interopLab

Interoperability of Bloombase StoreSafe and Ultra Electronics AEP Keyper for Data-at-Rest Encryption

April 2016

BLOOMBASE®

Executive Summary

Ultra Electronics AEP Keyper 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 Ultra Electronics AEP Keyper 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 Ultra Electronics AEP Keyper powered Bloombase StoreSafe with NetApp FAS unified storage system as backend storage.

Document No.: BLBS-TN-Bloombase-StoreSafe-Ultra-Electronics-AEP-Keyper-Interoperability-USLET-EN-R0.92

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Ultra Electronics AEP Keyper 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 Ultra Electronics AEP Keyper
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

Assumptions

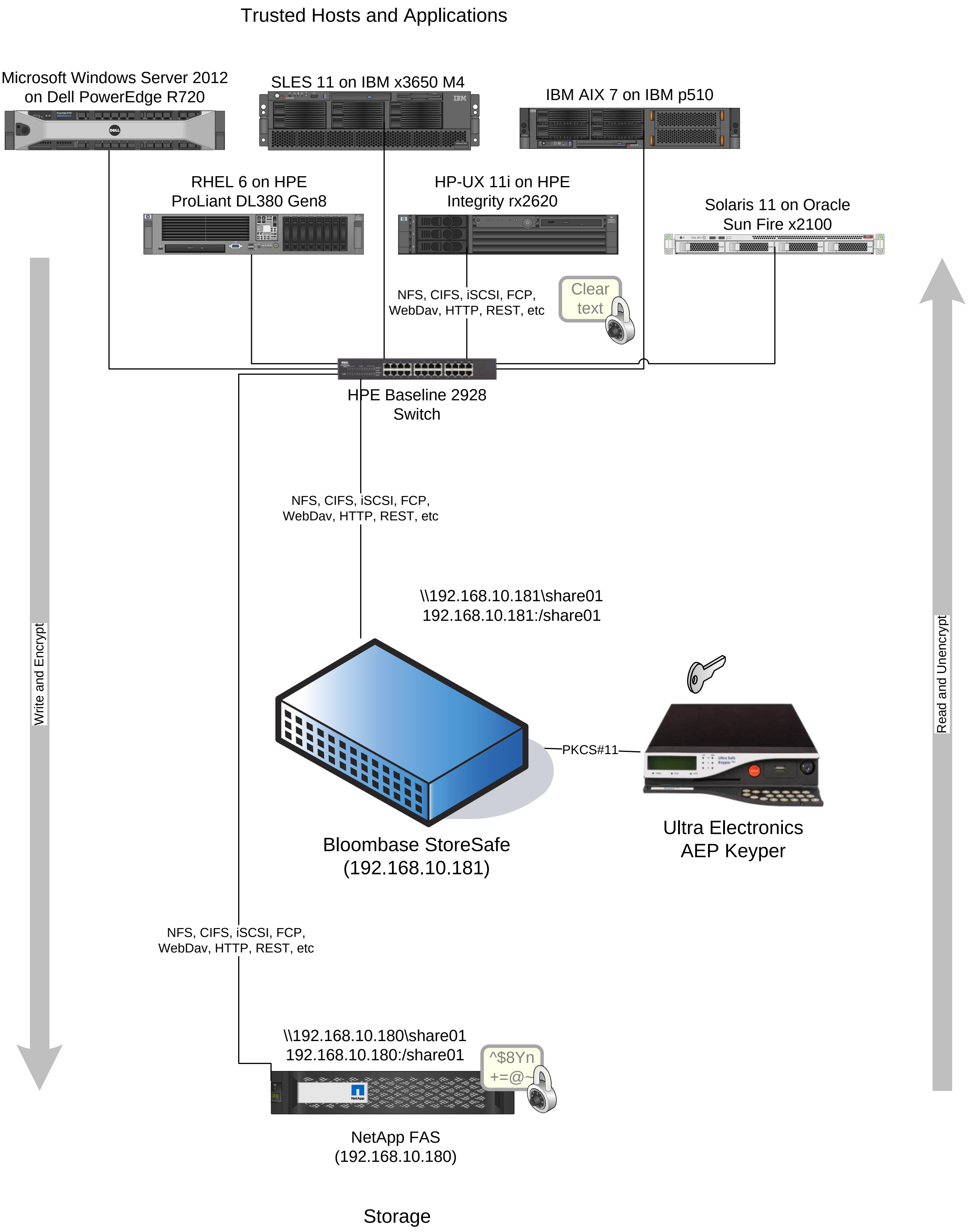
This document describes interoperability testing of Ultra Electronics AEP Keyper with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Ultra Electronics AEP Keyper, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX 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 Ultra Electronics AEP Keyper 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 Ultra Electronics AEP Keyper 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 and 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
PKCS#11
Bloombase StoreSafe (192.168.10.181)
Ultra Electronics AEP Keyper
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn +=@~
NetApp FAS (192.168.10.180)
Storage
Write and Encrypt
Read and Unencrypt

Hardware Security Module

Hardware Security Module	Ultra Electronics AEP Keyper

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 7
Keyper Client Software Package	PKCS11 API v5.05
Server	VMware Virtual Machine (VM) on VMware ESXi 5.5
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	NetApp FAS 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

Ultra Electronics AEP Keyper

Ultra Electronics AEP Keyper range of HSMs provides maximum-security key generation, key storage and key management to support a broad range of application and infrastructure security requirements. Typical applications include digital identity, PKI, DNSSEC, code signing, SSL/TLS VPN authentication, database encryption and digital rights managements (DRM). AEP Keyper hardware security modules are the only network-attached HSMs to employ FIPS 140-2 Level 4 technology, where the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the ability of detecting and responding to all unauthorized attempts at physical access. The key management and cryptographic functionalities provided by Ultra Electronics AEP Keyper are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

Ultra Electronics AEP Keyper Configurations

Assume Ultra Electronics AEP Keyper is configured with IP 192.168.10.50 and netmask 255.255.255.0 through the Keyper's front panel.

To configure Ultra Electronics AEP Keyper, install the configuration softwares (`displaytoken` and `inittoken,` located under `/mnt/cdrom/Software/PKCS11_vX.YY/Linux_x64/` of the CDROM supplied with the Keyper) on Bloombase StoreSafe, and connect StoreSafe to the network of the Ultra Electronics AEP Keyper.

To communicate with Keyper, edit `/etc/hosts` of StoreSafe with the following entry

```
<IP of the Keyper HSM>  HSM
```

A `machine` file may be used if non-default settings are to be configured with Ultra Electronics AEP Keyper. We first setup the Keyper environment variable as

```
export KEYPER_LIBRARY_PATH=<path to machine file>
```

An example of the `machine` file is shown below,

```
SlotList
{
NumSlots:REG_DWORD:1
SlotA:REG_SZ:HSMServerSlot
SlotA-ID:REG_DWORD:0
NumConnections:REG_DWORD:6
}
SlotA
{
TokenStore:REG_SZ:/opt/Keyper/token/storeA
Location:REG_SZ:<IP of the Keyper HSM>:<port>
Timeout:REG_DWORD:5000
}
Logging
{
Log:REG_DWORD:2
LogErrors:REG_DWORD:2
OutputFile:REG_SZ:/opt/Keyper/log/aep.log
ErrorLogFile:REG_SZ:/opt/Keyper/log/aep-err.log
}
```

Initialize Ultra Electronics AEP Keyper and Configure PKCS#11

Initializing the Keyper, with `inittoken`, allows the PKCS#11 user's PIN to be setup, and also creates the key mapping files `keymap.db` and `keymap.config.db`.

To initialize the Keyper, run `inittoken` with the following four items of information ready,

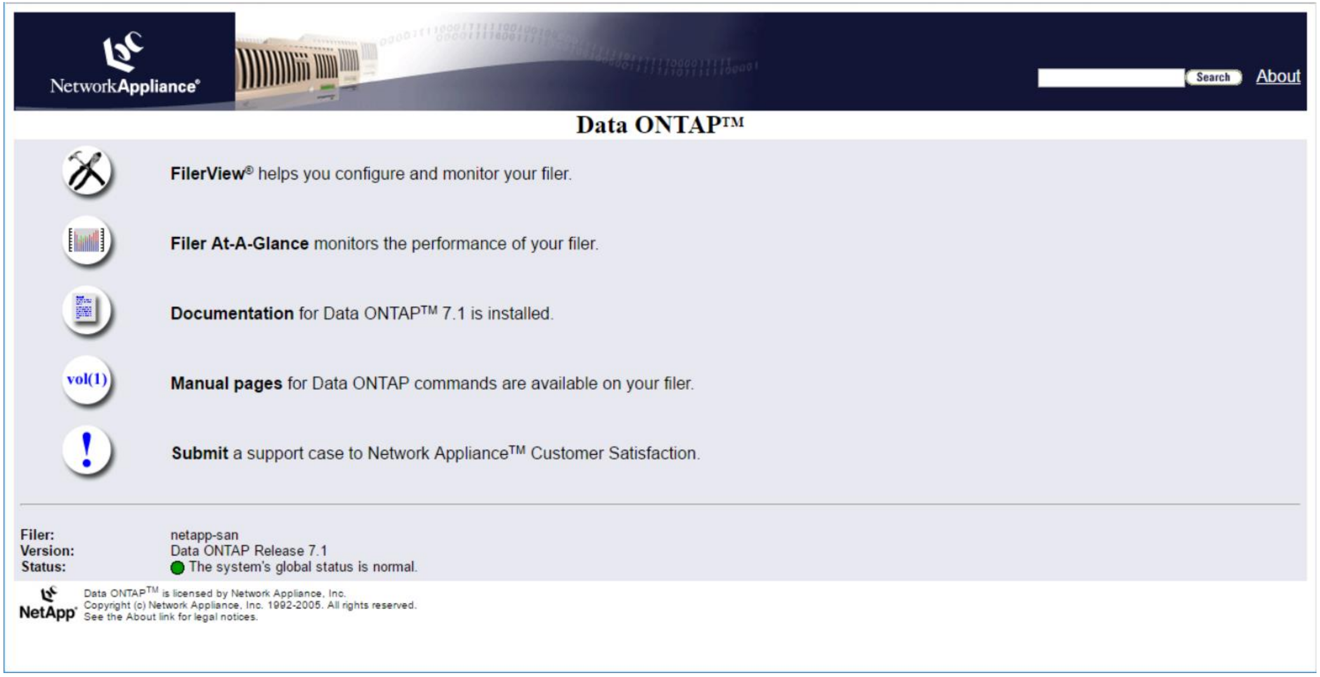
- Slot number
- Token label
- PKCS#11 User PIN
- PKCS#11 Security Officer PIN

Once the Keyper HSM is initialized, the PINs will be encrypted and together with the token label written to the `keymap.config.db` file. An empty `keymap.db` will then be created. It is advisable to backup the `keymap.config.db` file at this point.

The Keyper is now initialized and ready for use.

NetApp FAS

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



Data ONTAP™

FilerView® helps you configure and monitor your filer.

Filer At-A-Glance monitors the performance of your filer.

Documentation for Data ONTAP™ 7.1 is installed.

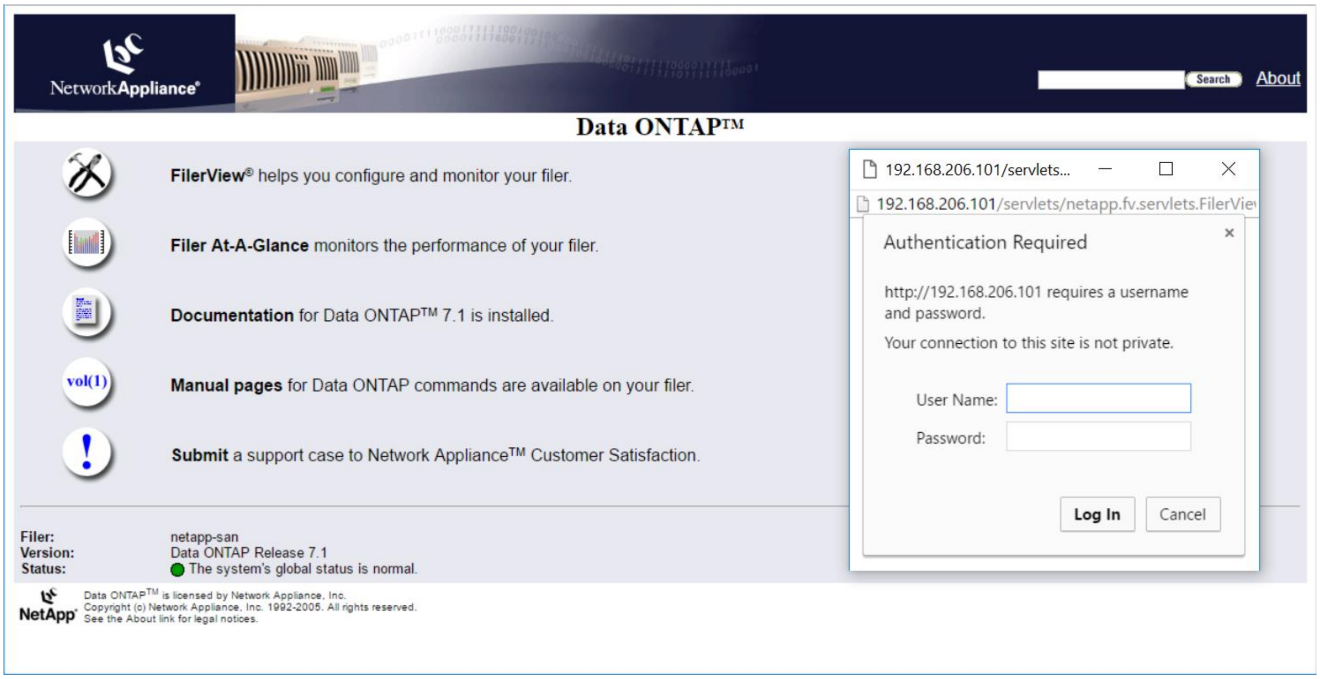
Manual pages for Data ONTAP commands are available on your filer.

Submit a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san
Version: Data ONTAP Release 7.1
Status: ● The system's global status is normal.

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc.
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.
See the About link for legal notices.

NetApp FAS is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FC, FCoE, iSCSI, etc.



Data ONTAP™

FilerView® helps you configure and monitor your filer.

Filer At-A-Glance monitors the performance of your filer.

Documentation for Data ONTAP™ 7.1 is installed.

Manual pages for Data ONTAP commands are available on your filer.

Submit a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san
Version: Data ONTAP Release 7.1
Status: ● The system's global status is normal.

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc.
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.
See the About link for legal notices.

192.168.206.101/servlets/netapp.fv.servlets.FilerVie

Authentication Required

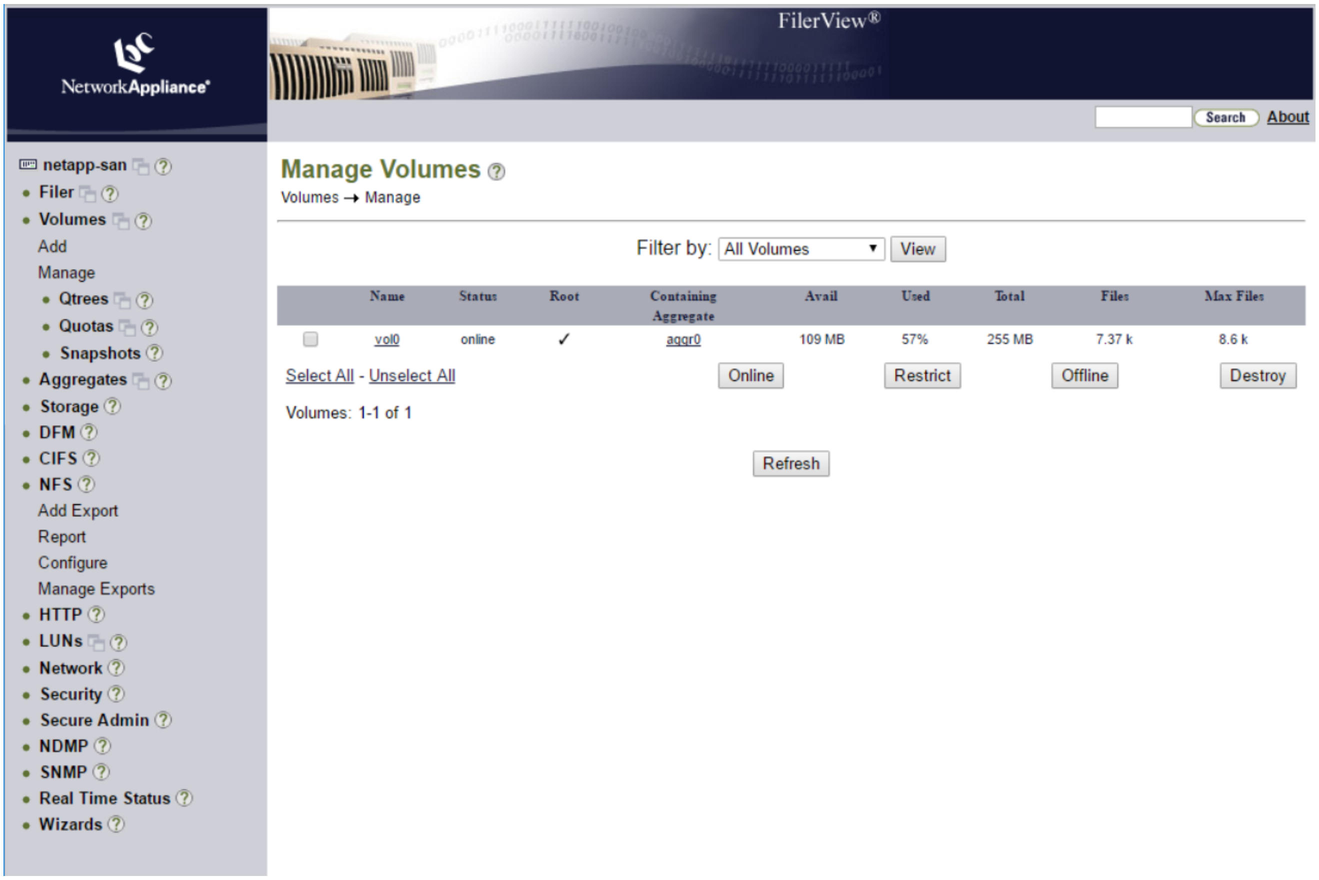
http://192.168.206.101 requires a username and password.

Your connection to this site is not private.

User Name:

Password:

CIFS and NFS storage resources are provisioned on NetApp FAS to be used in this testing.



Manage Volumes

Volumes → Manage

Filter by: All Volumes ▾ View

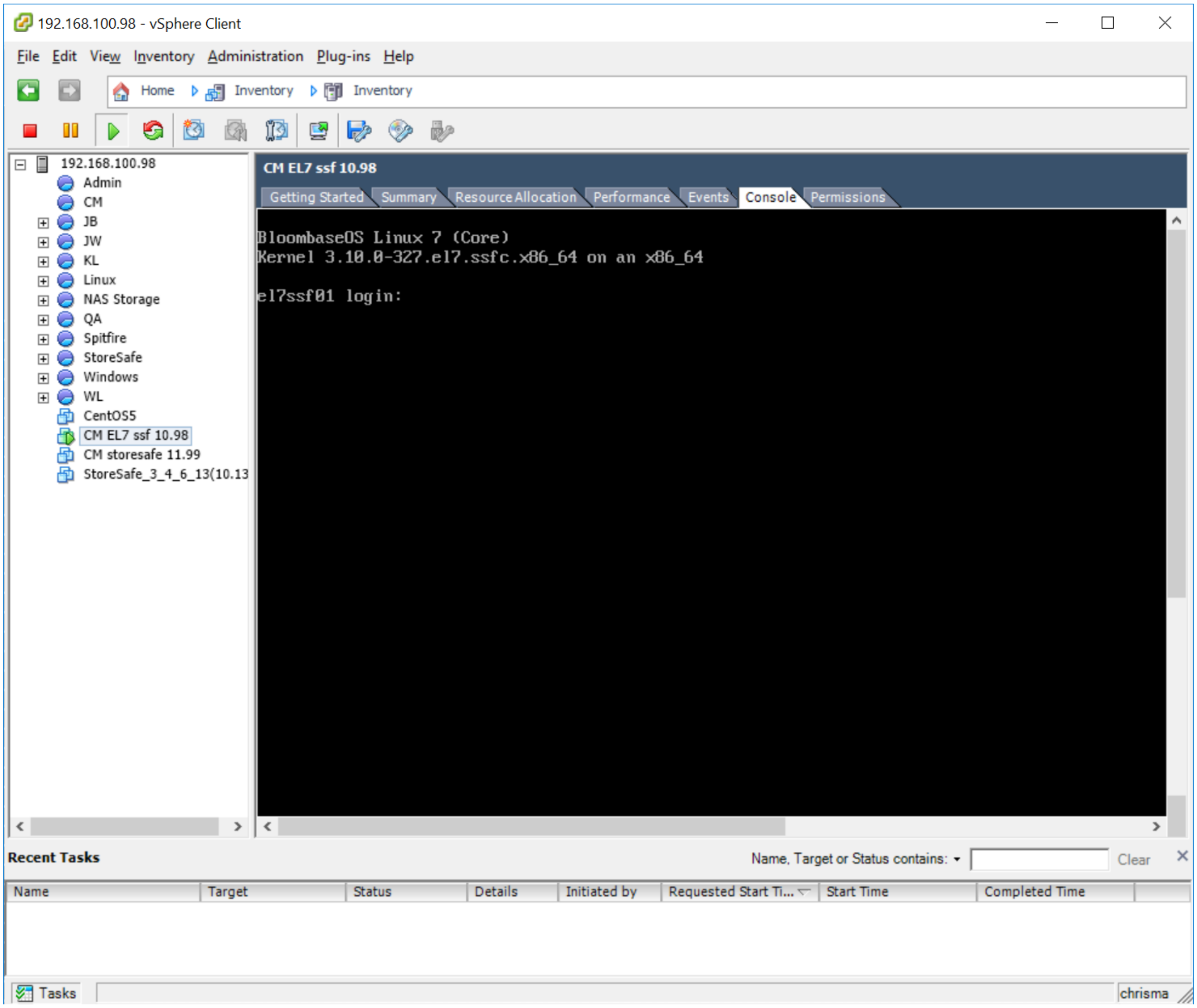
	Name	Status	Root	Containing Aggregate	Avail	Used	Total	Files	Max Files
□	vol0	online	✓	aggr0	109 MB	57%	255 MB	7.37 k	8.6 k

Select All - Unselect All

Volumes: 1-1 of 1

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 Ultra Electronics AEP Keyper HSM.



```
BloombaseOS Linux 7 (Core)
Kernel 3.10.0-327.el7.ssfc.x86_64 on an x86_64

el7ssf01 login:
```

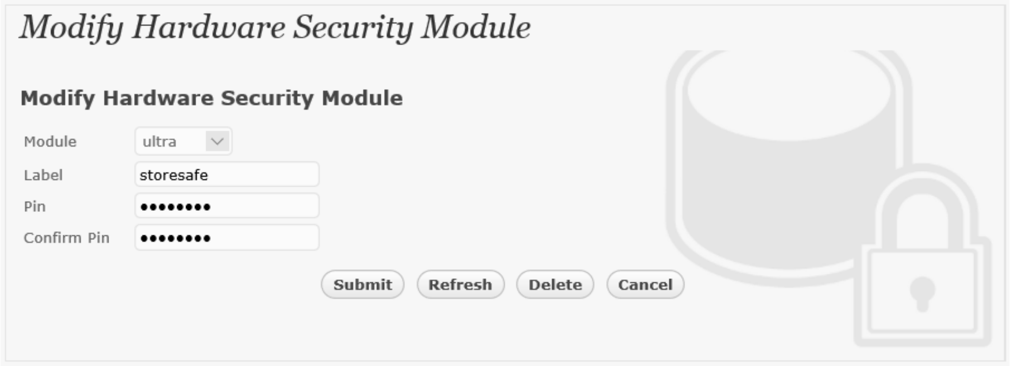
Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware ESXi.

Network Security, Trust and Authentication Configuration

In this interoperability test effort, Bloombase StoreSafe serves as the user of Ultra Electronics AEP Keyper for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Ultra Electronics AEP Keyper through the specification of PKCS#11 user pin.

Ultra Electronics AEP Keyper and Bloombase KeyCastle Integration

To configure Ultra Electronics AEP Keyper HSM at Bloombase web management console, select Module as 'ultra' which allows the embedded Bloombase KeyCastle module to utilize Ultra Electronics AEP Keyper driver to access Ultra Electronics AEP Keyper over standard PKCS#11 protocol.

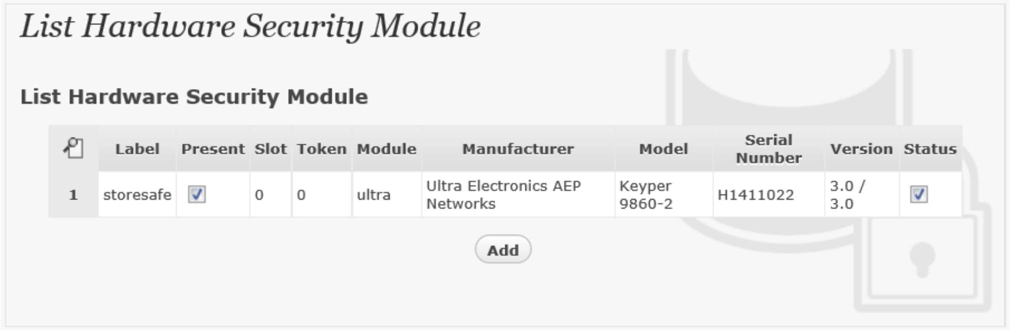


Modify Hardware Security Module

Modify Hardware Security Module

Module	ultra
Label	storesafe
Pin	••••••••
Confirm Pin	••••••••

In this scenario, use the Ultra Electronics AEP Keyper HSM with a token label 'storesafe' and user pin as Pin. When Ultra Electronics AEP Keyper HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as 'Active'.



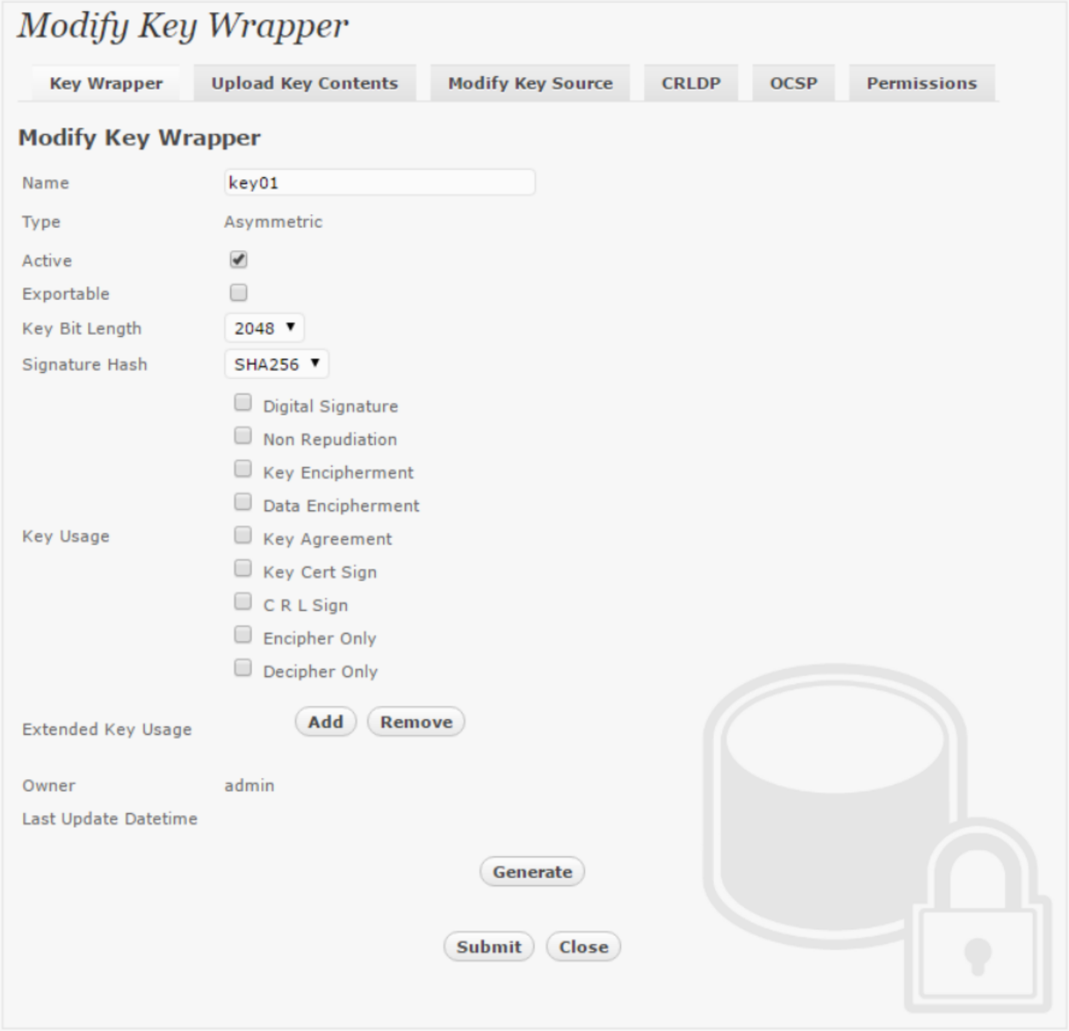
List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	storesafe	☑	0	0	ultra	Ultra Electronics AEP Networks	Keyper 9860-2	H1411022	3.0 / 3.0	☑

Encryption Key Provisioning

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

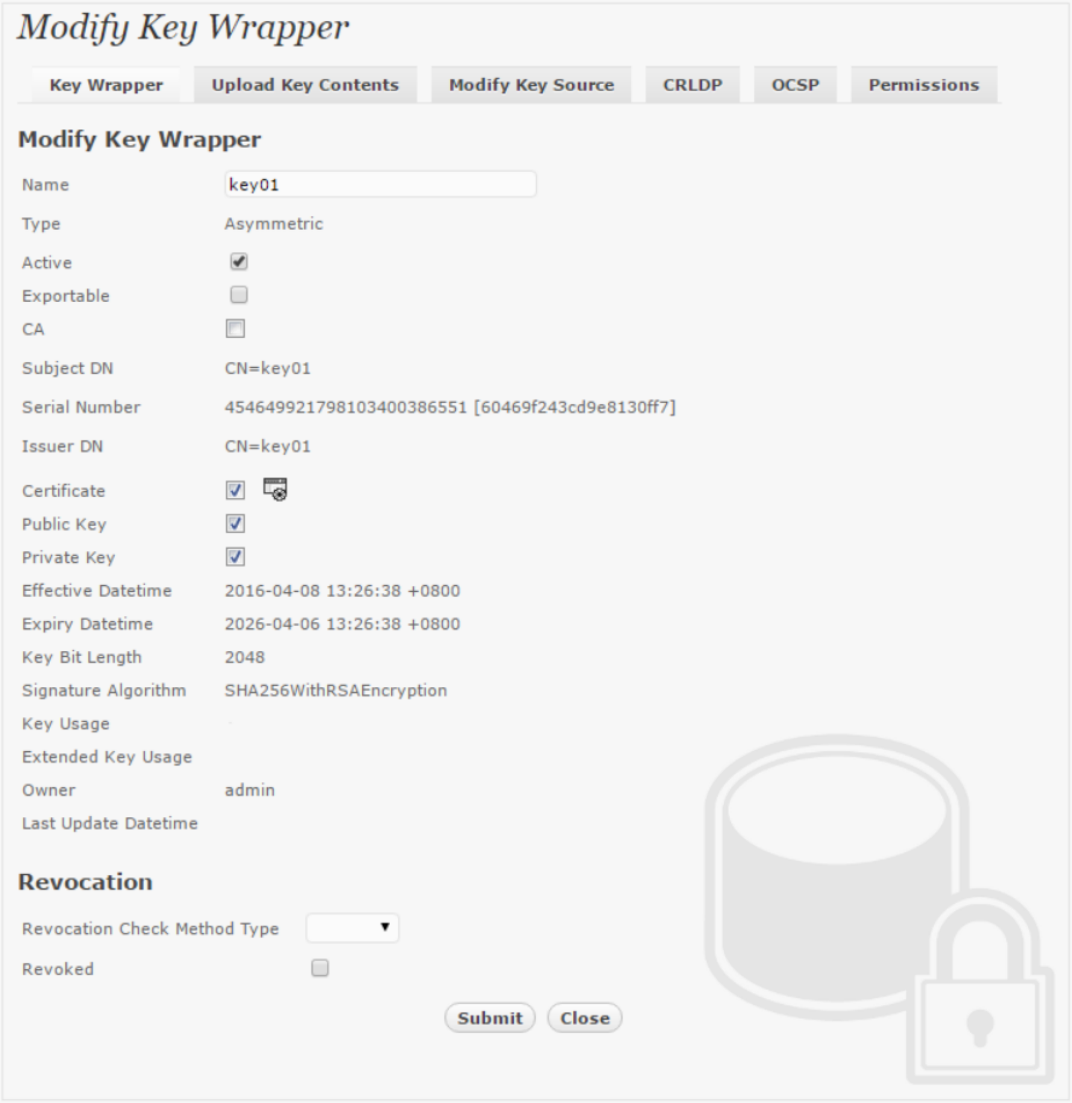


Modify Key Wrapper

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 Ultra Electronics AEP Keyper HSM, input details of the key and click ‘Generate’.



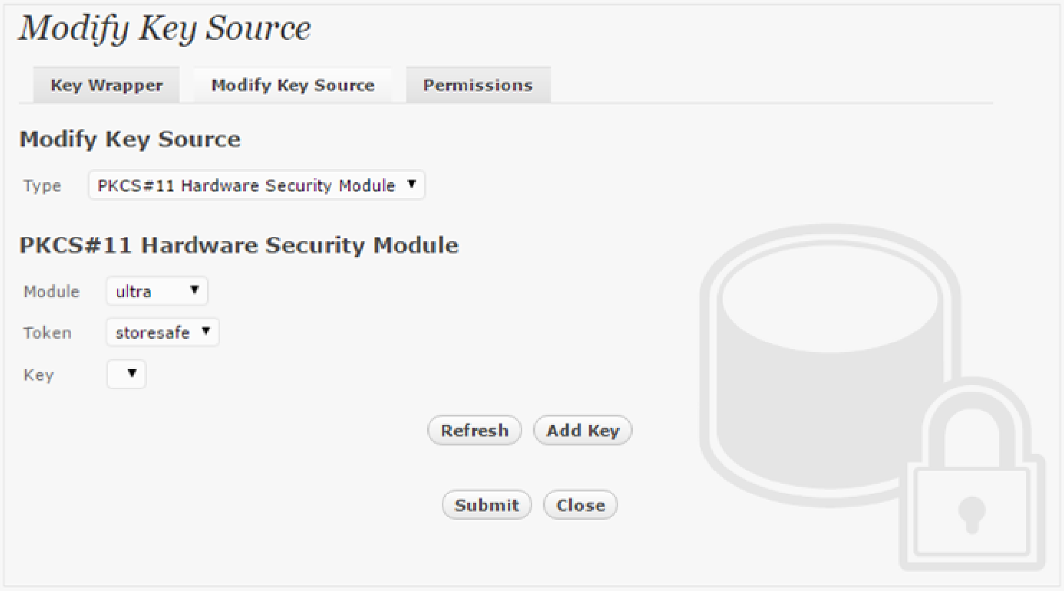
Modify Key Wrapper

Name	key01
Type	Asymmetric
Active	☑
Exportable	□
CA	□
Subject DN	CN=key01
Serial Number	454649921798103400386551 [60469f243cd9e8130ff7]
Issuer DN	CN=key01
Certificate	☑
Public Key	☑
Private Key	☑
Effective Datetime	2016-04-08 13:26:38 +0800
Expiry Datetime	2026-04-06 13:26:38 +0800
Key Bit Length	2048
Signature Algorithm	SHA256WithRSAEncryption
Key Usage	
Extended Key Usage	
Owner	admin
Last Update Datetime	

Revocation

Revocation Check Method Type	▾
Revoked	□

Then click 'Modify Key Source' and select Key Source Type as 'PKCS#11 Hardware Security Module', Module as 'ultra' and the assigned HSM token label, in this case 'storesafe'.



Modify Key Source

Modify Key Source

Type: PKCS#11 Hardware Security Module

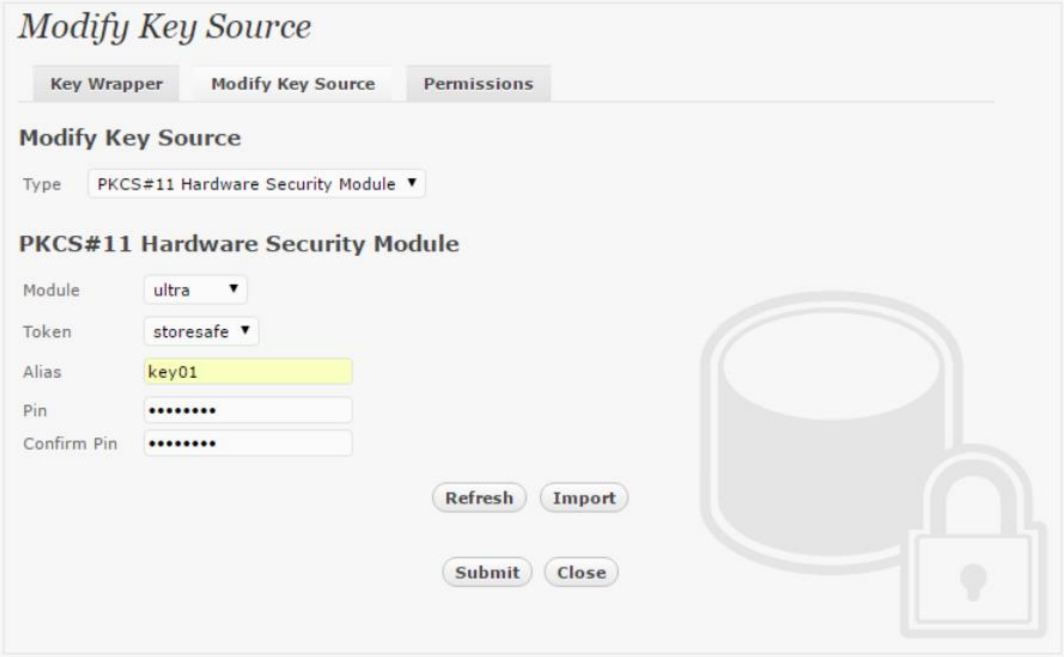
PKCS#11 Hardware Security Module

Module: ultra

Token: storesafe

Key:

Select 'Add Key' to input a unique alias as the key name, and input the user pin of the token to 'Import' a new key from the HSM before you submit the key wrapper.



Modify Key Source

Modify Key Source

Type: PKCS#11 Hardware Security Module

PKCS#11 Hardware Security Module

Module: ultra

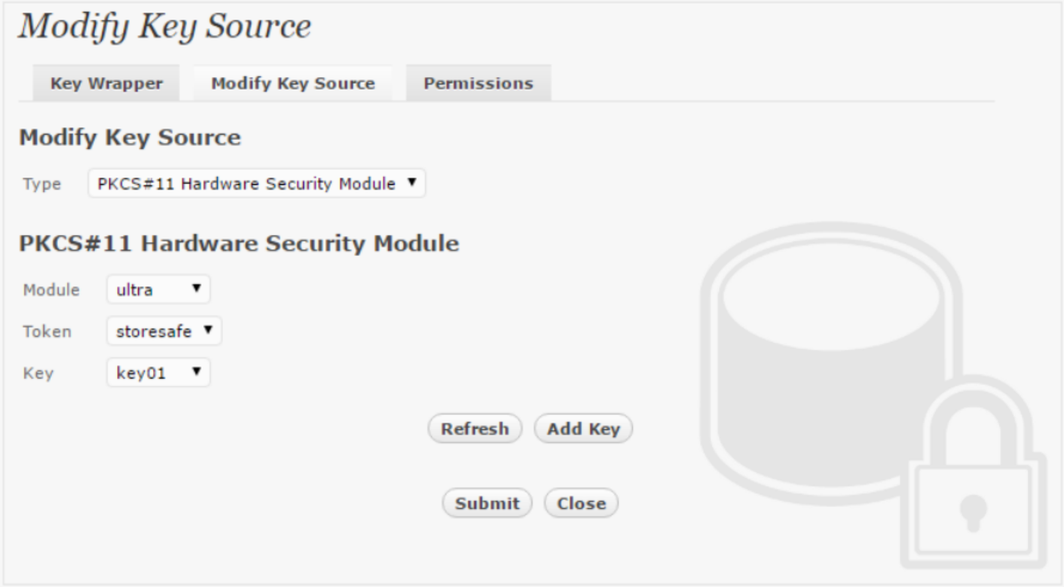
Token: storesafe

Alias: key01

Pin: ••••••••

Confirm Pin: ••••••••

Or if key already exists in the HSM, simply choose from the pull down box and click 'Add Key'.



Modify Key Source

Modify Key Source

Type: PKCS#11 Hardware Security Module

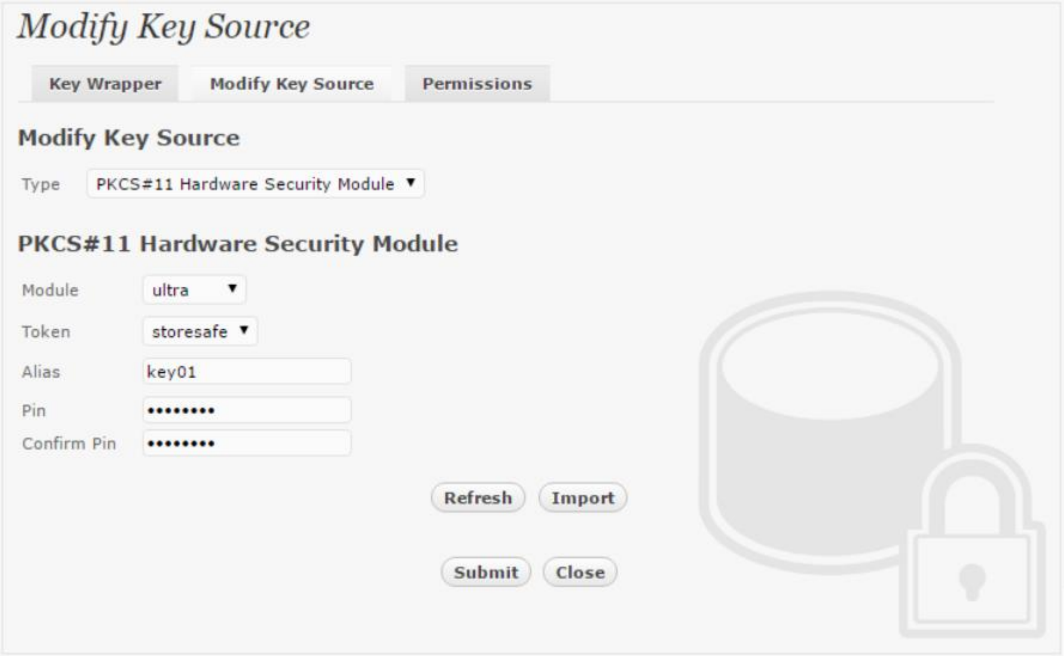
PKCS#11 Hardware Security Module

Module: ultra

Token: storesafe

Key: key01

And input the user pin of the token before submit the key wrapper.



Modify Key Source

Modify Key Source

Type: PKCS#11 Hardware Security Module

PKCS#11 Hardware Security Module

Module: ultra

Token: storesafe

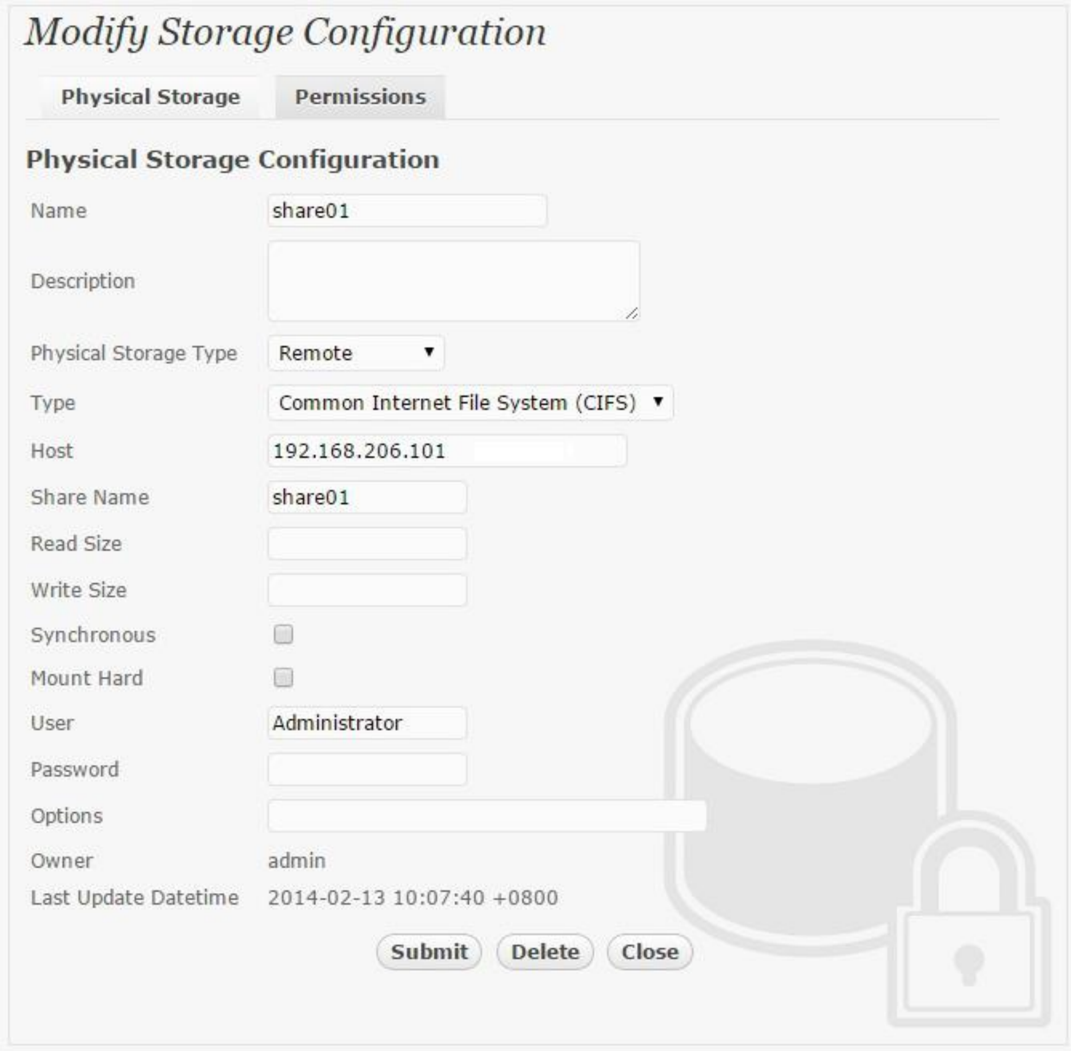
Alias: key01

Pin: ••••••••

Confirm Pin: ••••••••

Backend Physical Storage Configuration

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



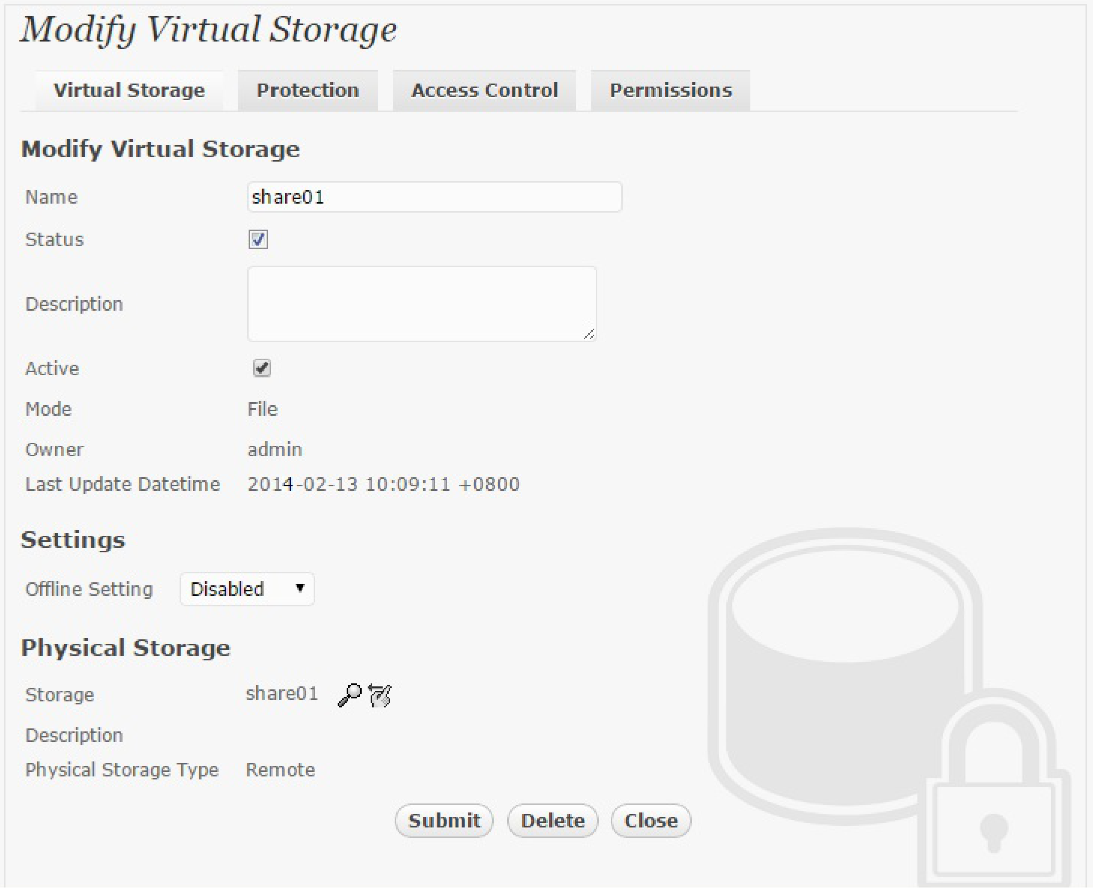
Modify Storage Configuration

Physical Storage Configuration

Name	share01
Description	
Physical Storage Type	Remote
Type	Common Internet File System (CIFS)
Host	192.168.206.101
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

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

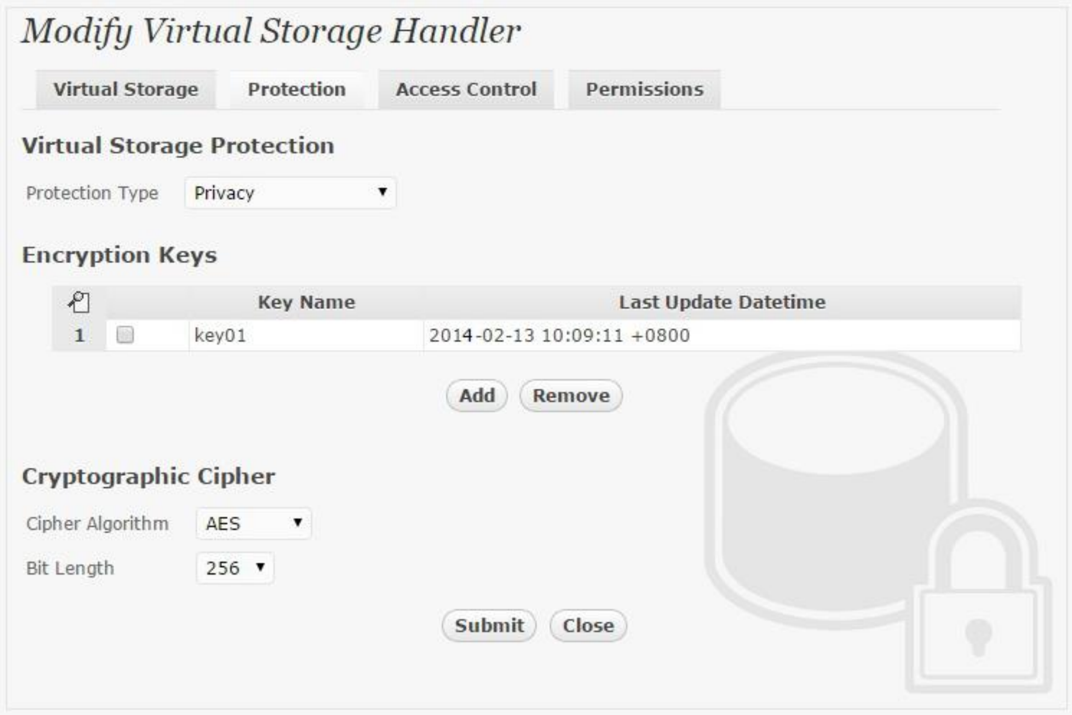
Settings

Offline Setting: Disabled

Physical Storage

Storage	share01
Description	
Physical Storage Type	Remote

Protection type is specified as 'Privacy' and secure the backend NetApp FAS storage using AES 256-bit encryption and encryption key 'key01' managed at Ultra Electronics AEP Keyper HSM.



Modify Virtual Storage Handler

Virtual Storage Protection

Protection Type: Privacy

Encryption Keys

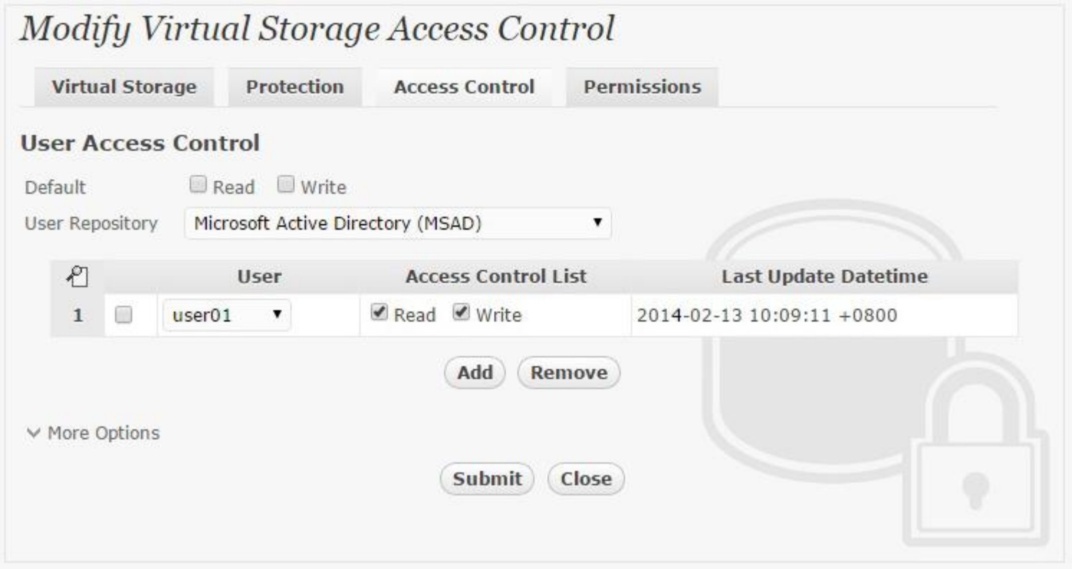
		Key Name	Last Update Datetime
1	□	key01	2014-02-13 10:09:11 +0800

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.



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

Conclusion

Hardware security module

- Ultra Electronics AEP Keyper

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

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

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 Ultra Electronics AEP 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. Ultra Electronics AEP Keyper, https://www.ultra-aep.com/ultra-safe-overview