Bloombase StoreSafe

Integration Guide

Utimaco GP HSM

utimaco®

Imprint

Copyright 2020	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	06/10/2025
Status	PUBLISHED
Document No.	IG-2025-0014

Table of Contents

1 Purpose and Scope

This document describes the steps necessary to integrate Utimaco GP HSM with Bloombase StoreSafe to deliver agentless, transparent encryption security of traditional storage systems and next-generation storage services for missioncritical applications. Specifically, we cover the following areas:

- Install and configure Bloombase StoreSafe software appliance
- Integrate Bloombase StoreSafe with Utimaco GP HSM
- Integrate Microsoft Windows 11 and Ubuntu 22.04 client systems with Bloombase StoreSafe and Utimaco GP HSM data-at-rest encryption security solution for Microsoft Windows Server 2025 and Rocky Linux 9 storage backends to demonstrate how high-bandwidth, agentless, application-transparent data encryption could be achieved for multiple network storage protocols namely SMB, NFS, iSCSI and NVMe/TCP.

2 Assumptions

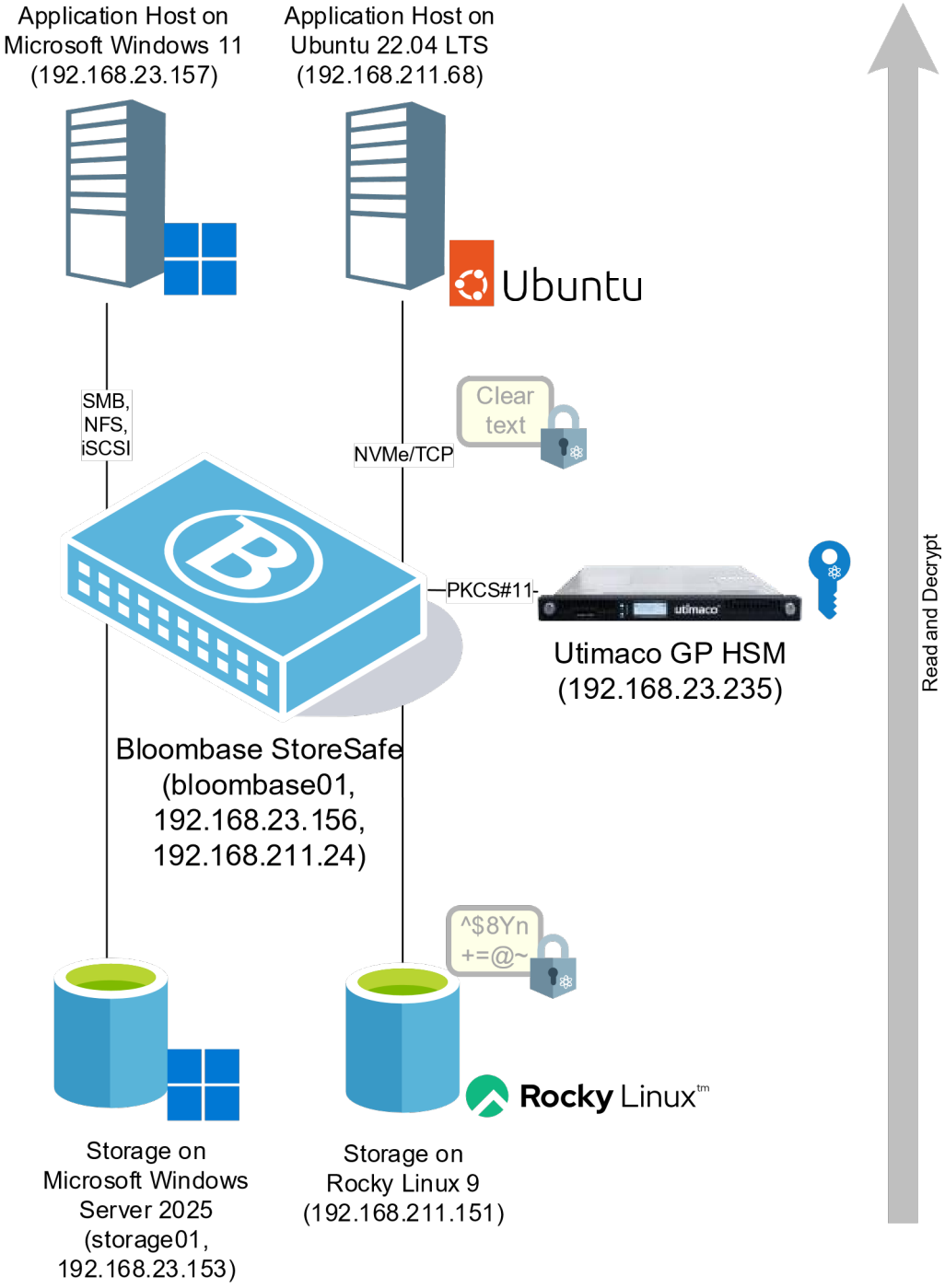
This document describes the integration of Utimaco GP HSM with Bloombase StoreSafe. It is assumed that you are familiar with operation of Utimaco GP HSM, storage systems, and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you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

As Utimaco GP HSM is third party option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of Utimaco GP HSM for your actual use cases. 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 and Bloombase SupPortal https://supportal.bloombase.com.

3 Infrastructure

3.1 Setup

The integration discussed in this guide is based on the system block diagram below:



3.2 Storage Encryption

Storage Encryption	Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v4.0
Server	VMware ESXi 6.5
Processor	4x Virtual CPU (vCPU)
Memory	8GB
Network Interface Card	NVIDIA ConnectX-5

3.3 Key Management System

Key Management System	Utimaco General Purpose Hardware Security Module (GP HSM) v4.80.0.0

3.4 Storage Systems

Storage Systems	Microsoft Storage Server on Microsoft Windows Server 2025	NVMe over Fabrics (NVMe-oF) storage services on Rocky Linux 9

3.5 Storage Hosts

Client Hosts	Microsoft Windows 11	Ubuntu 22.04 LTS

3.6 Networking

Ethernet Switch	Celestica Seastone DX010 32-port 100GbE ONIE Switch
Network Interface Card	NVIDIA ConnectX-5
Cables	NVIDIA/Mellanox 100GbE QSFP28 DAC Cables

4 Configuration Overview

4.1 Utimaco General Purpose Hardware Security Module (GP HSM)

Utimaco GP HSM is a hardware security module that secures cryptographic key material for servers and applications. It includes integration software that supports the industry standards (e.g. PKCS#11, Microsoft CSP/CNG, JCE…) which are used in many application scenarios, e.g., Enterprise PKI application and database encryption. The General Purpose HSM is available as PCIe embedded card or as network attached appliance. The key management and cryptographic functionalities provided by Utimaco GP HSM are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

In order to utilize the PKCS#11 functionality, the token must be initialized.

```
[root@cassf156 ~]# /opt/utimaco/Administration/csadm GetState

mode      = Operational Mode
state     = INITIALIZED (0x00100004)
temp      = 30.0 [C]
alarm     = OFF
bl_ver    = 5.01.10.0         (Model: Se-Series Gen2)
hw_ver    = 0.00.8.15
uid       = ca534d32 34347053                    | SM244pS        |
adm1      = 5554494d 41434f20  53493030 33303031 |UTIMACO SI003001|
adm2      = 53696d75 6c61746f  72000000 00000000 |Simulator       |
adm3      = 696e6974 5f646576  5f707562 00000000 |init dev pub    |
```

As an example, the Utimaco GP HSM is assigned a token label as follows

```
p11tool2 slot=0 Label=CryptoServer Login=ADMIN,ADMIN.key InitToken=<so pin>
```

A user pin will be needed for PKCS#11. To setup the user pin, run the following command,

```
p11tool2 slot=0 LoginSO=<so pin> InitPin=<user pin>
```

To check if Utimaco GP HSM is initialized, run

```
p11tool2 slot=0 ListSlots=status
```

```
[root@cassf156 ~]# /opt/utimaco/bin/p11tool2 ListSlots=status
      slot ID   token init.   PIN init.
      ---------------------------------
   0: 00000000  yes           yes
   1: 00000001  no            no
   2: 00000002  no            no
   3: 00000003  no            no
   4: 00000004  no            no
   5: 00000005  no            no
   6: 00000006  no            no
   7: 00000007  no            no
   8: 00000008  no            no
   9: 00000009  no            no
```

4.1.1 Ethernet Switch Configuration

Celestica Seastone DX010 32-port 100GbE ONIE switch has been used in this integration testing.

Ports 24 and 28 of the 100Gb Ethernet switch are connected to the NVIDIA ConnectX-5 NICs via DAC cables as shown in the SONiC console below.

```
Linux sonic 5.10.0-8-2-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64
You are on
  ____   ___  _   _ ___ ____
 / ___| / _ \| \ | |_ _/ ___|
 \___ \| | | |  \| || | |
  ___) | |_| | |\  || | |___
 |____/ \___/|_| \_|___\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.
```

```
admin@sonic:~$ sudo config vlan add 210
admin@sonic:~$ sudo config vlan member add -u 210 Ethernet24
admin@sonic:~$ sudo config vlan member add -u 210 Ethernet28
```

```
admin@sonic:~$ show vlan brief
+-----------+--------------+------------+----------------+-------------+-----------------------+
|   VLAN ID | IP Address   | Ports      | Port Tagging   | Proxy ARP   | DHCP Helper Address   |
+===========+==============+============+================+=============+=======================+
|       210 |              | Ethernet24 | untagged       | disabled    |                       |
|           |              | Ethernet28 | untagged       |             |                       |
+-----------+--------------+------------+----------------+-------------+-----------------------+
```

```
admin@sonic:~$ show interfaces status
  Interface            Lanes    Speed    MTU    FEC    Alias    Vlan    Oper    Admin             Type    Asym PFC
-----------  ---------------  -------  -----  -----  -------  ------  ------  -------  ---------------  ----------
  Ethernet0      65,66,67,68     100G   9100     rs     Eth1   trunk    down       up              N/A         N/A
  Ethernet4      69,70,71,72     100G   9100     rs     Eth2   trunk      up       up  QSFP28 or later         N/A
  Ethernet8      73,74,75,76     100G   9100    N/A     Eth3   trunk    down       up              N/A         N/A
 Ethernet12      77,78,79,80     100G   9100     rs     Eth4   trunk      up       up  QSFP28 or later         N/A
 Ethernet16      33,34,35,36     100G   9100     rs     Eth5   trunk    down       up  QSFP28 or later         N/A
 Ethernet20      37,38,39,40     100G   9100    N/A     Eth6   trunk    down       up              N/A         N/A
 Ethernet24      41,42,43,44     100G   9100    N/A     Eth7   trunk      up       up  QSFP28 or later         N/A
 Ethernet28      45,46,47,48     100G   9100    N/A     Eth8   trunk      up       up  QSFP28 or later         N/A
```

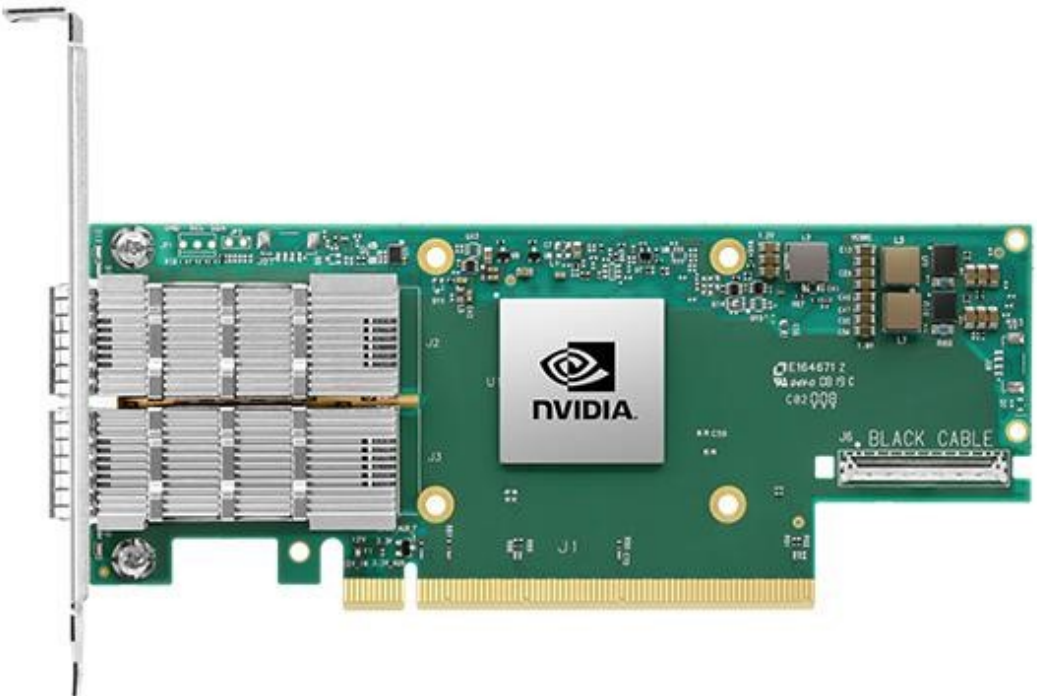
```
Ethernet24: SFP EEPROM detected
        Application Advertisement: N/A
        Connector: No separable connector
        Encoding: Unspecified
        Extended Identifier: Power Class 1(1.5W max)
        Extended RateSelect Compliance: QSFP+ Rate Select Version 1
        Identifier: QSFP28 or later
        Length Cable Assembly(m): 2
        Nominal Bit Rate(100Mbs): 255
        Specification compliance:
                Extended Specification compliance: 100GBASE-CR4, 25GBASE-CR CA-25G-L or 50GBASE-CR2
with RS
        Vendor Date Code(YYYY-MM-DD Lot): 2021-12-06
        Vendor Name: FS
        Vendor OUI: 00-02-c9
        Vendor PN: Q28-PC02
        Vendor Rev: A2
        Vendor SN: G2140009608-2
```

4.1.2 Direct Attach Copper (DAC) Cable

NVIDIA/Mellanox 100GbE QSFP28 DAC cables have been used in this interoperability testing.

4.1.3 Network Interface Card (NIC)

NVIDIA ConnectX-5 NIC has been used in this integration testing.



Install and configure NVIDIA ConnectX-5 NIC using the install image or the driver available from your distribution's repo.

```
user@ubuntu67:~$ lspci |grep mellanox -i
0b:00.0 Ethernet controller: Mellanox Technologies MT27800 Family [ConnectX-5 Virtual Function]
```

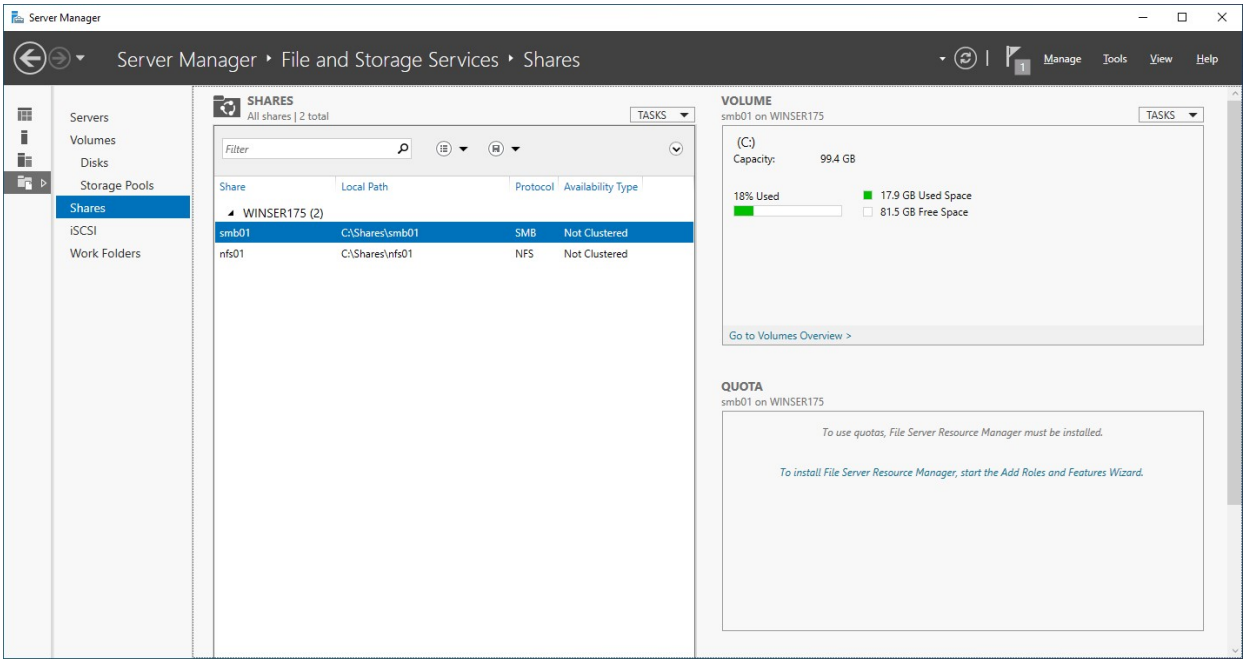
```
user@ubuntu67:~$ ibstat
CA 'mlx5_0'
        CA type: MT4120
        Number of ports: 1
        Firmware version: 16.35.2000
        Hardware version: 0
        Node GUID: 0x000c29fffe1dfb26
        System image GUID: 0xb8cef60300f2cc66
        Port 1:
                State: Active
                Physical state: LinkUp
                Rate: 100
                Base lid: 0
                LMC: 0
                SM lid: 0
                Capability mask: 0x00010000
                Port GUID: 0x020c29fffe1dfb26
                Link layer: Ethernet
```

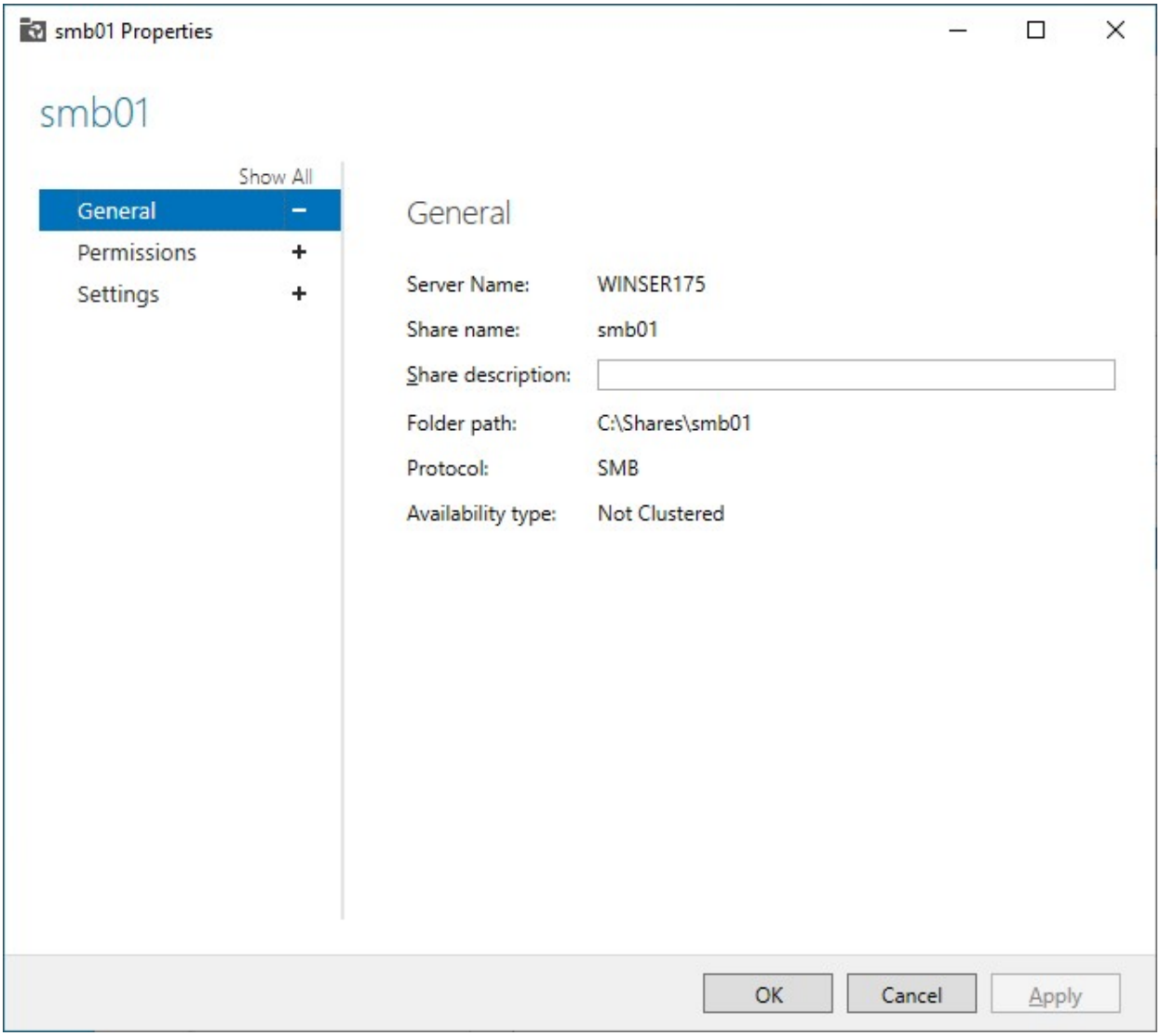
4.2 Microsoft Storage Server on Microsoft Windows Server 2025 Storage Backends

Microsoft Storage Server on Microsoft Windows Server 2025 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including iSCSI, NFS, SMB, CIFS, REST, etc.

Microsoft Windows Server 2025 is deployed as a virtual appliance (VA) on VMware ESXi.

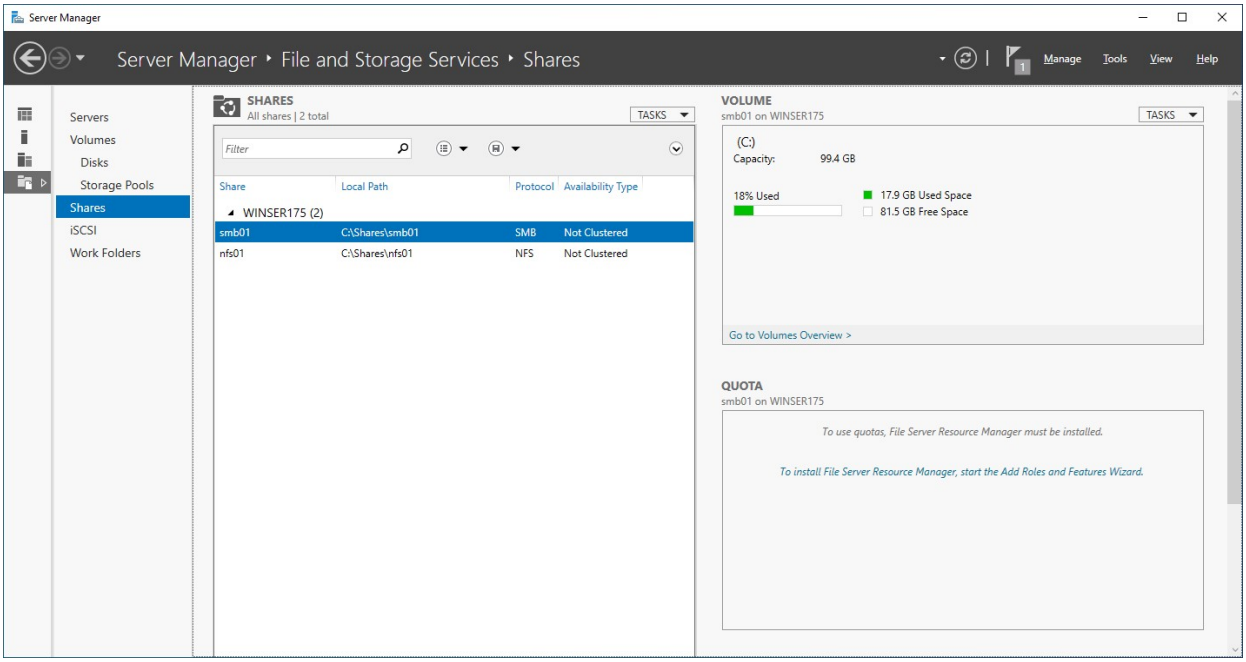
4.2.1 SMB Services Configuration

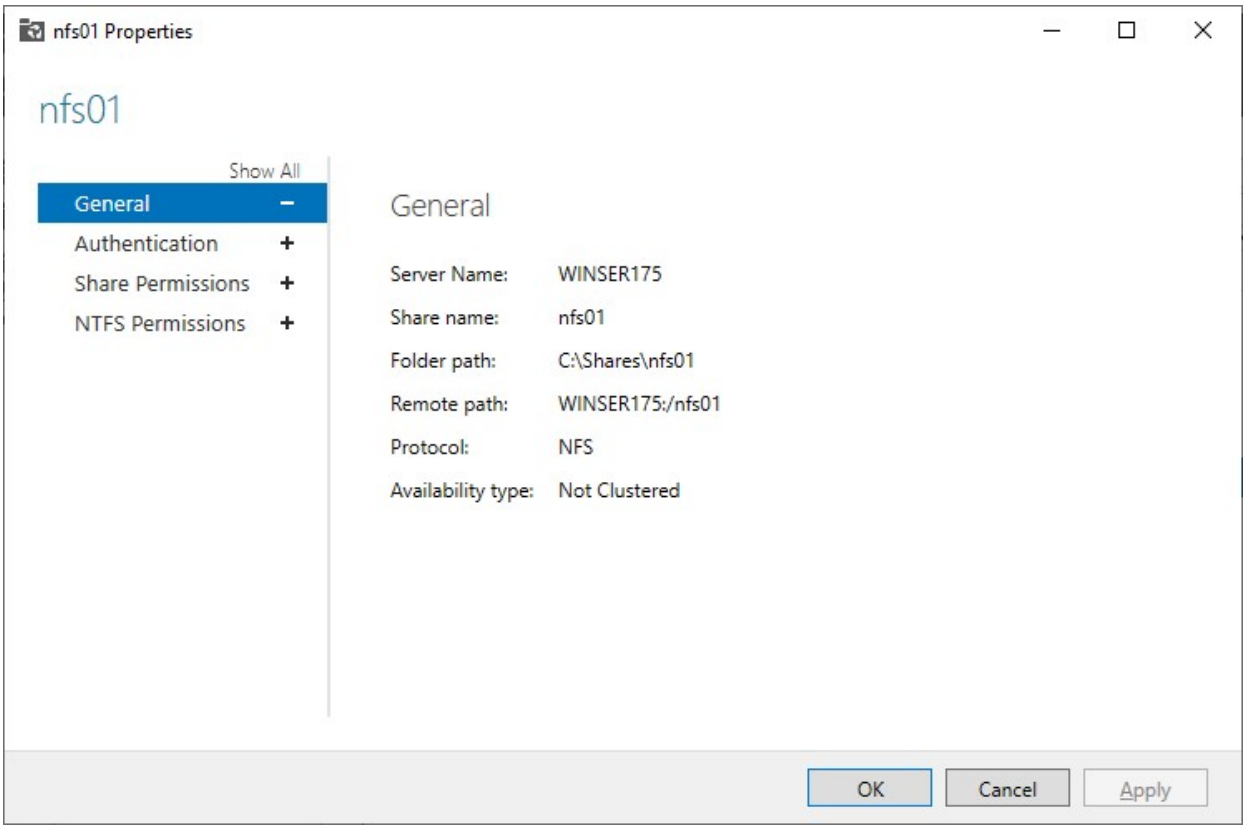




Microsoft Windows Server 2025 File Management is configured to provide the SMB share backend storage to client system users.

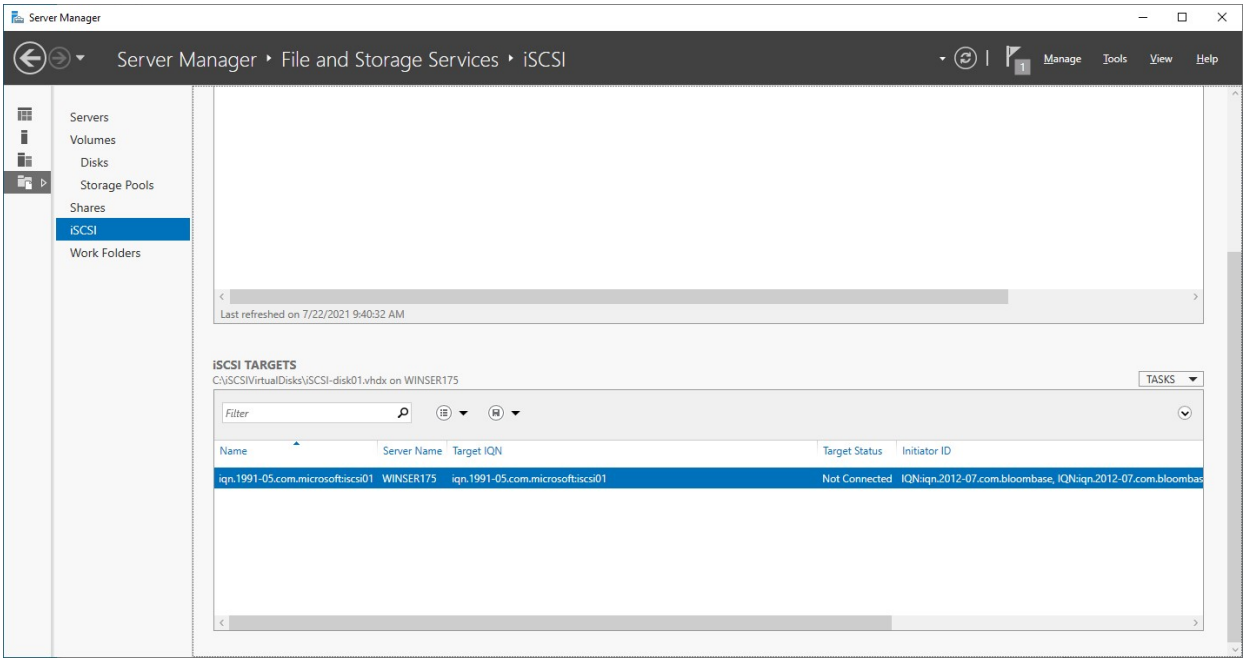
4.2.2 NFS Services Configuration





NFS storage service is provisioned on Microsoft Windows Server 2025 to be used in this integration testing.

4.2.3 iSCSI Services Configuration



iSCSI storage service is also provisioned on Microsoft Windows Server 2025 to be used in this integration testing.

4.3 NVMe over Fabrics (NVMe-oF) Storage Target on Rocky Linux 9 Storage Target

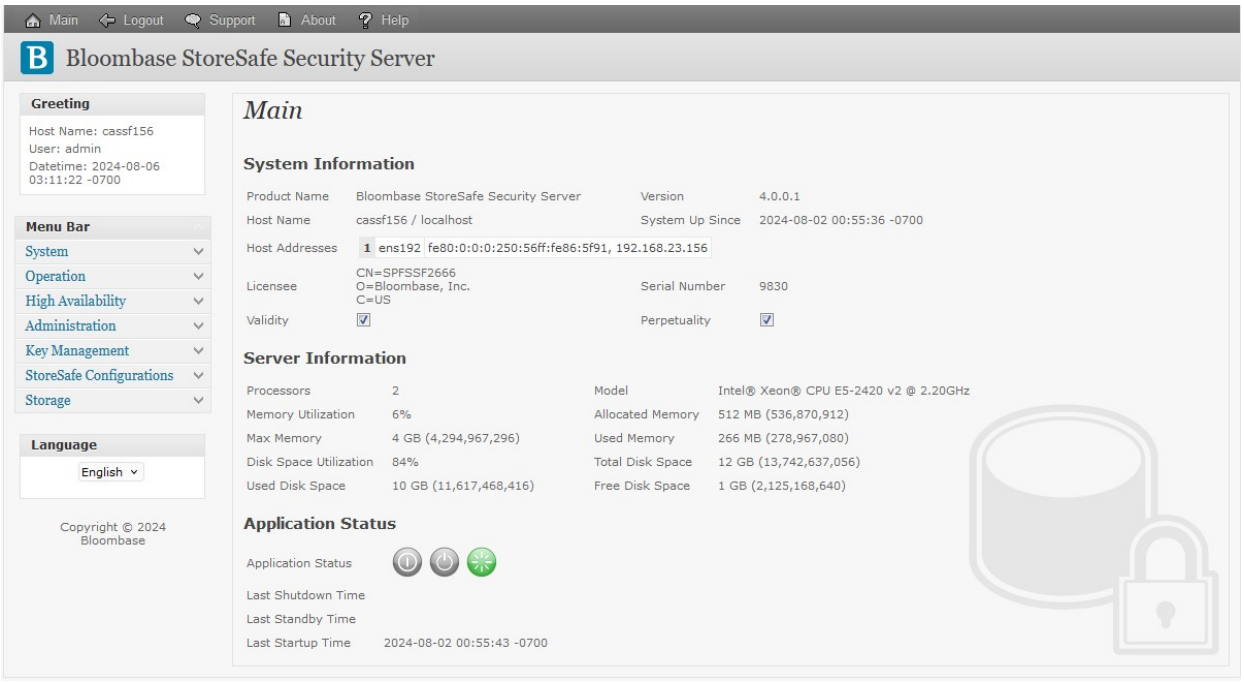
Linux NVMe-oF target software is used to be the storage backend secured by Bloombase StoreSafe Intelligent Storage Firewall.

```
[root@carocky151 ~]# nvmetcli
/> ls
o- / ..... [...]
  o- hosts ..... [...]
  | o- nqn.2014-08.org.nvmexpress:uuid:4af97520-1bfe-4c8d-9069-5fb9ab632709 ..... [...]
  o- ports ..... [...]
  | o- 1 ..... [trtype=tcp, traddr=192.168.211.151, trsvcid=4420, inline_data_size=16384]
  | | o- ana_groups ..... [...]
  | | | o- 1 ..... [state=optimized]
  | | o- referrals ..... [...]
  | | o- subsystems ..... [...]
  | |   o- nqn.2014-08.org.nvmexpress:NVMf:uuid:7079993e-7413-4338-9b9b-a3af82259b18 ..... [...]
  | o- 2 ..... [trtype=rdma, traddr=192.168.211.151, trsvcid=4420, inline_data_size=4096]
  |   o- ana_groups ..... [...]
  |   | o- 1 ..... [state=optimized]
  |   o- referrals ..... [...]
  |   o- subsystems ..... [...]
  |     o- nqn.2014-08.org.nvmexpress:NVMf:uuid:7079993e-7413-4338-9b9b-a3af82259b18 ..... [...]
  o- subsystems ..... [...]
    o- nqn.2014-08.org.nvmexpress:NVMf:uuid:7079993e-7413-4338-9b9b-a3af82259b18 [version=1.3, allow_any=0, serial=cdbdf55fefeea52243d3]
      o- allowed_hosts ..... [...]
      o- namespaces ..... [...]
        o- 1 ..... [path=/dev/nullb0, uuid=e581a156-7460-45e2-b6ae-0457e0762342, grpid=1, disabled]
```

4.4 Bloombase StoreSafe Intelligent Storage Firewall

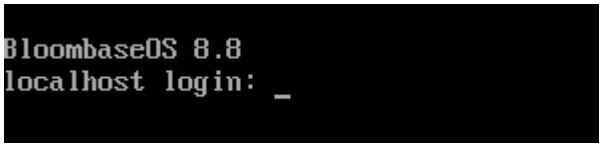
Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, both file-based and block-based encryption security services are validated against Bloombase StoreSafe with keys managed at Utimaco GP HSM.

Bloombase StoreSafe Intelligent Storage Firewall software appliance is deployed as a virtual appliance (VA).



4.4.1 Utimaco General Purpose Hardware Security Module (GP HSM) and Bloombase StoreSafe Integration

The Utimaco provided PKCS#11 libraries and tools need to be installed on the Bloombase Operating System (BloombaseOS). To modify files on the Bloombase StoreSafe OS filesystem, the administrator can access the TTY2 console (ALT+F2) and login as root or another user.



The following files need to be installed in their specific paths:

`/opt/utimaco/bin/p11tool2`

`/opt/utimaco/conf/cs_pkcs11_R3.cfg`

`/opt/utimaco/lib/libcs_pkcs11_R3.so`

Additionally: the following two environment variables need to be declared at the set environment parameter script of Bloombase StoreSafe:

`/spitfire/spitfire-storesafe/bin/setenv.sh`

```
### Utimaco HSM
export CS_PKCS11_R3_CFG=/opt/utimaco/conf/cs_pkcs11_R3.cfg
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/utimaco/lib
```

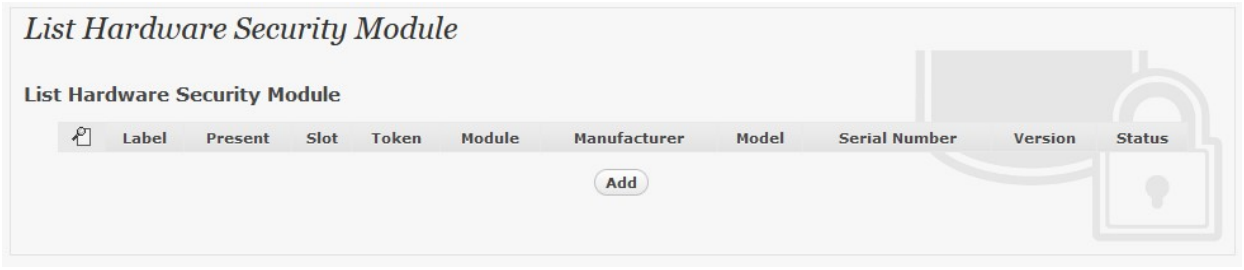
Ensure the

`cs_pkcs11_R3.cfg`

file is correctly configured to Utimaco instructions. The device ID or network IP needs to be specified in the file as such:

```
[CryptoServer]
# Device specifier (here: internal PCI device : cHSM on local u.trust Anchor device - last number represents cHSM slot (1))
Device = /dev/cs2.0.1
# Device specifier (here: cluster of remote devices - first with IP address, others using format <port>@<ip>)
Device = { 192.168.23.235 288@192.168.23.236 4001@192.168.23.237 }
```

To enable the built-in Bloombase KeyCastle to utilize keys managed in the Utimaco GP HSM, the hardware security module service configuration at Bloombase web management console has to be set up. This is done by clicking “Hardware Security Module” under “Key Management”.

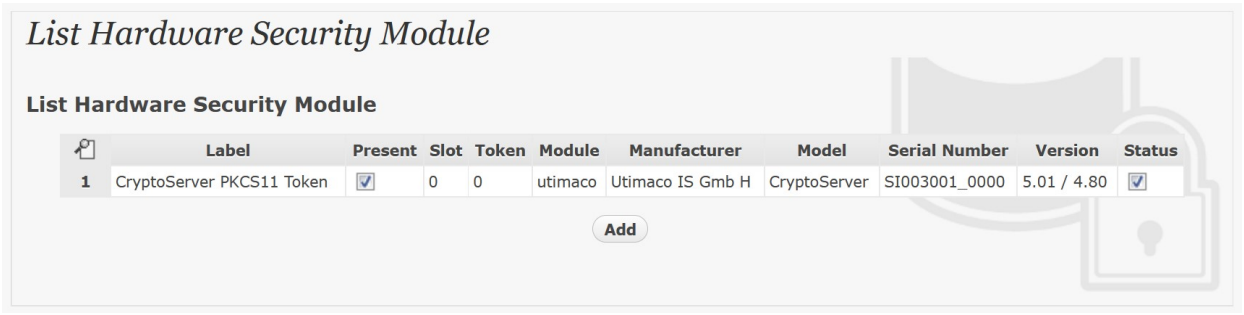


Input a name for the configuration, and select Model as

Utimaco

Input the token label of the Utimaco GP HSM, and the token user pin.

Click 'Submit' to commit the configuration. If the token is properly initialized and connected the "Present" and "Status" boxes will be checked.



4.4.2 Encryption Key Provisioning

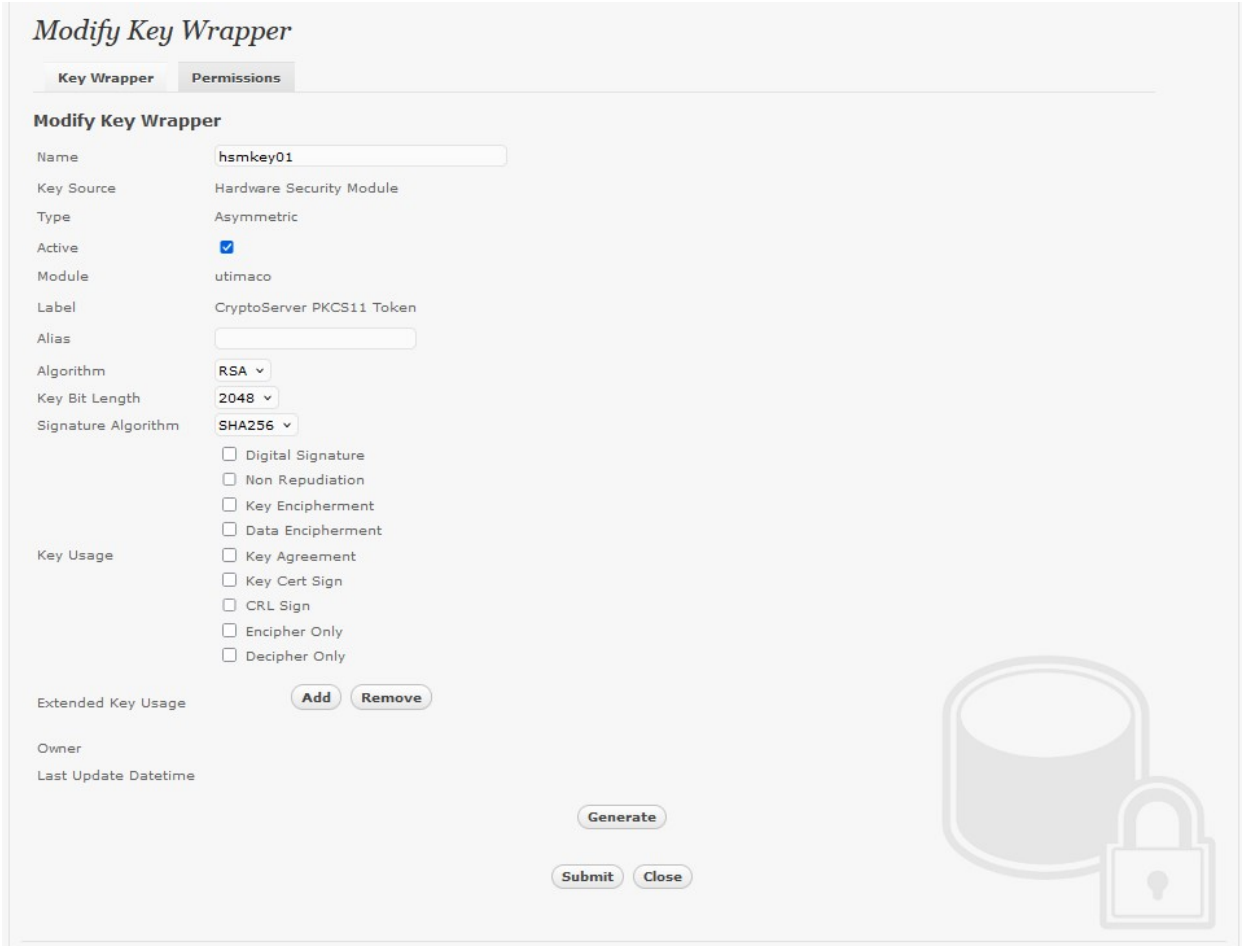
To generate key in attached Utimaco GP HSM, select Key Source Type as

```
Hardware Security Module
```

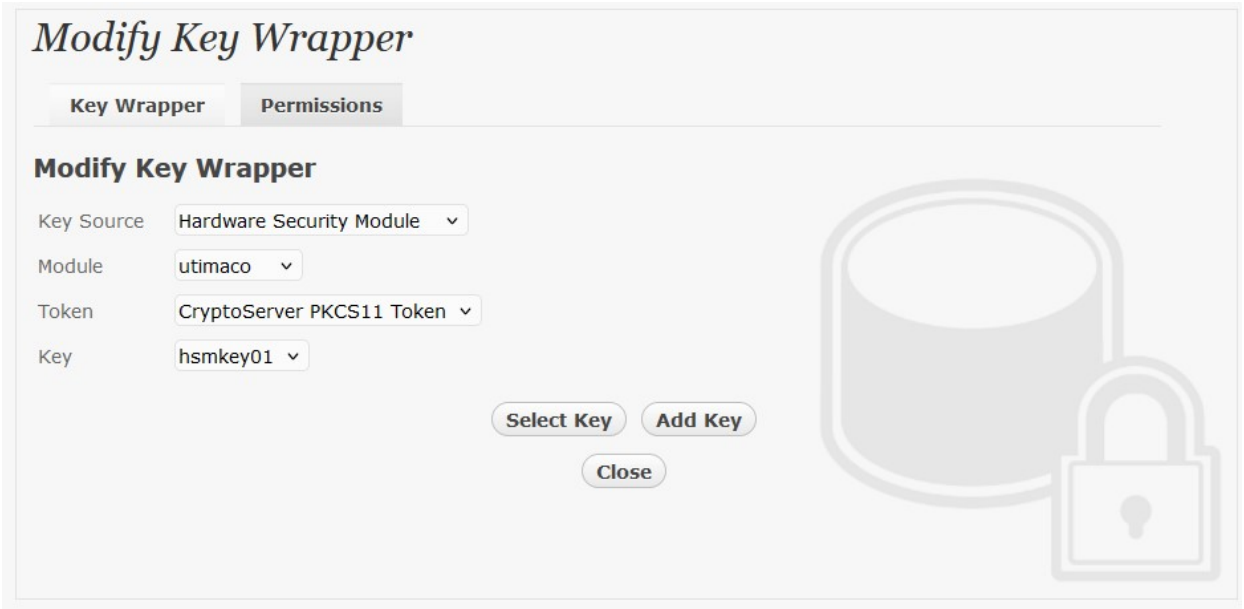
and the assigned Key Manager token, in this case

```
CryptoServer PKCS11 Token
```

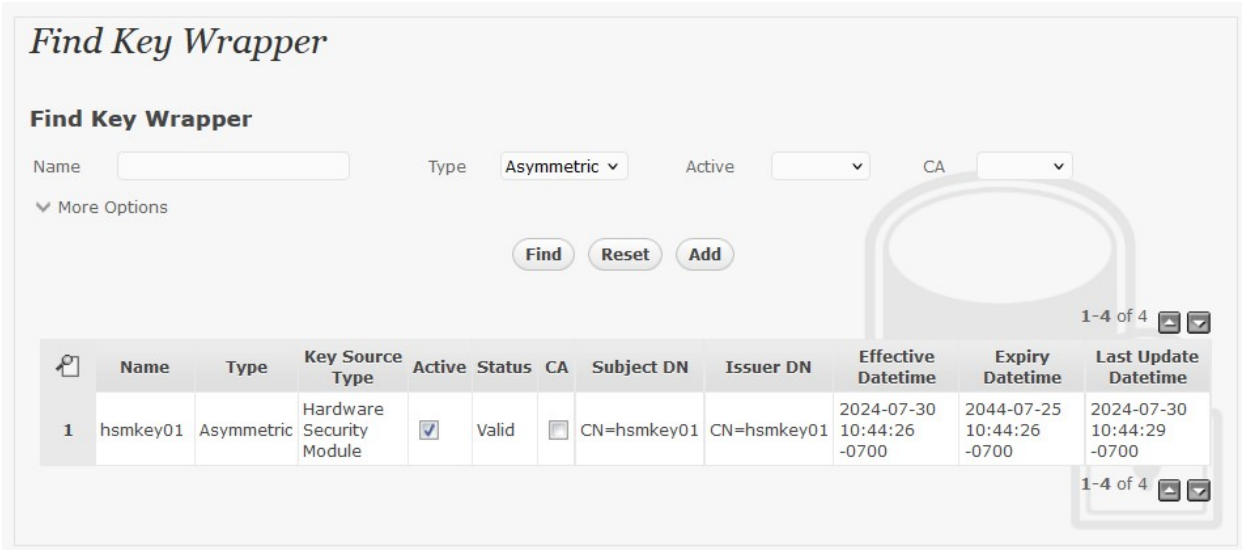
Select “Add Key” and “generate” to create a new key on the HSM.



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



Ensure you import a key from the key manager before you submit the key wrapper.



The new key can be found on the GP HSM as an object using the

`p11tool2`

tool.

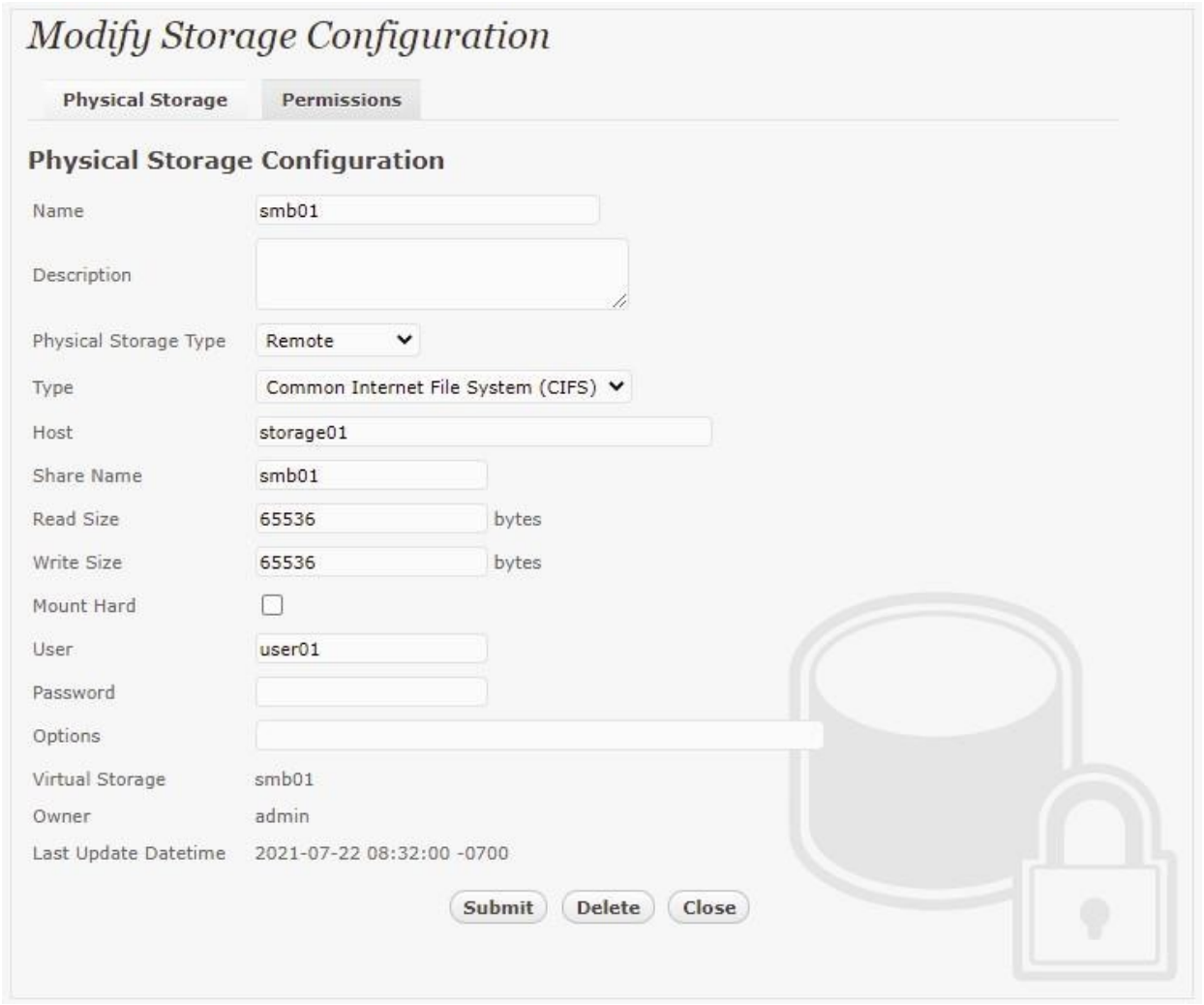
```
[root@cassf156 ~]# /opt/utimaco/bin/p11tool2 slot=0 LoginUser=1234567890 ListObjects


CKO_CERTIFICATE:

+ 1.1
  CKA_CERTIFICATE_TYPE          = CKC_X_509
  CKA_UNIQUE_ID                 = DA7F0FD0-2278-4DC1-8677-4C78047E95FB
  CKA_LABEL                     = hsmkey01
  CKA_ID                        = 0x68736D6B 65793031 (hsmkey01)
  CKA_SUBJECT                   =
               0x30133111 300F0603 5504030C 0868736D |0 1 0   U    hsm|
                 6B657930 31                         |key01          |



CKO_PRIVATE_KEY:

+ 2.1
  CKA_KEY_TYPE                  = CKK_RSA
  CKA_UNIQUE_ID                 = 8EC8F145-A68E-454A-AFE2-291CE5FB4EE3
  CKA_SENSITIVE                 = CK_FALSE
  CKA_EXTRACTABLE               = CK_TRUE
  CKA_LABEL                     =
  CKA_ID                        = 0x68736D6B 65793031 (hsmkey01)
```

4.4.3 Bloombase StoreSafe Data-at-Rest Encryption for SMB Configuration

Physical storage namely

`smb01`

is configured to be secured by Bloombase StoreSafe using encryption.



Virtual storage namely

`smb01`

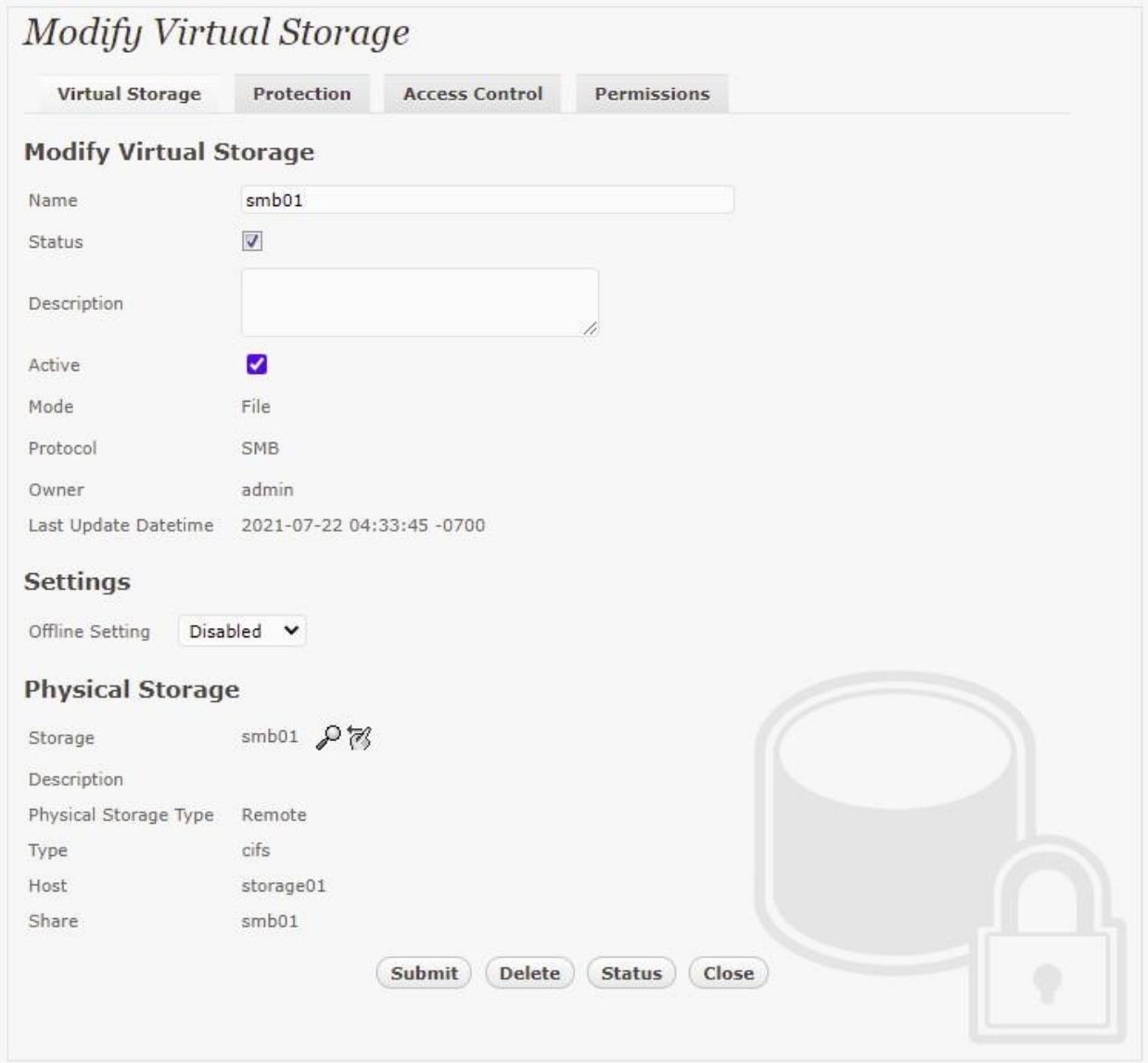
of type

`File`

is created to virtualize physical storage

`smb01`

for application transparent encryption protection over network file protocols including CIFS.



Protection type is specified as

`Privacy`

and secure the Microsoft Storage Server storage backend using

`AES 256-bit`

encryption and encryption key

`hsmkey01`

managed at Utimaco GP HSM.

SMB/CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource

`smb01`

is provisioned for user

`user01`

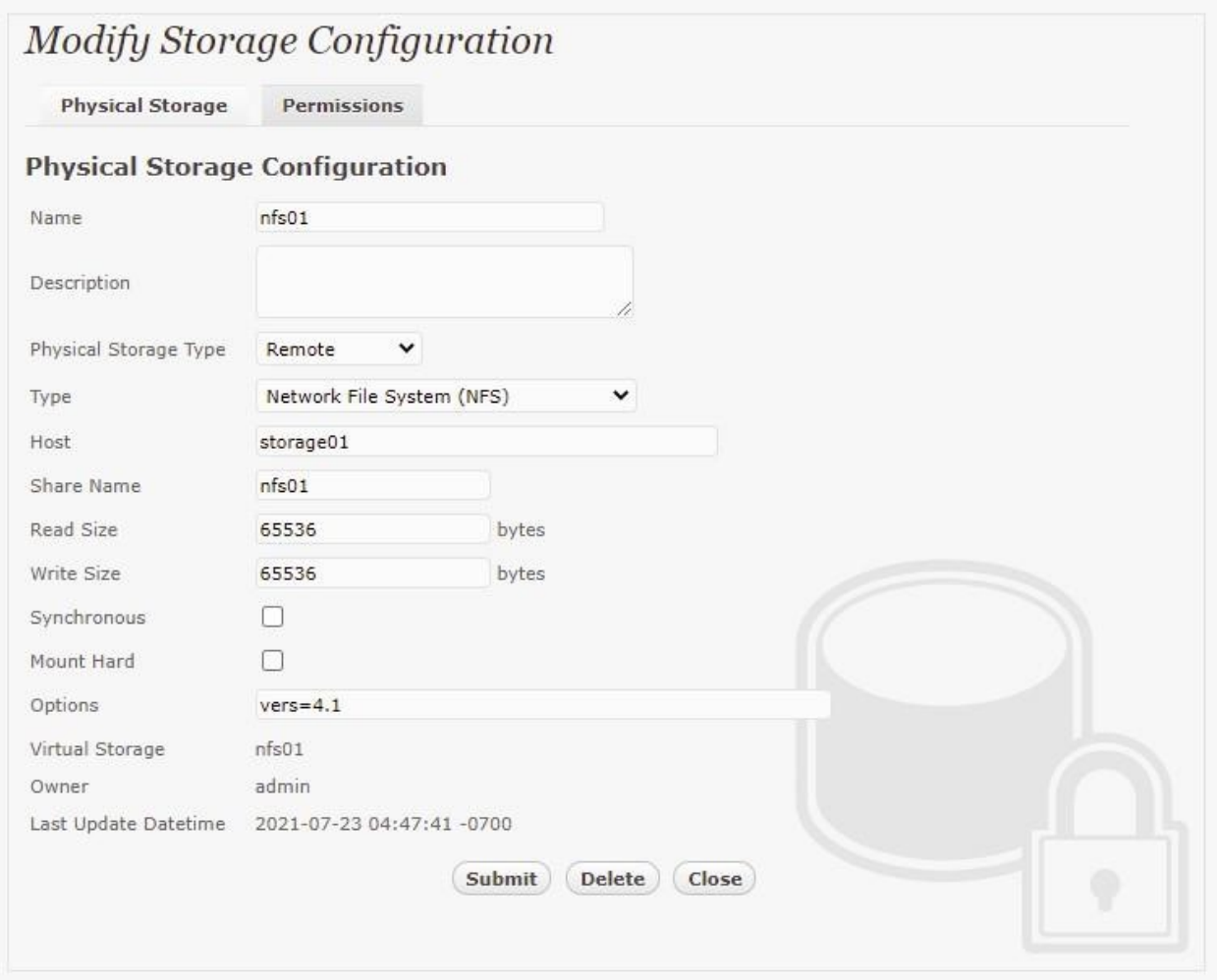
with Microsoft Active Directory integration for user-password authentication and single sign-on.

4.4.4 Bloombase StoreSafe Data-at-Rest Encryption for NFS Configuration

Physical storage namely

`nfs01`

is configured to be secured by Bloombase StoreSafe using encryption.



Virtual storage namely

`nfs01`

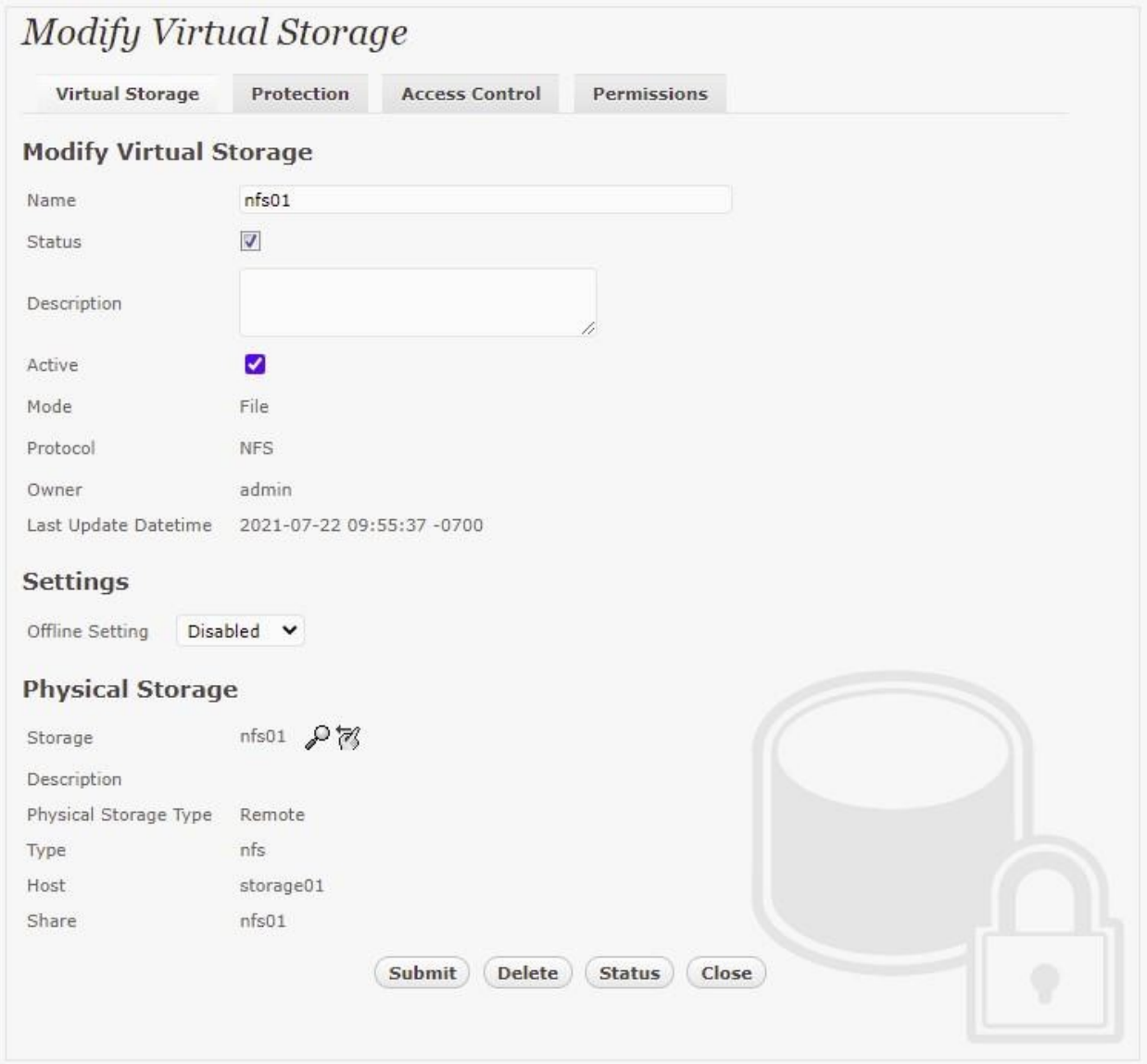
of type

`File`

is created to virtualize physical storage

`nfs01`

for application transparent encryption protection over network file protocols including NFS.



Protection type is specified as

`Privacy`

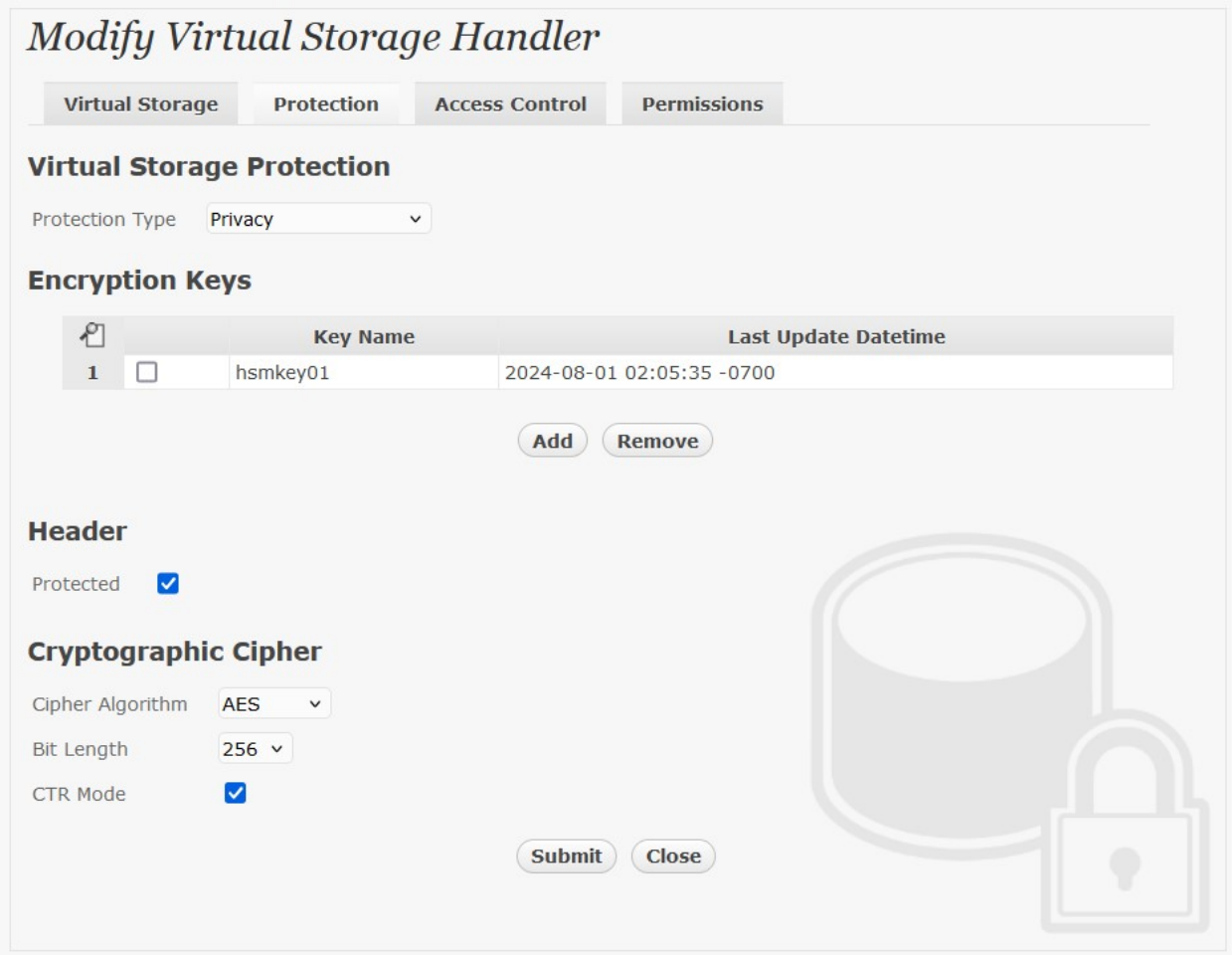
and secure the Microsoft Storage Server storage backend using

`AES 256-bit`

encryption and encryption key

`hsmkey01`

managed at Utimaco GP HSM.

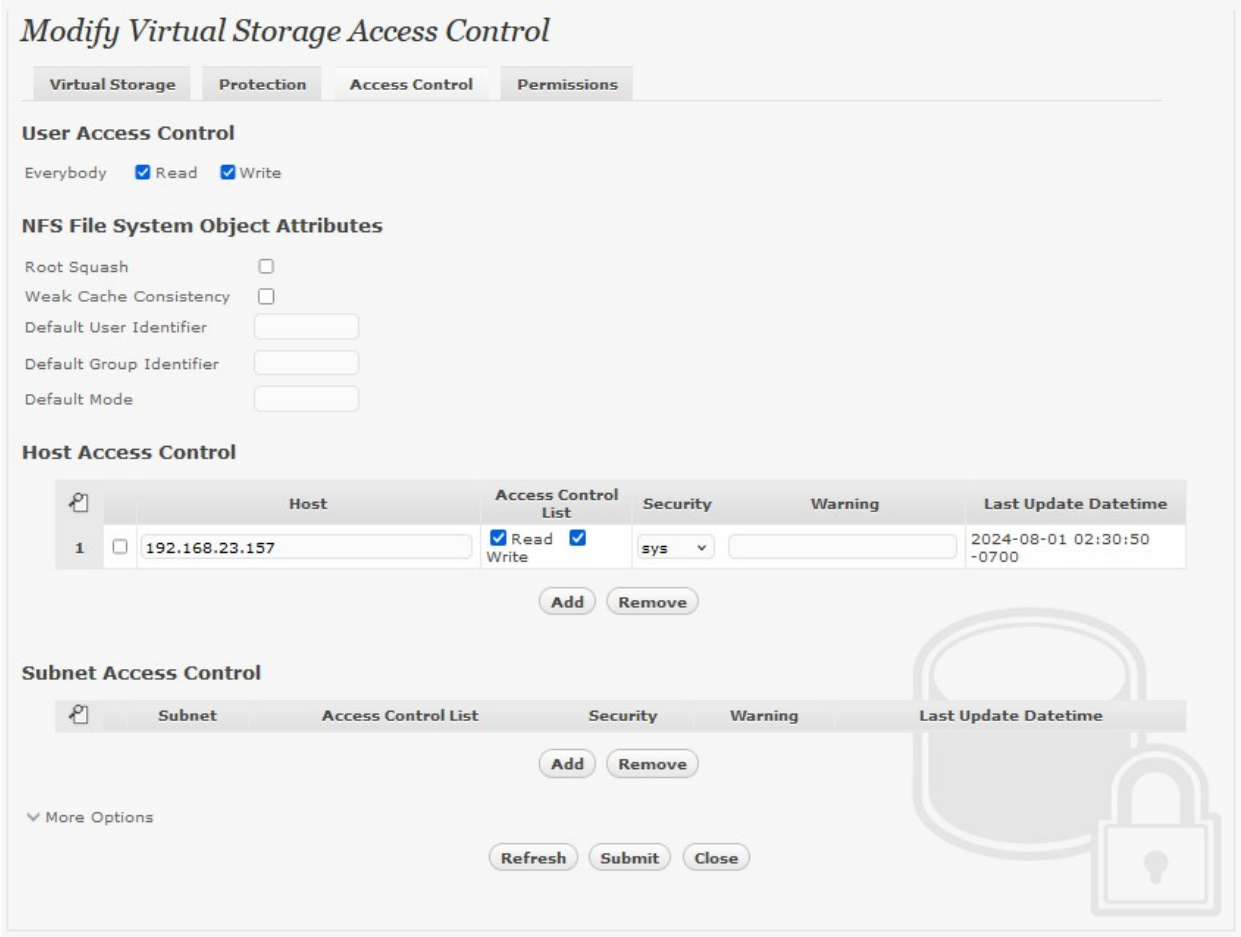


NFS storage protocol relies mainly on UID/GID and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

`nfs01`

is provisioned for client IP

`192.168.23.157`

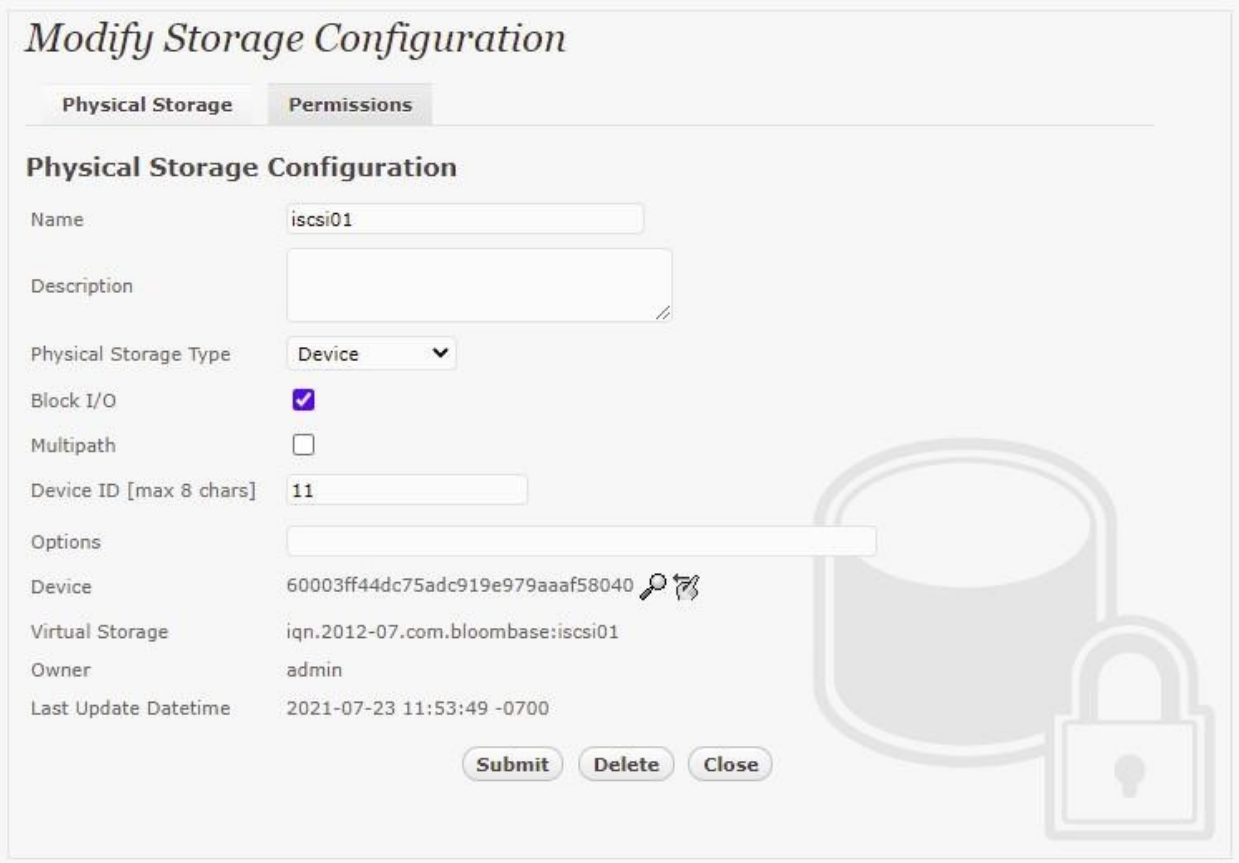


4.4.5 Bloombase StoreSafe Data-at-Rest Encryption for iSCSI Configuration

Physical storage namely

`iscsi01`

is configured to be secured by Bloombase StoreSafe using encryption.



Virtual storage namely

`iqn.2012-07.com.bloombase:iscsi01`

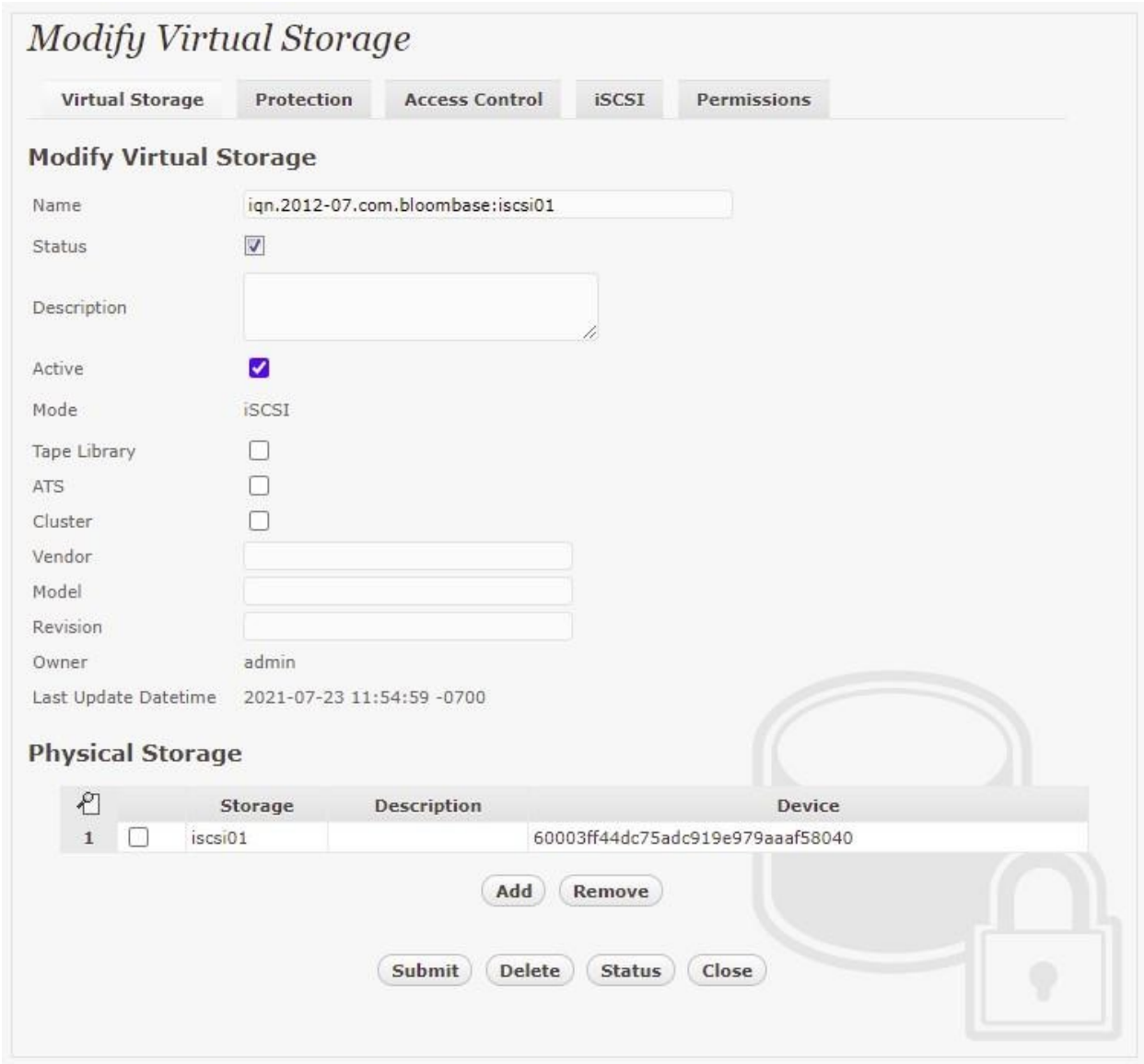
of type

`iSCSI`

is created to virtualize physical storage

`iscsi01`

for application transparent encryption protection over network file protocols including iSCSI.



Protection type is specified as

`Privacy`

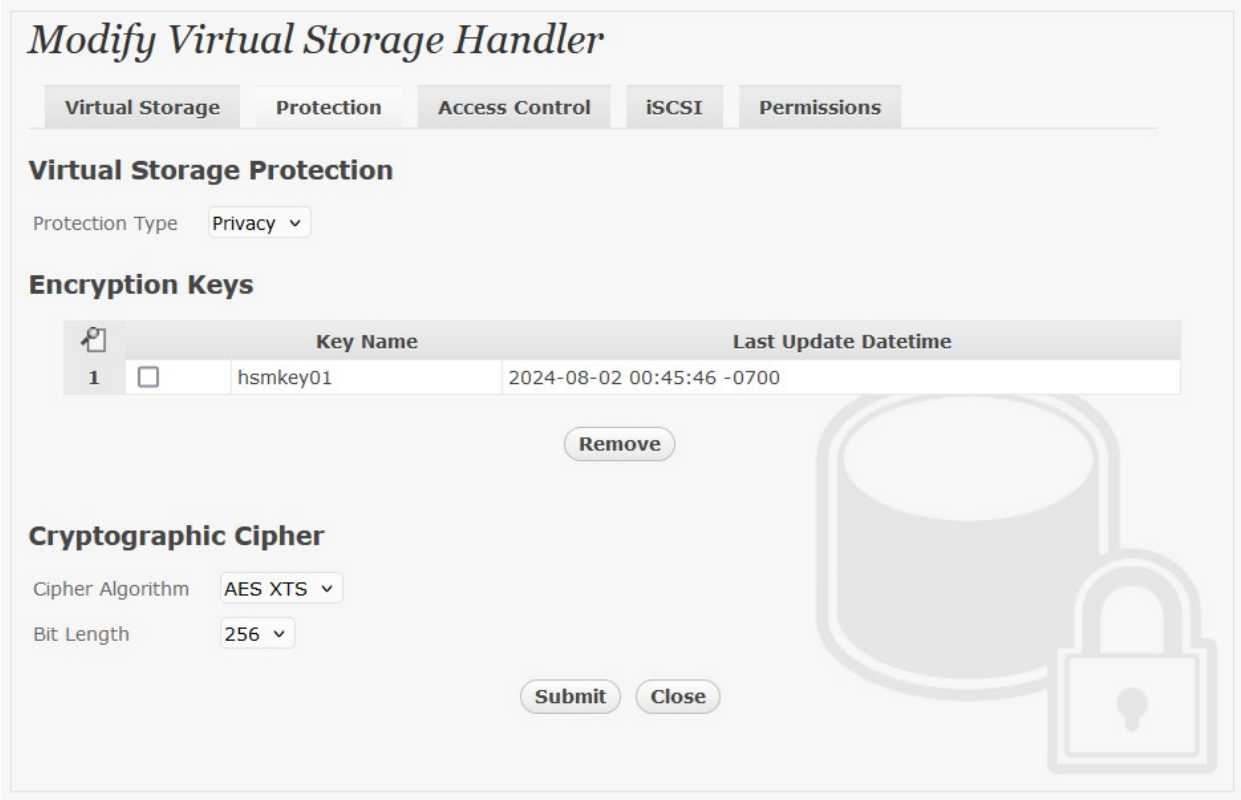
and secure the Microsoft Storage Server storage backend using

`AES XTS 256-bit`

encryption and encryption key

`hsmkey01`

managed at Utimaco GP HSM.

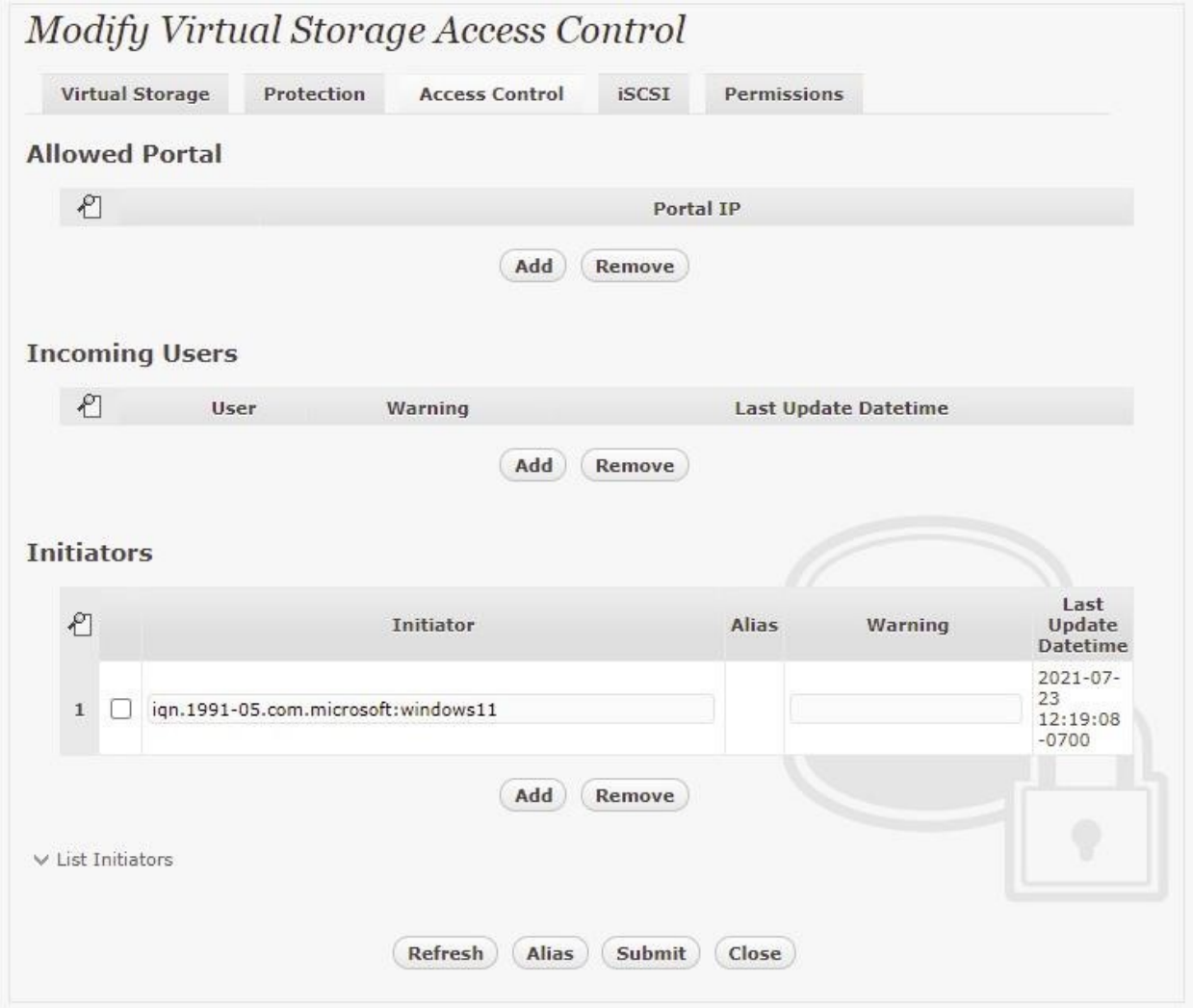


iSCSI storage protocol relies mainly on CHAP, IQN, and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

```
iqn.2012-07.com.bloombase:iscsi01
```

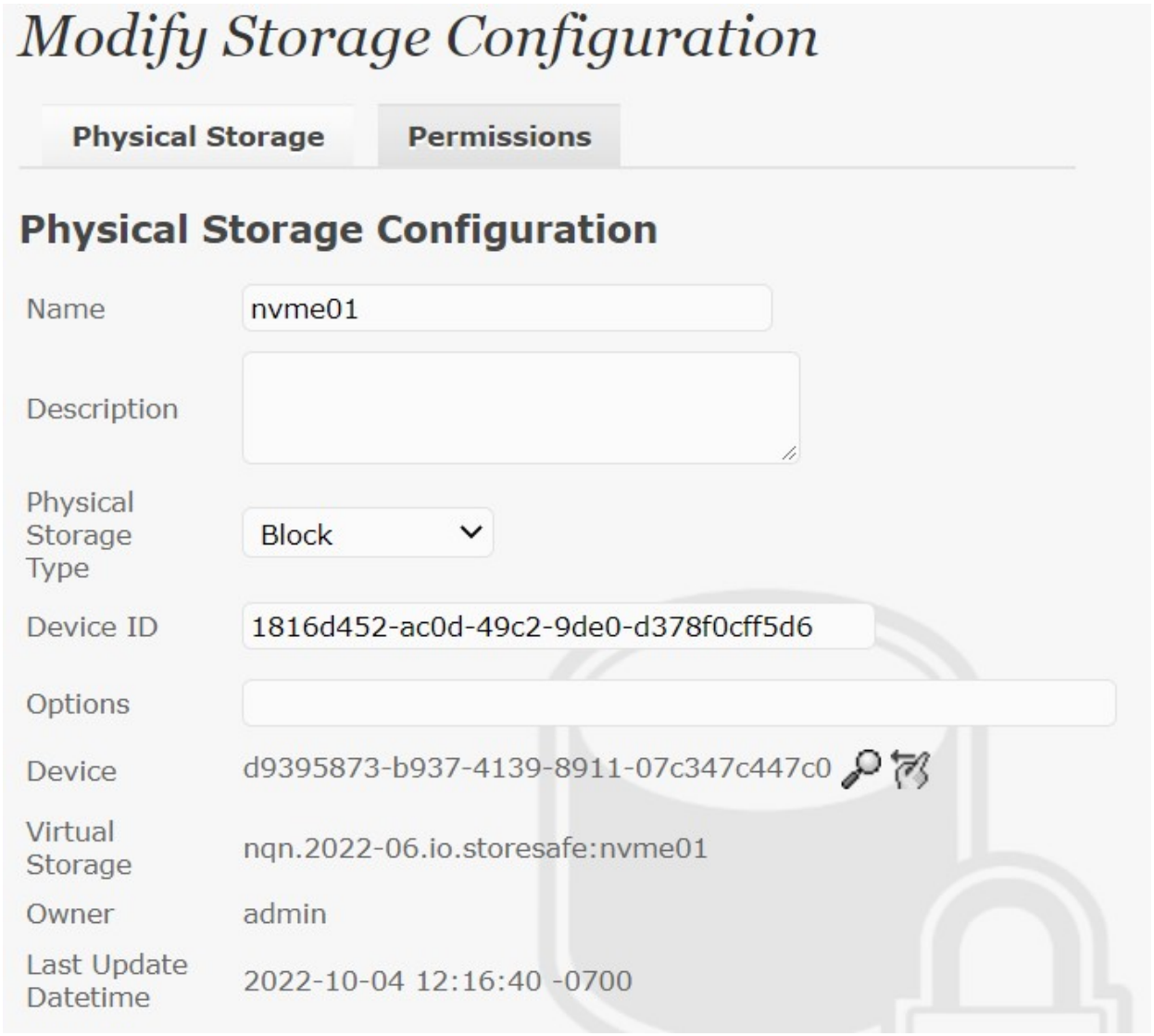
is provisioned for initiator

```
iqn.1991-05.com.microsoft:windows11
```

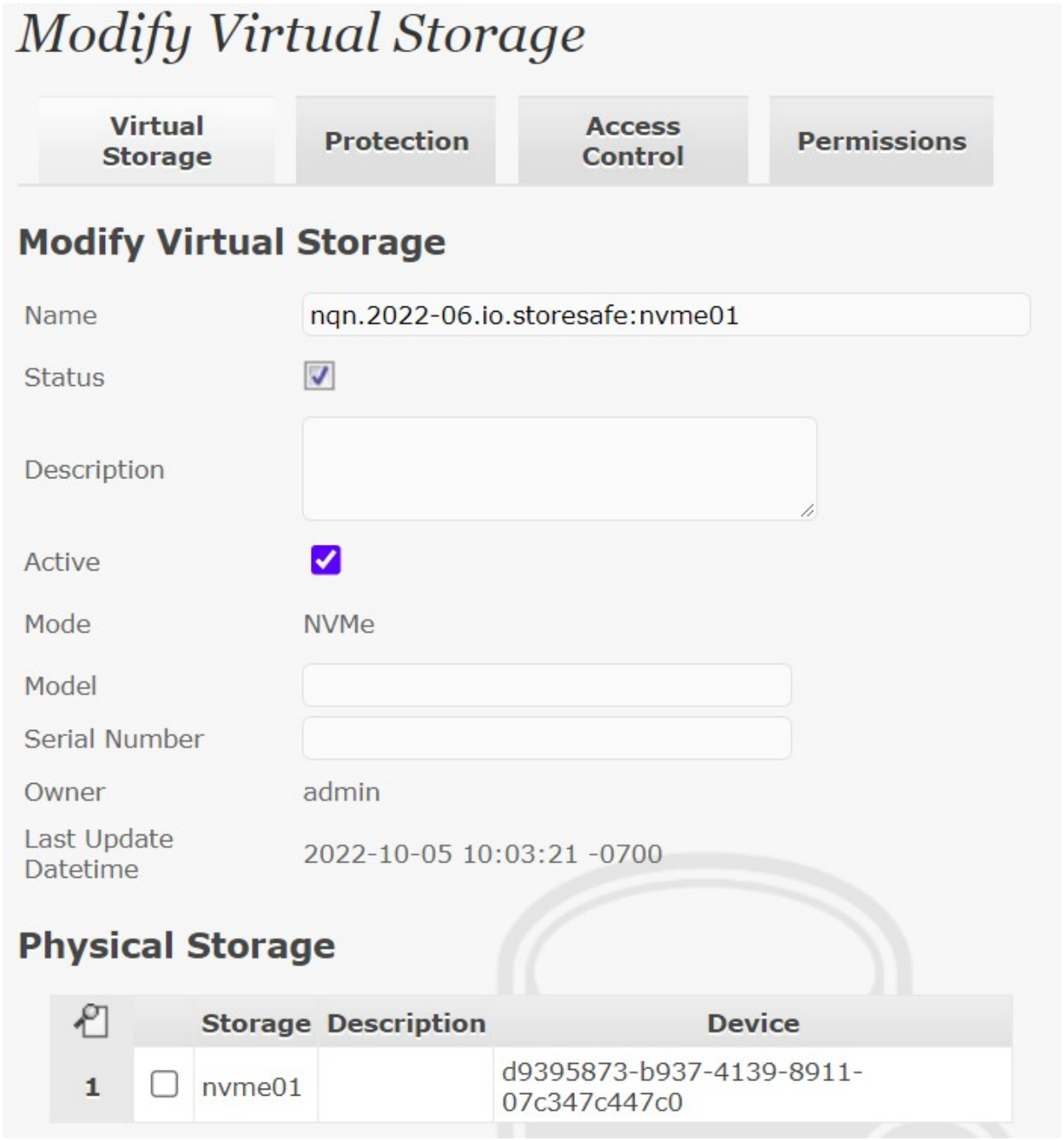


4.4.6 Bloombase StoreSafe Data-at-Rest Encryption for NVMe/TCP Configuration

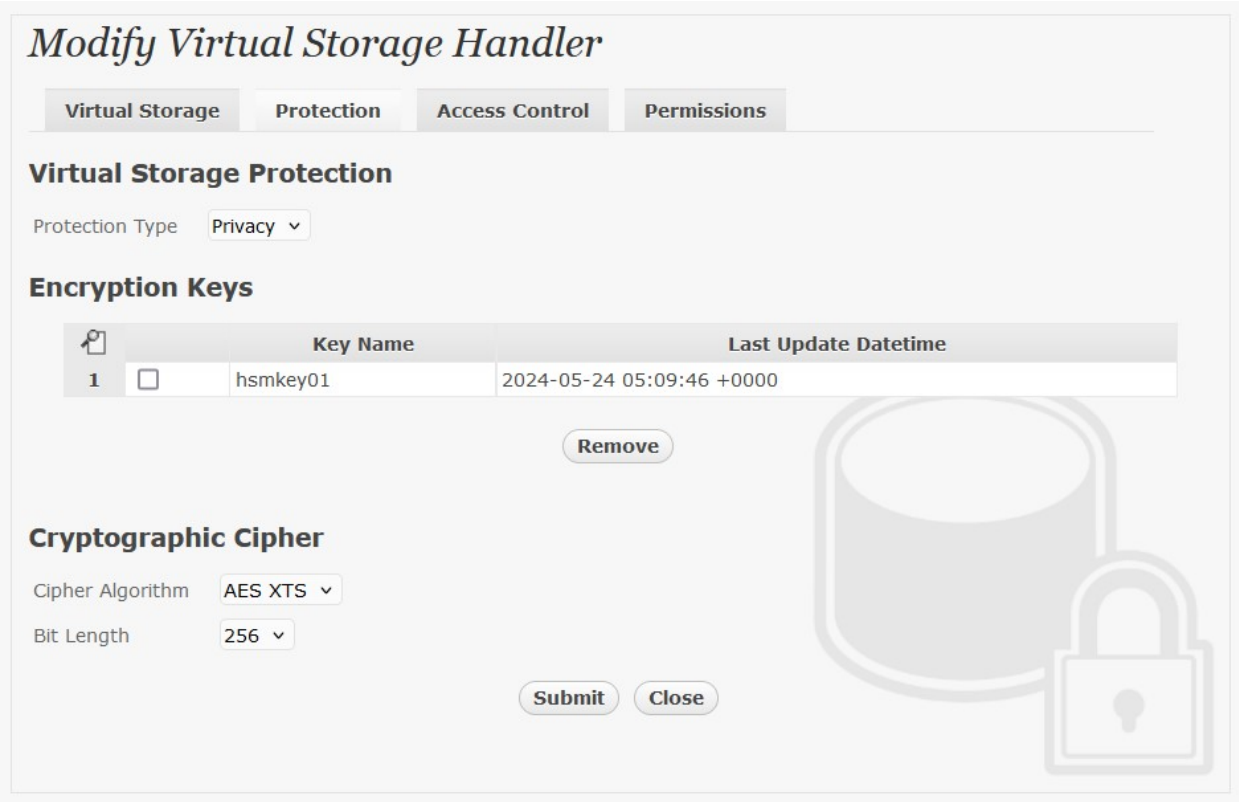
Physical storage with Intel Solid State Drive DC P3600 Series PCIe NVMe SSDs is configured to be secured by Bloombase StoreSafe Intelligent Storage Firewall.



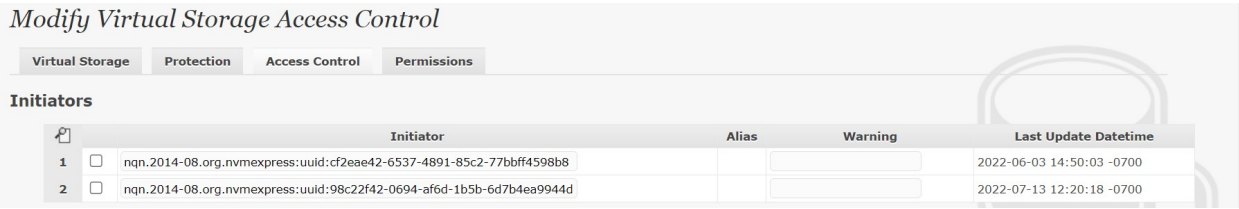
Virtual storage with “NVMe” mode is created to secure the just configured physical storage.



Select “Privacy” for protection type and select the encryption key. Choose the cipher algorithm and bit length.



Add clients' NVMe Qualified Name (NQN) that can access Bloombase StoreSafe virtual storage.



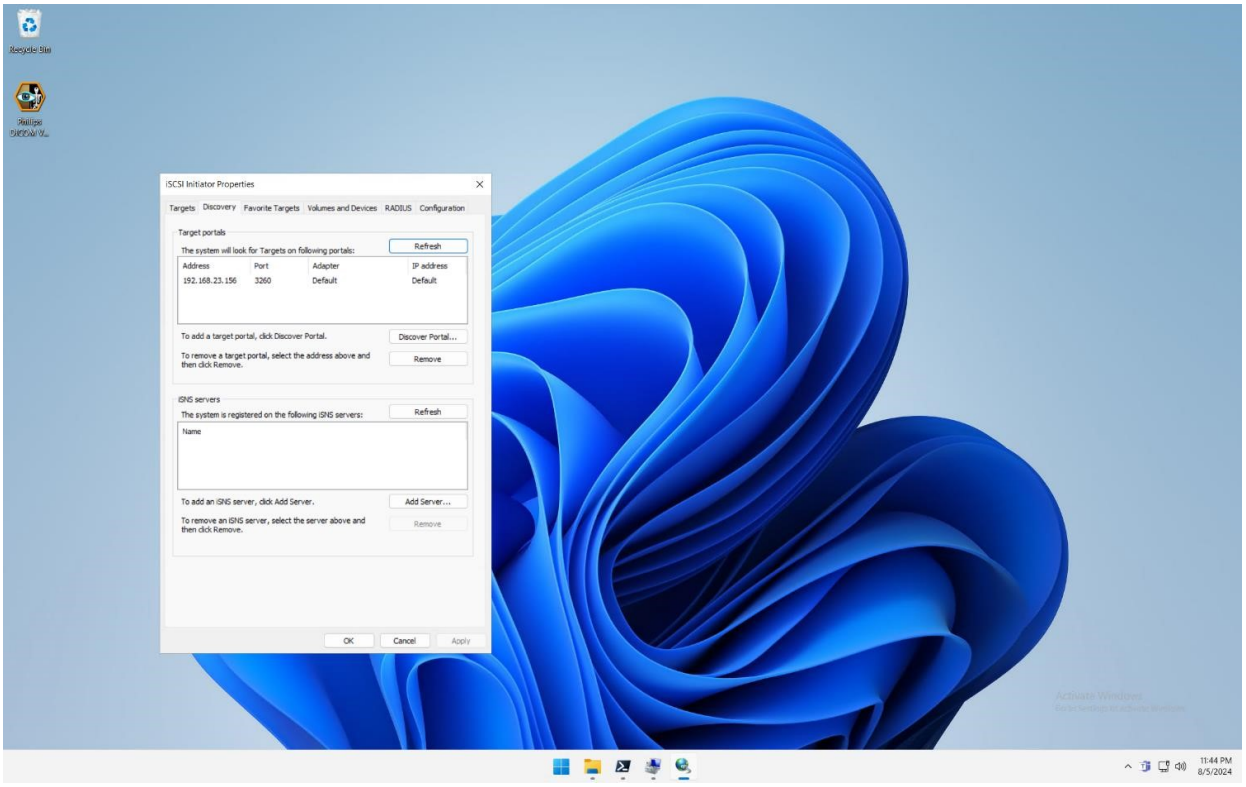
Start Bloombase StoreSafe virtual storage.


Virtual Storage Status
Virtual Storage
Name nqn.2022-06.io.storesafe:nvme01
Status
Active
Type NVMe
Physical Storage
Name nvme01
Type Unknown
Active Share Status
Share Name nqn.2022-06.io.storesafe:nvme01
Storage Type Unknown
Storage Path Target : nqn.2022-06.io.storesafe:nvme01 LUN 1:[_SS_nvme33n1__];
Sessions 2
Refresh
Stop
Start
Close

4.5 Storage Clients

4.5.1 Microsoft Windows 11

Client host running Microsoft Windows 11 is used to access Bloombase StoreSafe Intelligent Storage Firewall virtual storage.



4.5.2 Ubuntu 22.04 LTS

Client host running Ubuntu 22.04 LTS is used to access Bloombase StoreSafe Intelligent Storage Firewall virtual storage.

```
user@ubuntu68:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.2 LTS
Release:        22.04
Codename:       jammy
```

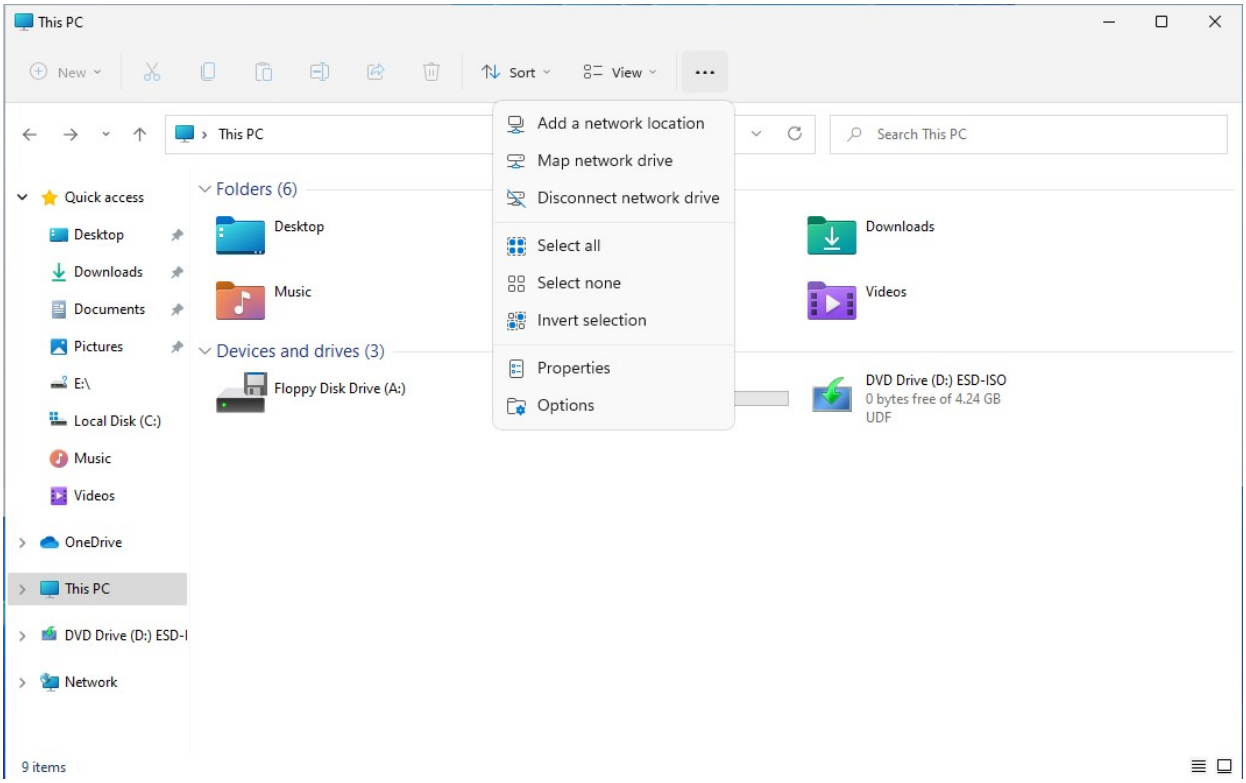
The client will need nvme initiator software installed.

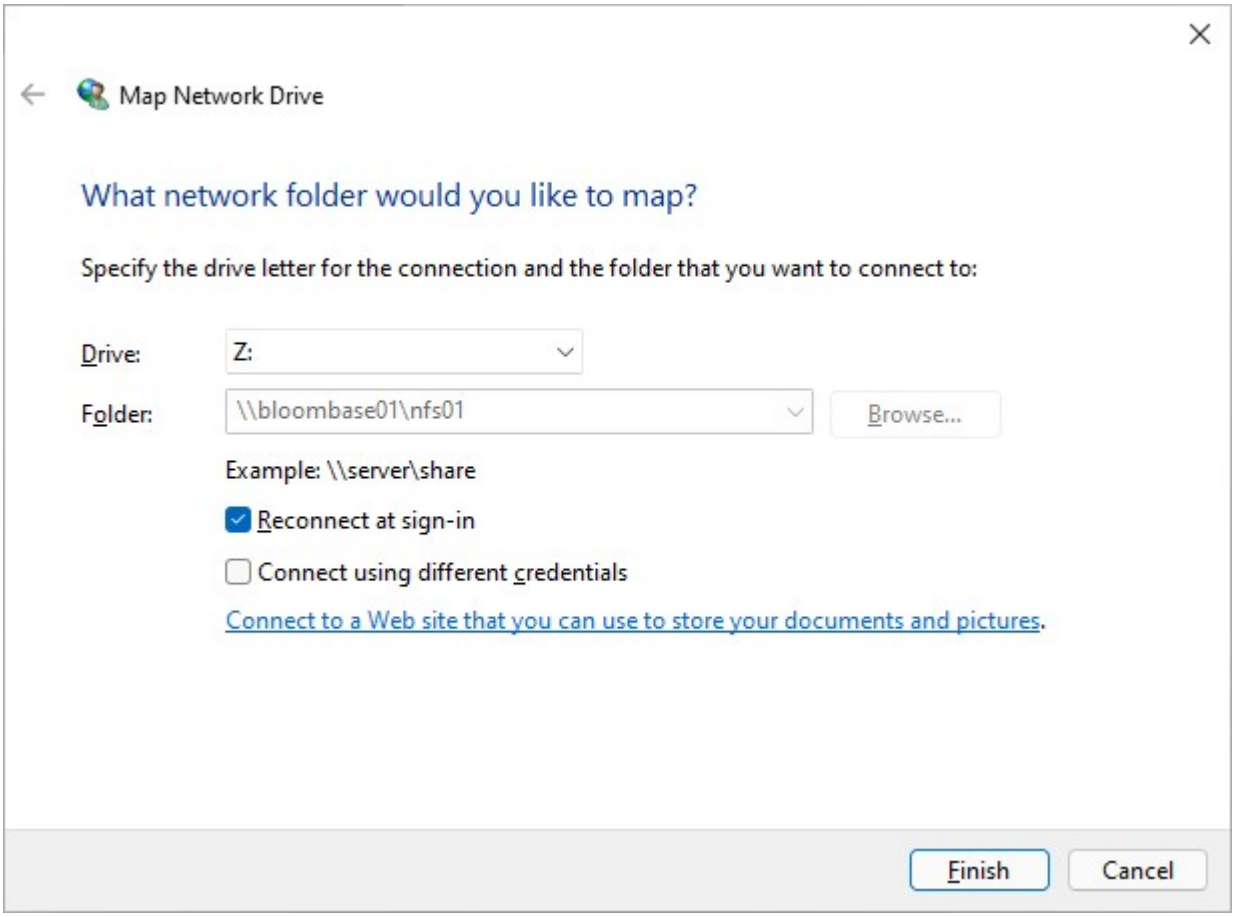
```
user@ubuntu68:~$ nvme --version
nvme version 1.16
```

5 Test Cases

5.1 Tests for Data-at-Rest Encryption over NFS

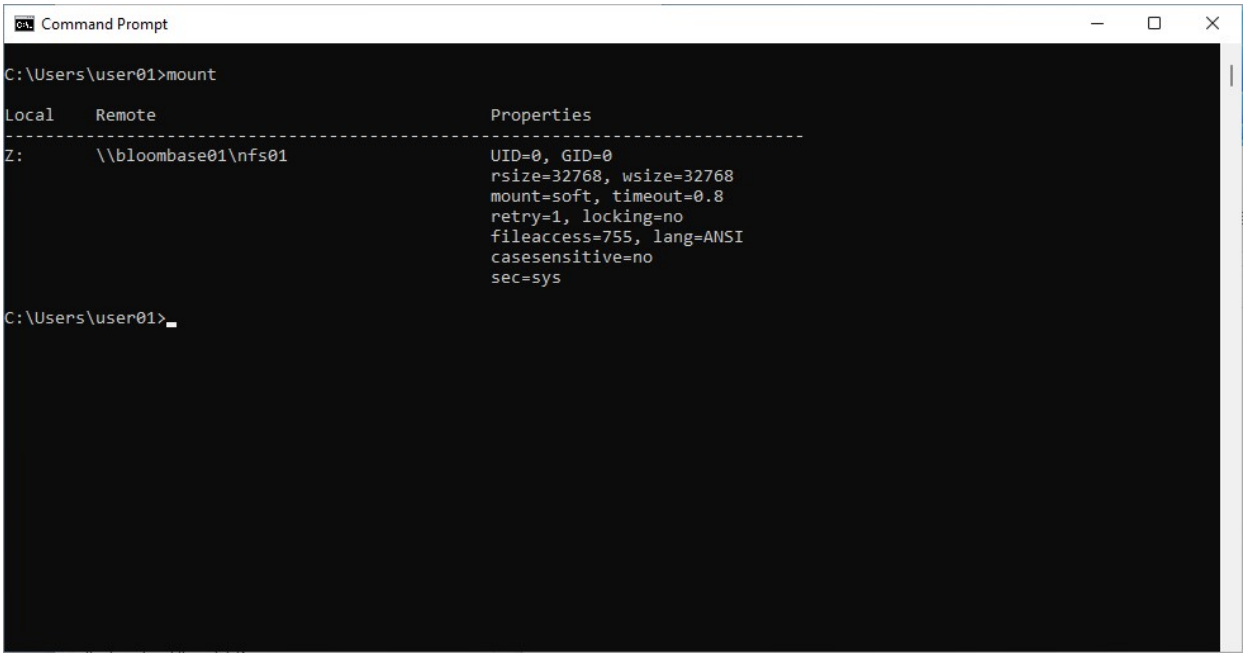
NFS shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2025 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.



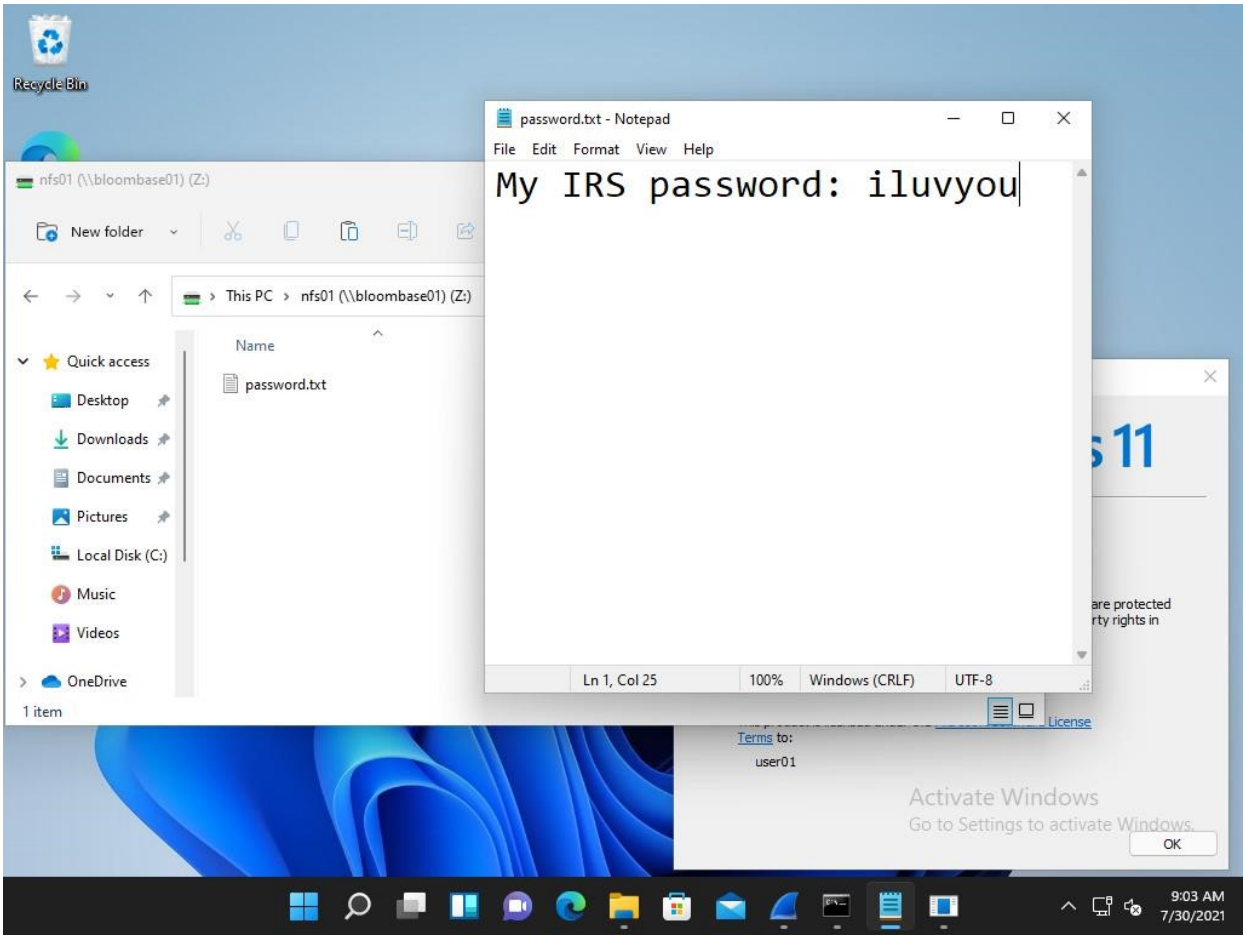


Microsoft Windows 11 clients can use the included map network drive option to add the NFS share presented by

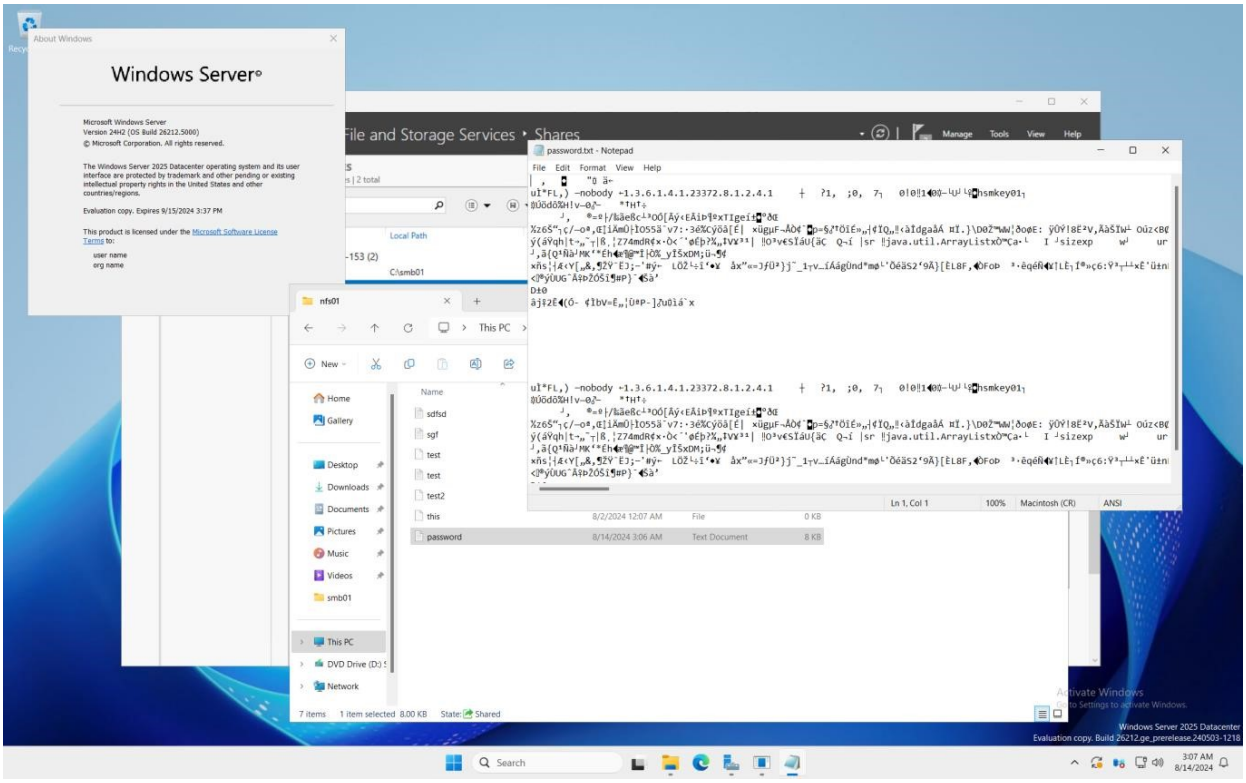
Bloombase StoreSafe Intelligent Storage Firewall with a drive letter. Data owners can alternatively use the mount command to specify additional mounting options.



On the demo virtual encrypted NFS share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Microsoft Windows Server 2025 backend share.



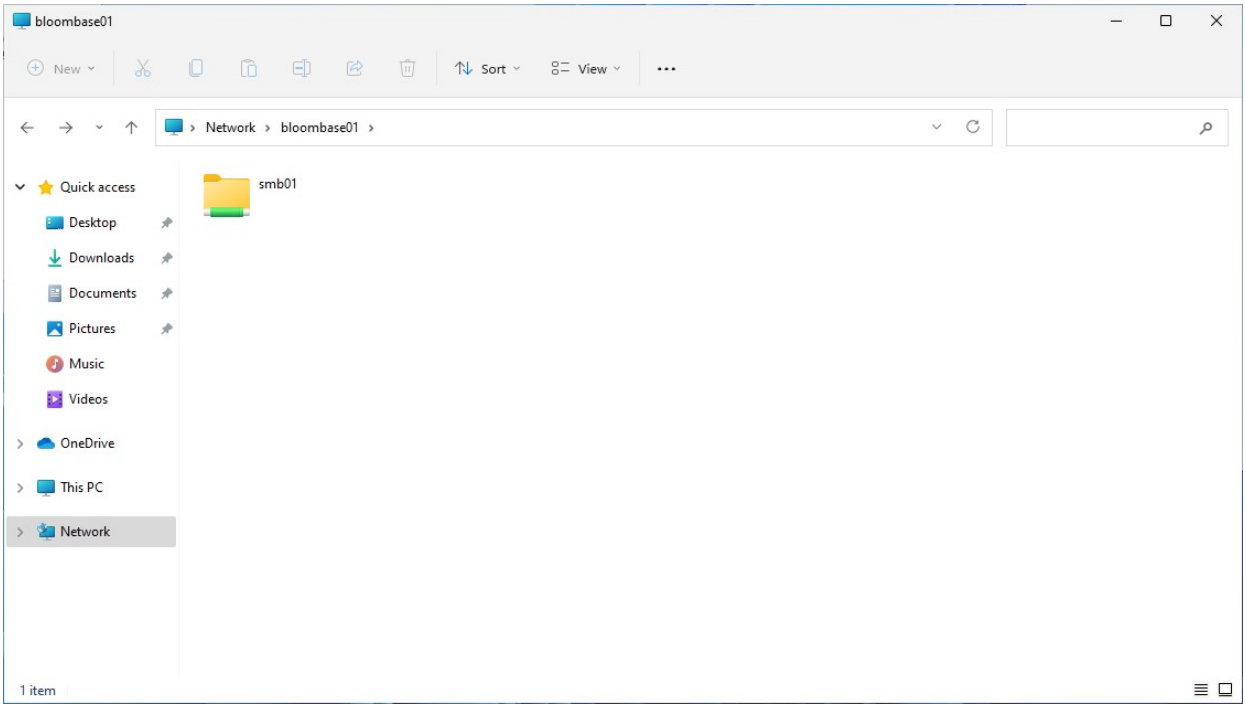
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.

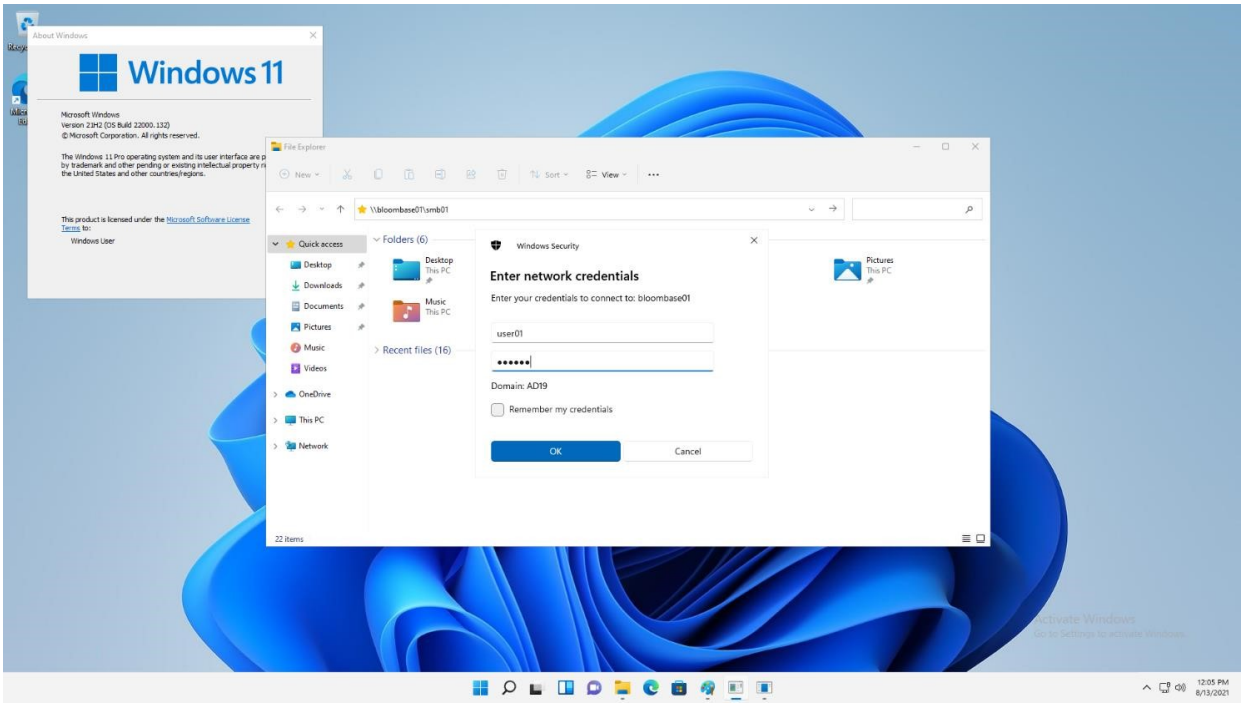


5.2 Tests for Data-at-Rest Encryption over SMB

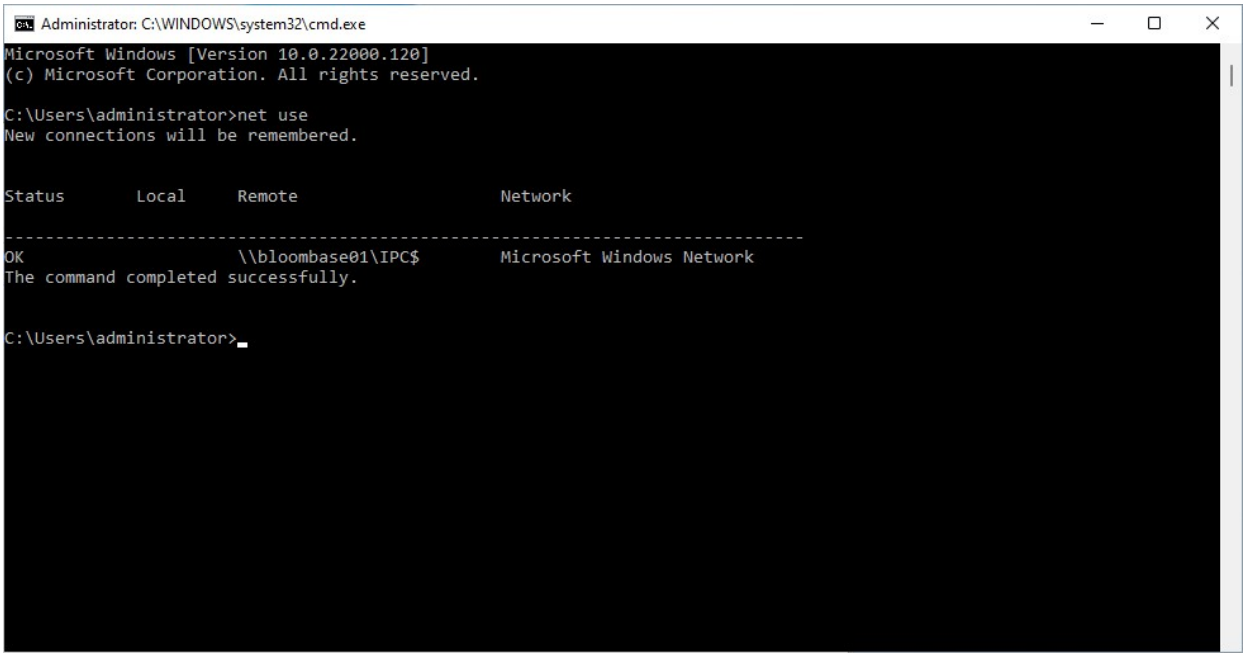
SMB shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2025 system that is accessible by domain users is created to act as backend storage. Bloombase

StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.

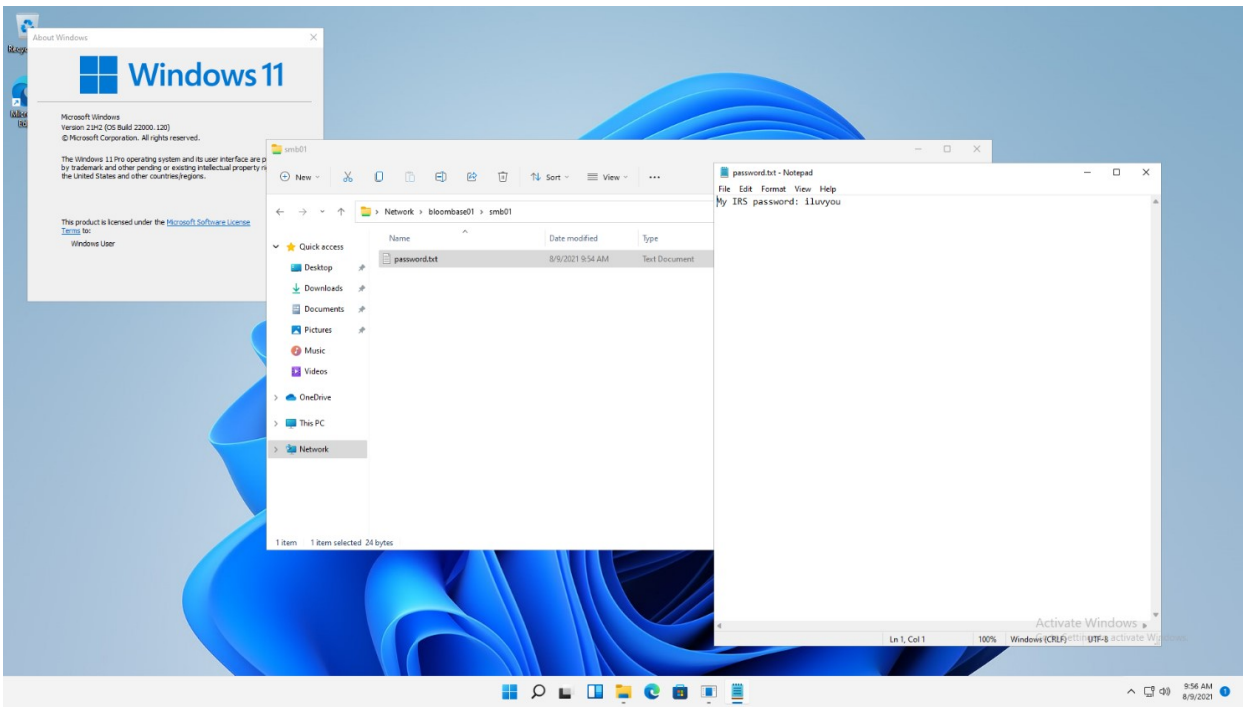




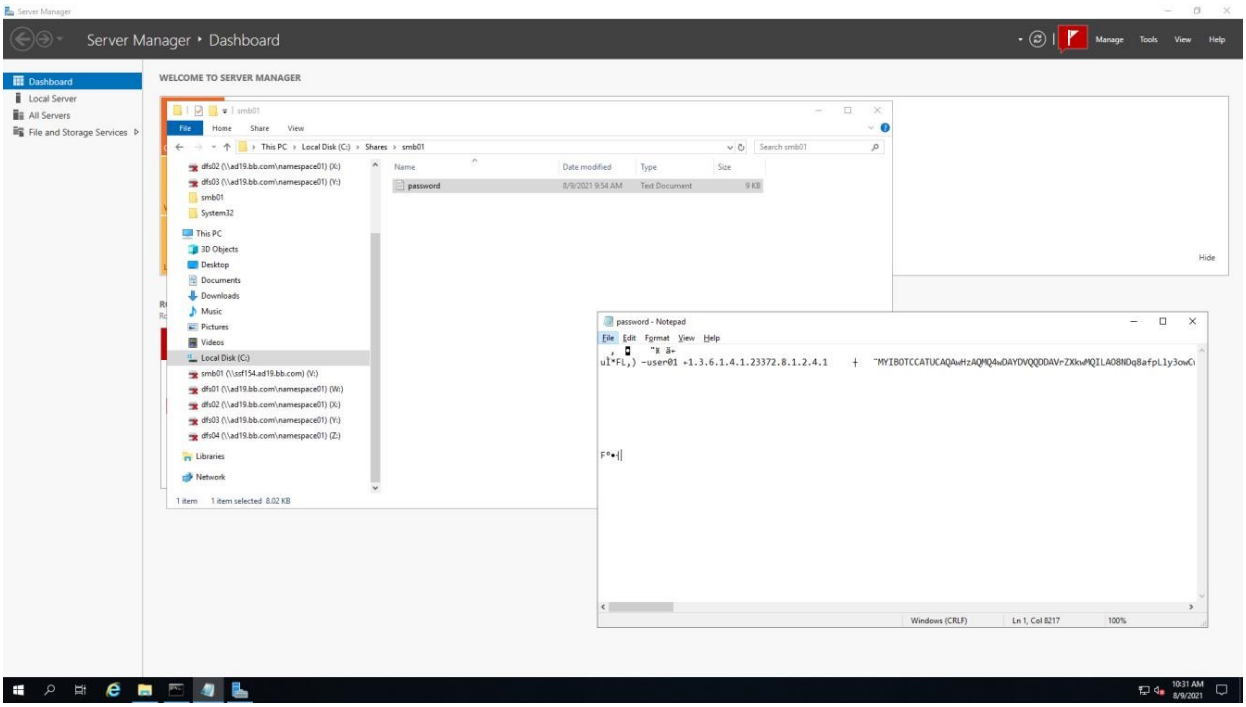
Microsoft Windows 11 clients can use the included network share on file manager to access the SMB share presented by Bloombase StoreSafe Intelligent Storage Firewall. Data owners can alternatively use the Net Use command to specify additional mounting options.



On the demo virtual encrypted SMB share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Windows Server 2025 backend share.

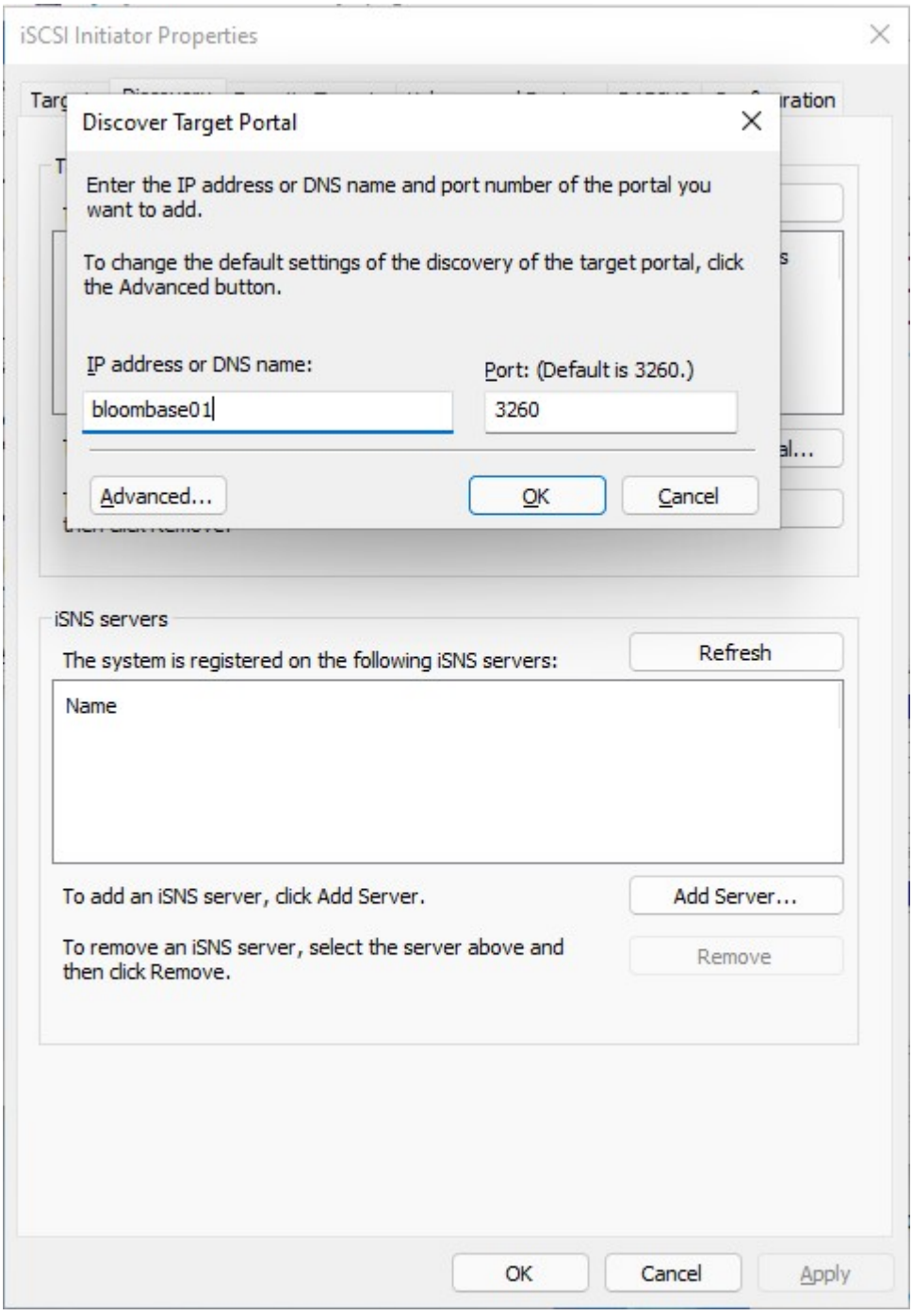


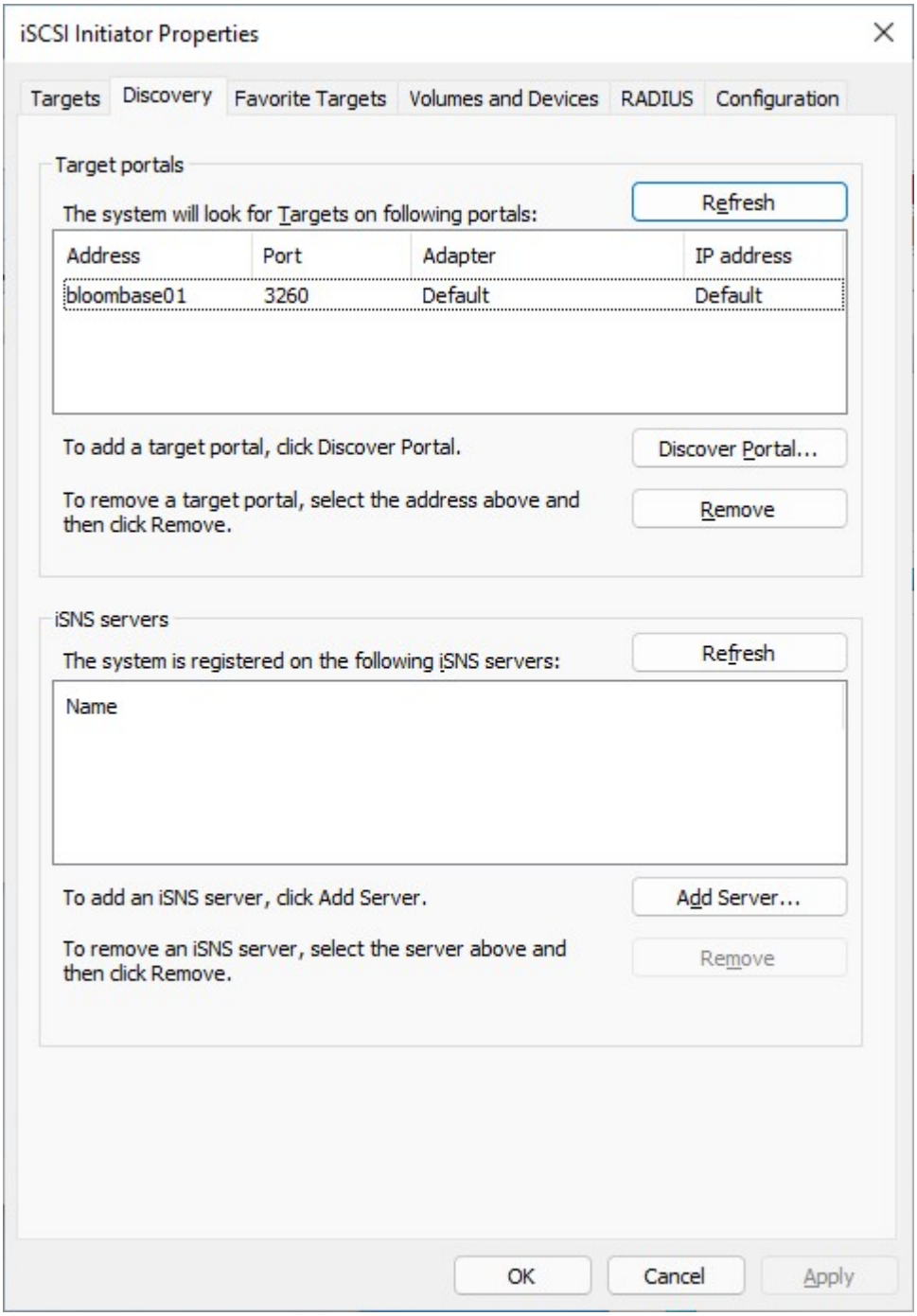
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



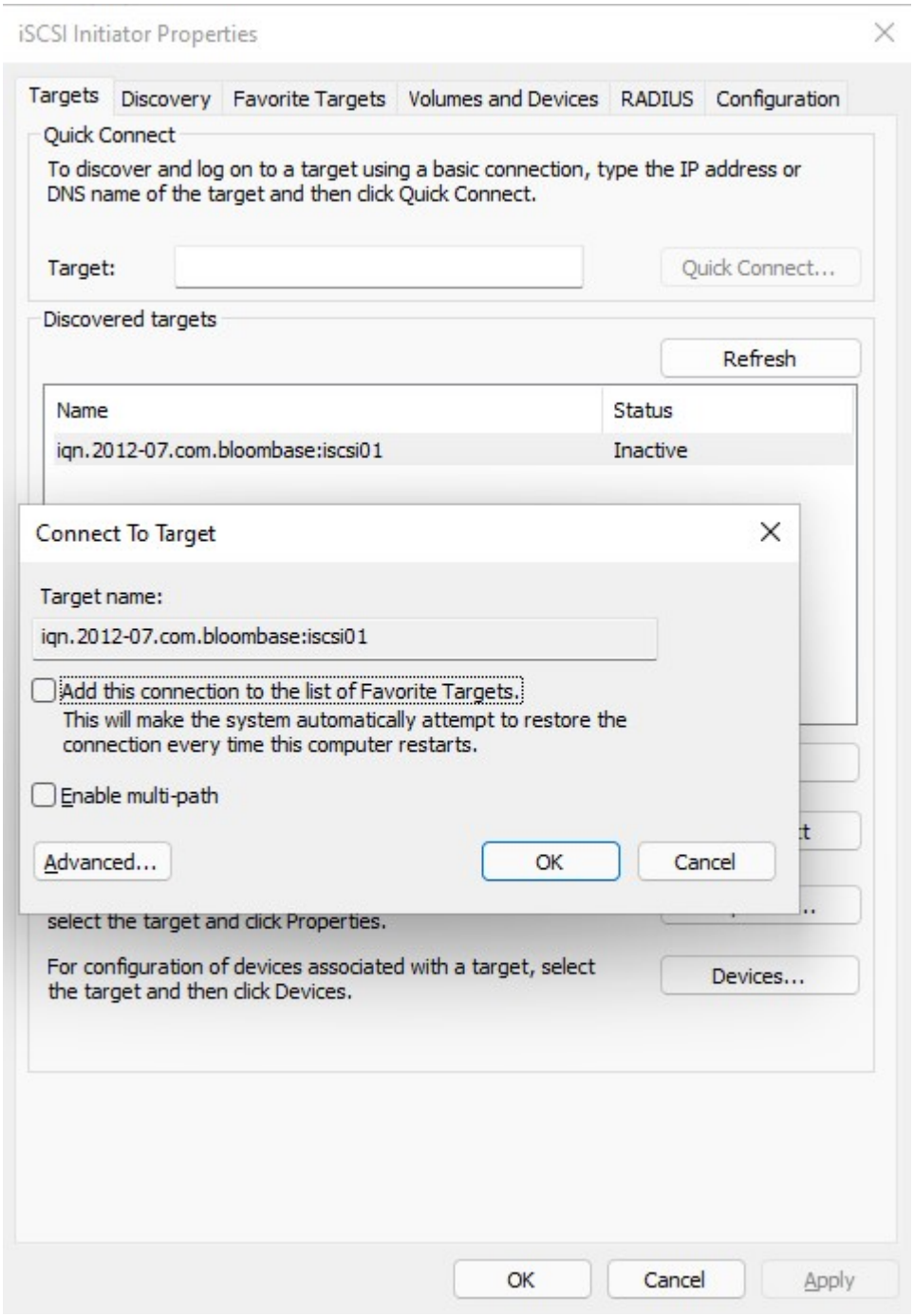
5.3 Tests for Data-at-Rest Encryption over iSCSI

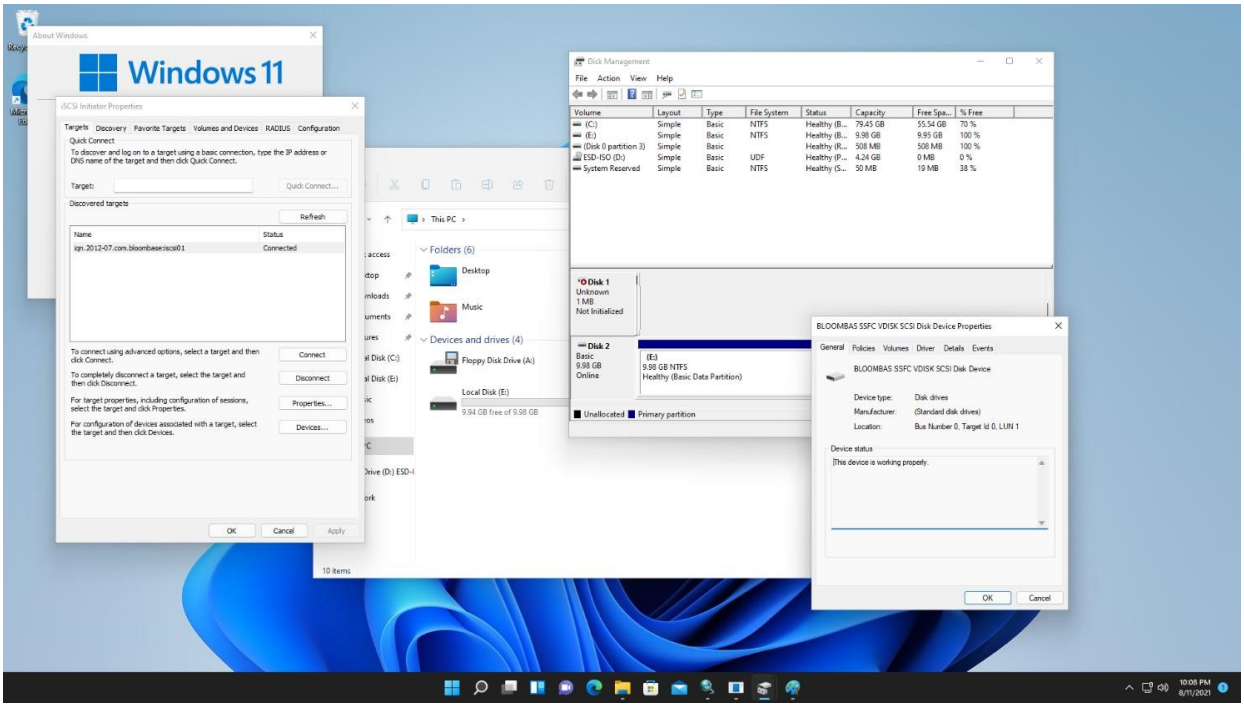
iSCSI targets are an example from the many protocols Bloombase StoreSafe supports for encryption. A target from a Microsoft Windows Server 2025 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.


iSCSI Initiator Properties
Discover Target Portal
Enter the IP address or DNS name and port number of the portal you want to add.
To change the default settings of the discovery of the target portal, click the Advanced button.
IP address or DNS name:
bloombase01
Port: (Default is 3260.)
3260
Advanced...
OK
Cancel
iSNS servers
The system is registered on the following iSNS servers:
Refresh
Name
To add an iSNS server, click Add Server.
Add Server...
To remove an iSNS server, select the server above and then click Remove.
Remove
OK
Cancel
Apply

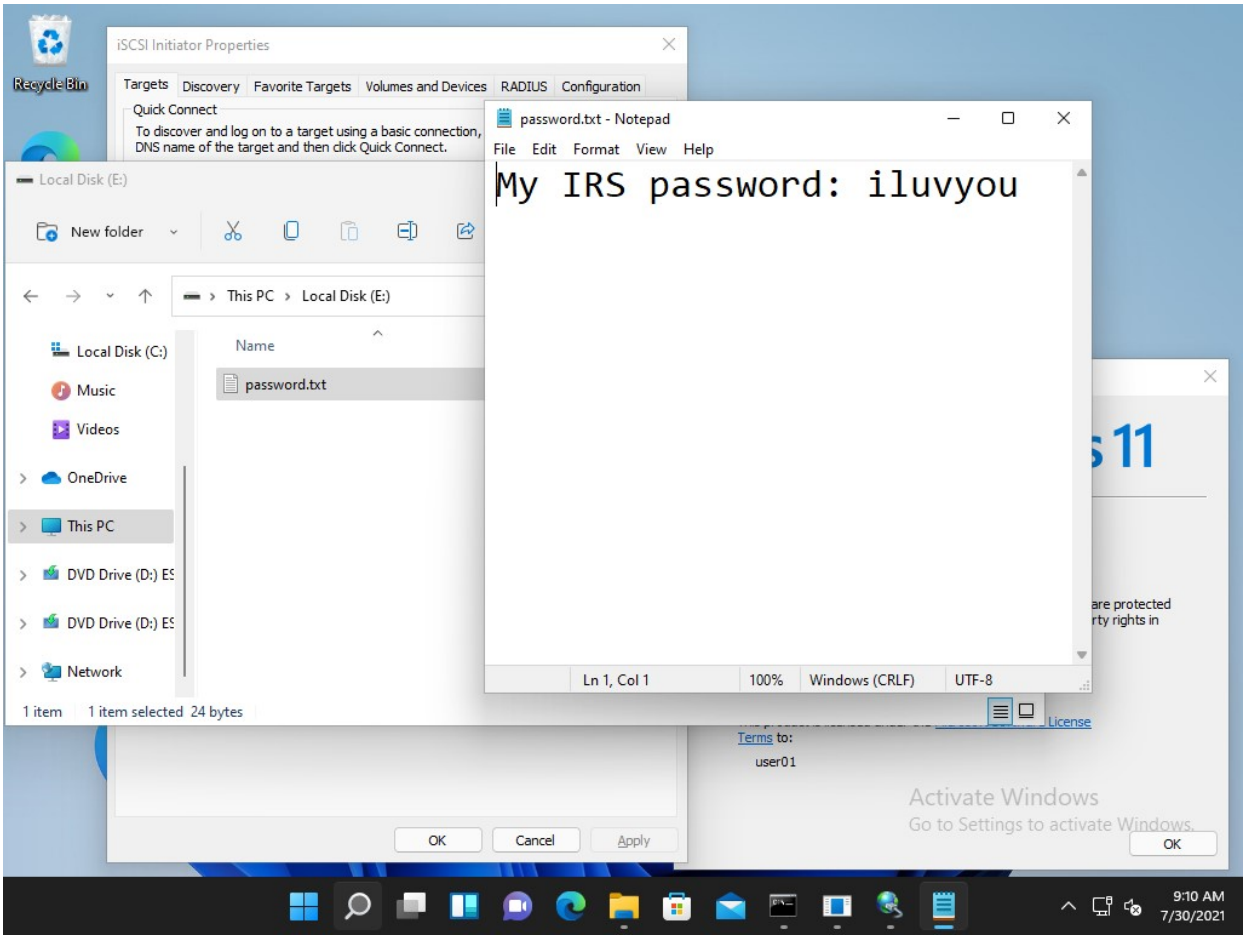


Microsoft Windows 11 clients can attach the virtual encrypted share with the default iSCSI initiator tool. Add the hostname and port to the discover tab, then connect to the iSCSI storage target presented by Bloombase StoreSafe Intelligent Storage Firewall. To access the Bloombase StoreSafe iSCSI disk, make sure the client IQN is be added the Bloombase StoreSafe configuration. The disk will be mounted to the system and it can be formatted with a filesystem.

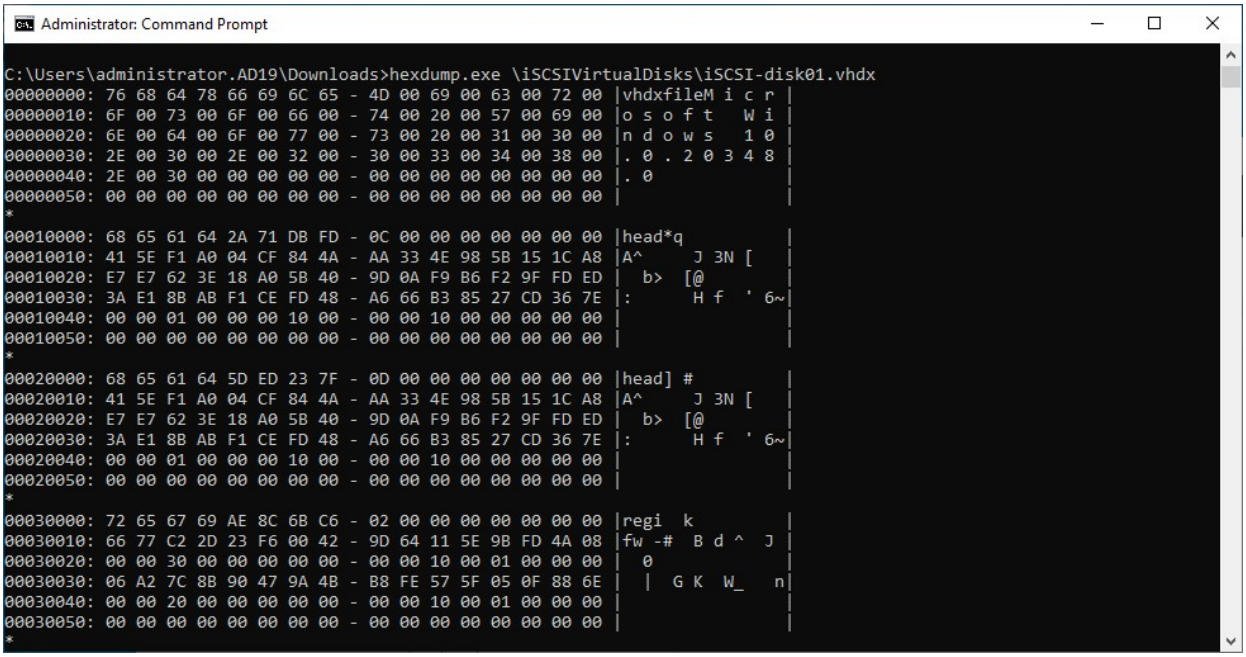

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
iqn.2012-07.com.bloombase:iscsi01
Inactive
Connect To Target
Target name:
iqn.2012-07.com.bloombase:iscsi01
Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.
Enable multi-path
Advanced...
OK
Cancel
select the target and click Properties.
For configuration of devices associated with a target, select the target and then click Devices.
Devices...
OK
Cancel
Apply

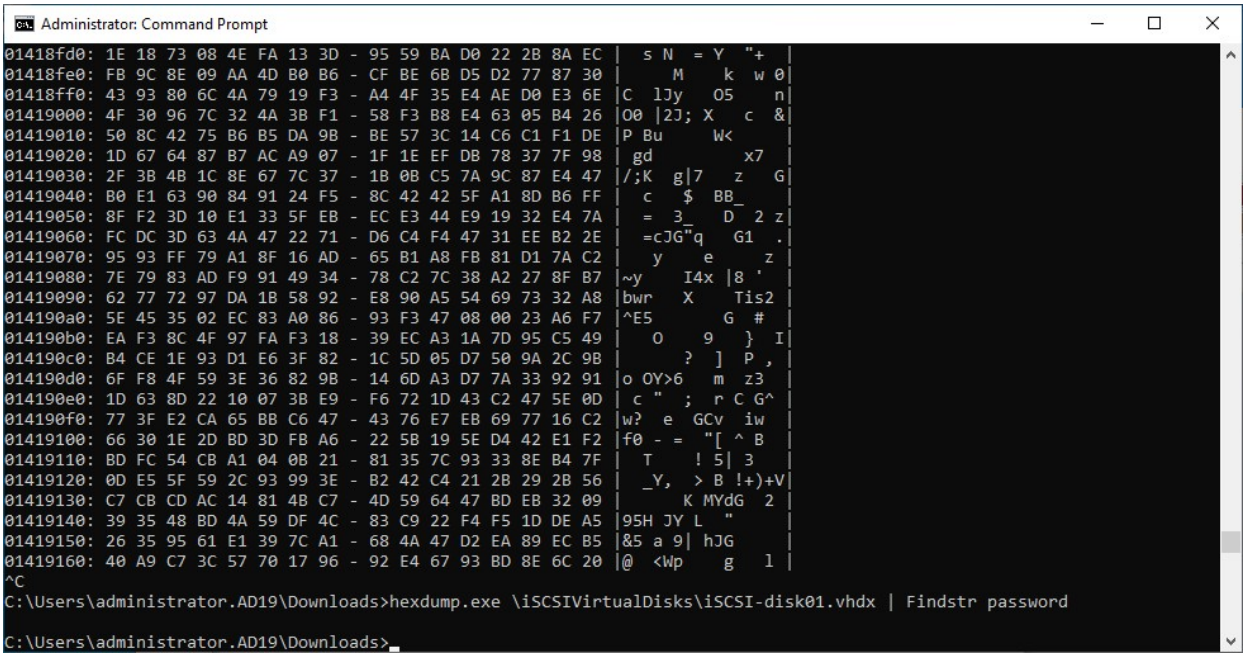


On the demo virtual encrypted iSCSI target, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine and stored on the Microsoft Windows Server 2025 storage backend.



If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.





5.4 Tests for Data-at-Rest Encryption over NVMe/TCP

Client that has appropriate access can discover Bloombase StoreSafe Intelligent Storage Firewall virtual storage over NVMe/TCP protocol.

```
[root@bb027 ~]# nvme discover -t tcp -a 192.168.211.24 -s 4420 -q nqn.2014-08.org.nvmexpress:uuid:cf
2eae42-6537-4891-85c2-77bbff4598b8
```

```
trtype:  tcp
adrfam:  ipv4
subtype: nvme subsystem
treq:    not required
portid:  1
trsvcid: 4420
subnqn:  nqn.2022-06.io.storesafe:nvme01
traddr:  192.168.211.24
sectype: none
```

Connect client to Bloombase StoreSafe Intelligent Storage Firewall NVMe/TCP virtual storage.

```
[root@bb027 ~]# nvme connect -t tcp -a 192.168.211.24 -s 4420 -q nqn.2014-08.org.nvmexpress:uuid:cf2
eae42-6537-4891-85c2-77bbff4598b8 -n nqn.2022-06.io.storesafe:nvme01
```

Ensure that Bloombase StoreSafe Intelligent Storage Firewall virtual storage is attached to the client after successful discovery and connection.

```
[root@bb027 ~]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda           8:0    0  1.8T  0 disk
├─sda1        8:1    0  600M  0 part /boot/efi
├─sda2        8:2    0    1G  0 part /boot
└─sda3        8:3    0  1.8T  0 part
  ├─rl-root 253:0    0   70G  0 lvm  /
  ├─rl-swap 253:1    0 15.7G  0 lvm  [SWAP]
  └─rl-home 253:2    0  1.8T  0 lvm  /home
nvme0n1     259:0    0  1.1T  0 disk
```

Format and mount Bloombase Storesafe Intelligent Storage Firewall NVMe/TCP virtual storage.

```
[root@bb027 ~]# mount /dev/nvme0n1 /nvme01
[root@bb027 ~]# mount | grep nvme01
/dev/nvme0n1 on /nvme01 type xfs (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
[root@bb027 ~]# cd /nvme01/
```

Sample plaintext files have been pre-added into Bloombase StoreSafe Intelligent Storage Firewall NVMe/TCP virtual storage.

```
[root@bb027 nvme01]# ls -l
total 261336
-rw-r--r--. 1 root root      3285 Aug 13  2021  0.seq
-rw-r--r--. 1 root root      3201 Aug 13  2021  100.seq
-rw-r--r--. 1 root root      3066 Aug 13  2021  101.seq
-rw-r--r--. 1 root root      3191 Aug 13  2021  102.seq
-rw-r--r--. 1 root root      3362 Aug 13  2021  103.seq
-rw-r--r--. 1 root root      3275 Aug 13  2021  104.seq
-rw-r--r--. 1 root root      3192 Aug 13  2021  105.seq
-rw-r--r--. 1 root root      3204 Aug 13  2021  106.seq
-rw-r--r--. 1 root root      3200 Aug 13  2021  107.seq
-rw-r--r--. 1 root root      3184 Aug 13  2021  108.seq
-rw-r--r--. 1 root root      3155 Aug 13  2021  109.seq
-rw-r--r--. 1 root root      2993 Aug 13  2021  10.seq
-rw-r--r--. 1 root root      3044 Aug 13  2021  110.seq
-rw-r--r--. 1 root root      3287 Aug 13  2021  111.seq
```

Trusted client is able to access and read the Bloombase StoreSafe encrypted files as if they are in clear-text.

```
//
LOCUS       AQ721632               506 bp    DNA     linear   GSS 09-MAY-2010
DEFINITION  HS_5563_B1_B06_T7A RPCI-11 Human Male BAC Library Homo sapiens
            genomic clone Plate=1139 Col=11 Row=D, genomic survey sequence.
ACCESSION   AQ721632
VERSION     AQ721632.1
DBLINK      BioSample: SAMN00183116
KEYWORDS    GSS.
SOURCE      Homo sapiens (human)
  ORGANISM  Homo sapiens
            Eukaryota; Metazoa; Chordata; Craniata; Vertebrata; Euteleostomi;
            Mammalia; Eutheria; Euarchontoglires; Primates; Haplorrhini;
            Catarrhini; Hominidae; Homo.
REFERENCE   1  (bases 1 to 506)
  AUTHORS   Mahairas,G.G., Wallace,J.C., Smith,K., Swartzell,S., Holzman,T.,
            Keller,A., Shaker,R., Furlong,J., Young,J., Zhao,S., Adams,M.D. and
            Hood,L.
  TITLE     Sequence-tagged connectors: A sequence approach to mapping and
            scanning the human genome
  JOURNAL   Proc. Natl. Acad. Sci. U.S.A. 96 (17), 9739-9744 (1999)
   PUBMED   10449764
COMMENT     Contact: Mahairas GG, Wallace JC, Hood L
            High Throughput Sequencing Center
            University of Washington
            401 Queen Anne Avenue North, Seattle, WA 98109, USA
            Tel: (206) 616-3618
            Fax: (206) 616-3887
            Email: jwallace@u.washington.edu
"100.seq" 60L, 3201C
```

Any file/data stored via Bloombase StoreSafe Intelligent Storage Firewall NVMe/TCP virtual storage is seamlessly encrypted at the storage with zero operational impact to end users, system administrators and software applications.

```
[root@bb024 ~]# hexdump -C /dev/nvme0n1
```

```
00391940  61 cd fa af e1 12 60 48  a0 b9 07 ee 96 c4 58 82  |a.....`H......X.|
00391950  b4 2a 9e 8c 44 ee 9e 93  22 d4 30 88 2e 1f 56 1a  |.*..D...".0...V.|
00391960  4e 21 56 87 78 a6 3c 5c  1b dd 93 28 d3 a3 c7 fe  |N!V.x.<\...(....|
00391970  02 c7 3f a3 51 2d 2b 7c  2b 32 aa 5a 21 55 06 53  |..?.Q-+|+2.Z!U.S|
00391980  b0 bf dd 43 32 a2 30 49  fc ce c7 e2 8a 51 fe 9d  |...C2.0I.....Q..|
00391990  1c af 55 9e 50 bc 4c a9  39 eb b0 96 bd d6 60 df  |..U.P.L.9.....`.|
003919a0  ed 48 25 bf ae 11 93 90  96 bc 46 5f 6d 18 25 5c  |.H%.......F_m.%\|
003919b0  e9 ea 62 b0 dc a2 45 75  5c ca 0b 22 df 78 fd b3  |..b...Eu\..".x..|
003919c0  05 19 15 26 0f 1c 70 f4  03 09 33 6d eb 67 e2 7e  |...&..p...3m.g.~|
003919d0  8f 38 fe 6f 5f 99 b3 d3  4f bb 21 71 9e 6b 67 8a  |.8.o_...O.!q.kg.|
003919e0  bb c9 d0 8f c2 10 99 13  fa a3 8d 65 34 36 d1 44  |...........e46.D|
003919f0  96 f0 3f 76 d4 a0 d4 6b  7b 77 c4 1f d8 db 2d db  |..?v...k{w....-.|
00391a00  ab 5f 41 9a d4 bc 00 89  6d 3b bb 1f 10 e0 c4 cb  |._A.....m;......|
00391a10  4d e0 a6 28 ab 3e e6 5a  fa ad fe 20 9a 9d ca cd  |M..(.>.Z... ....|
00391a20  e4 b9 22 fa 61 4a 6e 7b  c1 82 4c ad fe 3a 72 d1  |..".aJn{..L..:r.|
00391a30  16 81 a7 32 f6 8c ab 33  f4 ed a0 5d 78 75 d7 9b  |...2...3...]xu..|
00391a40  fe f8 7a dc 39 9f 87 75  c4 cd f7 3c bd c2 43 7e  |..z.9..u...<..C~|
00391a50  d8 a2 47 6f 98 ea da ed  d5 a2 40 c7 44 94 03 df  |..Go......@.D...|
```

```
[root@bb024 ~]# hexdump -C /dev/nvme0n1 | grep SAMN00183116
[root@bb024 ~]#
```

Create a new file to be secured by Bloombase StoreSafe Intelligent Storage Firewall.

```
[root@bb027 nvme01]# vi password.txt
```

```
My IRS password: iloveyou
My Citibank password: qwertyuiop
~
~
```

Trusted client is able to access and write files into Bloombase StoreSafe Intelligent Storage Firewall as if they are plain-text files.

```
[root@bb027 nvme01]# ls -l | grep password.txt
-rw-r--r--. 1 root root        60 Oct  5 08:03 password.txt
```

```
[root@bb027 nvme01]# cat password.txt
My IRS password: iloveyou
My Citibank password: qwertyuiop
```

Any file/data stored via Bloombase StoreSafe Intelligent Storage Firewall virtual storage is seamlessly encrypted at the storage with zero operational impact to end users, system administrators and software applications.

```
[root@bb024 ~]# hexdump -C /dev/nvme0n1
```

```
00391940  61 cd fa af e1 12 60 48  a0 b9 07 ee 96 c4 58 82  |a.....`H......X.|
00391950  b4 2a 9e 8c 44 ee 9e 93  22 d4 30 88 2e 1f 56 1a  |.*..D...".0...V.|
00391960  4e 21 56 87 78 a6 3c 5c  1b dd 93 28 d3 a3 c7 fe  |N!V.x.<\...(....|
00391970  02 c7 3f a3 51 2d 2b 7c  2b 32 aa 5a 21 55 06 53  |..?.Q-+|+2.Z!U.S|
00391980  b0 bf dd 43 32 a2 30 49  fc ce c7 e2 8a 51 fe 9d  |...C2.0I.....Q..|
00391990  1c af 55 9e 50 bc 4c a9  39 eb b0 96 bd d6 60 df  |..U.P.L.9.....`.|
003919a0  ed 48 25 bf ae 11 93 90  96 bc 46 5f 6d 18 25 5c  |.H%.......F_m.%\|
003919b0  e9 ea 62 b0 dc a2 45 75  5c ca 0b 22 df 78 fd b3  |..b...Eu\.."..x..|
003919c0  05 19 15 26 0f 1c 70 f4  03 09 33 6d eb 67 e2 7e  |...&..p...3m.g.~|
003919d0  8f 38 fe 6f 5f 99 b3 d3  4f bb 21 71 9e 6b 67 8a  |.8.o_...O.!q.kg.|
003919e0  bb c9 d0 8f c2 10 99 13  fa a3 8d 65 34 36 d1 44  |...........e46.D|
003919f0  96 f0 3f 76 d4 a0 d4 6b  7b 77 c4 1f d8 db 2d db  |..?v...k{w....-.|
00391a00  ab 5f 41 9a d4 bc 00 89  6d 3b bb 1f 10 e0 c4 cb  |._A.....m;......|
00391a10  4d e0 a6 28 ab 3e e6 5a  fa ad fe 20 9a 9d ca cd  |M..(.>.Z... ....|
00391a20  e4 b9 22 fa 61 4a 6e 7b  c1 82 4c ad fe 3a 72 d1  |..".aJn{..L..:r.|
00391a30  16 81 a7 32 f6 8c ab 33  f4 ed a0 5d 78 75 d7 9b  |...2...3...]xu..|
00391a40  fe f8 7a dc 39 9f 87 75  c4 cd f7 3c bd c2 43 7e  |..z.9..u...<..C~|
00391a50  d8 a2 47 6f 98 ea da ed  d5 a2 40 c7 44 94 03 df  |..Go......@.D...|
```

```
[root@bb024 ~]# hexdump -C /dev/nvme0n1 | grep password
[root@bb024 ~]#
```

6 Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall with Utimaco GP HSM to deliver on-the-fly encryption of multiple storage protocols including SMB, NFS, iSCSI and NVMe/TCP. The end result is a high-bandwidth, application-transparent storage encryption solution with centralized key management that locks down sensitive crown-jewel data on disks and helps mitigate information exfiltration threats for mission-critical systems and data services.

As a summary,

- Utimaco GP HSM 4.80.0.0

has been integrated with Bloombase StoreSafe Intelligent Storage Firewall to deliver encryption security of Microsoft Storage Server on Microsoft Windows Server 2025 over SMB/CIFS, NFS, iSCSI and Rocky Linux 9 via NVMe/TCP network storage protocols for software applications running on Microsoft Windows 11 and Ubuntu 22.04 LTS.

Bloombase Product	Client Systems	Storage Backends	Key Management System
Bloombase StoreSafe Intelligent Storage Firewall 4.0	▪ Microsoft Windows 11 ▪ Ubuntu 22.04 LTS	▪ Microsoft Windows Server 2025 ▪ Rocky Linux 9	Utimaco GP HSM 4.80.0.0

7 Disclaimer

The integration procedures 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 difference 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.

8 Acknowledgement

Bloombase InteropLab would like to thank Utimaco team for supporting the integration of Bloombase StoreSafe with Utimaco GP HSM.

9 Reference

1. Bloombase StoreSafe Technical Specifications, https://www.bloombase.com/content/8936QA88
2. Bloombase StoreSafe Hardware Compatibility Matrix, https://www.bloombase.com/content/e8Gzz281
3. Bloombase StoreSafe for VMware, https://marketplace.cloud.vmware.com/vsx/solutions/bloombase-storesafesecurity-server
4. Utimaco General Purpose Hardware Security Module (GP HSM), https://utimaco.com/solutions/applications/general-purpose-hardware-security-modules
5. OASIS PKCS #11 Cryptographic Token Interface Base Specification, https://docs.oasis-open.org/pkcs11/pkcs11base/v3.0/pkcs11-base-v3.0.html
6. Post-Quantum Cryptography (PQC), https://csrc.nist.gov/Projects/post-quantum-cryptography
7. NVIDIA ConnectX NICs, https://www.nvidia.com/en-us/networking/ethernet-adapters/
8. Bloombase StoreSafe for NVIDIA, https://resources.nvidia.com/en-us-accelerated-networking-resourcelibrary/bluefield-and-doca-bloombase
9. Bloombase StoreSafe for Red Hat, https://catalog.redhat.com/software/containerstacks/detail/5e9874cb3f398525a0ceb024
10. Bloombase StoreSafe for Microsoft, https://azuremarketplace.microsoft.com/enus/marketplace/apps/bloombase.bloombase-storesafe-3_4_7_0_el7_x86_64