interopLab

Interoperability of Bloombase StoreSafe and Futurex Vectera HSM for Data-at-Rest Encryption

August 2019

BLOOMBASE®

Executive Summary

Futurex Vectera 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 Futurex Vectera 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 have been tested with Futurex Vectera and Bloombase StoreSafe to secure Microsoft Storage Server on Microsoft Windows Server 2019 as the storage backend.

Document No.: BLBS-TN-Bloombase-StoreSafe-Futurex-Vectera-HSM-Interoperability-USLET-EN-R0.92

Table of Contents

Purpose and Scope

This document describes the steps necessary to integrate Futurex Vectera Hardware Security Module (HSM) 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 Futurex Vectera
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris with Microsoft Storage Server as storage backend

Assumptions

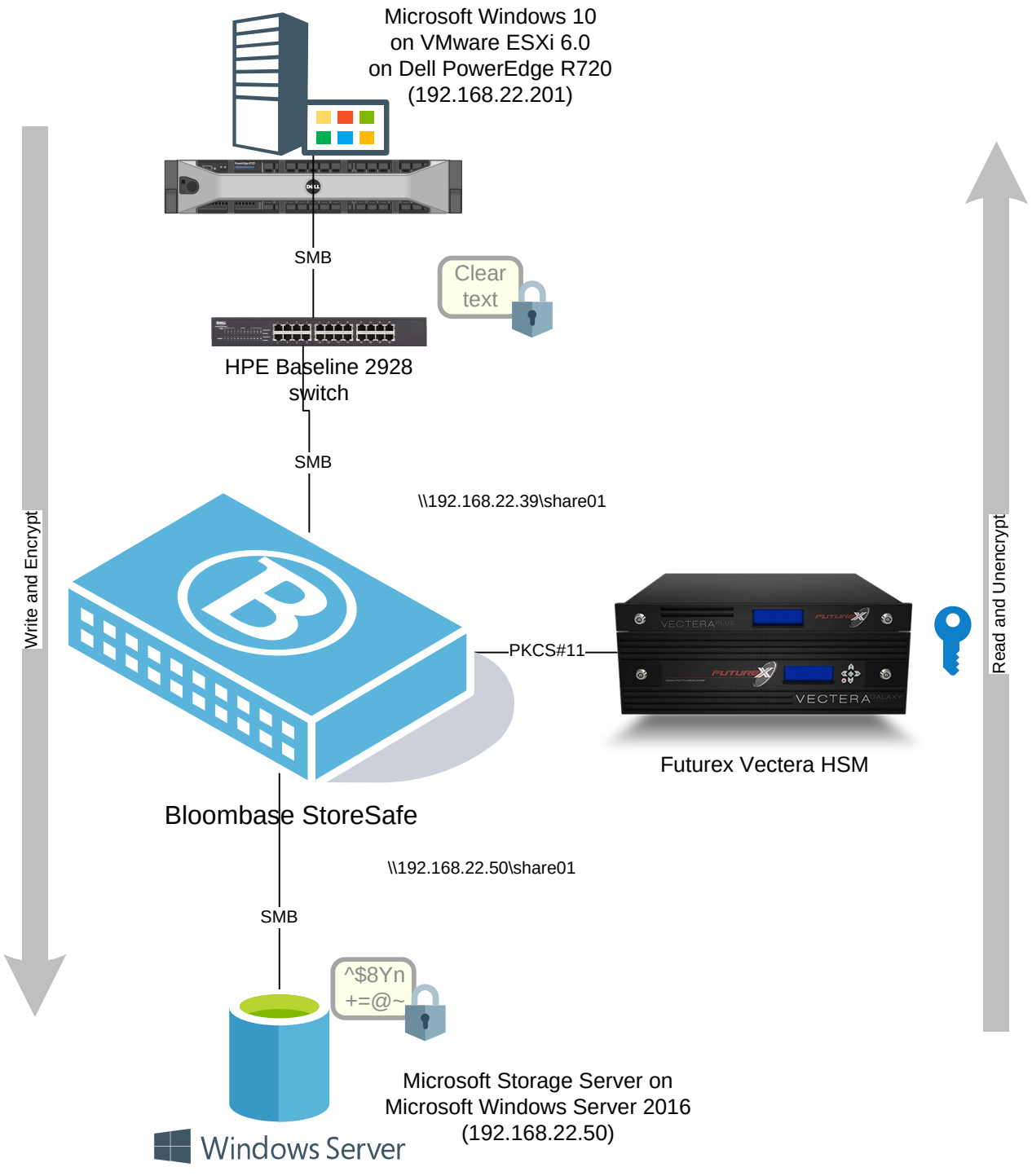
This document describes interoperability testing of Futurex Vectera with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of Futurex Vectera, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is 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 Futurex Vectera 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 Futurex Vectera 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 https://www.bloombase.com or Bloombase SupPortal https://supportal.bloombase.com.

Infrastructure

Setup

The validation testing environment is setup as in below diagram



Hardware Security Module

Hardware Security Module	Futurex Vectera HSM
Firmware Version	6.5.3.8

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.4.7
Futurex Client Software Package	4.1
FIPS Mode	Non-strict FIPS security world
Server	VMware Virtual Machine (VM) on VMware ESXi 6.0
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	Microsoft Storage Server on Microsoft Windows Server 2016 on VMware ESXi 6.0

Client Hosts

Hardware	Dell PowerEdge R720
Hypervisor	VMware ESXi 6.0
Operating System	Microsoft Windows 10

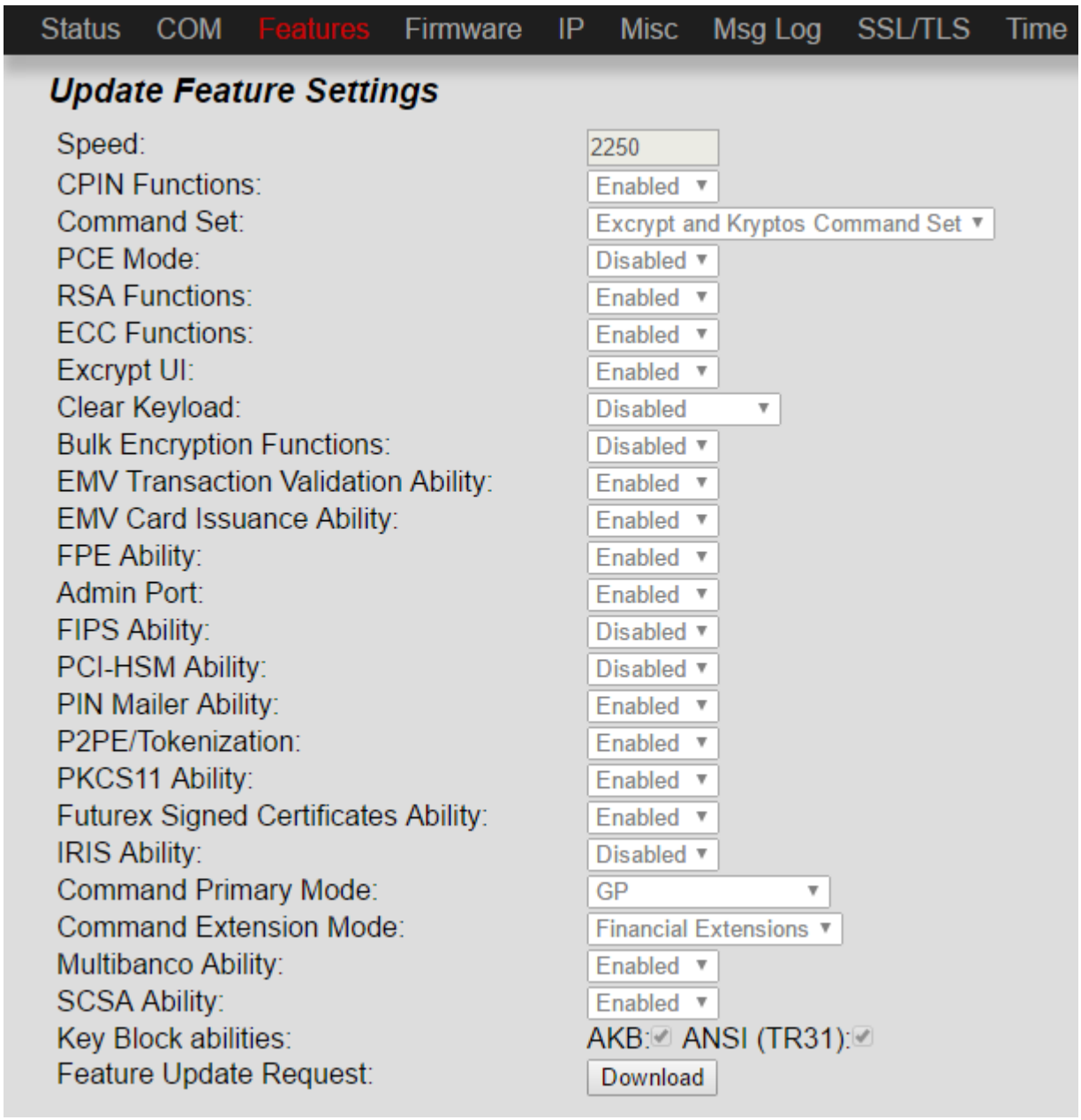
Configuration Overview

Futurex Vectera

Enabling PKCS#11 communication on Futurex Vectera

In order to utilize the Futurex Vectera as an external key manager, it must allow communication through the PKCS#11 protocol.

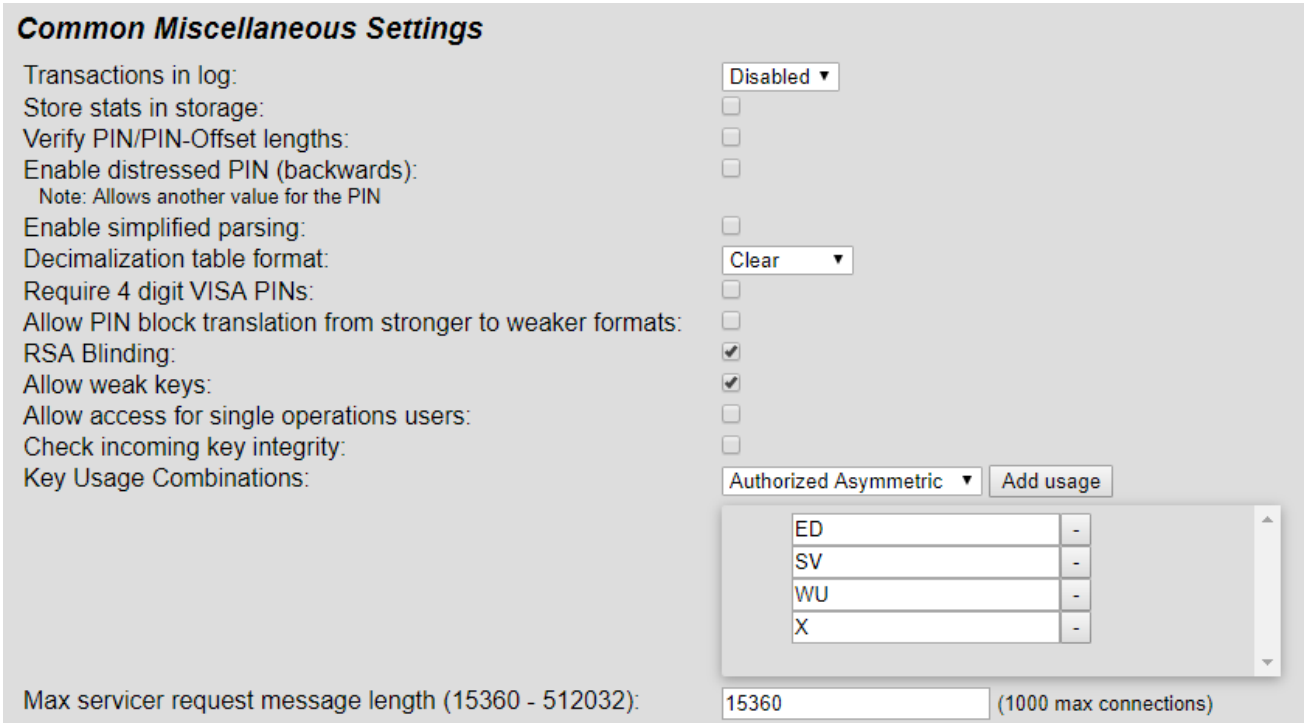
This requires the “General-Purpose Cryptographic License” on the Futurex HSM. To check for this license, access the web portal on your HSM. Under the Features tab check the status of the line labelled PKCS11 Ability. It should say Enabled.



Creating a Key Profile

Bloombase StoreSafe requires multi-purpose keys in order to encrypt and decrypt data as well as other keys functions. A custom profile must be created to allow for multi-purpose keys.

Accessing the Futurex Vectera web portal, please select "add usage" under Vectera Plus->Web Portal Configuration Panel->Common Miscellaneous Settings. Note that a profile will need to be created with the following usage: EDWUSVX



Key Usage Combinations: Allows multipurpose keys to be generated. Typically in high assurance environments, keys are bound to a single usage. However, various key usage combinations can be defined if required by an application integration. To define a new key usage combination, first select Authorized Asymmetric or Anonymous Asymmetric from the drop-down to specify which type of user can generate the key. Then select Add Usage. On the dialog window, select the applicable key usage options and select Save.

The above instructions can also be found in your Futurex Vectera user guide.

Futurex Vectera Client Setup

To communicate with the HSM, users must first configure the Futurex PKCS #11 library. This section describes the configuration files, the available options, and the configuration options necessary for establishing connection. The Futurex PKCS #11 library can be configured with a text editor or through the “Futurex Config Tool” application, which provides users a graphical user interface (GUI) through which to edit configuration options.

The configuration file, fxpkcs-11 software, and TLS certificates should be uploaded to the Bloombase StoreSafe and placed in the correct directories.

The default location where the configuration file is read from is:

```
/etc/fxpkcs11.cfg
```

The fxpkcs-11 software should be extracted to the following directory:

```
/opt/fxpkcs11/
```


Note: it is required to use the fxpkcs11-redhat software.

The TLS certificates can be placed in any directory but their paths must be declared in the configuration file under the following options:

```
<PROD-TLS-CA>          </PROD-TLS-CA>
<PROD-TLS-CERT>        </PROD-TLS-CERT>
<PROD-TLS-KEY>         </PROD-TLS-KEY>
```

Run command

```
/opt/fxpkcs11/x64/OpenSSL-1.0.x/PKCS11Manager
```

as the sanity check for if everything is working on the HSM and PKCS#11 layer.

```
Library Information:

       Manufacturer: Futurex
       Library: FxPKCS11
       Cryptoki Version: 2.20
       Library Version: 4.1
       Library Flags: 00000000
[2019-07-25 02:47:50] | INFO  | 7F3579A1B880 | C_GetSlotInfo: Slot
0 Flags: 0000
0007.

Slot Information:
       Slot: 0
       Manufacturer: Futurex
       Decription: Futurex Cryptoki Slot #0
       Hardware Version: 0.0
       Firmware Version: 4.1
       Flags: 00000007
[2019-07-25 02:47:50] | INFO  | 7F3579A1B880 | C_GetTokenInfo:
Token Flags: 0000
064D.

Token Information:
       Manufacturer: Futurex
       Token: us01hsm01test.virtucrypt.com:592
       Model: HSM
       Serial Number: 1831800266
       Flags: 0000064D
       Time on HSM:

Session Information:
       Session: 1
       Slot: 0
       State: 3
       Flags: 00000006
       Device Error: 00000000
```

In this interoperability test, Slot o has been used for key protection with the HSM as in the Bloombase StoreSafe registry.

HSM PKCS#11 integration uses standard SunPKCS11 provider. This makes selection of slot customer configurable. This can optionally be reconfigured, by modifying

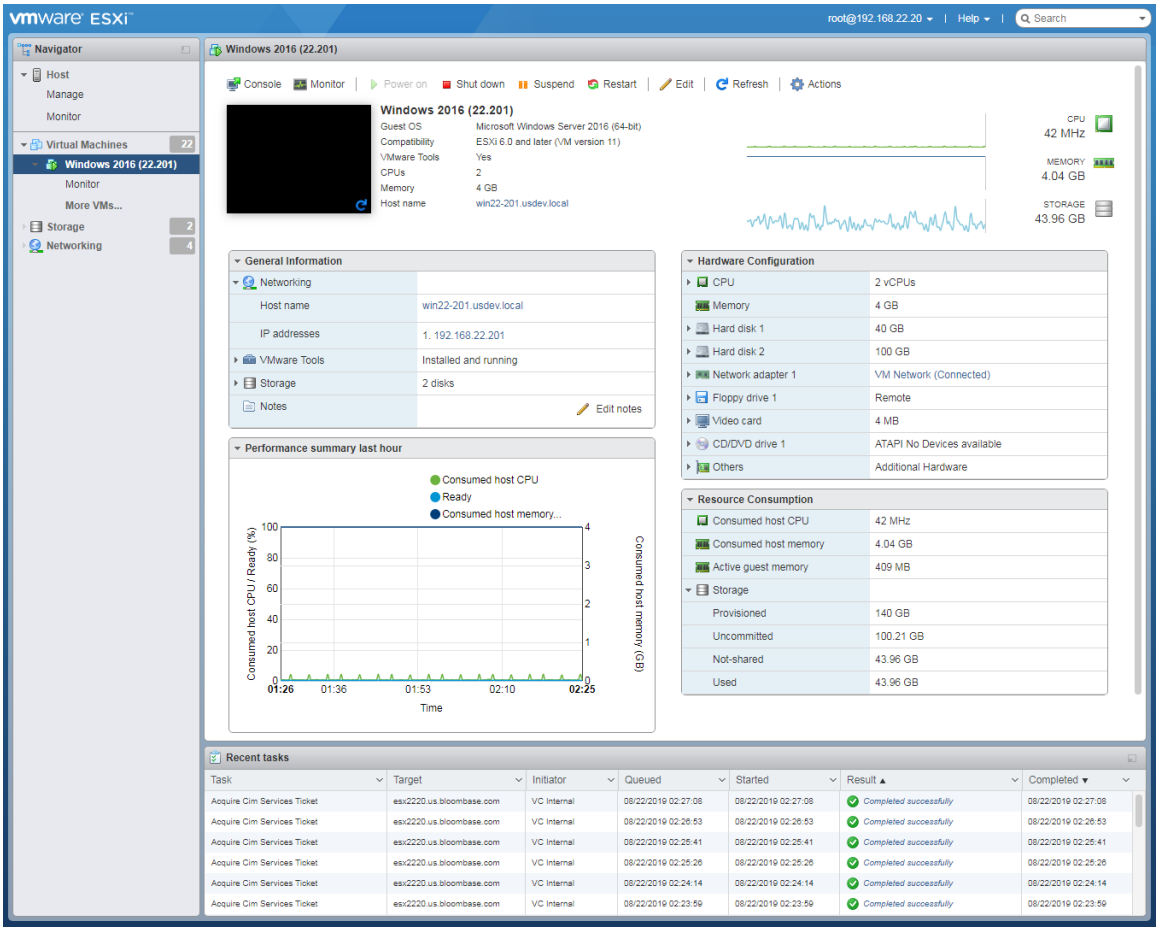
```
slotListIndex
```

entry in Bloombase StoreSafe.

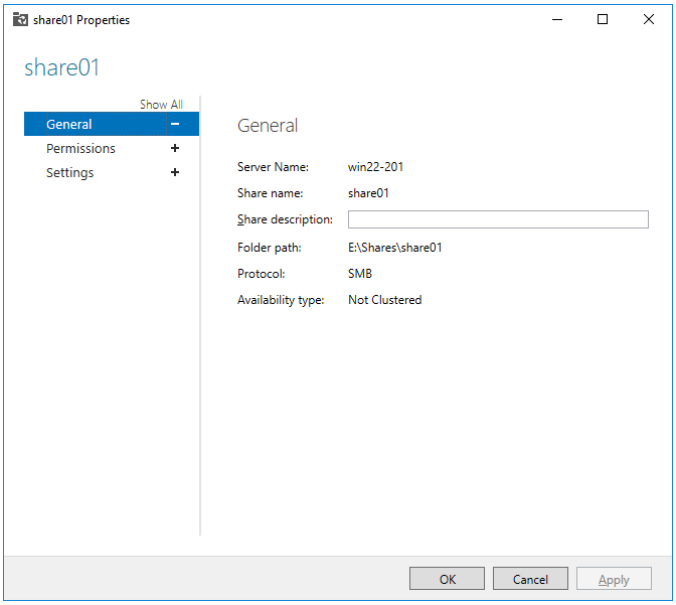
Please refer to “nShield Connect User Guide” for detailed setup and configurations.

Microsoft Storage Server on Microsoft Windows Server 2016

Microsoft Windows Server 2016 is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.

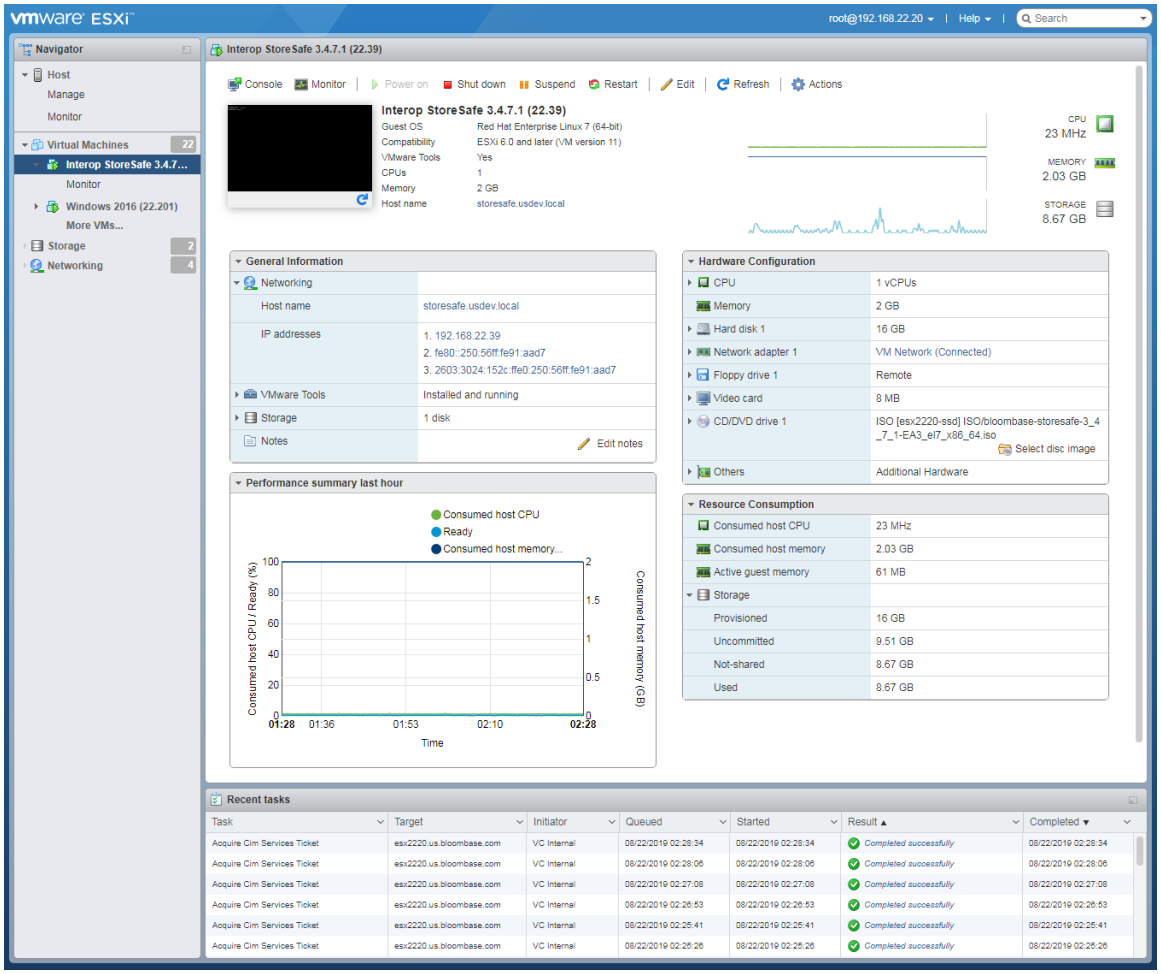


A Windows network share is provisioned for Bloombase StoreSafe encryption using keys from Futurex Vectera HSM.

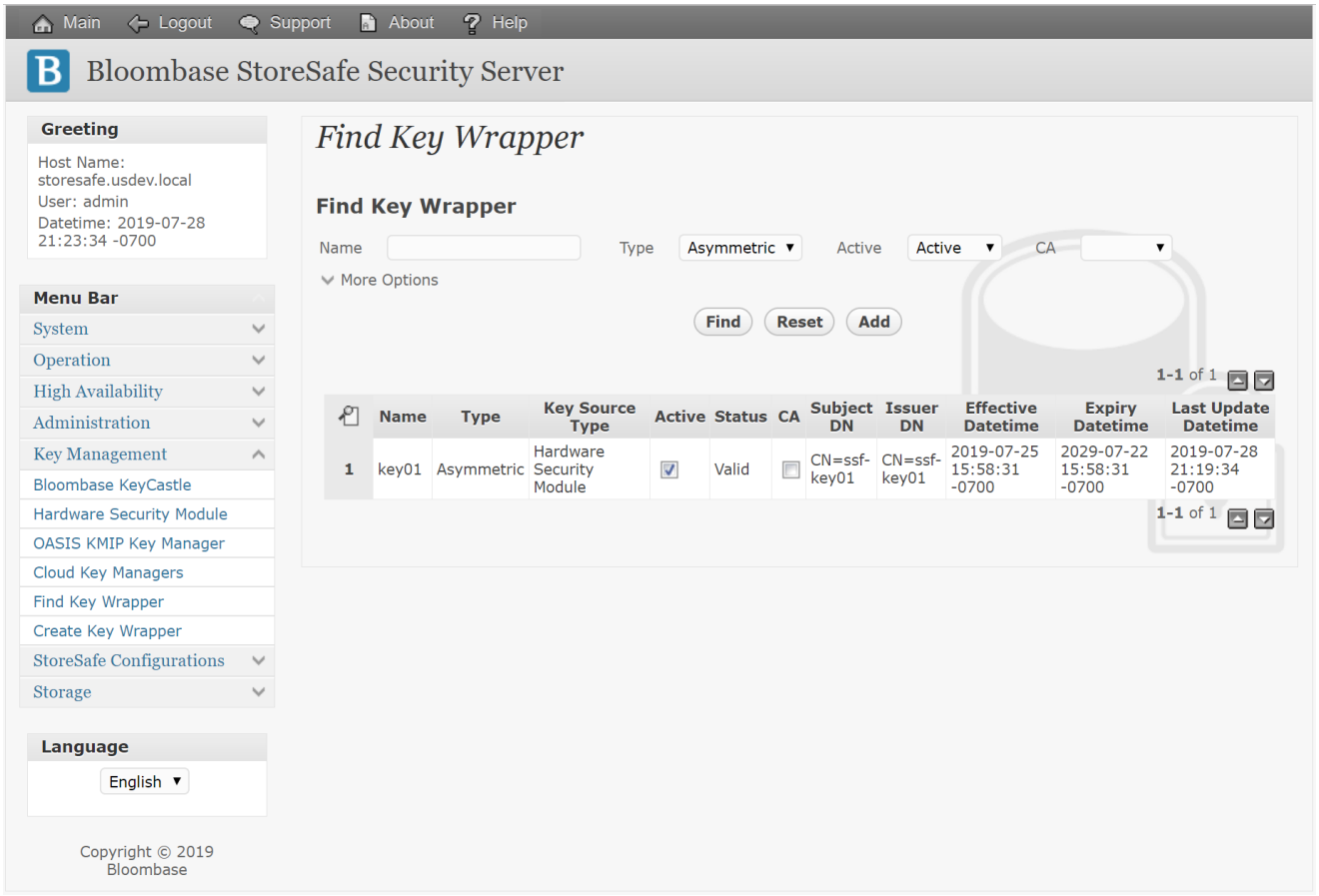


Bloombase StoreSafe

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 Futurex Vectera HSM.



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



Futurex Vectera and Bloombase KeyCastle Integration

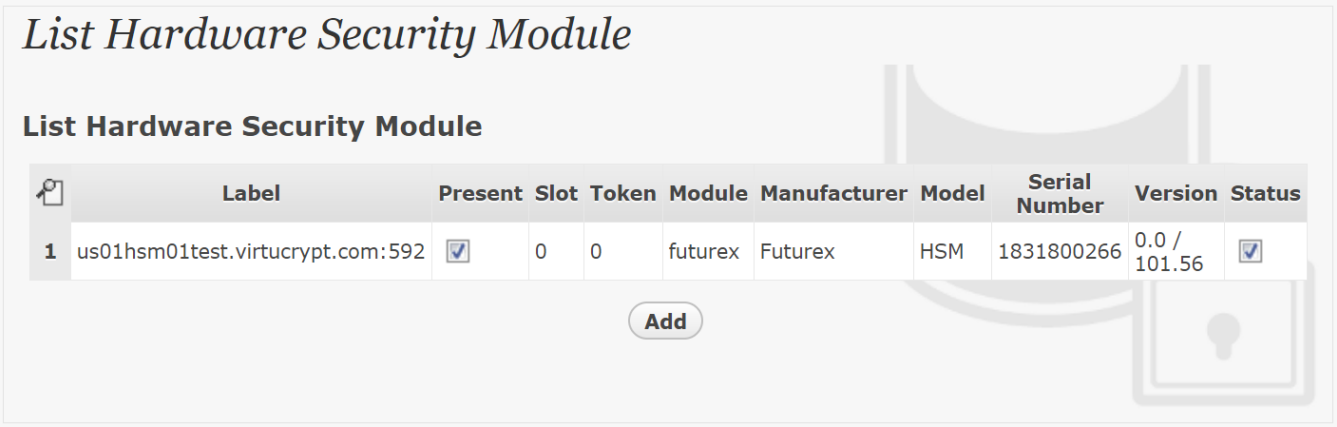
To enable the built-in Bloombase KeyCastle to utilize keys in the network attached Futurex Vectera HSM. The hardware security module configuration at Bloombase web management console must be set up.

Bloombase supports Futurex Vectera out of the box. When a Futurex Vectera is configured at Bloombase web management console, select Module as ‘futurex’ which allows embedded Bloombase KeyCastle module to utilize Futurex fxpkcs11 driver to access Futurex Vectera HSM over standard PKCS#11 protocol.

In this scenario, the Futurex Vectera HSM is assigned a token label namely ‘uso1hsmo1test.virtucrypt.com:592’. Again, the use of slot is customer configurable. This can optionally be reconfigured, by modifying entry in Bloombase StoreSafe registry.

When prompted for pins, enter the password of the “CRYPTO-OPR” declared in the cfg file.

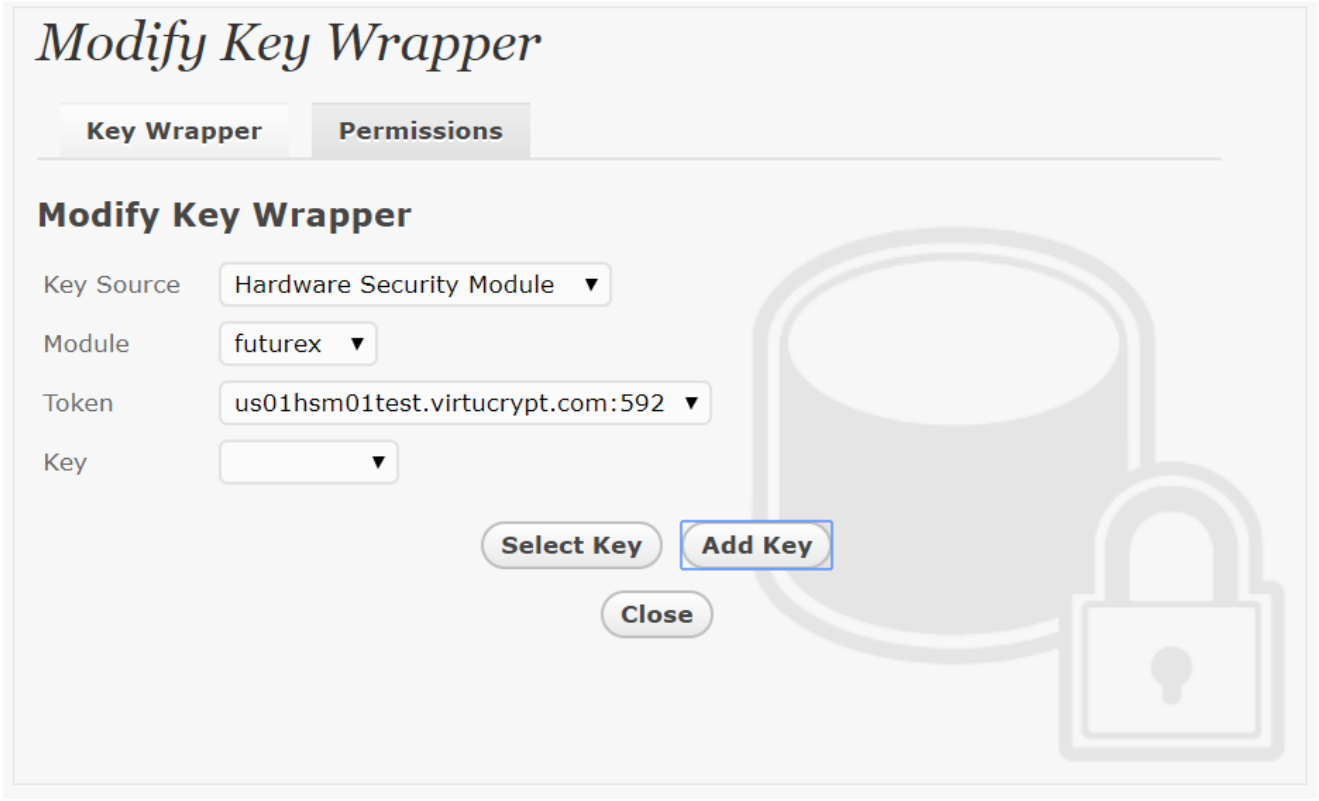
When Futurex Vectera HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as 'Active'.



Encryption Key Provisioning

Generate encryption key with name 'keyo1' in bundled Bloombase KeyCastle key life-cycle management tool

To generate key in attached Futurex Vectera HSM, select Key Source Type as “Hardware Security Module”, Module as “futurex” and the assigned HSM token label, in this case “us01hsm01test.virtucrypt.com:592”. Ensure you import a key from the HSM before you submit the key wrapper.



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

Backend Physical Storage Configuration

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

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.

Protection type is specified as 'Privacy' and secure the Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key 'key01' managed at Futurex Vectera.

SMB/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.

Conclusion

Hardware security module

- Futurex Vectera HSM

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	Futurex Vectera HSM

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 Futurex for supporting this interoperability testing.

Technical Reference

Bloombase StoreSafe Technical Specifications, http://www.bloombase.com/content/8936QA88

Bloombase StoreSafe Hardware Compatibility Matrix, http://www.bloombase.com/content/e8Gzz281

Futurex Vectera HSM, https://www.futurex.com/products/vectera-series