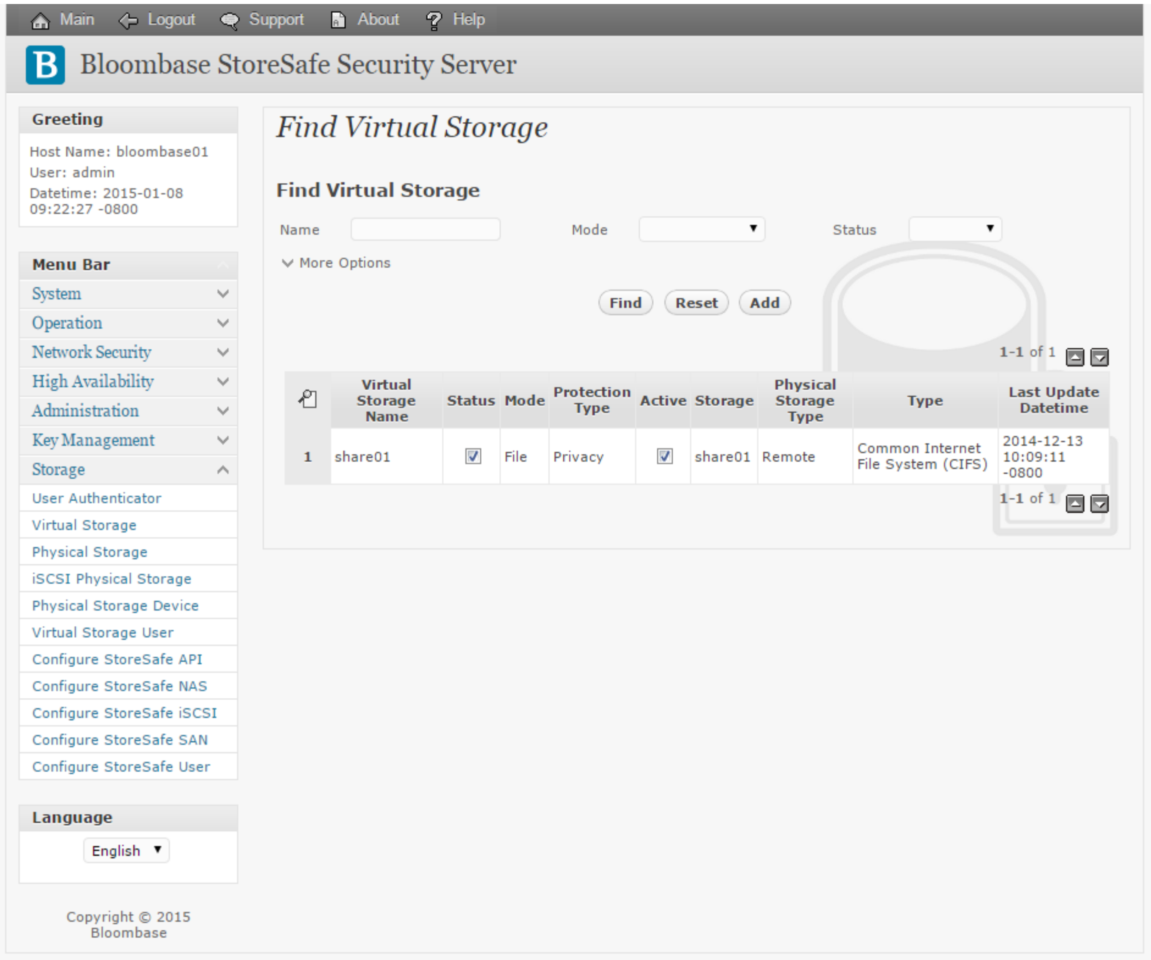


Modify Storage Configuration

Physical Storage Configuration

Name	share01
Description	
Physical Storage Type	Remote ▼
Type	Common Internet File System (CIFS) ▼
Host	192.168.10.180
Share Name	share01
Read Size	
Write Size	
Synchronous	□
Mount Hard	□
User	Administrator
Password	
Options	
Owner	admin
Last Update Datetime	2014-02-13 10:07:40 +0800

Secure Storage Configuration



Host Name: bloombase01
User: admin
Datetime: 2015-01-08 09:22:27 -0800

Find Virtual Storage

Find Virtual Storage

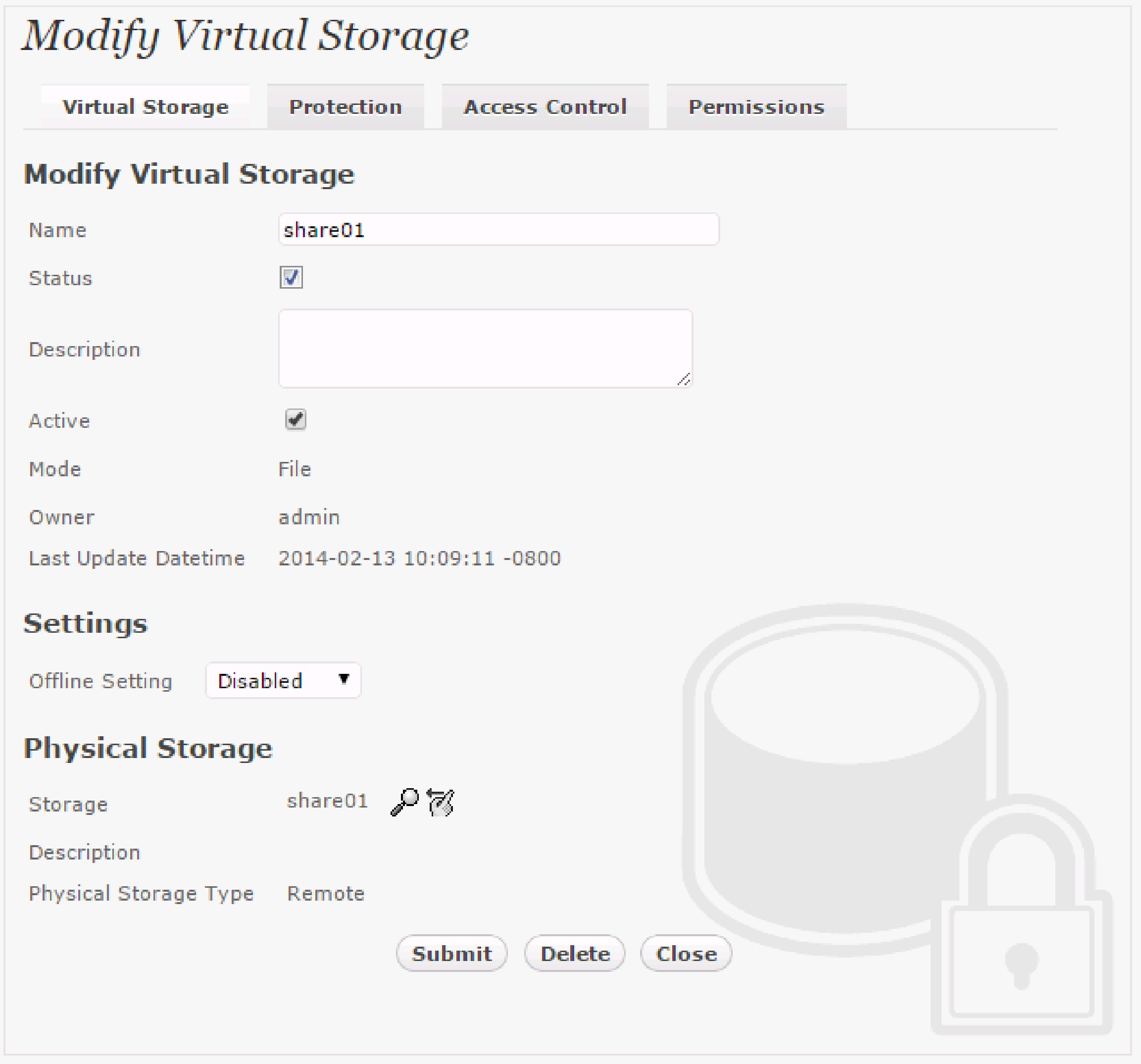
Name
Mode
Status

1-1 of 1

	Virtual Storage Name	Status	Mode	Protection Type	Active	Storage	Physical Storage Type	Type	Last Update Datetime
1	share01	☑	File	Privacy	☑	share01	Remote	Common Internet File System (CIFS)	2014-12-13 10:09:11 -0800

1-1 of 1

Virtual storage namely ‘share01’ of type ‘File’ is created to virtualize physical storage ‘share01’ for application transparent encryption protection over network file protocols including CIFS and NFS.



Modify Virtual Storage

Modify Virtual Storage

Name	share01
Status	☑
Description	
Active	☑
Mode	File
Owner	admin
Last Update Datetime	2014-02-13 10:09:11 -0800

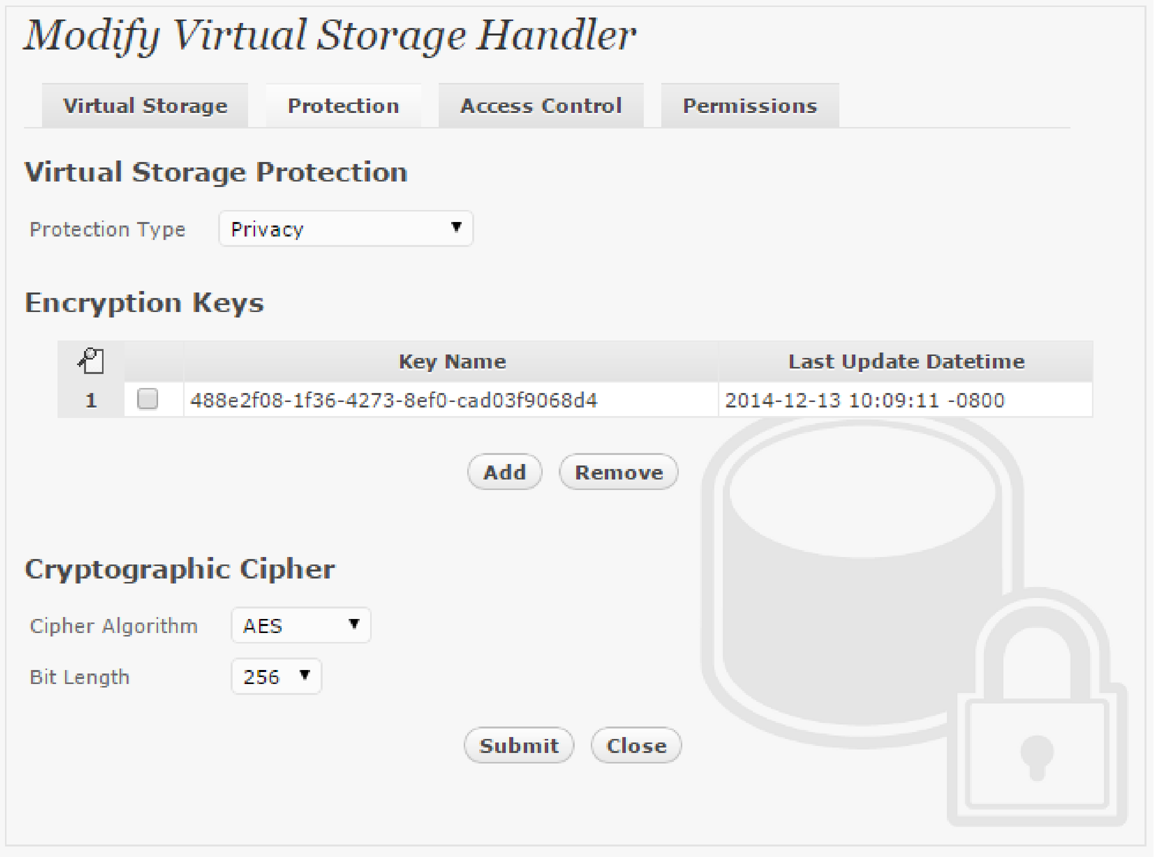
Settings

Offline Setting: Disabled

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as ‘Privacy’ and secure contents of the backend Microsoft Windows Server storage using AES 256-bit encryption with encryption key “488e2f08-1f36-4273-8ef0-cad03f9068d4” managed at HPE ESKM.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

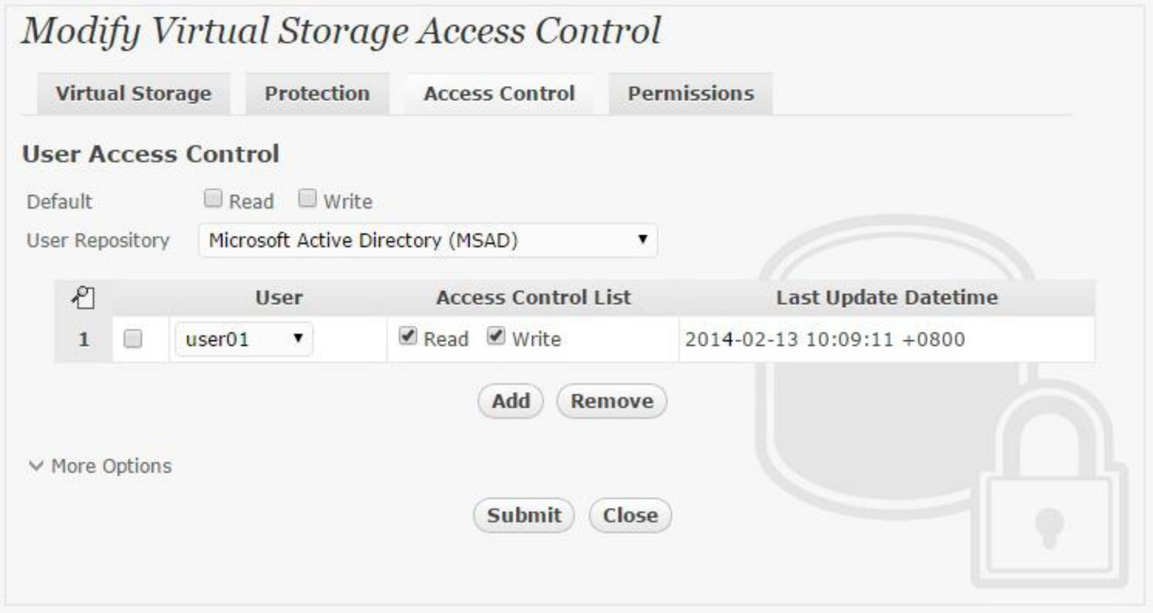
		Key Name	Last Update Datetime
1	□	488e2f08-1f36-4273-8ef0-cad03f9068d4	2014-12-13 10:09:11 -0800

Cryptographic Cipher

Cipher Algorithm: AES

Bit Length: 256

CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource ‘share01’ is provisioned for user ‘user01’ with Microsoft Active Directory integration for user-password authentication and single sign-on.



Modify Virtual Storage Access Control

User Access Control

Default	□ Read □ Write
User Repository	Microsoft Active Directory (MSAD) ▾

		User	Access Control List	Last Update Datetime
1	□	user01 ▾	☑ Read ☑ Write	2014-02-13 10:09:11 +0800

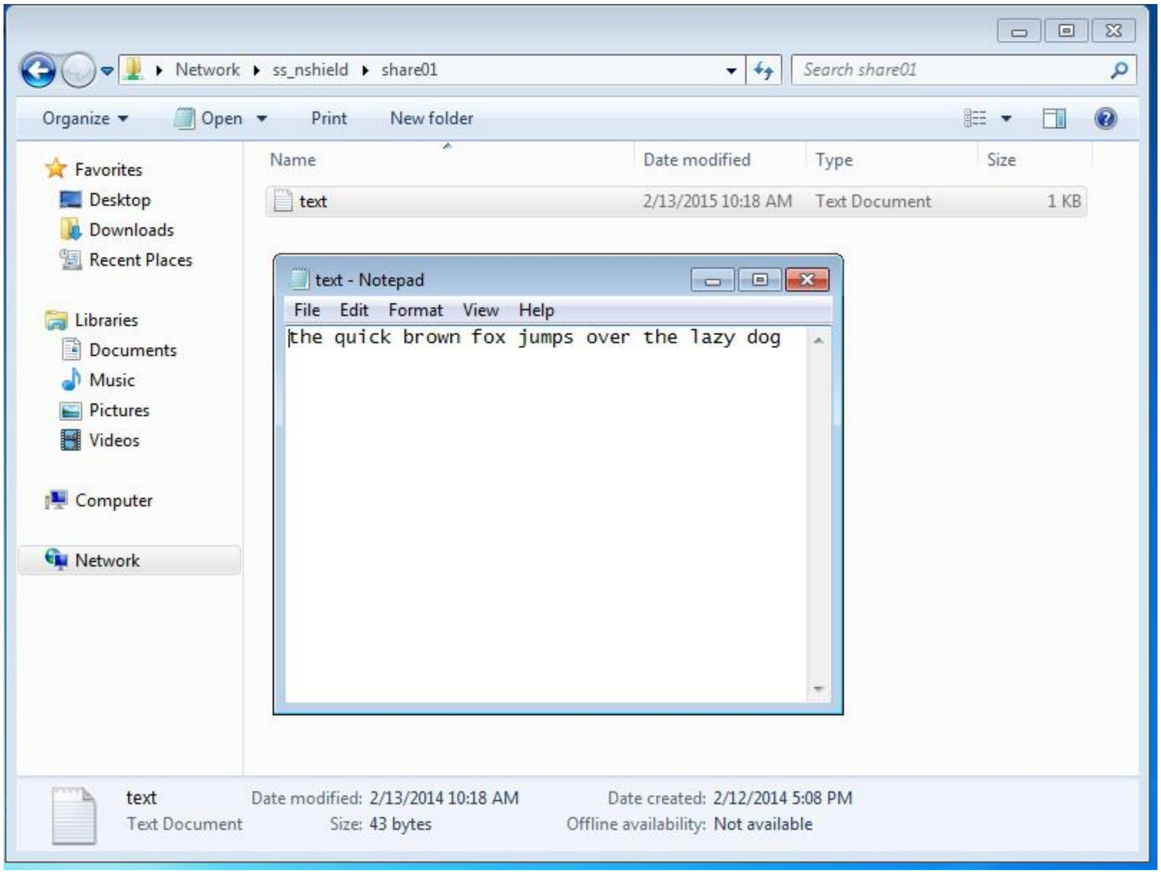
Validation Tests

Test Scenarios

Function Tests

Bloombase StoreSafe delivers turnkey, non-disruptive, application transparent data at-rest encryption with zero operational change and user workflow. Bloombase StoreSafe enables trusted hosts and clients to access encrypted files, objects and volumes as if they are in the clear.

To access Bloombase StoreSafe secured CIFS storage resource, enter \\192.168.10.181\share01 at Windows Explorer

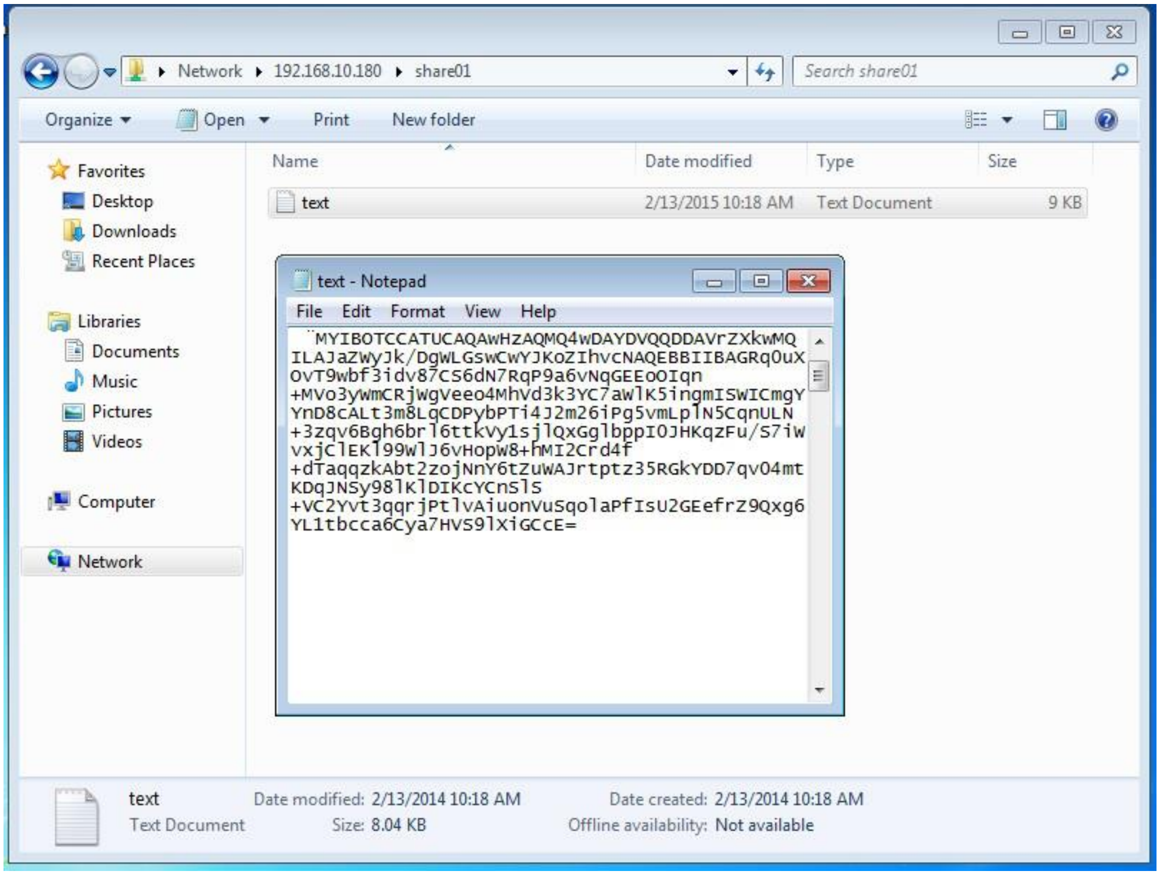


Name	Date modified	Type	Size
text	2/13/2015 10:18 AM	Text Document	1 KB

```
the quick brown fox jumps over the lazy dog
```

text
Text Document
Date modified: 2/13/2014 10:18 AM
Size: 43 bytes
Date created: 2/12/2014 5:08 PM
Offline availability: Not available

To validate if the files stored at backend Microsoft Windows Server are actually encrypted, enter \\192.168.10.180\share01 at Windows Explorer



Name	Date modified	Type	Size
text	2/13/2015 10:18 AM	Text Document	9 KB

```
¨MYIBOTCCATUCAQAwHZAQMQ4wDAYDVQQDDAVrZXkwMQ
ILAJaZWyJk/DgWLGswCwYJKoZIhvcNAQEBBIIBAGRq0uX
OvT9wbf3idv87CS6dN7RqP9a6vNqGEEoOIqn
+MVo3yWmCRjWgVeeo4MhVd3k3YC7aWlK5ingmISWICmgY
YnD8cALt3m8LqCDPybPTi4J2m26iPg5vmLplN5CqnULN
+3zqv6Bgh6brl6ttkVy1sjlQxGglbppI0JHKqzFu/S7iW
vxjClEKl99WlJ6vHopW8+hMI2Crd4f
+dTaqqzkAbt2zojNnY6tZuWAJrtptz35RGkYDD7qv04mt
KDqJNSy98lKlDIKcYCnSlS
+VC2Yvt3qqrjPtlvAiuonVuSqolaPfIsU2GEefrZ9Qxg6
YL1tbcca6Cya7HVS9lXiGCcE=
```

text
Text Document
Date modified: 2/13/2014 10:18 AM
Size: 8.04 KB
Date created: 2/13/2014 10:18 AM
Offline availability: Not available

Validation Matrix

Validation tests span across models of HPE ESKM, Bloombase StoreSafe, client hardware platform, and host operating system.

Test Condition	Candidate
Hardware Security Module	• HPE Enterprise Security Key Manager (ESKM)
Encryption Product	• Bloombase StoreSafe
Client Server Appliance	• Intel x86 • Intel IA-64
Client Host Operating System	• Microsoft Windows Server 2012 • Red Hat Enterprise Linux 6

- SUSE Linux Enterprise Server 11
- HP-UX 11i

File System Tests

The following tests are carried out at storage hosts to access encrypted backend storage system via Bloombase StoreSafe with data encryption keys stored and managed at HPE ESKM

Test	Description
Directory creation	Platform equivalence of UNIX's mkdir
Directory rename	Platform equivalence of UNIX's mv
Directory removal	Platform equivalence of UNIX's rm
Directory move	Platform equivalence of UNIX's mv
File creation	Platform equivalence of UNIX's echo XXX >
File rename	Platform equivalence of UNIX's mv
File removal	Platform equivalence of UNIX's rm
File move	Platform equivalence of UNIX's mv
File append – by character	Platform equivalence of UNIX's echo XXX >>
File append – by block	Platform equivalence of UNIX's echo XXX >>
File parameters inquiry	Platform equivalence of UNIX's ls *X
File permission configurations	• Platform equivalence of UNIX's chmod • Valid for UNIX-based storage host systems only (Linux, HP-UX)
Softlink/Symbolic link removal	• Platform equivalence of UNIX's rm • Valid for UNIX-based storage host systems only (Linux, HP-UX)
Softlink/Symbolic link move	• Platform equivalence of UNIX's mv • Valid for UNIX-based storage host systems only (Linux, HP-UX)

Result

File System Tests

Test	Validation Pass	Remarks
Directory creation	✓	
Directory rename	✓	
Directory removal	✓	
Directory move	✓	
File creation	✓	
File rename	✓	
File removal	✓	
File move	✓	
File append – by character	✓	
File append – by block	✓	
File parameters inquiry	✓	
File permission configurations	✓	Valid for UNIX-based storage host systems only (Linux, HP-UX)
Softlink/Symbolic link removal	✓	Valid for UNIX-based storage host systems only (Linux, HP-UX)
Softlink/Symbolic link move	✓	Valid for UNIX-based storage host systems only (Linux, HP-UX)

Conclusion

HPE

- Enterprise Security Key Manager (ESKM)

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	**Client Operating System**	**Hardware Security Module**
Bloombase StoreSafe	Microsoft Windows Server	• HPE Enterprise Security Key Manager (ESKM)
	Red Hat Enterprise Linux (RHEL)	• HPE Enterprise Security Key Manager (ESKM)
	SUSE Linux Enterprise Server (SLES)	• HPE Enterprise Security Key Manager (ESKM)
	HP-UX	• HPE Enterprise Security Key Manager (ESKM)

Disclaimer

The tests described in this paper were conducted in the Bloombase InteropLab. Bloombase has not tested this configuration with all the combinations of hardware and software options available. There may be significant differences in your configuration that will change the procedures necessary to accomplish the objectives outlined in this paper. If you find that any of these procedures do not work in your environment, please contact us immediately.

Acknowledgement

Bloombase InteropLab would like to thank HPE Atalla team for supporting this interoperability testing.

Technical Reference

1. Bloombase StoreSafe Technical Specifications, http://www.bloombase.com/content/8936QA88
2. Bloombase StoreSafe Hardware Compatibility Matrix, http://www.bloombase.com/content/e8Gzz281
3. HPE Enterprise Security Key Manager (ESKM), http://www8.hp.com/us/en/software-solutions/eskm-enterprise-secure-key-management
4. OASIS KMIP, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip