interopLab

Interoperability of Bloombase StoreSafe and Thales payShield® for Data-at-Rest Encryption

December 2015

BLOOMBASE®

Executive Summary

Thales payShield enterprise Hardware Security Module (HSM) 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 Thales payShield HSM 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 tested with Thales payShield powered Bloombase StoreSafe with EMC VNX unified storage system as backend storage.

Document No.: BLBS-TN-Bloombase-StoreSafe-Thales-payShield-Interoperability-USLET-EN-R5

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Thales payShield Hardware Security Module (HSM) with Bloombase StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Thales payShield
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

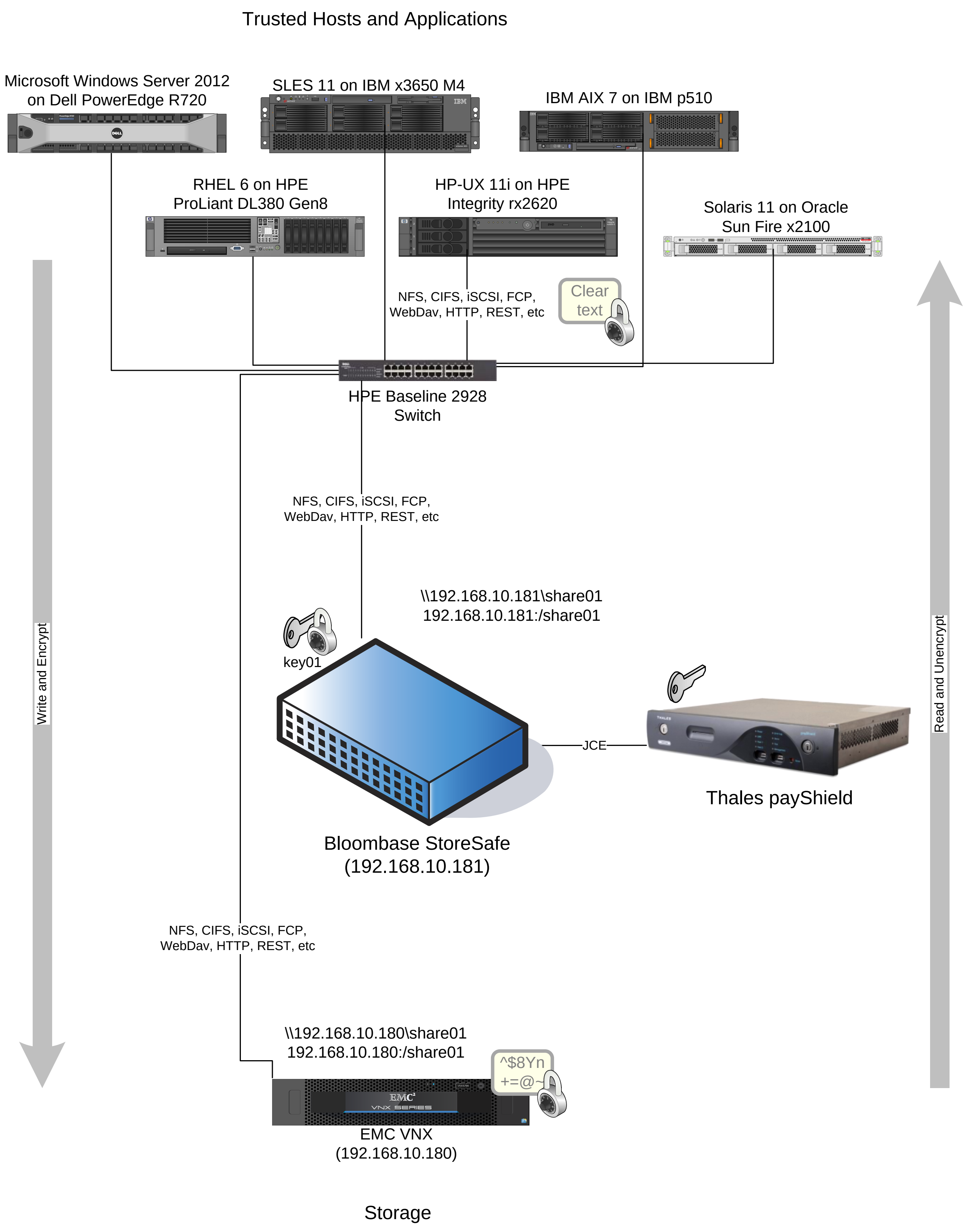
This document describes interoperability testing of Thales payShield with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Thales payShield, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that the reader possesses basic UNIX administration skill-set. The examples provided may require modifications before they could be run in reader's IT environment.

As Thales payShield is a third party hardware option to Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model of Thales payShield for the actual use case. We assume the reader has 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 set up as in below diagram:


Trusted Hosts and Applications
Microsoft Windows Server 2012 on Dell PowerEdge R720
SLES 11 on IBM x3650 M4
IBM AIX 7 on IBM p510
RHEL 6 on HPE ProLiant DL380 Gen8
HP-UX 11i on HPE Integrity rx2620
Solaris 11 on Oracle Sun Fire x2100
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
Clear text
HPE Baseline 2928 Switch
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
key01
JCE
Thales payShield
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 +=@~
EMC VNX (192.168.10.180)
Storage

Thales Hardware Security Module

Hardware Security Module	Thales payShield 9000

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 5
payShield Client Software Package	PayShield API 1.1.15
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	HPE ProLiant DL380 Gen8	IBM System x3650 M4	HPE 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

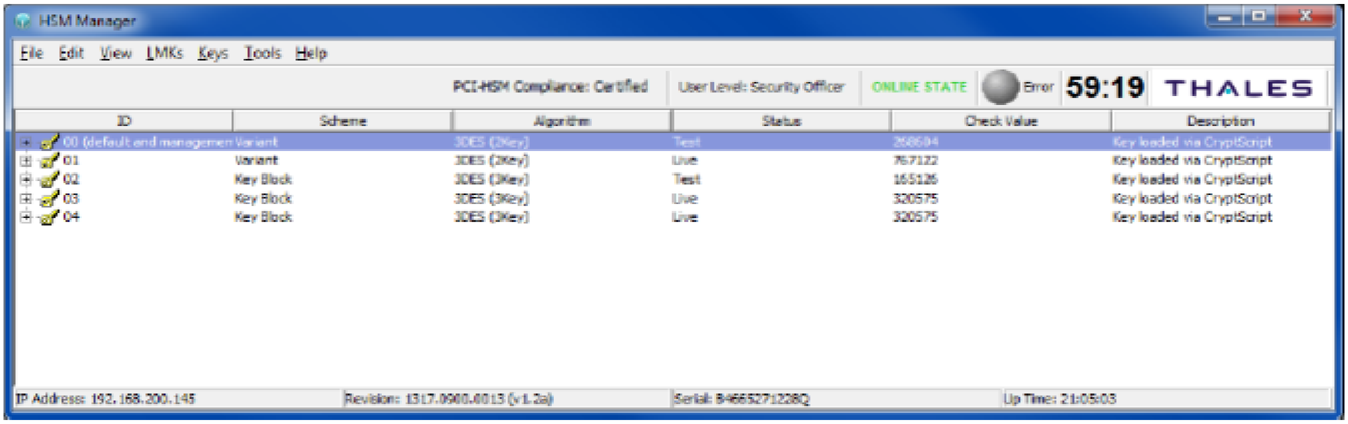
Thales payShield

Thales payShield is a hardware security module that provides the cryptographic protection needed for payment card transactions. It is deployed as an external peripheral for servers running payment-card-related software applications. The key management and cryptographic functionalities provided by Thales payShield can also be used by Bloombase StoreSafe for encryption protection of data-at-rest for payment and general-purpose use cases.

Thales payShield can be managed through the Graphical User Interface (GUI) of the local HSM Manager by connecting the ethernet management port of the Thales payShield to a computer running the HSM Manager CD with an ethernet cable. Users may utilize remote HSM Manager to manage the HSM remotely across a TCP/IP network.

Thales payShield Configurations

Once Thales payShield is connected physically with a laptop computer, open the GUI of the local HSM Manager, and select “connect” from the File Menu. Then “Login” Thales PsyShield from the File Menu using one or two smartcards to access Operator or Security Officer functions.



PCI-HSM Compliance: Certified | User Level: Security Officer | ONLINE STATE | 59:19

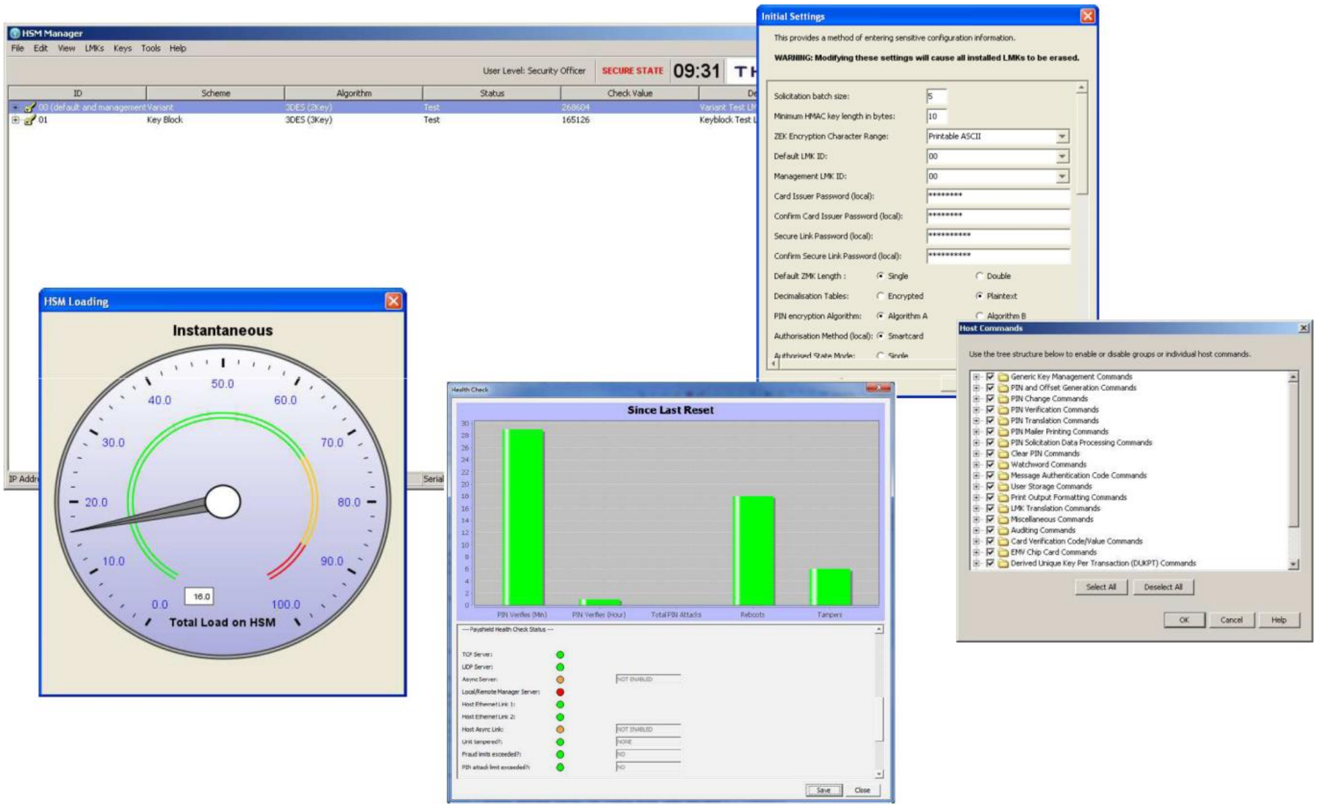
ID	Scheme	Algorithm	Status	Check Value	Description
00 (default and managemen	Variant	3DES (2Key)	Test	268604	Key loaded via CryptScript
01	Variant	3DES (2Key)	Live	767122	Key loaded via CryptScript
02	Key Block	3DES (3Key)	Test	165126	Key loaded via CryptScript
03	Key Block	3DES (3Key)	Live	320575	Key loaded via CryptScript
04	Key Block	3DES (3Key)	Live	320575	Key loaded via CryptScript

IP Address: 192.168.200.145 | Revision: 1317.0900.0013 (v1.2a) | Serial: B46652712280 | Up Time: 21:05:03

Under the “Edit” Menu, select the appropriate choice to configure the IP address, time and date, secure host communication through TLS and IP White List, and logging of Thales payShield.

Under the “LMKs” Menu, generate a new Local Master Key (LMK) onto smart cards and import it into the HSM, or load an existing LMK.

Under the “Tools” Menu, setup the certificates for secure host communication through TLS.



User Level: Security Officer | SECURE STATE | 09:31

ID	Scheme	Algorithm	Status	Check Value	De
00 (default and management Variant		3DES (2Key)	Test	268604	Variant Test LM
01	Key Block	3DES (3Key)	Test	165126	Keyblock Test L

Initial Settings

This provides a method of entering sensitive configuration information.

WARNING: Modifying these settings will cause all installed LMKs to be erased.

Solicitation batch size: 5
Minimum HMAC key length in bytes: 10
ZEK Encryption Character Range: Printable ASCII
Default LMK ID: 00
Management LMK ID: 00
Card Issuer Password (local): ********
Confirm Card Issuer Password (local): ********
Secure Link Password (local): **********
Confirm Secure Link Password (local): **********
Default ZMK Length : ● Single ○ Double
Decimalisation Tables: ○ Encrypted ● Plaintext
PIN encryption Algorithm: ● Algorithm A ○ Algorithm B
Authorisation Method (local): ● Smartcard
Authorised State Mode: ○ Single

Host Commands

Use the tree structure below to enable or disable groups or individual host commands.

- ☑ Generic Key Management Commands
- ☑ PIN and Offset Generation Commands
- ☑ PIN Change Commands
- ☑ PIN Verification Commands
- ☑ PIN Translation Commands
- ☑ PIN Mailer Printing Commands
- ☑ PIN Solicitation Data Processing Commands
- ☑ Clear PIN Commands
- ☑ Watchword Commands
- ☑ Message Authentication Code Commands
- ☑ User Storage Commands
- ☑ Print Output Formatting Commands
- ☑ LMK Translation Commands
- ☑ Miscellaneous Commands
- ☑ Auditing Commands
- ☑ Card Verification Code/Value Commands
- ☑ EMV Chip Card Commands
- ☑ Derived Unique Key Per Transaction (DUKPT) Commands

--- Payshield Health Check Status ---

TCP Server: ●
UDP Server: ●
Async Server: ● NOT ENABLED
Local/Remote Manager Server: ●
Host Ethernet Link 1: ●
Host Ethernet Link 2: ●
Host Async Link: ● NOT ENABLED
Unit tampered?: ● NONE
Fraud limits exceeded?: ● NO
PIN attack limit exceeded?: ● NO

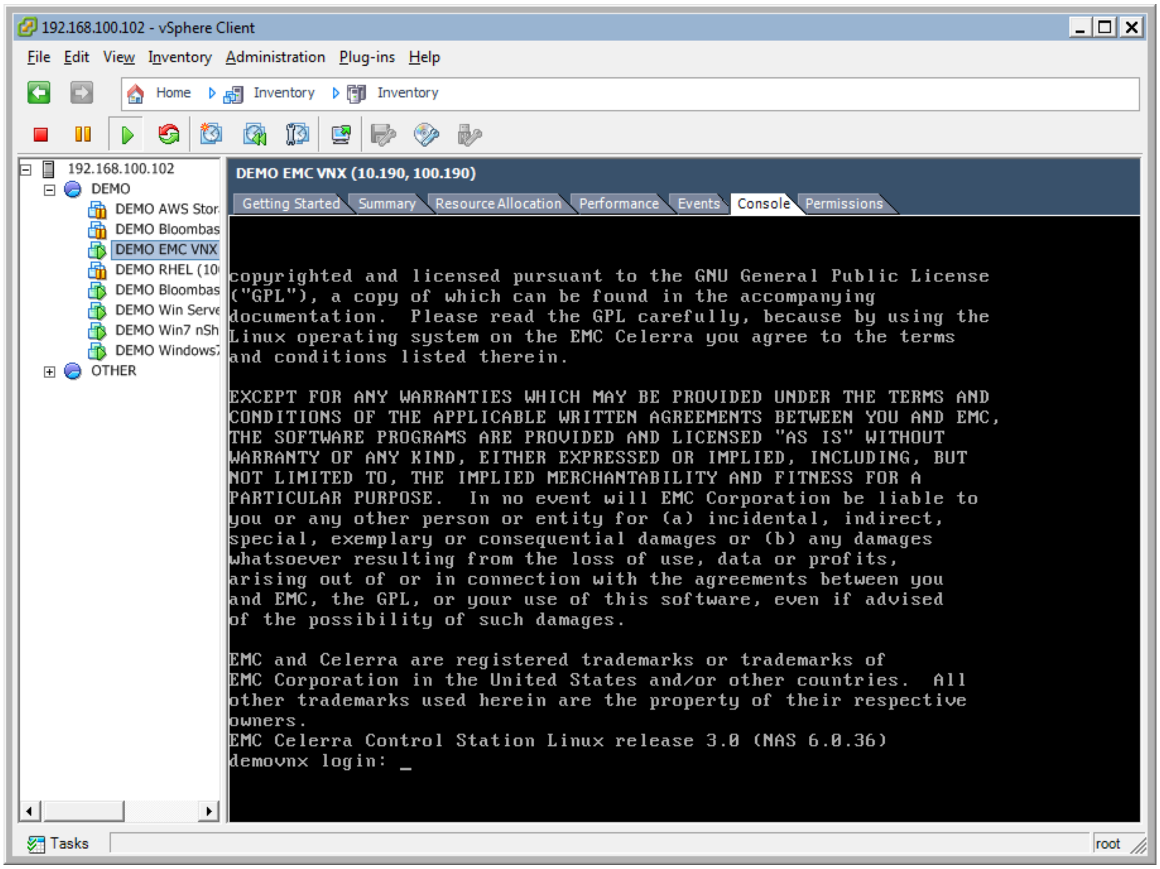
Network Security, Trust and Authentication Configuration

To enable secure communications through TLS between Bloombase StoreSafe and Thales payShield, their corresponding public key certificate signed by the same CA needs to be exchanged between the Bloombase StoreSafe and the Thales payShield beforehand. To create the signed certificate at the Thales payShield, a Security Officer will instruct the Thales payShield to generate a keypair and a Certificate Signing Request (CSR) containing the public key in PKCS#10 format, and output this to the console or HSM Manager screen. The Security Officer will have the public key signed by his/her chosen CA and return the public key certificate and CA's certificate chain to the Thales payShield. The same certificate will also be uploaded to the Bloombase StoreSafe's trust key store. The Security Office will also import the public key certificate of Bloombase StoreSafe and its associated CA's certificate chain to the Thales payShield for authentication purpose.

Notice that a connection between the Bloombase StoreSafe and the Thales payShield will fail if the Secure Host Communications session is attempted to establish using an out-of-date (i.e., expired or not-yet-valid) certificate.

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.

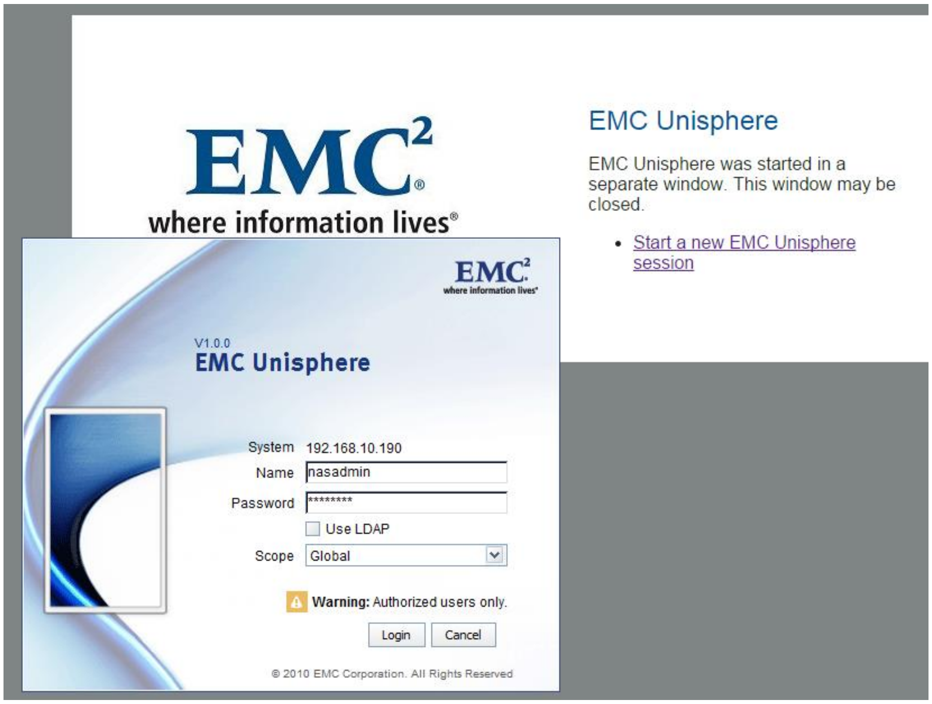


```
copyrighted and licensed pursuant to the GNU General Public License
("GPL"), a copy of which can be found in the accompanying
documentation.  Please read the GPL carefully, because by using the
Linux operating system on the EMC Celerra you agree to the terms
and conditions listed therein.

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

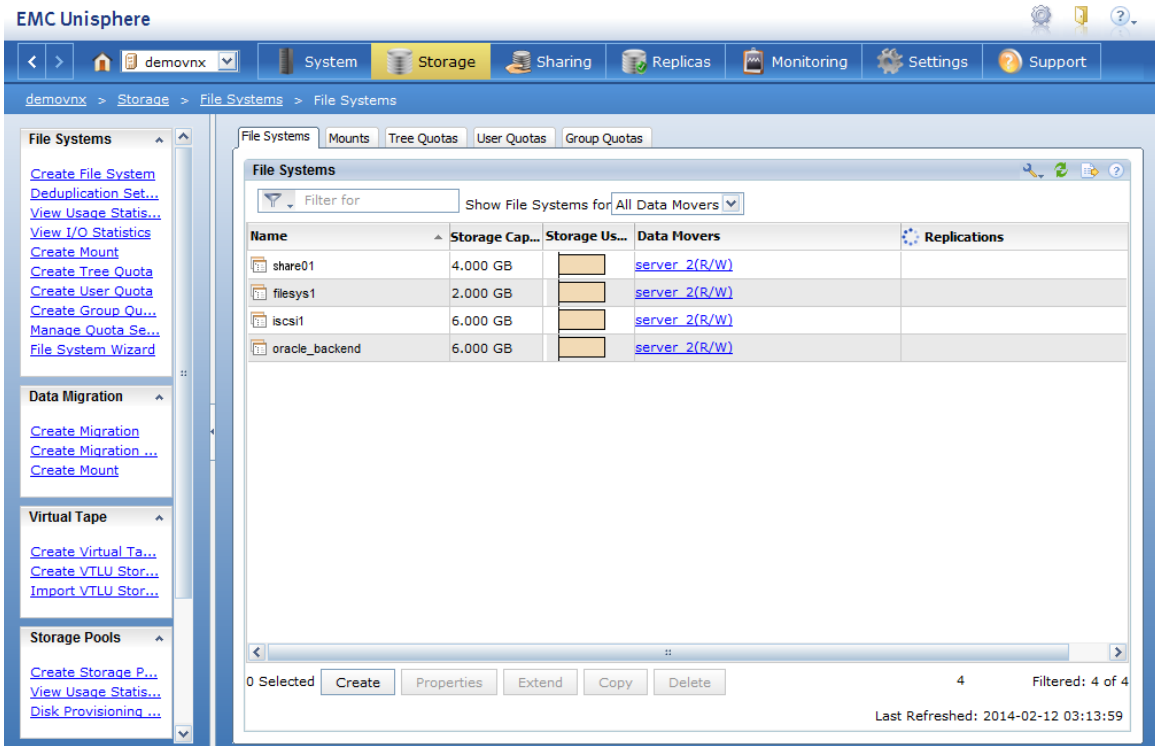
V1.0.0
EMC Unisphere

System 192.168.10.190
Name nasadmin
Password ********
□ Use LDAP
Scope Global

Warning: Authorized users only.

© 2010 EMC Corporation. All Rights Reserved

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



EMC Unisphere

demovnx > Storage > File Systems > File Systems

File Systems

Show File Systems for All Data Movers

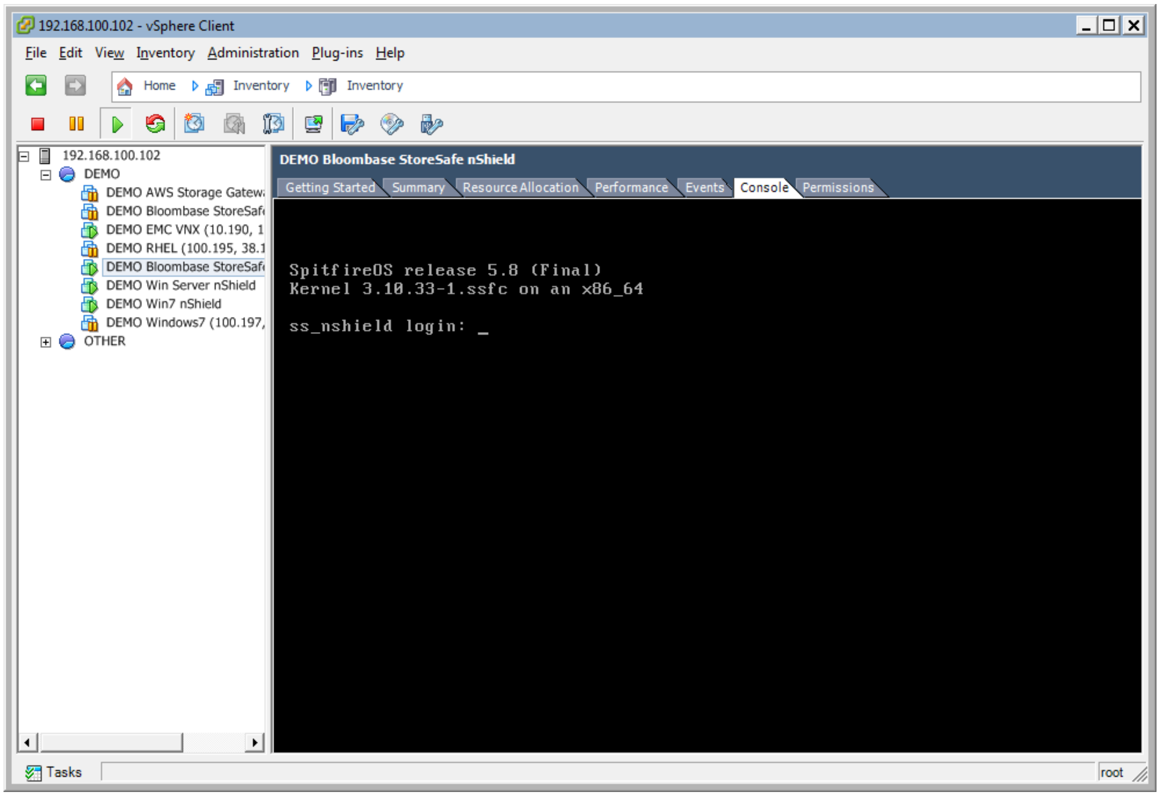
Name	Storage Cap...	Storage Us...	Data Movers	Replications
share01	4.000 GB		server_2(R/W)	
filesys1	2.000 GB		server_2(R/W)	
iscsi1	6.000 GB		server_2(R/W)	
oracle_backend	6.000 GB		server_2(R/W)	

0 Selected 4 Filtered: 4 of 4

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

Bloombase StoreSafe

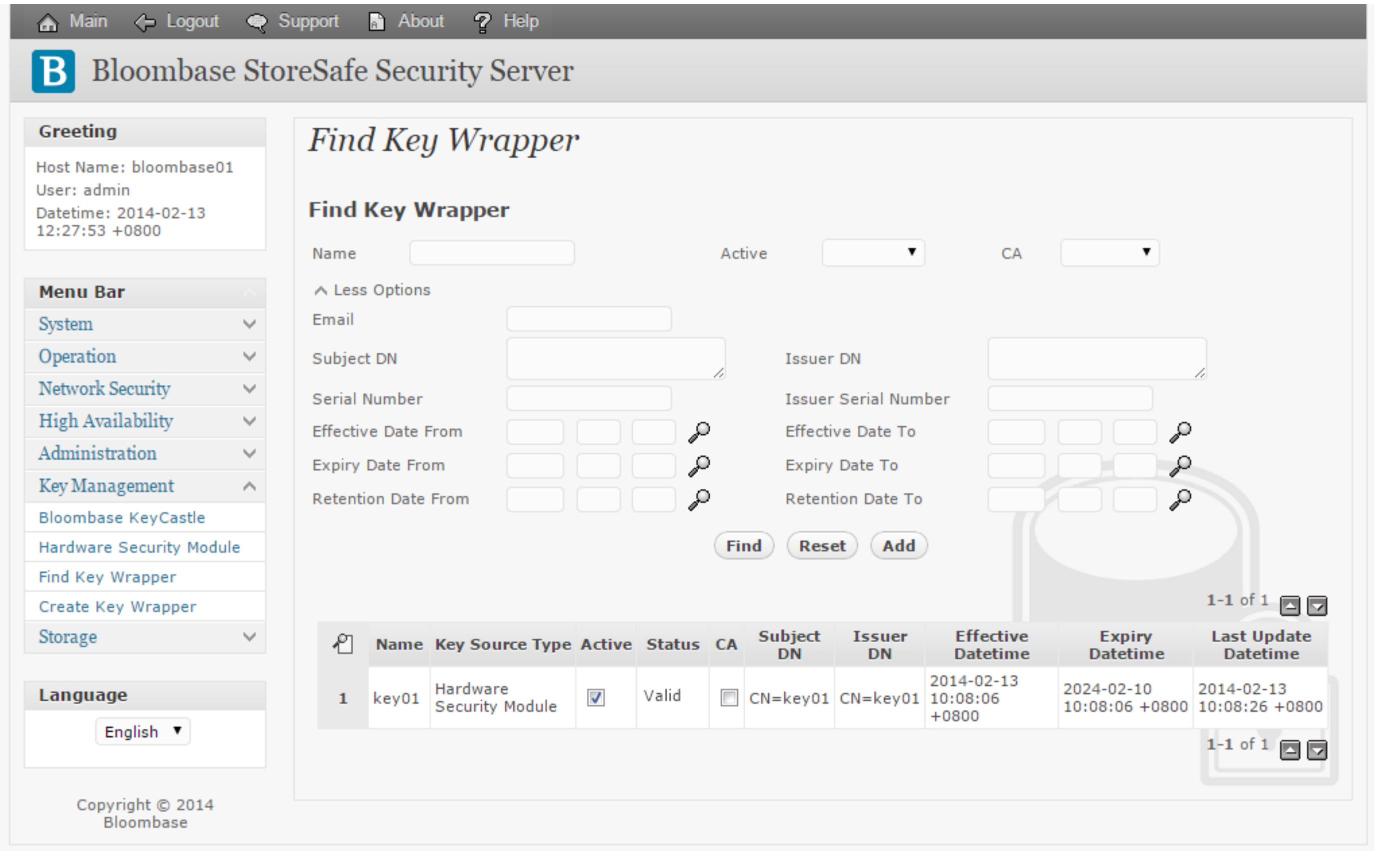
Bloombase StoreSafe delivers unified data-at-rest encryption security of block storage volumes, files, objects, sequential storage devices, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Thales payShield HSM.



```
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: 2014-02-13 12:27:53 +0800

Language: English

Find Key Wrapper

Find Key Wrapper

Name | Active | CA

Email

Subject DN | Issuer DN

Serial Number | Issuer Serial Number

Effective Date From | Effective Date To

Expiry Date From | Expiry Date To

Retention Date From | Retention Date To

1-1 of 1

	Name	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	Hardware Security Module	☑	Valid	☐	CN=key01	CN=key01	2014-02-13 10:08:06 +0800	2024-02-10 10:08:06 +0800	2014-02-13 10:08:26 +0800

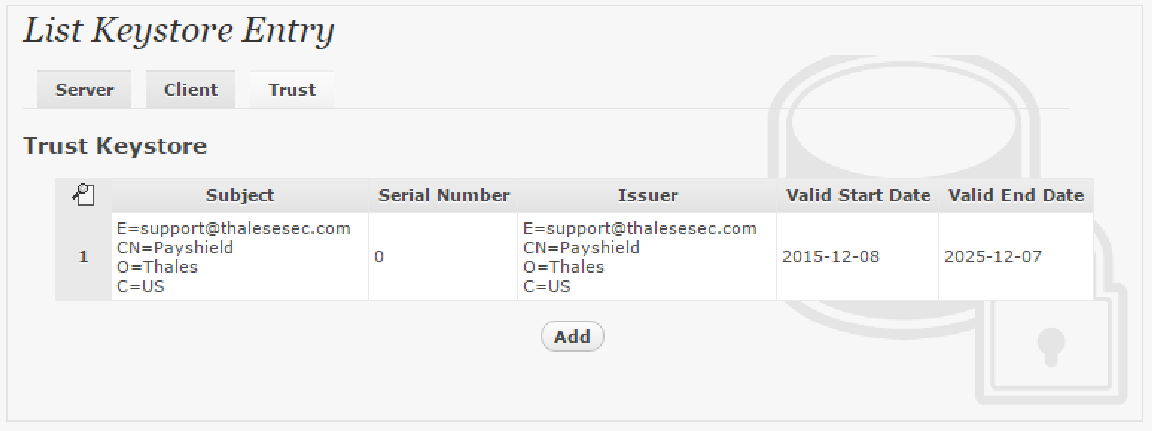
1-1 of 1

Network Security, Trust and Authentication Configuration

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

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

Thales payShield's security service is trusted by adding the certificate authority of its certificate to Bloombase StoreSafe's trust key store.

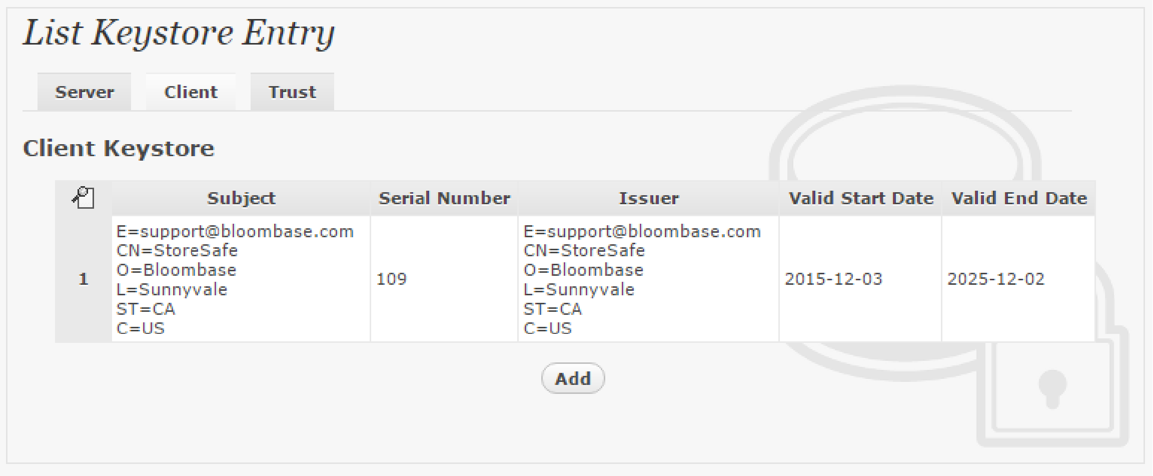


Trust Keystore

	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
1	E=support@thalesesec.com CN=Payshield O=Thales C=US	0	E=support@thalesesec.com CN=Payshield O=Thales C=US	2015-12-08	2025-12-07

Thales payShield 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 Thales payShield as a trusted credential which allows access of security services by trusted Bloombase StoreSafe instance from over remote network.



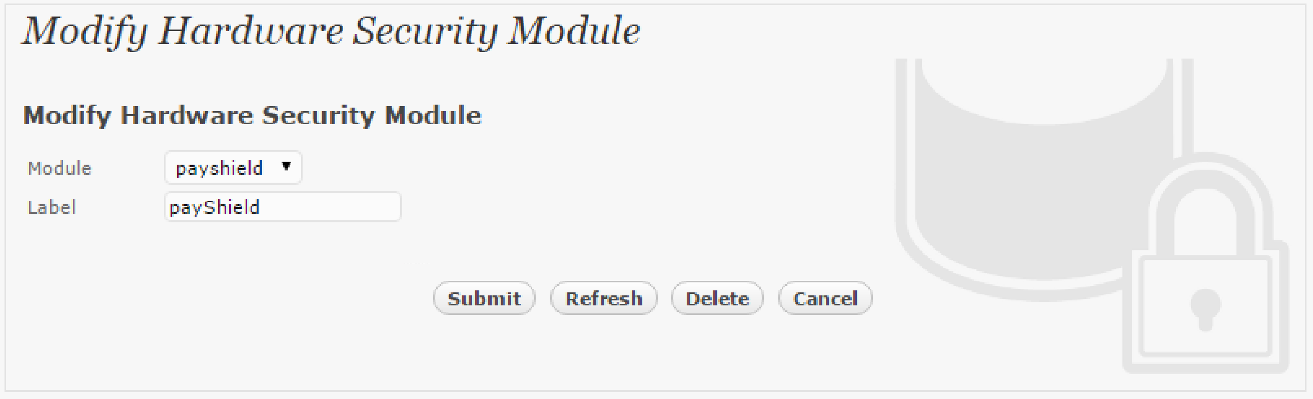
Client Keystore

	Subject	Serial Number	Issuer	Valid Start Date	Valid End Date
1	E=support@bloombase.com CN=StoreSafe O=Bloombase L=Sunnyvale ST=CA C=US	109	E=support@bloombase.com CN=StoreSafe O=Bloombase L=Sunnyvale ST=CA C=US	2015-12-03	2025-12-02

Thales payShield and Bloombase KeyCastle Integration

To enable the built-in Bloombase KeyCastle to utilize keys in the network attached Thales payShield HSM, the JAR package of the Thales payShield API, its license file, and its dependencies (in JAR format) need to be imported through Bloombase Storesafe CLI console, and the hardware security module configuration at Bloombase web management console has to be set up.

When a Thales payShield is configured at Bloombase web management console, select Module as 'payshield' which allows embedded Bloombase KeyCastle module to utilize Thales PayShield Command/Response API to access Thales payShield HSM via JCE interface.



Modify Hardware Security Module

Modify Hardware Security Module

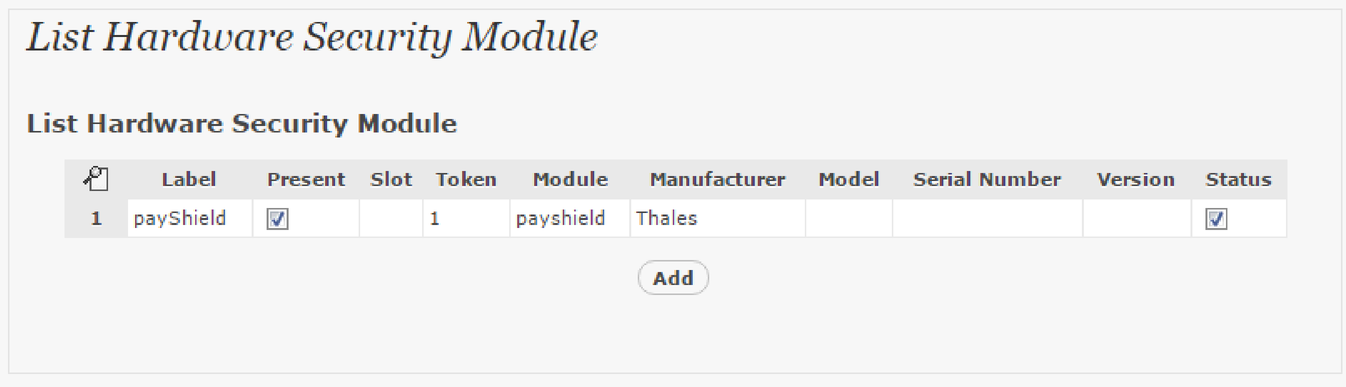
Module	payshield ▼
Label	payShield

In this scenario, the Thales payShield HSM is assigned a token label namely ‘payShield’. Different settings for connection with Thales payShield can be configured by modifying entries in Thales payShield property file

```
payment.properties
```

deployed at Bloombase StoreSafe instance.

When Thales payShield HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as ‘Active’.



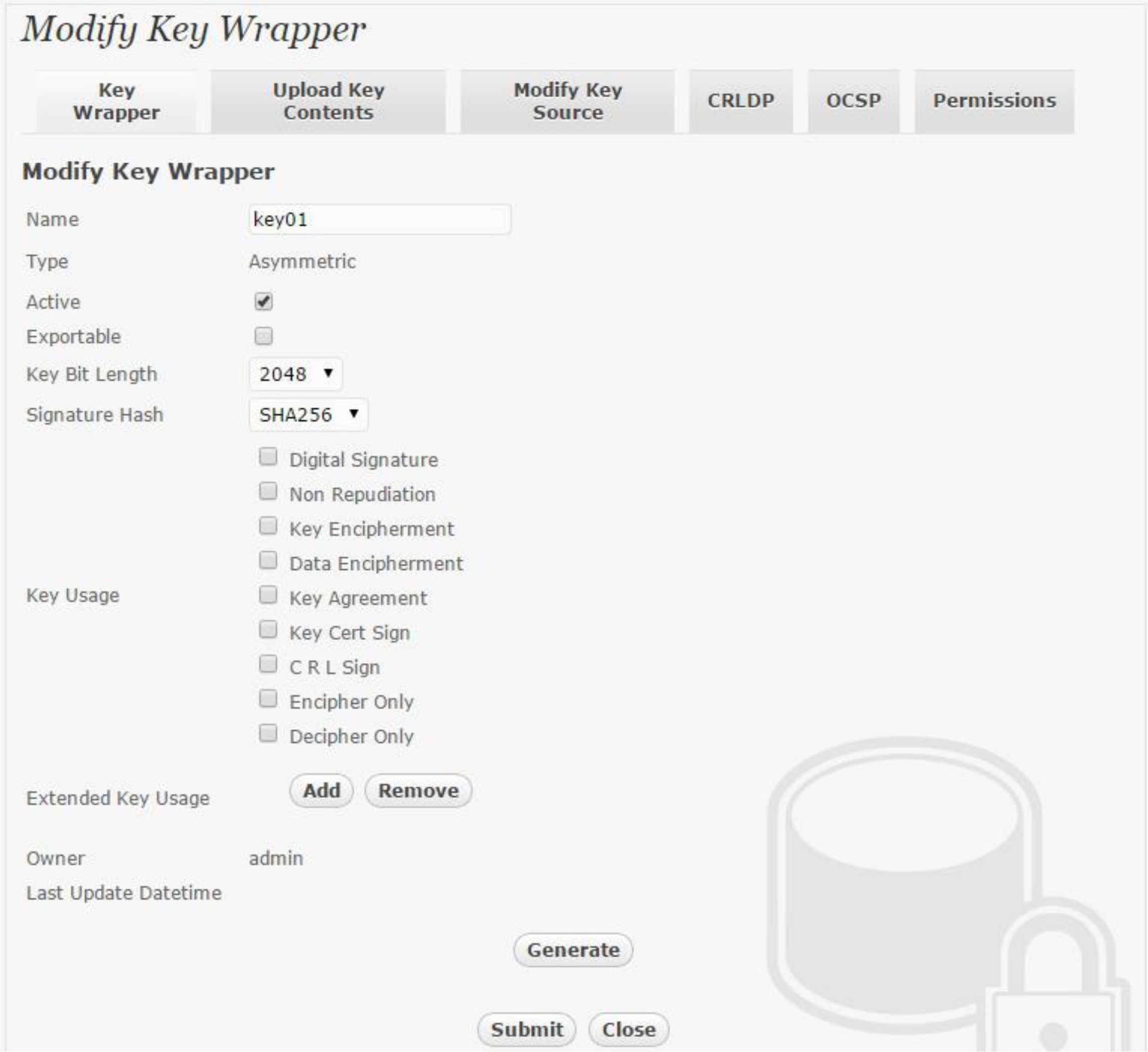
List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	payShield	☑		1	payshield	Thales				☑

Encryption Key Provisioning

Generate encryption key with name ‘key01’ in bundled Bloombase KeyCastle key life-cycle management tool



Modify Key Wrapper

Name: key01

Type: Asymmetric

Active: ☑

Exportable: □

Key Bit Length: 2048

Signature Hash: SHA256

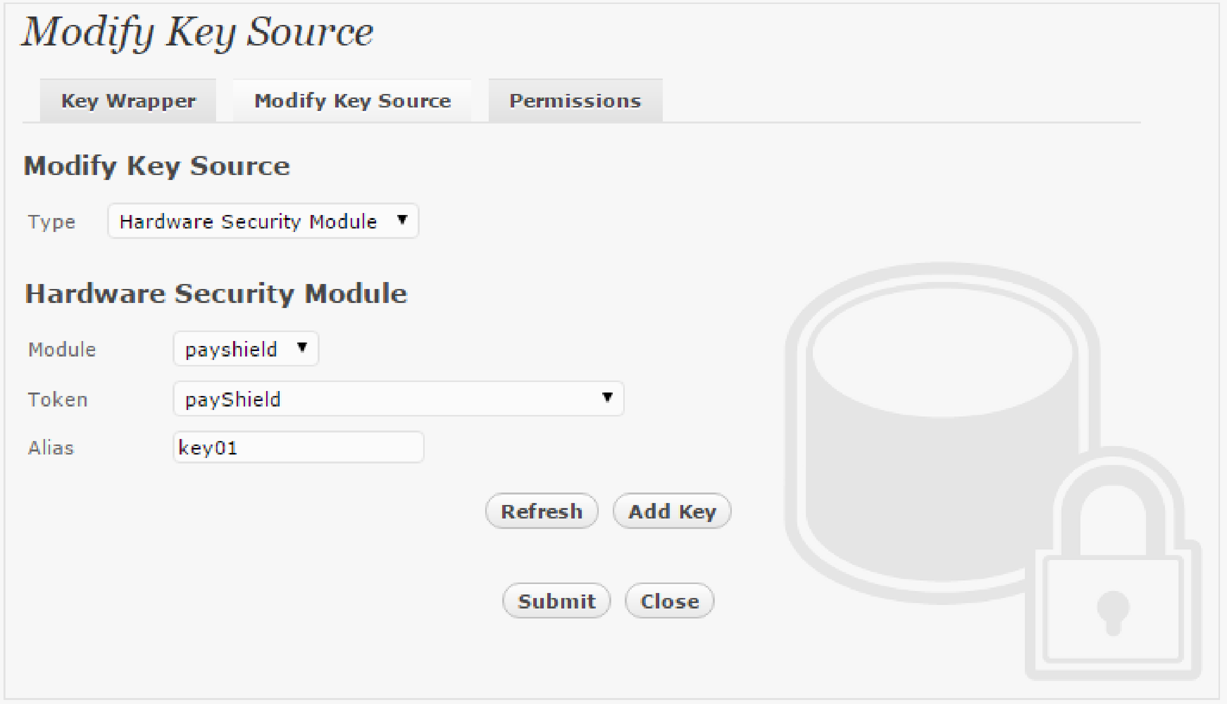
Key Usage:
- □ Digital Signature
- □ Non Repudiation
- □ Key Encipherment
- □ Data Encipherment
- □ Key Agreement
- □ Key Cert Sign
- □ C R L Sign
- □ Encipher Only
- □ Decipher Only

Extended Key Usage

Owner: admin

Last Update Datetime

To generate key in attached Thales payShield HSM, select Key Source Type as “Hardware Security Module”, Module as “payshield” and the assigned HSM token label, in this case “payShield”. Ensure you import a key from the HSM before you submit the key wrapper.



Modify Key Source

Modify Key Source

Type: Hardware Security Module

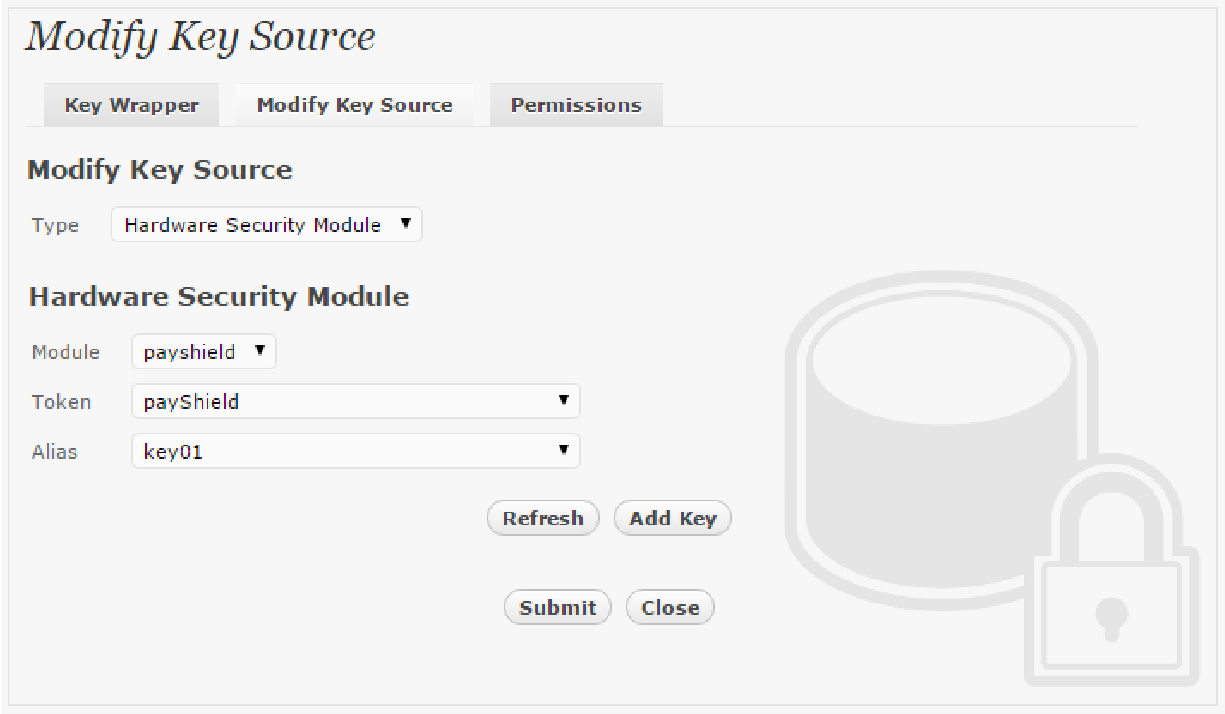
Hardware Security Module

Module: payshield

Token: payShield

Alias: key01

Or if key already exists, simply choose from the pull down box.



Modify Key Source

Modify Key Source

Type: Hardware Security Module

Hardware Security Module

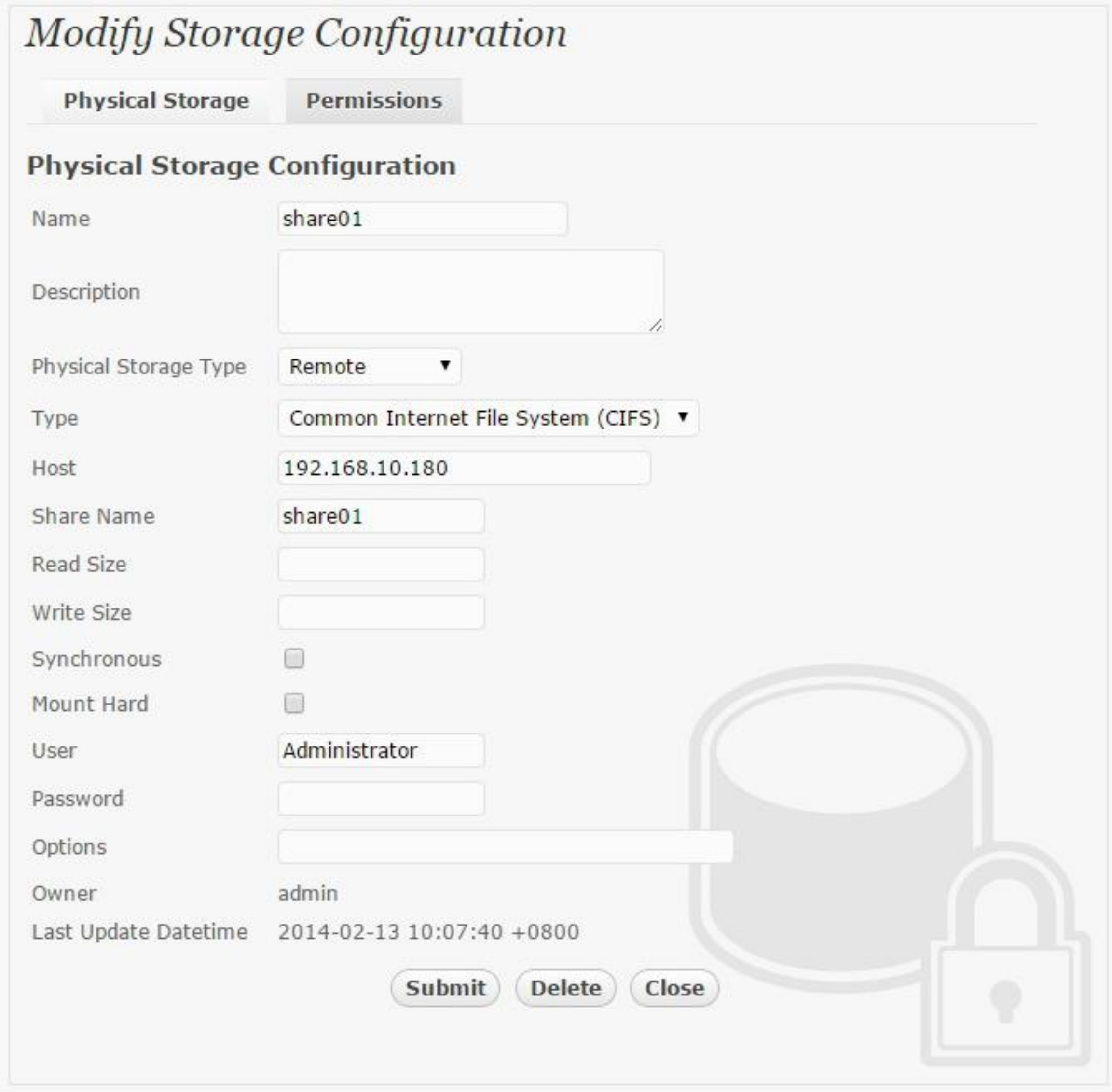
Module: payshield

Token: payShield

Alias: key01

Backend Physical Storage Configuration

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



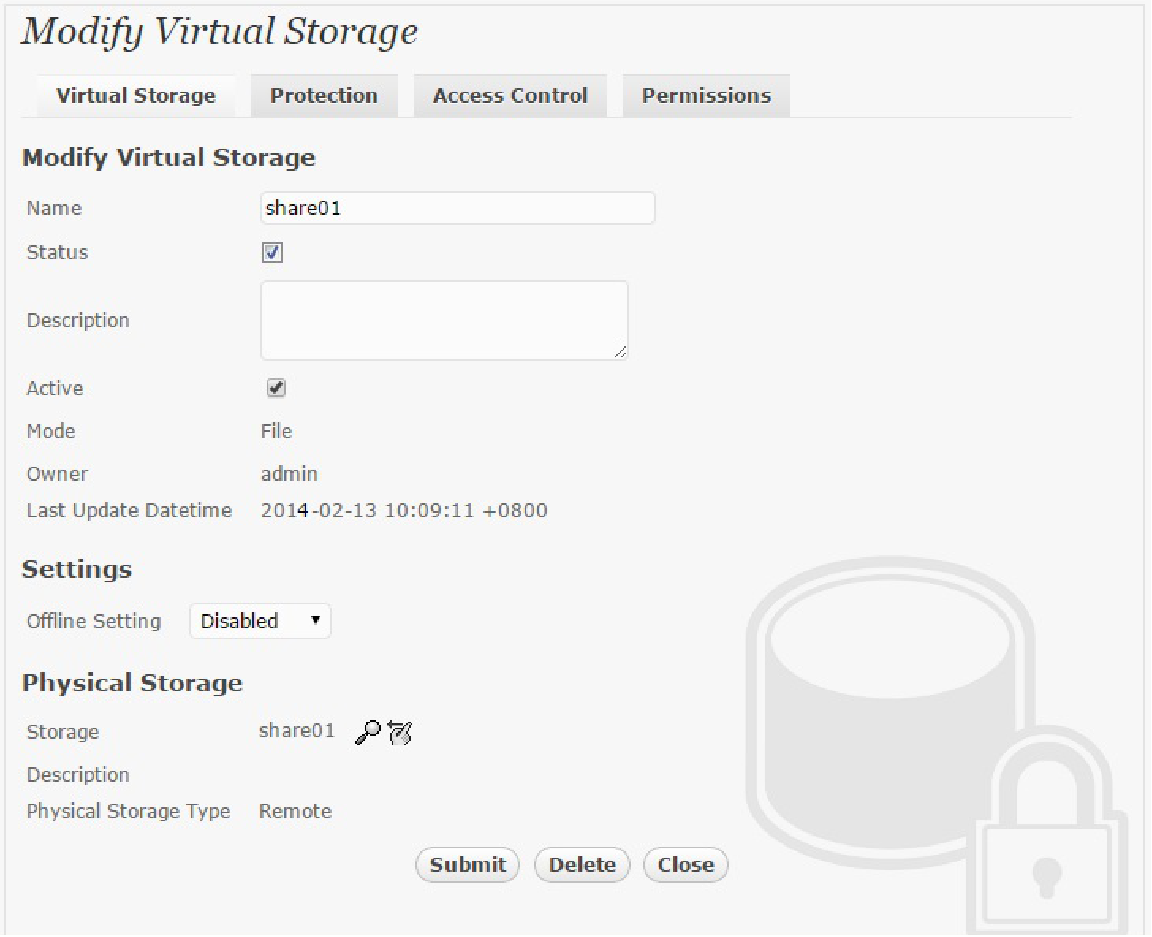
Modify Storage Configuration

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

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

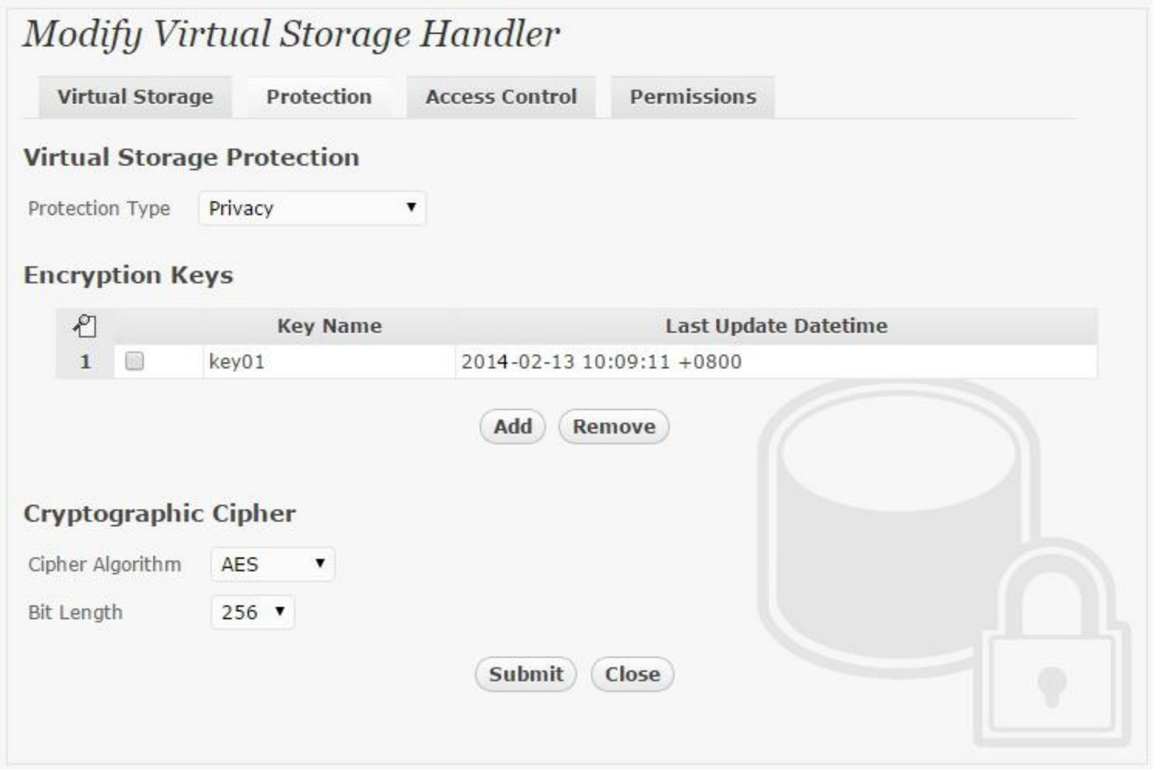
Settings

Offline Setting: Disabled

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as ‘Privacy’ and secure the backend EMC VNX storage using AES 256-bit encryption and encryption key ‘key01’ managed at Thales payShield HSM.



Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

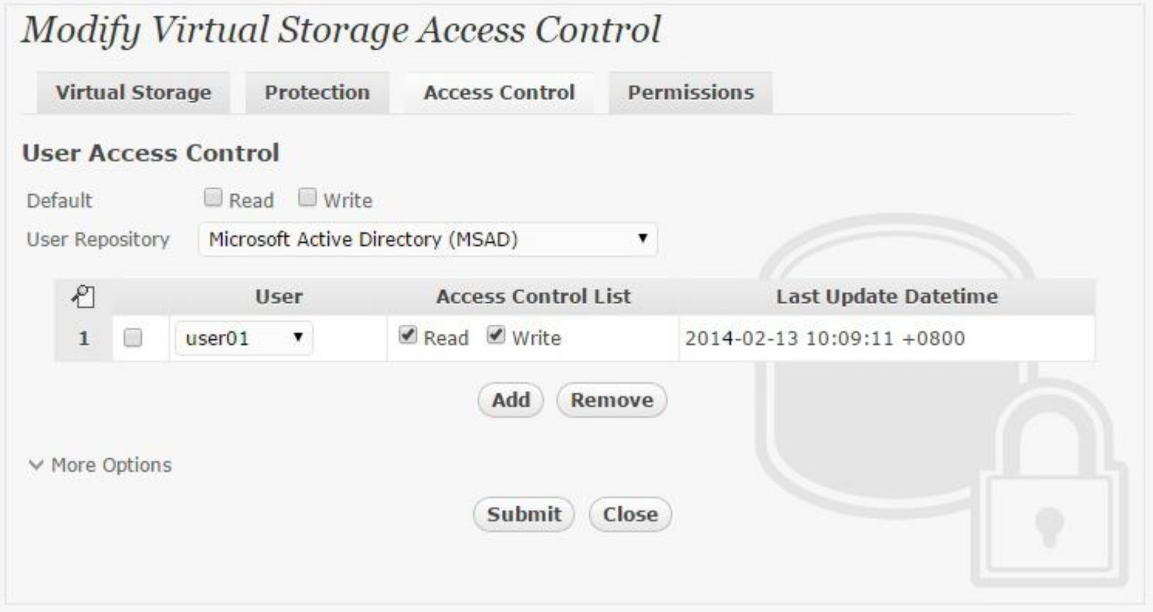
		Key Name	Last Update Datetime
1	□	key01	2014-02-13 10:09:11 +0800

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

Hardware security module

- Thales payShield 9000

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	• Thales payShield 9000
	Red Hat Enterprise Linux (RHEL)	• Thales payShield 9000
	SUSE Linux Enterprise Server (SLES)	• Thales payShield 9000
	Oracle Solaris	• Thales payShield 9000
	IBM AIX	• Thales payShield 9000
	HP-UX	• Thales payShield 9000

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 payShield 9000, https://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules/payment-hsms/payshield-9000
4. Bloombase Thales ASAP partner profile, https://www.thales-esecurity.com/partners/technology-partners/bloombase