interopLab

Interoperability of Bloombase StoreSafe and Thales e-Security keyAuthority® for Data At-Rest Encryption

April, 2015

BLOOMBASE®

Executive Summary

Thales e-Security keyAuthority 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 keyAuthority 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), Oracle Sun Solaris, IBM AIX and HP-UX are validated against Thales powered Bloombase StoreSafe with EMC VNX unified storage system as backend storage.

Document No.: BLBS-TN-Bloombase-StoreSafe-Thales-e-Security-keyAuthority-Interoperability-USLET-EN-R3

Table of Contents

Table of Contents 3

Purpose and Scope 5

Assumptions 6

Infrastructure 7

Setup 7

Thales e-Security keyAuthority 9

Bloombase StoreSafe 9

Storage System 9

Client Hosts 9

Configuration Overview 10

Thales e-Security keyAuthority 10

EMC VNX Storage 14

Bloombase StoreSafe 17

Network Security, Trust and Authentication Configuration 18

keyAuthority and Bloombase KeyCastle Integration 19

Encryption Key Provisioning 21

Backend Physical Storage Configuration 21

Secure Storage Configuration 23

Conclusion 26

Disclaimer 28

Acknowledgement 29

Technical Reference 30

Purpose and Scope

This document describes the steps necessary to integrate Thales e-Security keyAuthority 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 keyAuthority
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

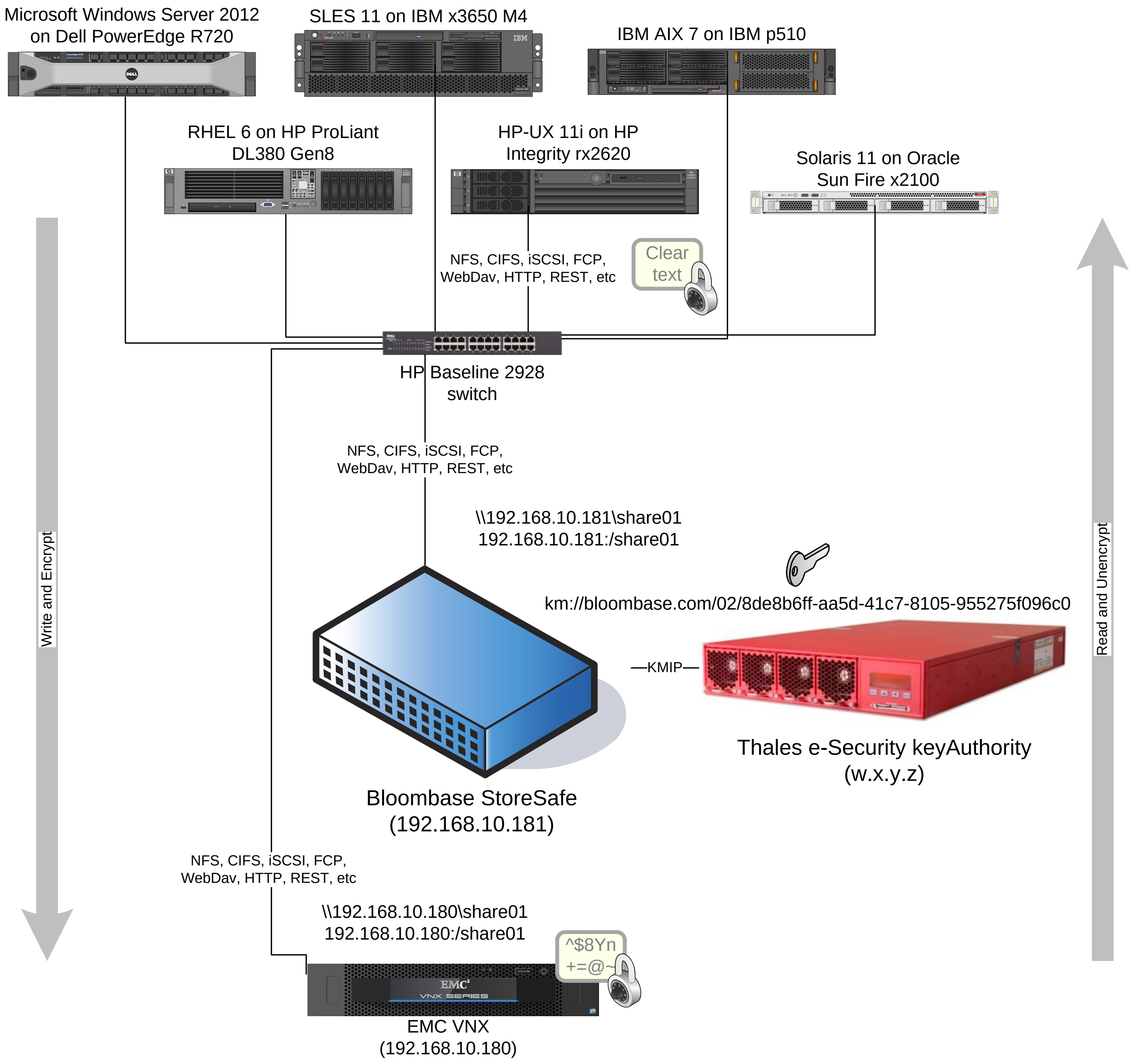
This document describes interoperability testing of keyAuthority with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of keyAuthority, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of operating system.

As keyAuthority key manager 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 keyAuthority 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


Microsoft Windows Server 2012
on Dell PowerEdge R720
SLES 11 on IBM x3650 M4
IBM AIX 7 on IBM p510
RHEL 6 on HP ProLiant
DL380 Gen8
HP-UX 11i on HP
Integrity rx2620
Solaris 11 on Oracle
Sun Fire x2100
NFS, CIFS, iSCSI, FCP,
WebDav, HTTP, REST, etc
Clear
text
HP Baseline 2928
switch
NFS, CIFS, iSCSI, FCP,
WebDav, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0
—KMIP—
Thales e-Security keyAuthority
(w.x.y.z)
Bloombase StoreSafe
(192.168.10.181)
NFS, CIFS, iSCSI, FCP,
WebDav, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn
+=@~
EMC VNX
(192.168.10.180)
Write and Encrypt
Read and Unencrypt

Thales e-Security keyAuthority

KMIP Key Manager	keyAuthority

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	EMC VNX Virtual Appliance on ESXi 5.5

Client Hosts

Model	Dell PowerEdge R720	HP ProLiant DL380 Gen8	IBM System x3650 M4	HP Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
Operating System	Microsoft Windows Server 2012	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

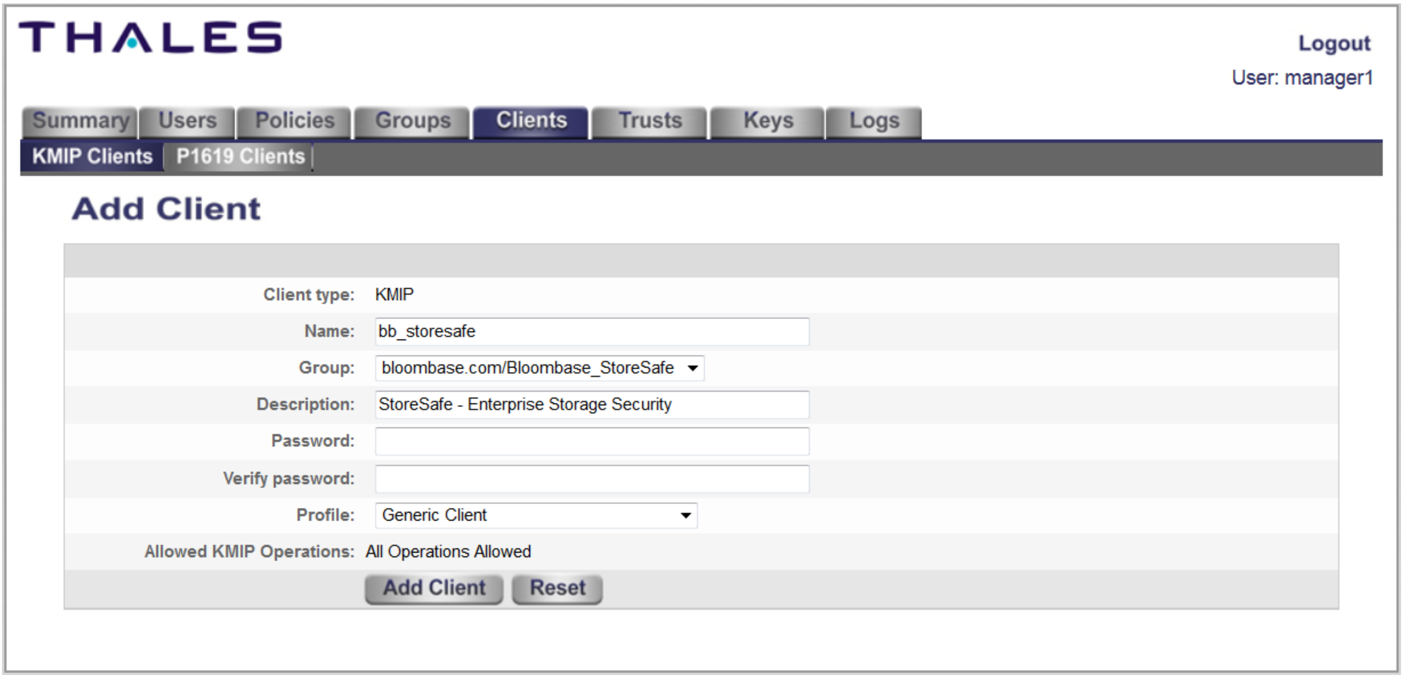
Configuration Overview

Thales e-Security keyAuthority

keyAuthority is installed and configured as a network attached appliance with IP address w.x.y.z assigned.

For the purpose of this interoperability testing, domain “bloombase.com” is provisioned and assigned for the Bloombase StoreSafe software appliance instance.

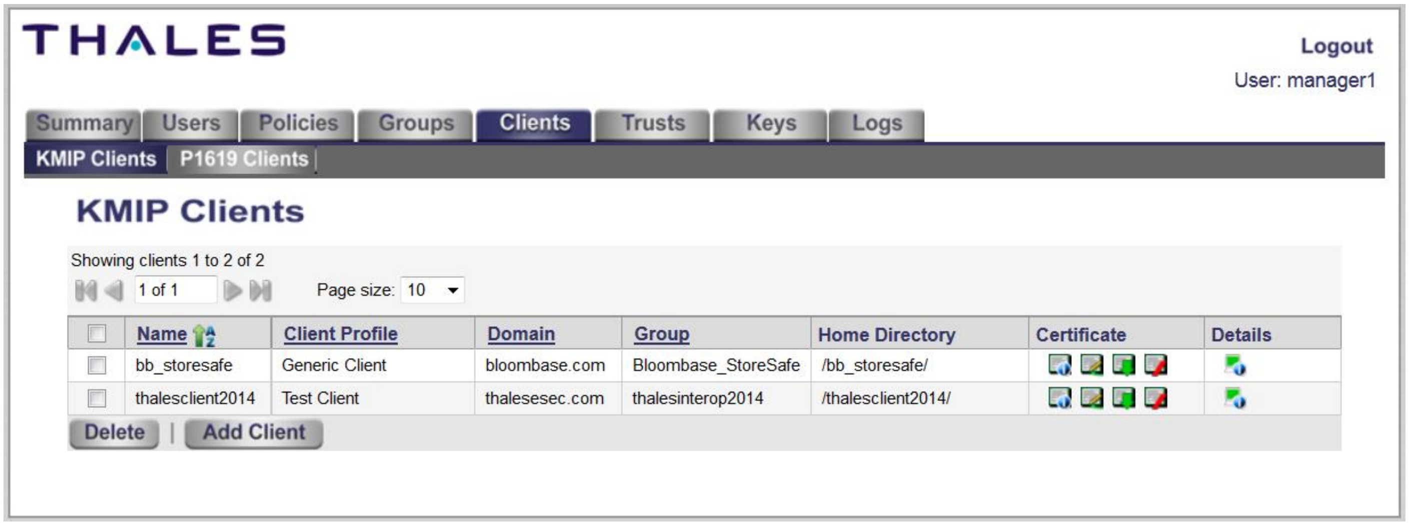
X.509 key pair “CN=bloombase, O=Thales, OU=Support, L=Milpitas, ST=CA, C=US, E=support@thales.com” is created and assigned as the authentication key pair for Bloombase StoreSafe.



Add Client

Client type:	KMIP
Name:	bb_storesafe
Group:	bloombase.com/Bloombase_StoreSafe
Description:	StoreSafe - Enterprise Storage Security
Password:	
Verify password:	
Profile:	Generic Client
Allowed KMIP Operations:	All Operations Allowed

Client authentication key is signed and registered.



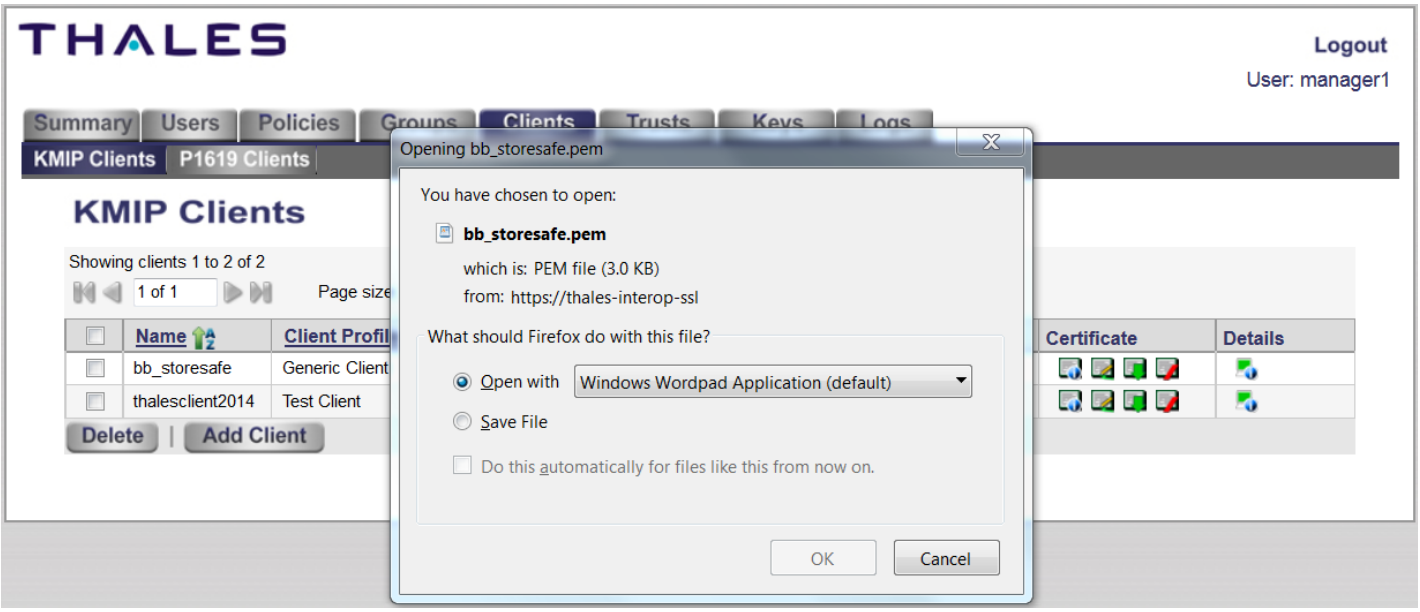
KMIP Clients

Showing clients 1 to 2 of 2

1 of 1 Page size: 10

□	Name	Client Profile	Domain	Group	Home Directory	Certificate	Details
□	bb_storesafe	Generic Client	bloombase.com	Bloombase_StoreSafe	/bb_storesafe/		
□	thalesclient2014	Test Client	thalesesec.com	thalesinterop2014	/thalesclient2014/		

Signed client authentication certificate in PEM format is exported from keyAuthority web management console and imported to Bloombase StoreSafe client key store via web management console.



KMIP Clients

Showing clients 1 to 2 of 2

1 of 1

□	Name	Client Profil	Certificate	Details
□	bb_storesafe	Generic Client		
□	thalesclient2014	Test Client		

Opening bb_storesafe.pem

You have chosen to open:

bb_storesafe.pem

which is: PEM file (3.0 KB)

from: https://thales-interop-ssl

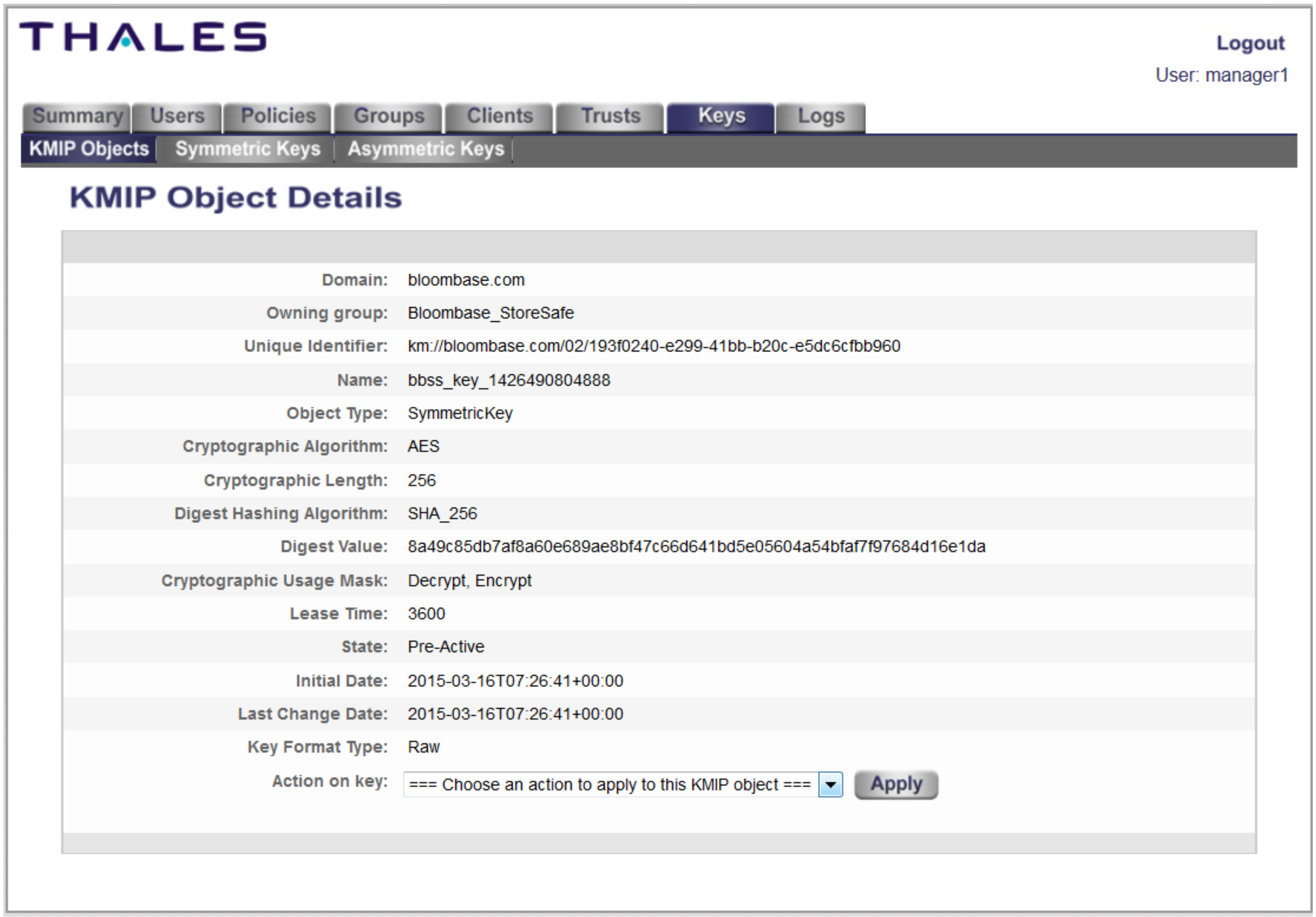
What should Firefox do with this file?

● Open with Windows Wordpad Application (default)

○ Save File

□ Do this automatically for files like this from now on.

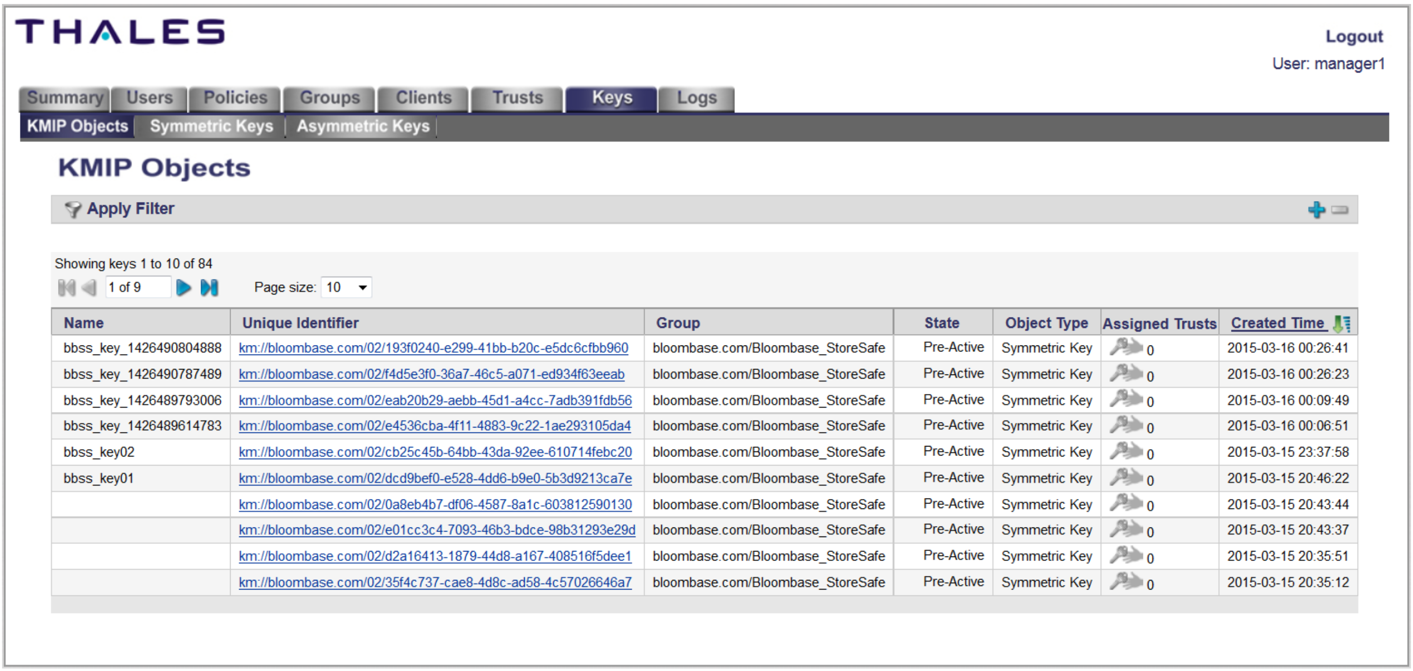
An AES-256 key of identifier “km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0” is generated and provisioned for Bloombase StoreSafe’s actual data at-rest encryption use.



KMIP Object Details

Domain:	bloombase.com
Owning group:	Bloombase_StoreSafe
Unique Identifier:	km://bloombase.com/02/193f0240-e299-41bb-b20c-e5dc6cfbb960
Name:	bbss_key_1426490804888
Object Type:	SymmetricKey
Cryptographic Algorithm:	AES
Cryptographic Length:	256
Digest Hashing Algorithm:	SHA_256
Digest Value:	8a49c85db7af8a60e689ae8bf47c66d641bd5e05604a54bfaf7f97684d16e1da
Cryptographic Usage Mask:	Decrypt, Encrypt
Lease Time:	3600
State:	Pre-Active
Initial Date:	2015-03-16T07:26:41+00:00
Last Change Date:	2015-03-16T07:26:41+00:00
Key Format Type:	Raw
Action on key:	=== Choose an action to apply to this KMIP object === ▾ Apply

KMIP key objects are listed.



KMIP Objects

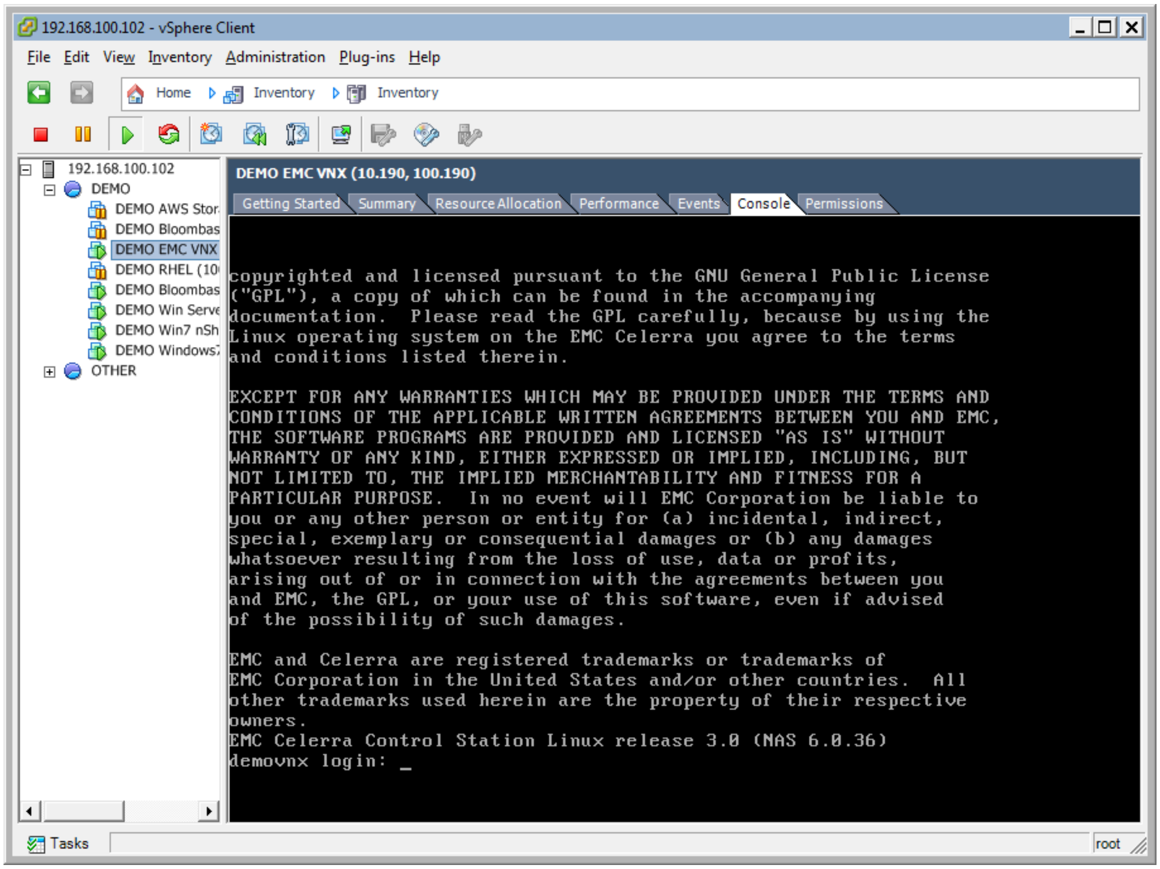
Showing keys 1 to 10 of 84

1 of 9 Page size: 10

Name	Unique Identifier	Group	State	Object Type	Assigned Trusts	Created Time
bbss_key_1426490804888	km://bloombase.com/02/193f0240-e299-41bb-b20c-e5dc6cfbb960	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-16 00:26:41
bbss_key_1426490787489	km://bloombase.com/02/f4d5e3f0-36a7-46c5-a071-ed934f63eeab	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-16 00:26:23
bbss_key_1426489793006	km://bloombase.com/02/eab20b29-aebb-45d1-a4cc-7adb391fdb56	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-16 00:09:49
bbss_key_1426489614783	km://bloombase.com/02/e4536cba-4f11-4883-9c22-1ae293105da4	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-16 00:06:51
bbss_key02	km://bloombase.com/02/cb25c45b-64bb-43da-92ee-610714febc20	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 23:37:58
bbss_key01	km://bloombase.com/02/dcd9bef0-e528-4dd6-b9e0-5b3d9213ca7e	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 20:46:22
	km://bloombase.com/02/0a8eb4b7-df06-4587-8a1c-603812590130	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 20:43:44
	km://bloombase.com/02/e01cc3c4-7093-46b3-bdce-98b31293e29d	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 20:43:37
	km://bloombase.com/02/d2a16413-1879-44d8-a167-408516f5dee1	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 20:35:51
	km://bloombase.com/02/35f4c737-cae8-4d8c-ad58-4c57026646a7	bloombase.com/Bloombase_StoreSafe	Pre-Active	Symmetric Key	0	2015-03-15 20:35:12

EMC VNX Storage

EMC VNX virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.

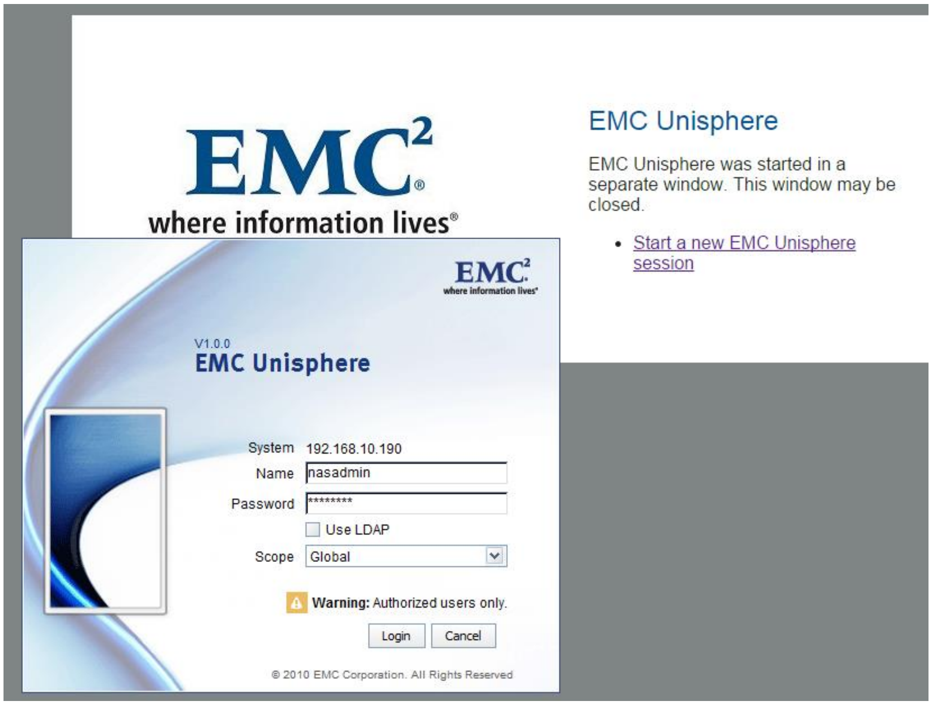


```
copyrighted and licensed pursuant to the GNU General Public License
("GPL"), a copy of which can be found in the accompanying
documentation.  Please read the GPL carefully, because by using the
Linux operating system on the EMC Celerra you agree to the terms
and conditions listed therein.

EXCEPT FOR ANY WARRANTIES WHICH MAY BE PROVIDED UNDER THE TERMS AND
CONDITIONS OF THE APPLICABLE WRITTEN AGREEMENTS BETWEEN YOU AND EMC,
THE SOFTWARE PROGRAMS ARE PROVIDED AND LICENSED "AS IS" WITHOUT
WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT
NOT LIMITED TO, THE IMPLIED MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE.  In no event will EMC Corporation be liable to
you or any other person or entity for (a) incidental, indirect,
special, exemplary or consequential damages or (b) any damages
whatsoever resulting from the loss of use, data or profits,
arising out of or in connection with the agreements between you
and EMC, the GPL, or your use of this software, even if advised
of the possibility of such damages.

EMC and Celerra are registered trademarks or trademarks of
EMC Corporation in the United States and/or other countries.  All
other trademarks used herein are the property of their respective
owners.
EMC Celerra Control Station Linux release 3.0 (NAS 6.0.36)
demovnx login: _
```

EMC VNX is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FCP, FCoE, iSCSI, etc.



EMC Unisphere

EMC Unisphere was started in a separate window. This window may be closed.

- Start a new EMC Unisphere session

System 192.168.10.190

Name nasadmin

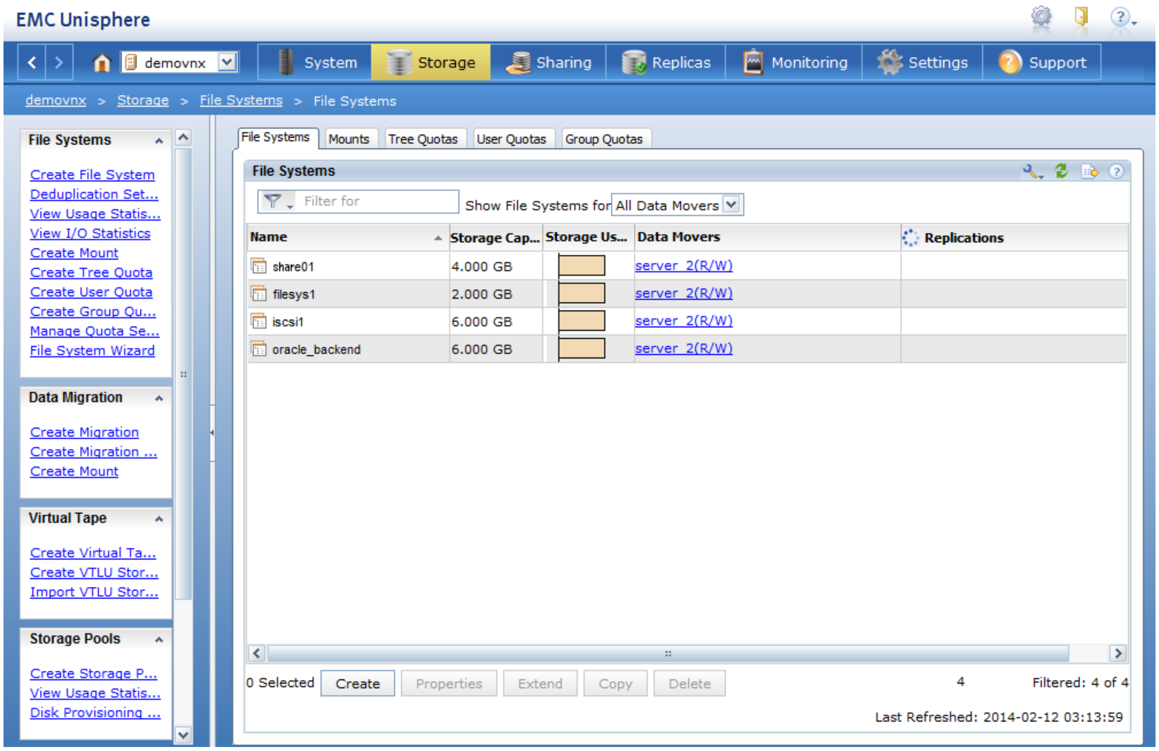
Password ********

□ Use LDAP

Scope Global

Warning: Authorized users only.

CIFS and NFS storage resources are provisioned on EMC VNX to be used in this testing.



Show File Systems for All Data Movers

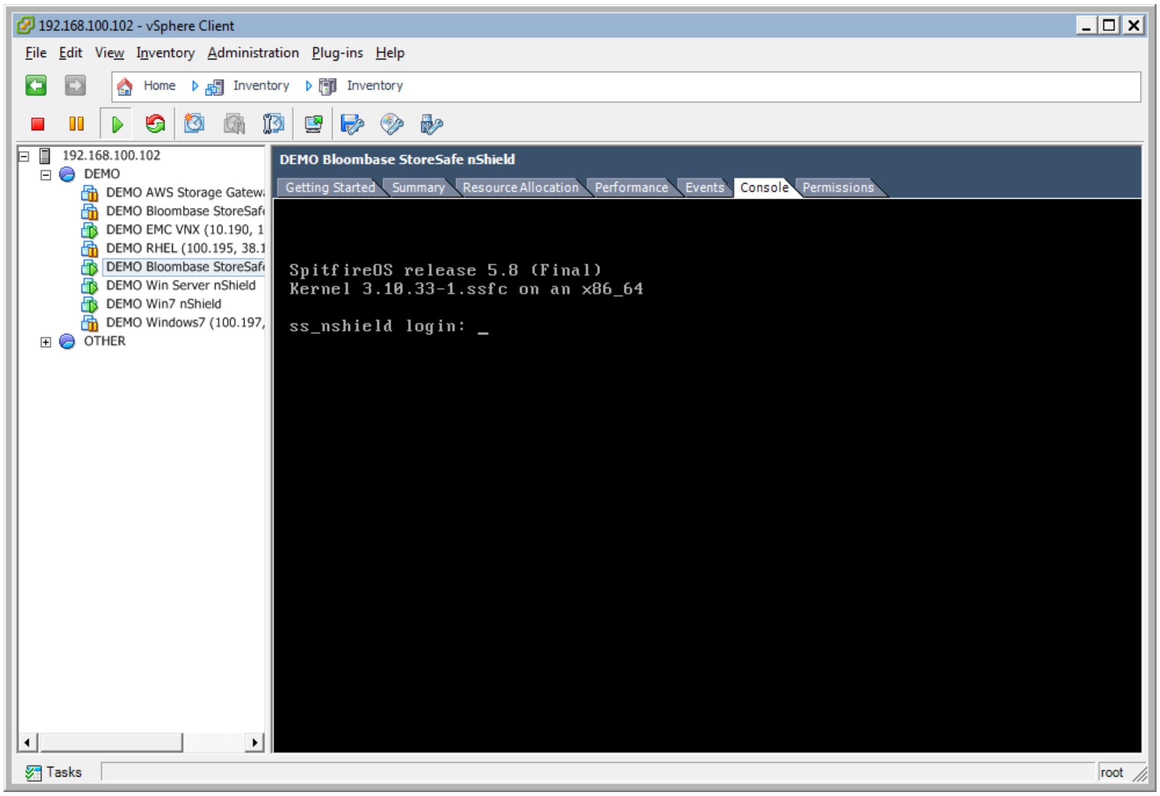
Name	Storage Cap...	Storage Us...	Data Movers	Replications
share01	4.000 GB		server_2(R/W)	
filesys1	2.000 GB		server_2(R/W)	
iscsi1	6.000 GB		server_2(R/W)	
oracle_backend	6.000 GB		server_2(R/W)	

0 Selected 4 Filtered: 4 of 4

Last Refreshed: 2014-02-12 03:13:59

Bloombase StoreSafe

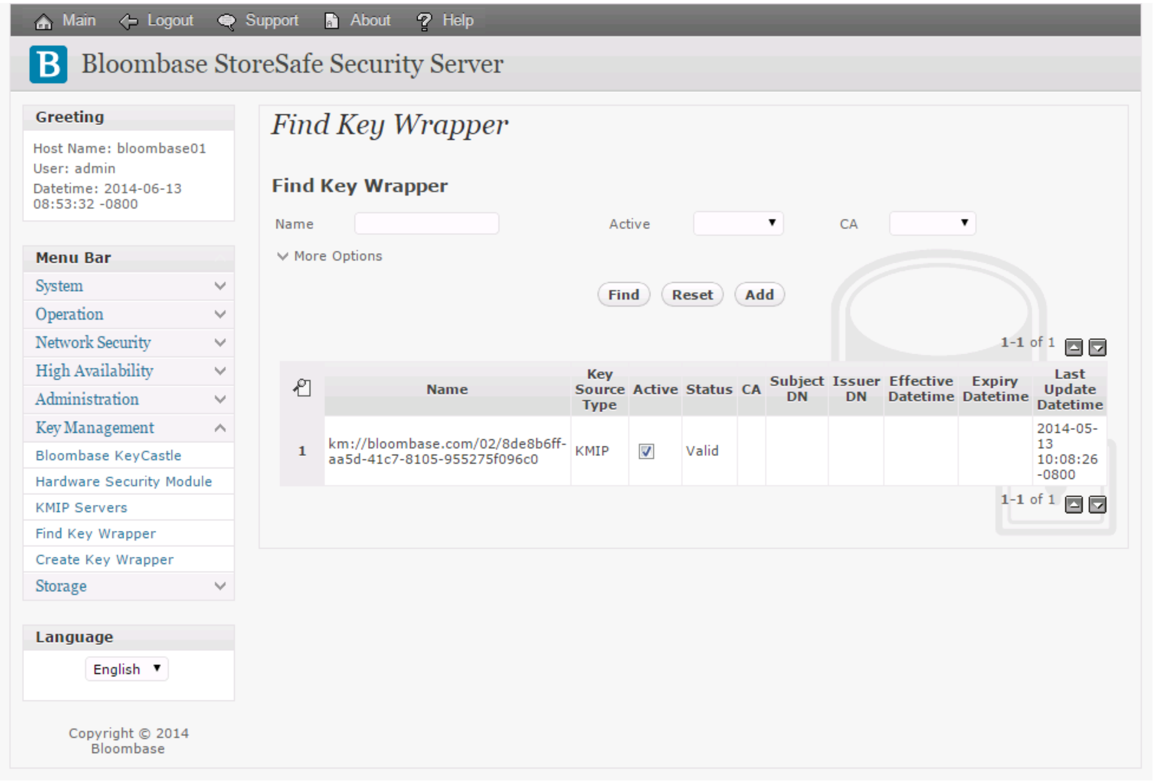
Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at keyAuthority key manager.



```
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: 2014-06-13 08:53:32 -0800

Find Key Wrapper

Find Key Wrapper

Name

Active

CA

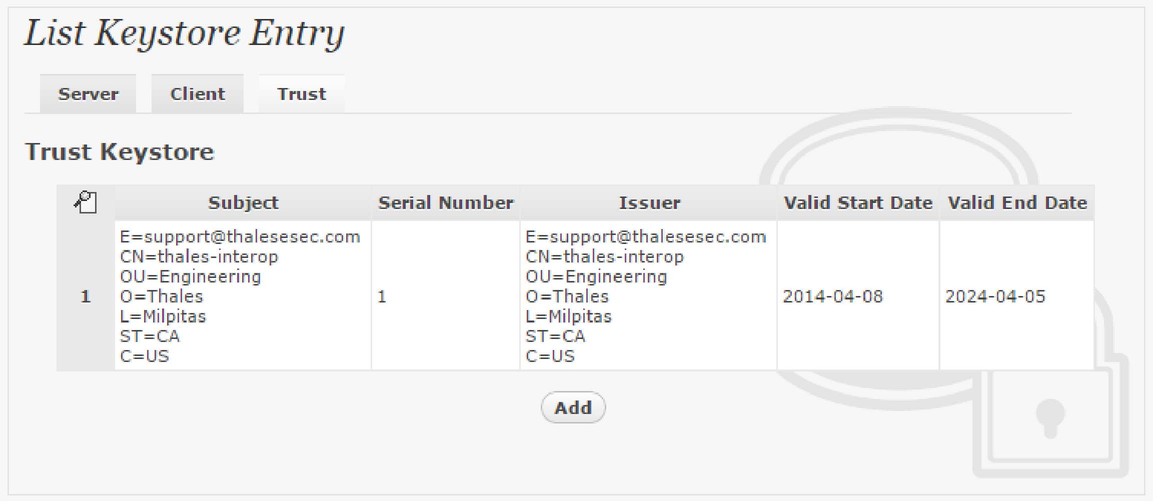
	Name	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0	KMIP	☑	Valid						2014-05-13 10:08:26 -0800

Network Security, Trust and Authentication Configuration

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

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

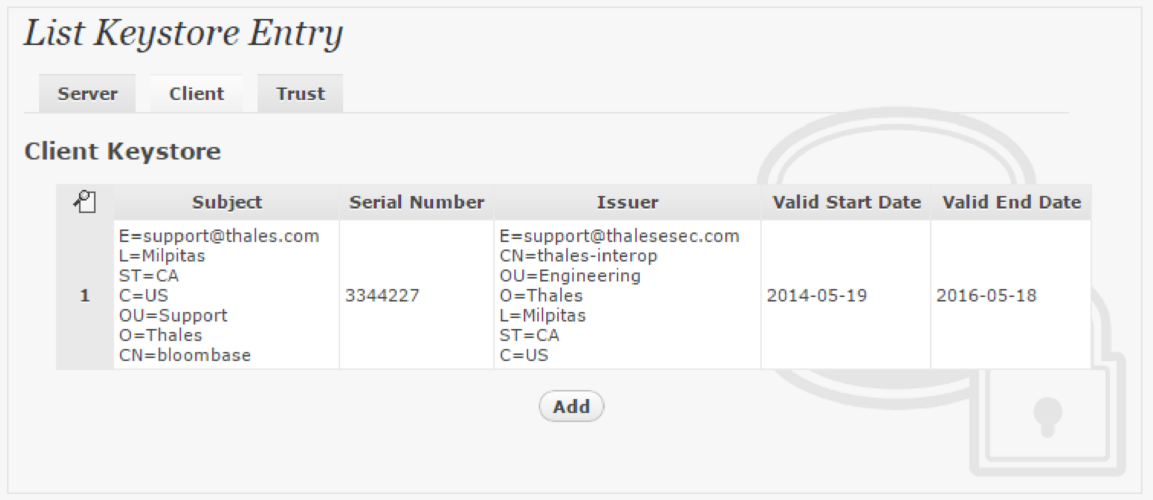
keyAuthority’s KMIP service is trusted by adding the certificate authority of KMIP server certificate to Bloombase StoreSafe’s trust key store.



	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
1	E=support@thalesesec.com CN=thales-interop OU=Engineering O=Thales L=Milpitas ST=CA C=US	1	E=support@thalesesec.com CN=thales-interop OU=Engineering O=Thales L=Milpitas ST=CA C=US	2014-04-08	2024-04-05

keyAuthority utilizes certificate-based authentication for client access control. An X.509 compliant key pair is generated and entered into Bloombase StoreSafe's client key store.

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

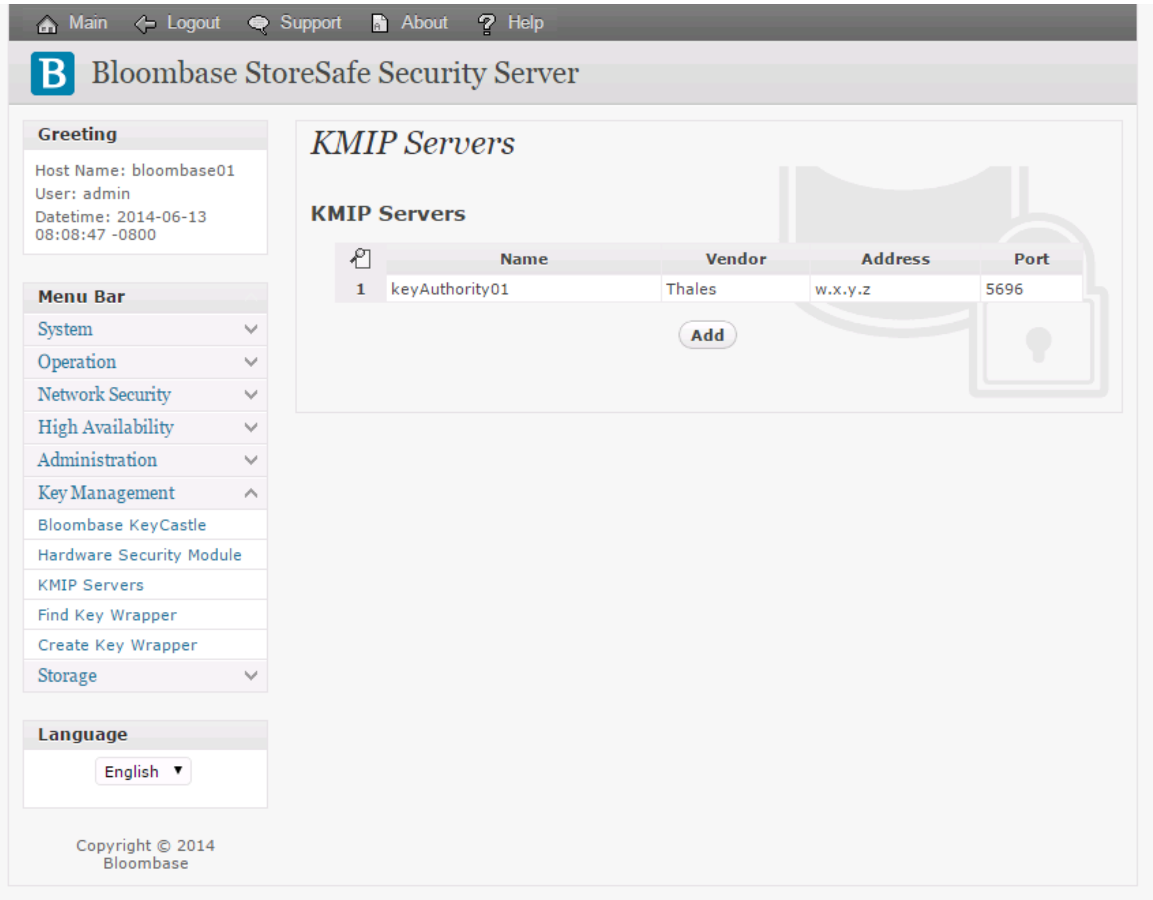


	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
1	E=support@thales.com L=Milpitas ST=CA C=US OU=Support O=Thales CN=bloombase	3344227	E=support@thalesesec.com CN=thales-interop OU=Engineering O=Thales L=Milpitas ST=CA C=US	2014-05-19	2016-05-18

keyAuthority and Bloombase KeyCastle Integration

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

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



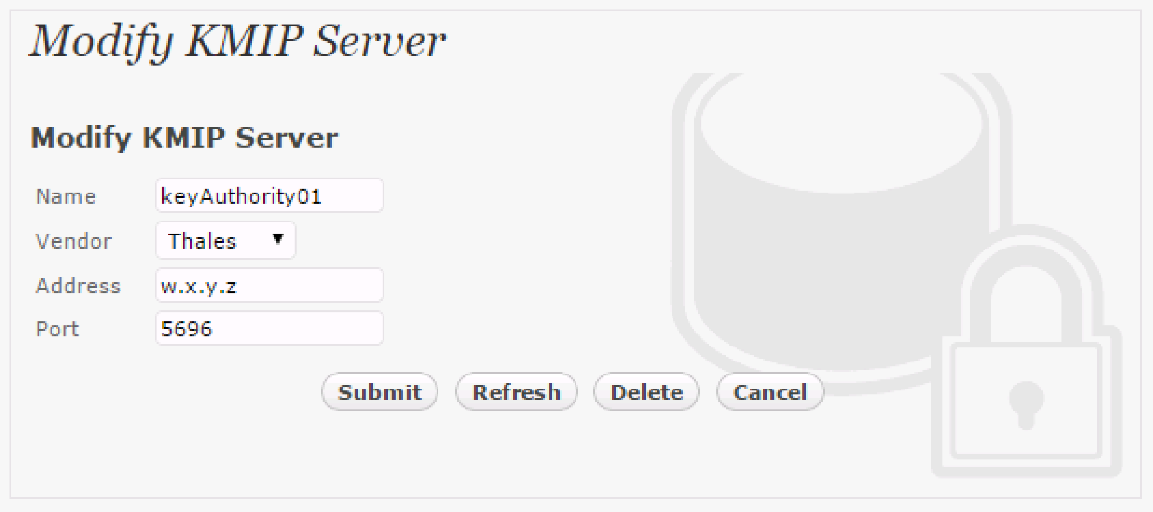
Host Name: bloombase01
User: admin
Datetime: 2014-06-13 08:08:47 -0800

KMIP Servers

KMIP Servers

	Name	Vendor	Address	Port
1	keyAuthority01	Thales	w.x.y.z	5696

keyAuthority server setting is properly configured at Bloombase StoreSafe web management console and assigned the name ‘keyAuthority01’.



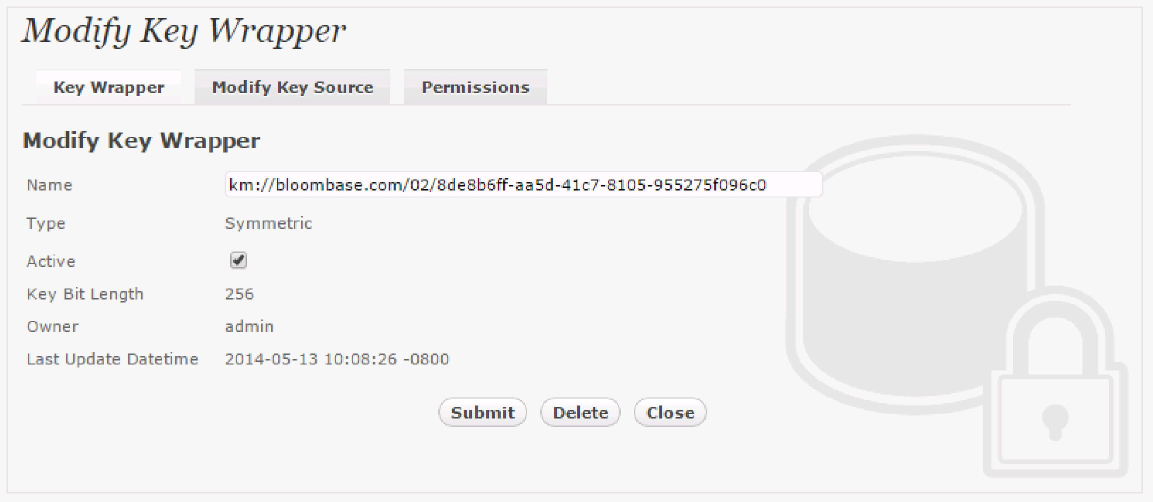
Modify KMIP Server

Modify KMIP Server

Name: keyAuthority01
Vendor: Thales
Address: w.x.y.z
Port: 5696

Encryption Key Provisioning

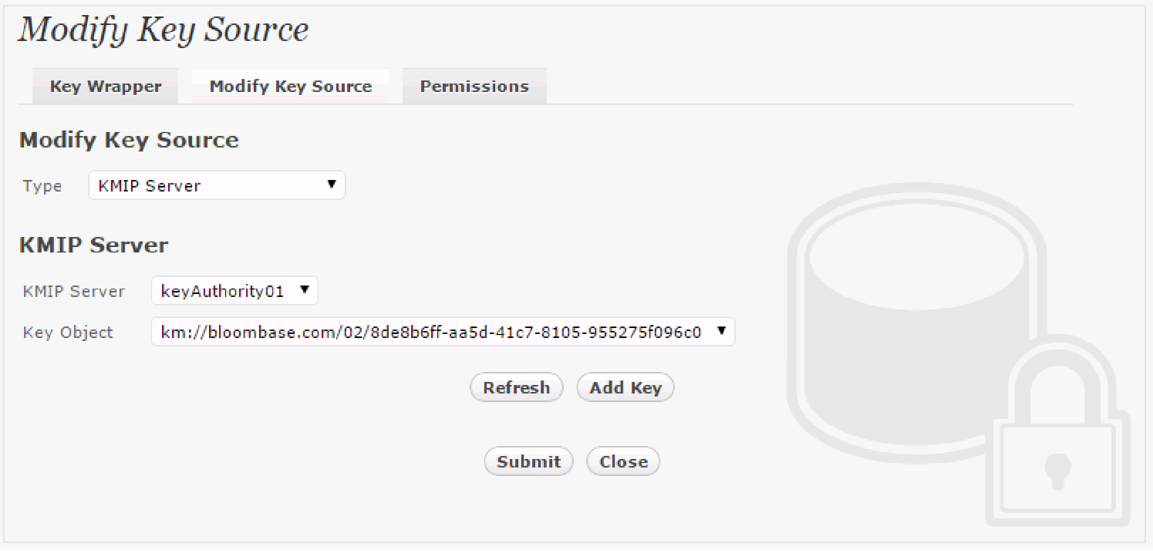
Existing keyAuthority key “km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0” has to be linked to Bloombase StoreSafe before it can be used for secure storage configuration delivering stored data encryption services.



Modify Key Wrapper

Name	km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0
Type	Symmetric
Active	☑
Key Bit Length	256
Owner	admin
Last Update Datetime	2014-05-13 10:08:26 -0800

To properly associate an existing key object at keyAuthority from built-in Bloombase KeyCastle, select Key Source Type as “KMIP Server”, KMIP Server as the identifier “keyAuthority01” and select the encryption key to be used for data encryption, in this case “km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0”.



Modify Key Source

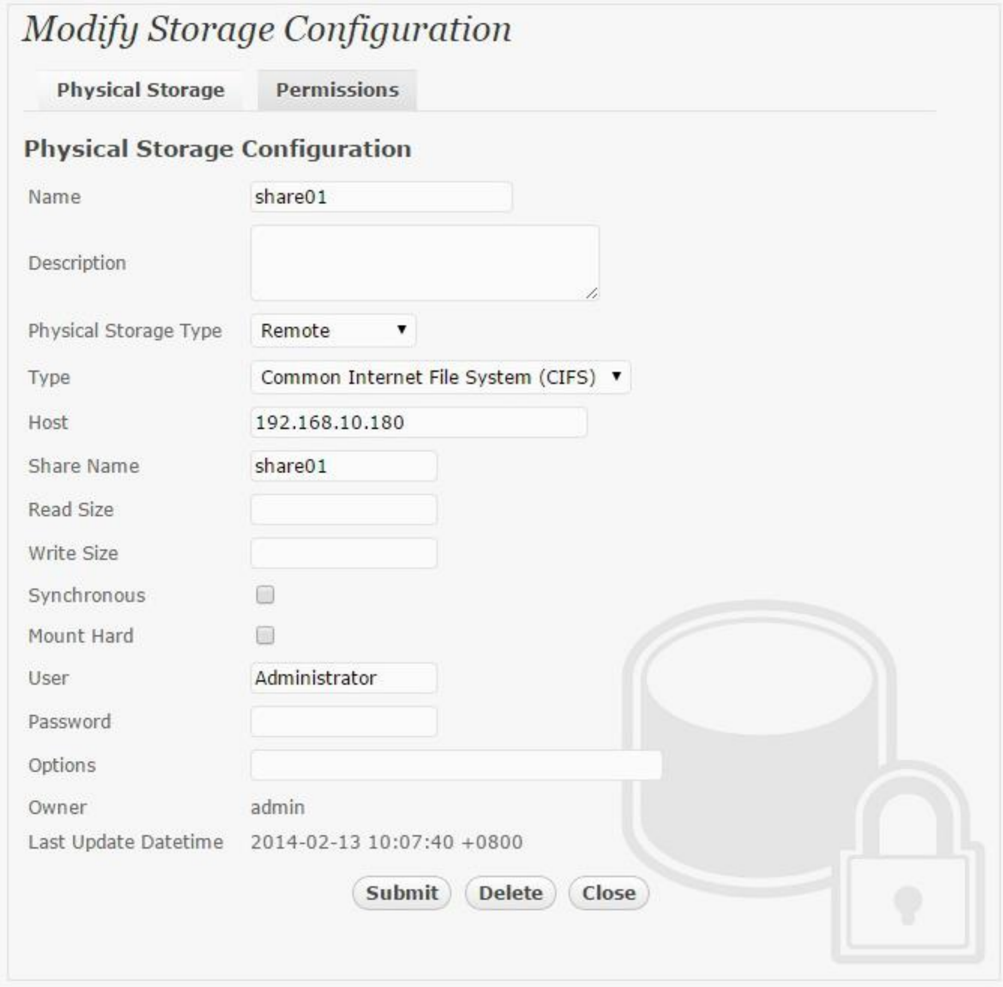
Type: KMIP Server

KMIP Server

KMIP Server	keyAuthority01
Key Object	km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0

Backend Physical Storage Configuration

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

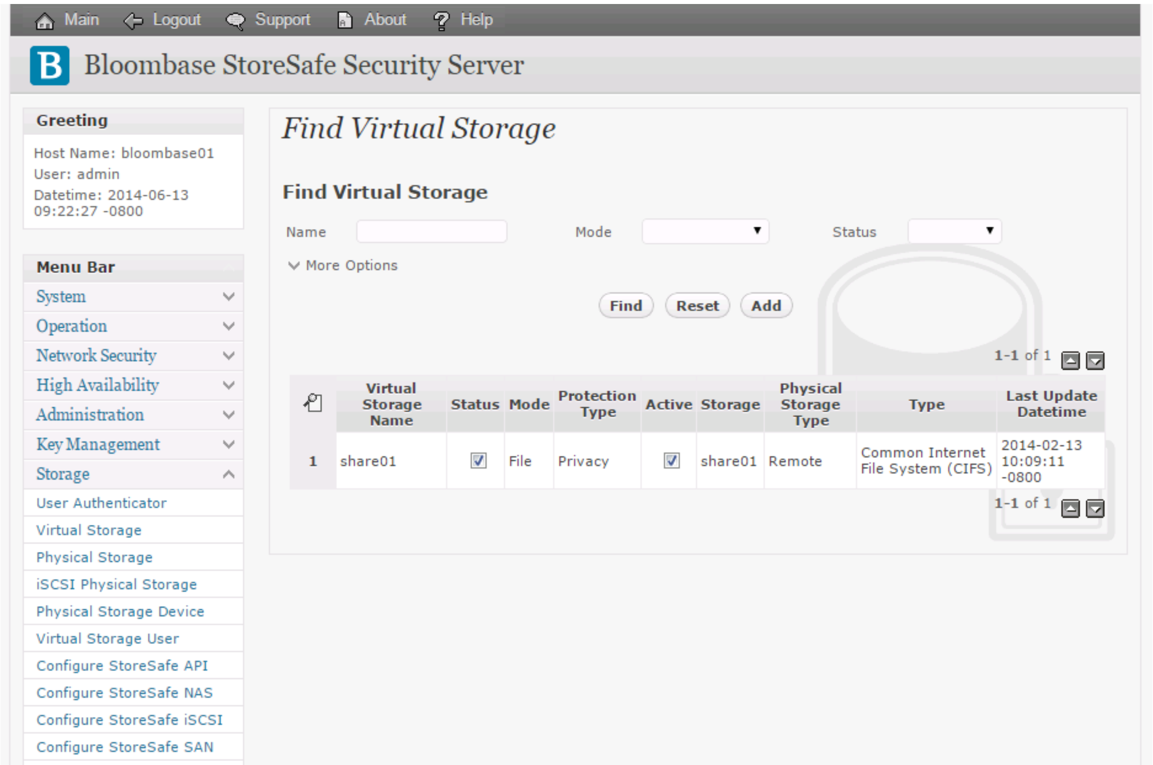


Modify Storage Configuration

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



Greeting

Host Name: bloombase01
User: admin
Datetime: 2014-06-13 09:22:27 -0800

Find Virtual Storage

Find Virtual Storage

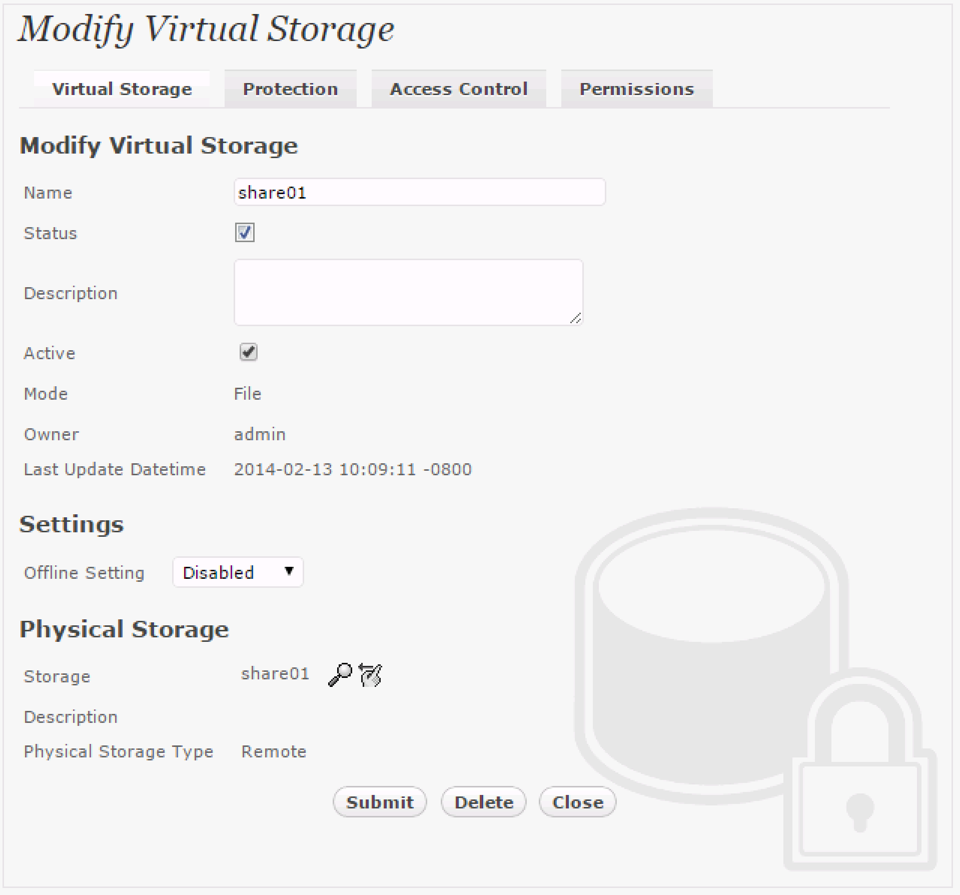
Name

Mode

Status

	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)	2014-02-13 10:09:11 -0800

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

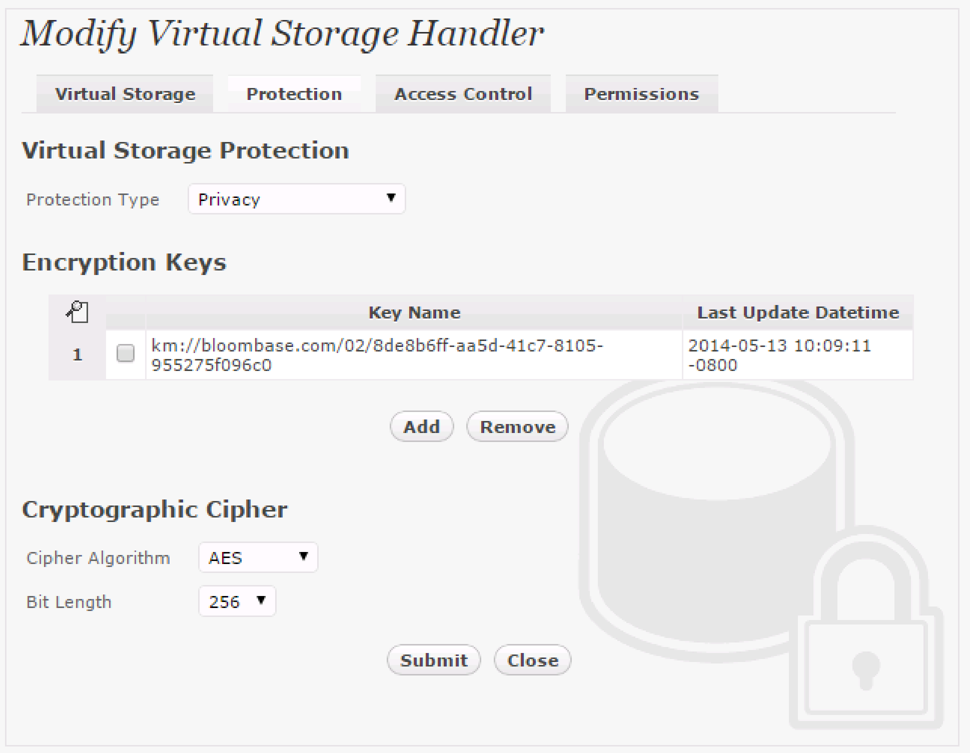
Settings

Offline Setting	Disabled

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as ‘Privacy’ and secure contents of the backend EMC VNX storage using AES 256-bit encryption with encryption key “km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0” managed at keyAuthority.



Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

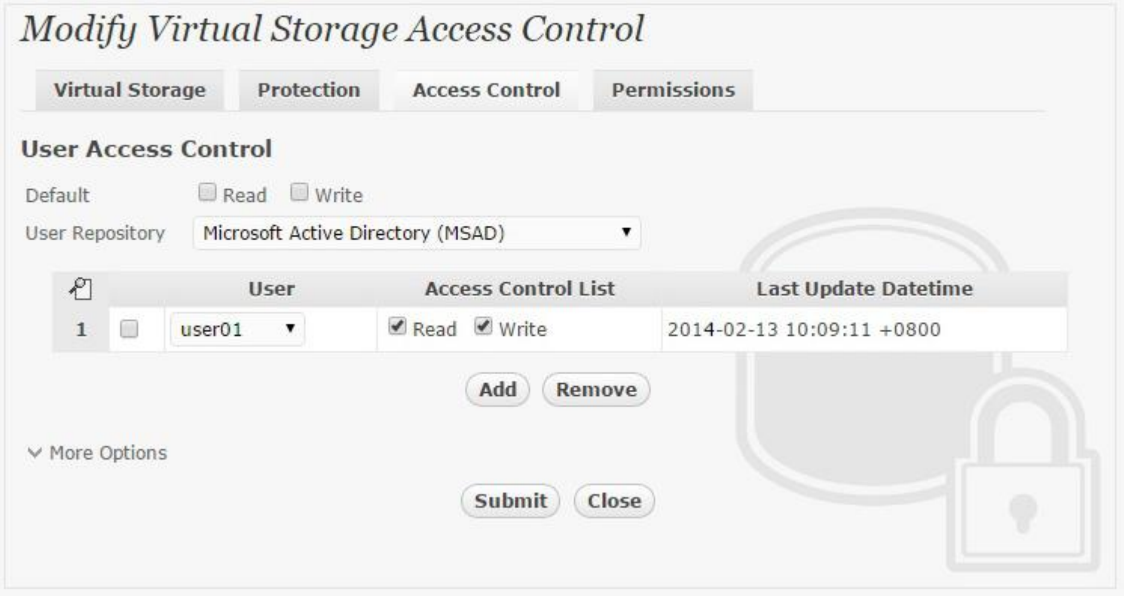
		Key Name	Last Update Datetime
1	□	km://bloombase.com/02/8de8b6ff-aa5d-41c7-8105-955275f096c0	2014-05-13 10:09:11 -0800

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.



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

Conclusion

KMIP key manager

- Thales e-Security keyAuthority

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	KMIP Key Manager
Bloombase StoreSafe	Microsoft Windows Server	• keyAuthority
	Red Hat Enterprise Linux (RHEL)	• keyAuthority
	SUSE Linux Enterprise Server (SLES)	• keyAuthority
	Oracle Solaris	• keyAuthority
	IBM AIX	• keyAuthority
	HP-UX	• keyAuthority

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 Thales 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. Thales e-Security keyAuthority, https://www.thales-esecurity.com/products-and-services/products-and-services/key-management-systems/keyauthority

4. OASIS KMIP, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip