



Bloombase StoreSafe and Entrust nShield 5c Hardware Security Module (HSM) Integration Guide for Data-at-Rest Encryption

July 2025

BLOOMBASE[®]

Executive Summary

Entrust nShield 5c Hardware Security Module (HSM) has been validated by Bloombase InteropLab to run with Bloombase StoreSafe Intelligent Storage Firewall. This document describes the steps carried out to integrate Entrust nShield 5c HSM with Bloombase StoreSafe software appliance on Broadcom VMware ESXi to deliver high bandwidth transparent storage encryption on Terabit Ethernet for mission critical software applications. Client host systems Microsoft Windows 11 and Canonical Ubuntu 22.04 LTS have been tested with Entrust nShield 5c HSM and Bloombase StoreSafe Intelligent Storage Firewall solution to secure Microsoft Storage Server 2025 and Rocky Linux 9 storage backends via storage networking protocols including SMB/CIFS, NFS, iSCSI and NVMe/TCP.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase, Inc.

Bloombase, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, Inc, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase, Inc. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, Inc, and neither the document nor any such information may be released without the written consent of Bloombase, Inc.

© 2025 Bloombase, Inc.

Bloombase, Keyparc, Spitfire, StoreSafe are either registered trademarks or trademarks of Bloombase in the United States and/or other countries.

Entrust and nShield are trademarks of Entrust and/or its affiliated companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document No.: BLBS-TN - Bloombase StoreSafe - Entrust nShield 5c Hardware Security Module (HSM) Integration Guide - USLET-EN-R1.0

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Storage Encryption	8
Key Management System	9
Storage Systems	9
Storage Hosts	9
Networking	9
Configuration Overview	10
Entrust nShield 5c Hardware Security Module (HSM)	10
Entrust nShield 5c HSMs Network Configuration	10
nShield Failover Cluster Configuration	11
Entrust nShield Remote Administration	12
Entrust nShield Remote Administration Client Configuration	12
Entrust Trusted Verification Device (TVD) Integration	12

nShield Remote Administration Cards Initialization and Operations	13
Network Configuration	13
Ethernet Switch Configuration	13
Direct Attach Copper (DAC) Cable	15
Network Interface Card (NIC)	15
Microsoft Storage Server on Microsoft Windows Server 2025 Storage Backends	16
SMB/CIFS Services Configuration	17
NFS Services Configuration	19
iSCSI Services Configuration	21
NVMe over Fabrics (NVMe-oF) Storage Target on Rocky Linux 9 Storage Target	21
Bloombase StoreSafe Intelligent Storage Firewall	22
Entrust nShield 5c Hardware Security Module (HSM) and Bloombase StoreSafe Integration	23
Encryption Key Provisioning	25
Bloombase StoreSafe Data-at-Rest Encryption for SMB/CIFS Configuration	28
Bloombase StoreSafe Data-at-Rest Encryption for NFS Configuration	31
Bloombase StoreSafe Data-at-Rest Encryption for iSCSI Configuration	35
Bloombase StoreSafe Data-at-Rest Encryption for NVMe/TCP Configuration	39
Storage Clients	42
Microsoft Windows 11	42
Canonical Ubuntu 22.04 LTS	43
Tests for Data-at-Rest Encryption over SMB/CIFS	44
Tests for Data-at-Rest Encryption over NFS	47
Tests for Data-at-Rest Encryption over iSCSI	52
Tests for Data-at-Rest Encryption over NVMe/TCP	58
Conclusion	62
Disclaimer	63
Acknowledgement	64
Reference	65

Purpose and Scope

This document describes the steps necessary to integrate Entrust nShield 5c HSM with Bloombase StoreSafe to deliver agentless, transparent encryption security of traditional storage systems and next-generation storage services for mission-critical applications. Specifically, we cover the following areas:

- Install and configure Bloombase StoreSafe software appliance
- Integrate Bloombase StoreSafe with Entrust nShield 5c HSM
- Integrate Microsoft Windows 11 and Canonical Ubuntu 22.04 client systems with Bloombase StoreSafe and Entrust nShield 5c 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.

Assumptions

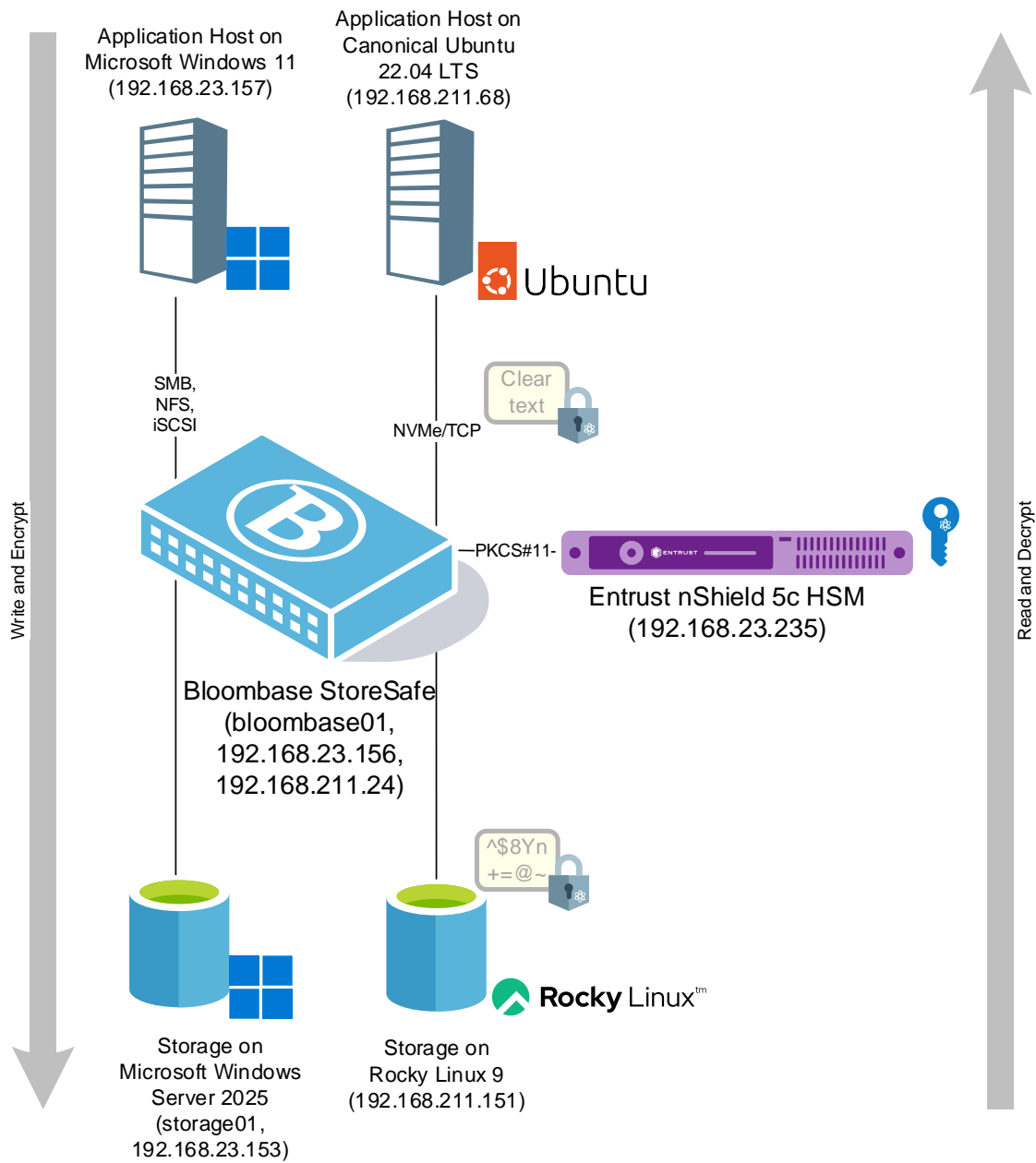
This document describes the integration of Entrust nShield 5c HSM with Bloombase StoreSafe. It is assumed that you are familiar with operation of Entrust nShield 5c HSM, storage systems, and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also 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 Entrust nShield 5c 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 Entrust nShield 5c 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>.

Infrastructure

Setup

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



Storage Encryption

Storage Encryption

Server

Processor

Memory

Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v4.0

Broadcom VMware ESXi 6.5 on Dell PowerEdge T440 server

4x Virtual CPU (vCPU)

8GB

Network Interface Card | NVIDIA ConnectX-6

Key Management System

Key Management System | Entrust nShield 5c Hardware Security Module (HSM) v13.2.4

Storage Systems

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

Storage Hosts

Client Hosts | Microsoft Windows 11 | Canonical Ubuntu 22.04 LTS

Networking

Ethernet Switch | Celestica Seastone DX010 32-port 100GbE ONIE Switch
Network Interface Card | NVIDIA ConnectX-6
Network Cables | NVIDIA/Mellanox 100GbE QSFP28 DAC Cables

Configuration Overview

Entrust nShield 5c Hardware Security Module (HSM)

Entrust nShield 5c Hardware Security Module (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 nShield HSM is available as PCIe embedded card or as network attached appliance. The key management and cryptographic functionalities provided by Entrust nShield 5c HSM are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases via PKCS#11 API.

Entrust nShield 5c HSMs Network Configuration

The following operations can be performed by any user in the nFast group. Administrator access is needed for stopping and starting the hardserver. First install the Security World Software for Linux 64-bit.

After installation of the Entrust nShield Security World Software is complete, the HSM can be configured.

The Entrust nShield 5c HSM is installed with network settings provisioned. In this integration as an example, the Entrust nShield 5c HSM is provided with IP address and Security World. The provided Security World files should be placed in the

kmdata

directory as stated in the Entrust nShield User Guide.

nShield Failover Cluster Configuration

If you have multiple HSMs to be used in high-availability mode, create the cknfastrc file in the \$NFAST_HOME (typically /opt/nfast/) directory, with the entry:

```
CKNFAST_LOADSHARING=1
```

Run command

```
/opt/nfast/bin/ckcheckinst
```

as the sanity check to confirm if everything is working on the HSM and PKCS#11 layer. Ensure Loadsharing and Failover is enabled.

```
[root@storeSAFE ~] # /opt/nfast/bin/ckcheckinst
PKCS#11 library interface version 2.40
      flags 0
      manufacturerID "nCipher Corp. Ltd"
      libraryDescription "nCipher PKCS#11 13.6.11-256-40ea"
      implementation version 13.06
      Loadsharing and Failover enabled

Slot  Status          Label
====  =====
  0  Fixed token      "loadshared accelerator"
  1  Soft token        "storesafe"

No removable tokens present.
Please insert an operator card into at least one available slot and enter 'R' retry.
If you have not created an operator card or there are no physical slots,
enter a fixed token slot number,
or 'E' to exit this program and create a card set before continuing.

Enter a fixed token slot number, 'R'etry or 'E'xit: 1
Using slot number 1.

Please enter the passphrase for this token (No echo set).
Passphrase:

Test                Pass/Failed
----                -
1 Generate RSA key pair  Pass
2 Generate DSA key pair  Pass
3 Encryption/Decryption  Pass
4 Signing/Verification  Pass

Deleting test keys      ok

PKCS#11 library test successful.
```

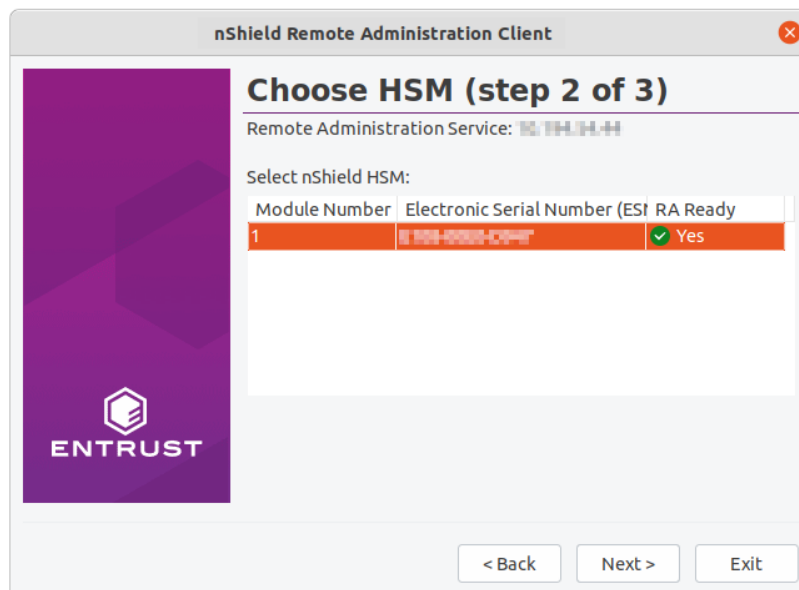
Entrust nShield Remote Administration

Please note that if using nShield Trusted Verification Device (TVD) protection, only 1-of-N persistent cardset is supported. You must have an operator card inserted into every slot from the same 1-of-N card set, at the time of application startup. This setup was tested with this 1-of-N configuration. However, if you want to use K-of-N TVD cardset, you may be able to use Entrust provided 'preload' utility for loading keys on a particular slot. Please refer to Entrust Connect User guide for details.

Entrust nShield Remote Administration Client Configuration

To utilize a cardset with nShield Trusted Verification Device (TVD), the Entrust nShield Remote Administration Client must be installed on a physically accessible machine and the TVD attached to one of its ports.

If you are using and connected to multiple HSMs, you will see a list of them along with the associated ESNs. You will need to repeat this process for each ESN to ensure the cardset is active on them all and utilize high-availability.

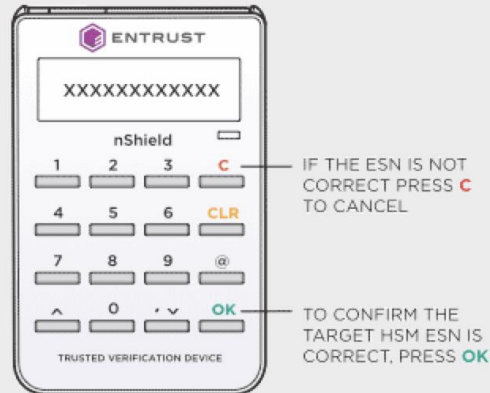


Entrust Trusted Verification Device (TVD) Integration

When prompted, the user must insert a blank card into the Trusted Verification Device (TVD) slot. As with the below screen, the user must be present in-person to see the HSM ESN matches and confirm by pressing OK.

Important: This step establishes the secure channel between the inserted smart card and the target HSM.

To confirm the target HSM ESN is correct press 'OK'. If the ESN is not correct press 'C' to cancel.



nShield Remote Administration Cards Initialization and Operations

Use the following command on a blank card inserted into the Trusted Verification Device (TVD) to create the operator cardset.

```
createocs -m 1 -p -Q 1/1 -N storesafe --remotely-readable
```

Repeat this step for every card in set inserting each one at a time into the Trusted Verification Device (TVD).

Network Configuration

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-6 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

SONiC

-- 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
```

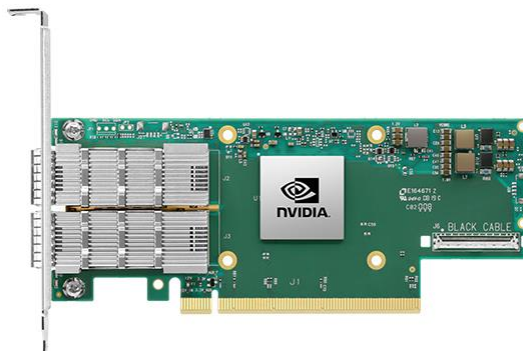
Direct Attach Copper (DAC) Cable

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



Network Interface Card (NIC)

NVIDIA ConnectX-6 NIC has been used in this integration testing.



Install and configure NVIDIA ConnectX-6 NIC using the install image or the driver available from your distribution's repo.

```
[root@rocky24 ~]# lspci |grep ConnectX
01:00.0 Ethernet controller: Mellanox Technologies MT42822 BlueField-2 integrated ConnectX-6 Dx network controller (rev 01)
01:00.1 Ethernet controller: Mellanox Technologies MT42822 BlueField-2 integrated ConnectX-6 Dx network controller (rev 01)
```

```
[root@rocky24 ~]# ibstat
CA 'mlx5_0'
  CA type: MT41686
  Number of ports: 1
  Firmware version: 24.39.2048
  Hardware version: 1
  Node GUID: 0xb8cef60300d214b2
  System image GUID: 0xb8cef60300d214b2
  Port 1:
    State: Active
    Physical state: LinkUp
    Rate: 40
    Base lid: 0
    LMC: 0
    SM lid: 0
    Capability mask: 0x00010000
    Port GUID: 0xbacef6fffd214b2
    Link layer: Ethernet
CA 'mlx5_1'
  CA type: MT41686
  Number of ports: 1
  Firmware version: 24.39.2048
  Hardware version: 1
  Node GUID: 0xb8cef60300d214b3
  System image GUID: 0xb8cef60300d214b2
  Port 1:
    State: Active
    Physical state: LinkUp
    Rate: 40
    Base lid: 0
    LMC: 0
    SM lid: 0
    Capability mask: 0x00010000
    Port GUID: 0xbacef6fffd214b3
    Link layer: Ethernet
```

Microsoft Storage Server on Microsoft Windows Server 2025 Storage Backends

Microsoft Storage Server on Microsoft Windows Server 2025 running on Broadcom 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 Broadcom VMware ESXi.

SMB/CIFS Services Configuration

The screenshot displays the Windows Server Manager interface. The navigation pane on the left shows the hierarchy: Servers > File and Storage Services > Shares. The main area is divided into two sections: SHARES and VOLUME.

SHARES
All shares | 2 total

Share	Local Path	Protocol	Availability Type
WINSER175 (2)			
smb01	C:\Shares\smb01	SMB	Not Clustered
nfs01	C:\Shares\nfs01	NFS	Not Clustered

VOLUME
smb01 on WINSER175

(C:) Capacity: 99.4 GB

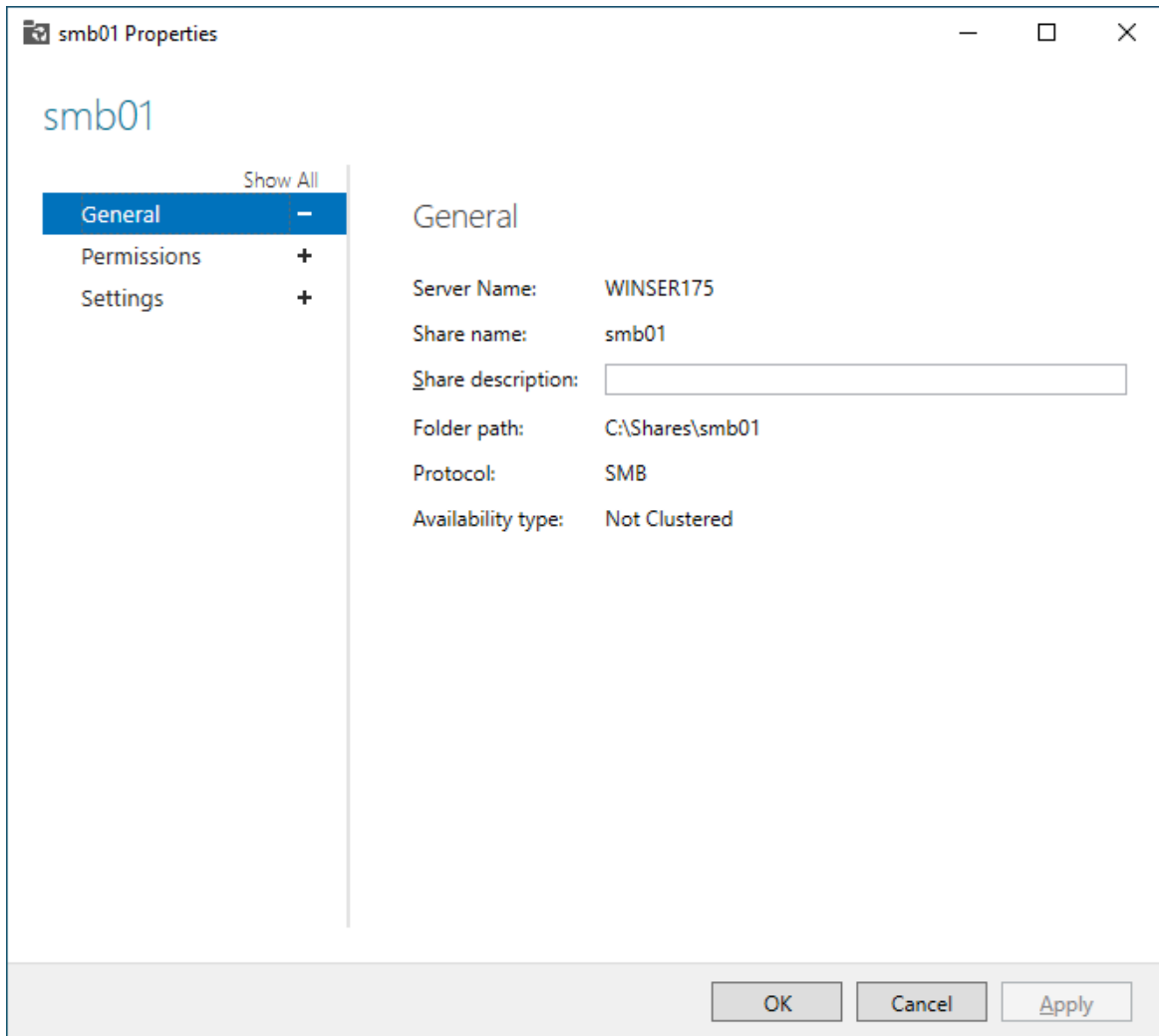
18% Used 17.9 GB Used Space
81.5 GB Free Space

Go to Volumes Overview >

QUOTA
smb01 on WINSER175

To use quotas, File Server Resource Manager must be installed.

To install File Server Resource Manager, start the Add Roles and Features Wizard.



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

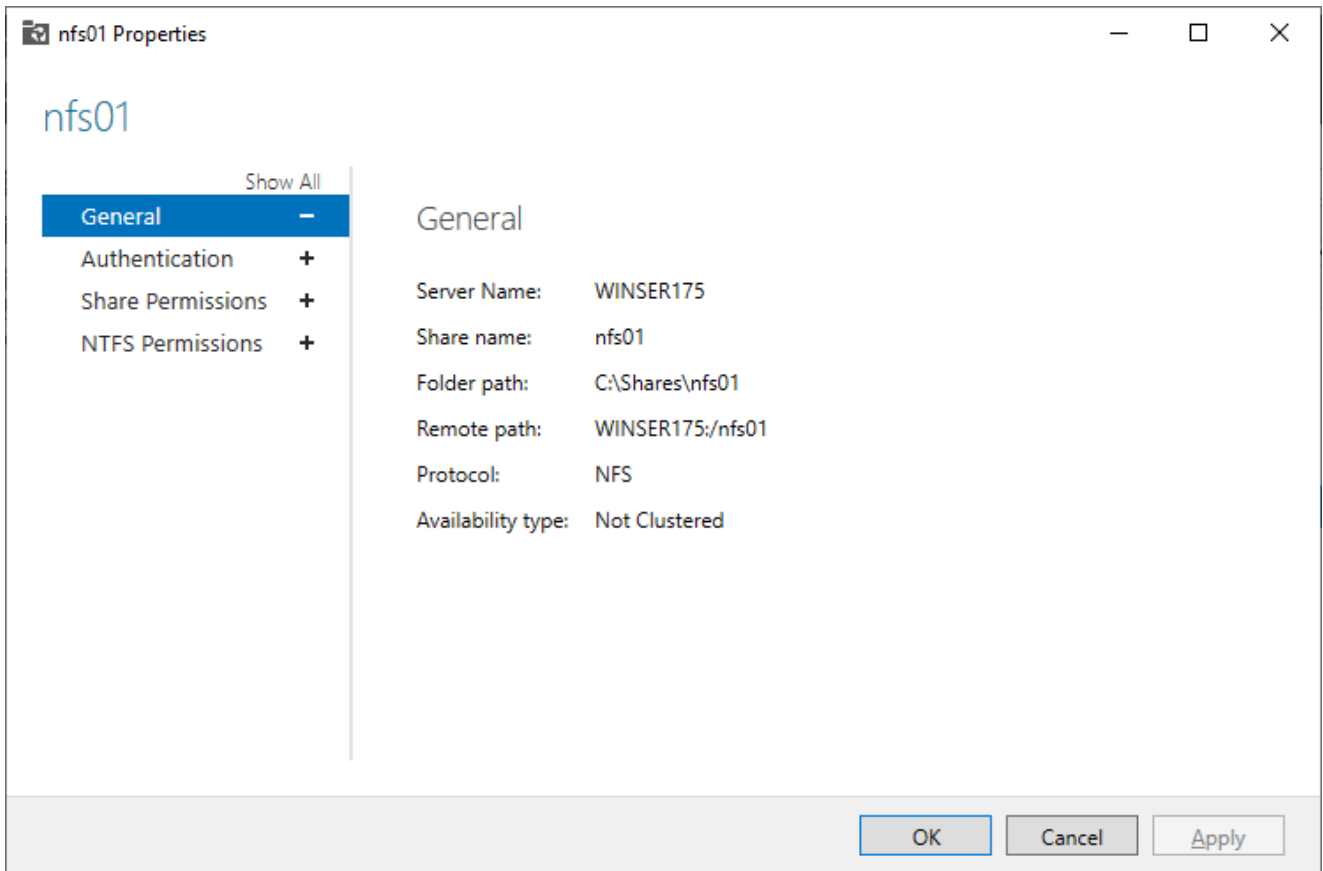
NFS Services Configuration

The screenshot displays the Windows Server Manager interface for configuring shares. The left-hand navigation pane includes Servers, Volumes, Disks, Storage Pools, Shares, iSCSI, and Work Folders. The main area is titled 'Server Manager > File and Storage Services > Shares'. The 'SHARES' section shows 'All shares | 2 total' and a table with the following data:

Share	Local Path	Protocol	Availability Type
WINSER175 (2)			
smb01	C:\Shares\smb01	SMB	Not Clustered
nfs01	C:\Shares\nfs01	NFS	Not Clustered

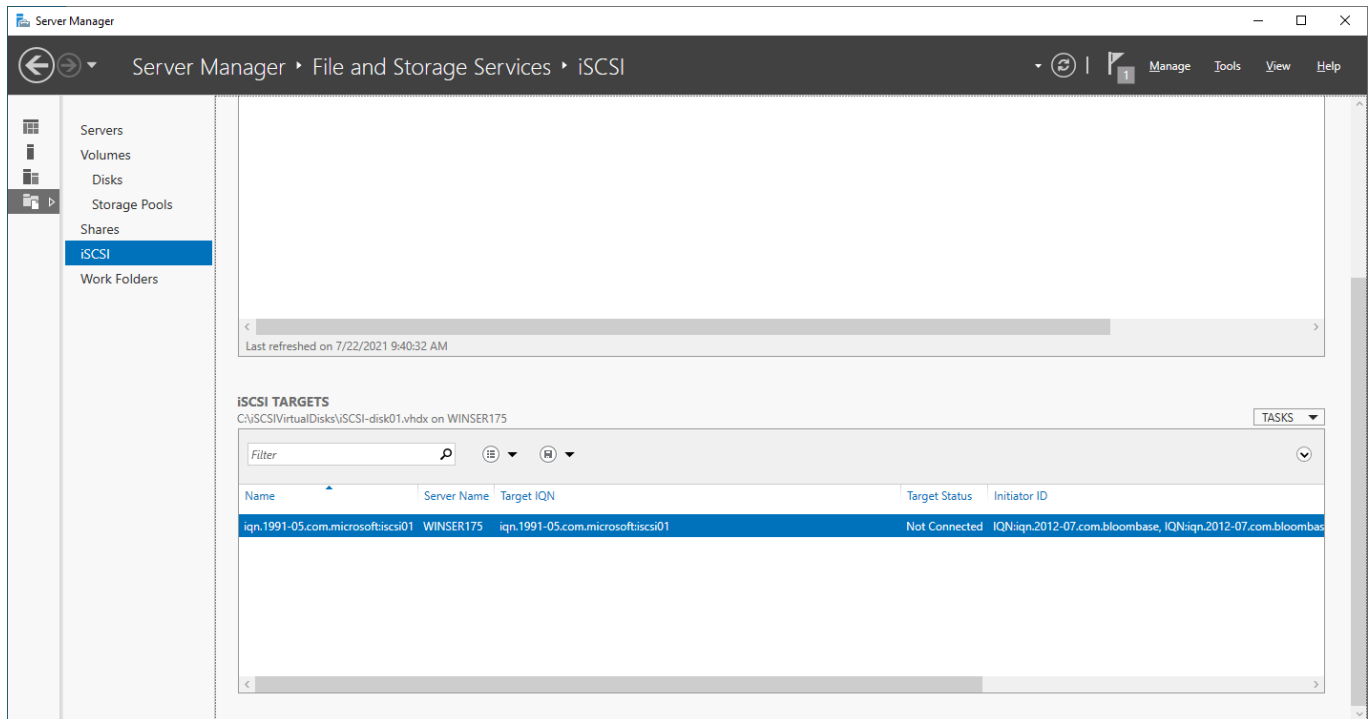
The 'VOLUME' section for 'smb01 on WINSER175' shows a capacity of 99.4 GB. A progress bar indicates 18% used space (17.9 GB) and 81.5 GB of free space. Below this, the 'QUOTA' section for 'smb01 on WINSER175' contains the following text:

To use quotas, File Server Resource Manager must be installed.
To install File Server Resource Manager, start the Add Roles and Features Wizard.



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

iSCSI Services Configuration



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

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 ~# nmactcli
/> ls
o- /
o- hosts ..... [..]
| o- nqn.2014-08.org.nvmeexpress: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.nvmeexpress: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.nvmeexpress:NVMF:uuid:7079993e-7413-4338-9b9b-a3af82259b18 ..... [..]
o- subsystems ..... [..]
o- nqn.2014-08.org.nvmeexpress:NVMF:uuid:7079993e-7413-4338-9b9b-a3af82259b18 [version=1.3, allow_any=0, serial=cdbdf55fefea52243d3]
o- allowed_hosts ..... [..]
o- namespaces ..... [..]
| o- 1 ..... [path=/dev/nullb0, uuid=e581a156-7460-45e2-b6ae-0457e0762342, grpId=1, disabled]

```

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 Entrust nShield 5c HSM.

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

The screenshot shows the Bloombase StoreSafe Security Server web interface. The main content area is titled "Main" and contains several sections:

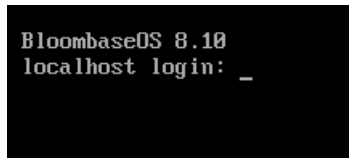
- Greeting:** Host Name: cassf156, User: admin, Datetime: 2024-08-06 03:11:22 -0700.
- Menu Bar:** System, Operation, High Availability, Administration, Key Management, StoreSafe Configurations, Storage.
- Language:** English.
- System Information:**

Product Name	Bloombase StoreSafe Security Server	Version	4.0.0.1
Host Name	cassf156 / localhost	System Up Since	2024-08-02 00:55:36 -0700
Host Addresses	1 ens192 fe80:0:0:250:56ff:fe86:5f91, 192.168.23.156		
Licensee	CN=SPFSSF2666 O=Bloombase, Inc. C=US	Serial Number	9830
Validity	<input checked="" type="checkbox"/>	Perpetuality	<input checked="" type="checkbox"/>
- Server Information:**

Processors	2	Model	Intel® Xeon® CPU E5-2420 v2 @ 2.20GHz
Memory Utilization	6%	Allocated Memory	512 MB (536,870,912)
Max Memory	4 GB (4,294,967,296)	Used Memory	266 MB (278,967,080)
Disk Space Utilization	84%	Total Disk Space	12 GB (13,742,637,056)
Used Disk Space	10 GB (11,617,468,416)	Free Disk Space	1 GB (2,125,168,640)
- Application Status:**
 - Application Status:
 - Last Shutdown Time
 - Last Standby Time
 - Last Startup Time: 2024-08-02 00:55:43 -0700

Entrust nShield 5c Hardware Security Module (HSM) and Bloombase StoreSafe Integration

The Entrust 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.



Install the Entrust nShield client software on the Bloombase OS as per nShield Documentation for Linux systems. The Security World files need to be copied in their specific paths:

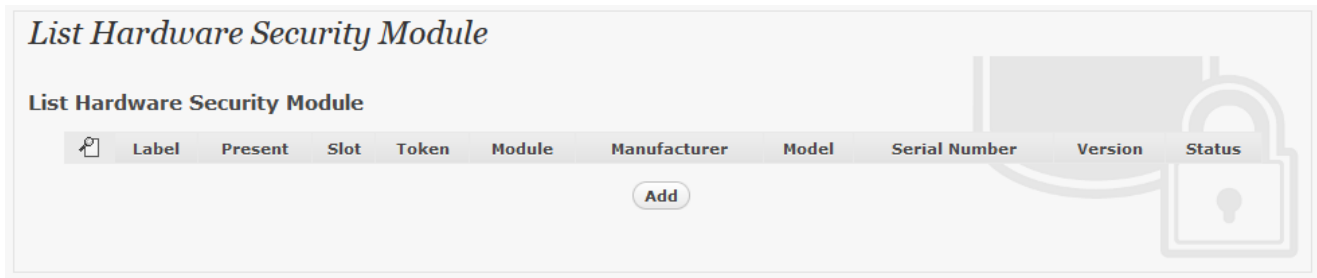
```
/opt/nfast/kmdata/
```

Bloombase StoreSafe software appliance can be registered as the HSM client by nCSS enroll utility, use the included client tool:

```
/opt/nfast/bin/nethsmenroll
```

The HSM key protection will typically be an Operator Card Set (OCS), but can alternatively be a softcard. Please refer to "nShield 5c User Guide" for detailed setup and configurations.

Bloombase supports Entrust nShield HSM out of the box. To enable the built-in Bloombase KeyCastle to utilize keys managed in the Entrust nShield 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

```
nfast
```

Input the token label of the Entrust nShield 5c HSM, and the token user pin.

Modify Hardware Security Module

Modify Hardware Security Module

Module:

Label / Username:

Pin:

Confirm Pin:

Click 'Submit' to commit the configuration.

In this integration, Slot 1 has been used for key protection with the HSM by default in Bloombase StoreSafe.

HSM PKCS#11 integration uses standard SunPKCS11 provider. This makes selection of slot customer configurable. If another slot is used, the StoreSafe webconsole registry can be changed in the following path:

Registry > System > SunPKCS11 > Providers > nfast

Then modify the parameter

slotListIndex

If the token is properly initialized and connected, the "Present" and "Status" boxes will be checked.

List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	storesafe	<input checked="" type="checkbox"/>	1	1	nfast	null	NH2096-0F	9C7A-9CAA-2934	13.2.4 / 13.6.11	<input checked="" type="checkbox"/>

Encryption Key Provisioning

To generate key in attached Entrust nShield 5c HSM, select Key Source Type as

Hardware Security Module

Module as

nfast

and the assigned Key Manager token, in this case

storesafe


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

Modify Key Wrapper

Key Wrapper | **Permissions**

Modify Key Wrapper

Name	<input type="text"/>
Key Source	Hardware Security Module
Type	Asymmetric
Active	<input checked="" type="checkbox"/>
Module	nfast
Label	storesafe
Alias	<input type="text"/>
Algorithm	RSA ▾
Key Bit Length	2048 ▾
Signature Algorithm	SHA256 ▾
Key Usage	<input type="checkbox"/> Digital Signature
	<input type="checkbox"/> Non Repudiation
	<input type="checkbox"/> Key Encipherment
	<input type="checkbox"/> Data Encipherment
	<input type="checkbox"/> Key Agreement
	<input type="checkbox"/> Key Cert Sign
	<input type="checkbox"/> CRL Sign
	<input type="checkbox"/> Encipher Only
<input type="checkbox"/> Decipher Only	
Extended Key Usage	<input type="button" value="Add"/> <input type="button" value="Remove"/>
Owner	admin
Last Update Datetime	



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

Modify Key Wrapper

Key Wrapper | **Permissions**


Modify Key Wrapper

Key Source:

Module:

Token:

Key:



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

Find Key Wrapper

Name Type Active CA

1-1 of 1

<input type="checkbox"/>	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	Asymmetric	Hardware Security Module	<input checked="" type="checkbox"/>	Valid	<input type="checkbox"/>	CN=key01	CN=key01	2025-06-11 08:23:33 -0700	2035-06-09 08:23:33 -0700	2025-06-11 08:23:43 -0700

1-1 of 1

The new key can be found on the Entrust nShield HSM using the Entrust provided tool:

```
/opt/nfast/bin/nfkminfo
```

```
[root@localhost ~]# /opt/nfast/bin/nfkminfo -k
Key list - 2 keys
AppName pkcs11          Ident uc873793d6d844ee323685015b892a360d632262c0-fd32f6a37b048260b1b0d02238b7a71528e0a83f
AppName pkcs11          Ident um873793d6d844ee323685015b892a360d632262c0-4fd140f44f2c94d0b15032375af479f1ad5b4d5b
```

Bloombase StoreSafe Data-at-Rest Encryption for SMB/CIFS Configuration

Physical storage namely

smb01


is configured to be secured by Bloombase StoreSafe using encryption.

Modify Storage Configuration

Physical Storage | Permissions

Physical Storage Configuration

Name	<input type="text" value="smb01"/>
Description	<input type="text"/>
Physical Storage Type	Remote <input type="button" value="v"/>
Type	Common Internet File System (CIFS) <input type="button" value="v"/>
Host	<input type="text" value="storage01"/>
Share Name	<input type="text" value="smb01"/>
Read Size	<input type="text" value="65536"/> bytes
Write Size	<input type="text" value="65536"/> bytes
Mount Hard	<input type="checkbox"/>
User	<input type="text" value="user01"/>
Password	<input type="password"/>
Options	<input type="text"/>
Virtual Storage	smb01
Owner	admin
Last Update Datetime	2021-07-22 08:32:00 -0700



Virtual storage namely

smb01

of type

File

is created to virtualize physical storage

smb01

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

Modify Virtual Storage

Virtual Storage | Protection | Access Control | Permissions

Modify Virtual Storage

Name: smb01

Status:

Description:

Active:

Mode: File

Protocol: SMB



Owner: admin

Last Update Datetime: 2021-07-22 04:33:45 -0700

Settings

Offline Setting: Disabled

Physical Storage

Storage: smb01  


Description:

Physical Storage Type: Remote

Type: cifs

Host: storage01

Share: smb01



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 Entrust nShield 5c HSM.

The screenshot shows a web interface titled "Modify Virtual Storage Handler" with four tabs: "Virtual Storage", "Protection", "Access Control", and "Permissions". The "Protection" tab is active. Under "Virtual Storage Protection", the "Protection Type" is set to "Privacy". Under "Encryption Keys", there is a table with one entry:

	Key Name	Last Update Datetime
1	key01	

Below the table are "Add" and "Remove" buttons. The "Header" section has a "Protected" checkbox checked. Under "Cryptographic Cipher", the "Cipher Algorithm" is "AES", "Bit Length" is "256", and "CTR Mode" is checked. "Submit" and "Close" buttons are at the bottom. A large lock icon is on the right side of the interface.

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 (MSAD) integration for user-password authentication and single sign-on.

Modify Virtual Storage Access Control

Virtual Storage | Protection | **Access Control** | Permissions

User Access Control

Warning: Deny access will override allow access

Everybody Read Write
 Deny Read Deny Write

User Repository: Local

	User	Access Control List	Deny Access Control List	Warning	Last Update Datetime
1	<input type="checkbox"/> user01	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input type="checkbox"/> Deny Read <input type="checkbox"/> Deny Write		2021-07-22 04:33:45 -0700

More Options

Bloombase StoreSafe Data-at-Rest Encryption for NFS Configuration

Physical storage namely

nfs01


is configured to be secured by Bloombase StoreSafe using encryption.

Modify Storage Configuration

Physical Storage **Permissions**

Physical Storage Configuration

Name	<input type="text" value="nfs01"/>
Description	<input type="text"/>
Physical Storage Type	Remote ▾
Type	Network File System (NFS) ▾
Host	<input type="text" value="storage01"/>
Share Name	<input type="text" value="nfs01"/>
Read Size	<input type="text" value="65536"/> bytes
Write Size	<input type="text" value="65536"/> bytes
Synchronous	<input type="checkbox"/>
Mount Hard	<input type="checkbox"/>
Options	<input type="text" value="vers=4.1"/>
Virtual Storage	nfs01
Owner	admin
Last Update Datetime	2021-07-23 04:47:41 -0700



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.

Modify Virtual Storage

Virtual Storage | Protection | Access Control | Permissions

Modify Virtual Storage

Name: nfs01

Status:

Description:

Active:

Mode: File

Protocol: NFS



Owner: admin

Last Update Datetime: 2021-07-22 09:55:37 -0700

Settings

Offline Setting: Disabled

Physical Storage

Storage: nfs01  


Description:

Physical Storage Type: Remote

Type: nfs

Host: storage01

Share: nfs01



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 Entrust nShield 5c HSM.

Modify Virtual Storage Handler

Virtual Storage Protection Access Control Permissions


Virtual Storage Protection
Protection Type

Encryption Keys

	Key Name	Last Update Datetime
1 <input type="checkbox"/>	key01	

Header
Protected

Cryptographic Cipher
Cipher Algorithm
Bit Length
CTR Mode



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

Modify Virtual Storage Access Control

Virtual Storage | Protection | Access Control | Permissions

User Access Control

Everybody Read Write

NFS File System Object Attributes

Root Squash
Weak Cache Consistency
Default User Identifier
Default Group Identifier
Default Mode

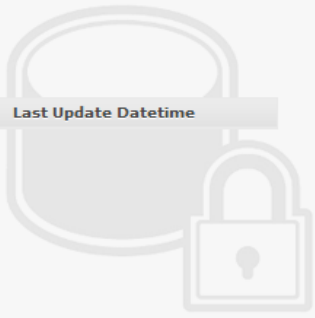
Host Access Control

	Host	Access Control List	Security	Warning	Last Update Datetime
1	<input type="text" value="192.168.23.157"/>	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	sys	<input type="text"/>	2024-08-01 02:30:50 -0700

Subnet Access Control

Subnet	Access Control List	Security	Warning	Last Update Datetime
--------	---------------------	----------	---------	----------------------

▼ More Options



Bloombase StoreSafe Data-at-Rest Encryption for iSCSI Configuration

Physical storage namely

iscsi01


is configured to be secured by Bloombase StoreSafe using encryption.

Modify Storage Configuration

Physical Storage | **Permissions**

Physical Storage Configuration

Name	<input type="text" value="iscsi01"/>
Description	<input type="text"/>
Physical Storage Type	Device ▾
Block I/O	<input checked="" type="checkbox"/>
Multipath	<input type="checkbox"/>
Device ID [max 8 chars]	<input type="text" value="11"/>
Options	<input type="text"/>
Device	60003ff44dc75adc919e979aaaf58040 🔍 🗑️
Virtual Storage	iqn.2012-07.com.bloombase:iscsi01
Owner	admin
Last Update Datetime	2021-07-23 11:53:49 -0700



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.

Modify Virtual Storage

Virtual Storage Protection Access Control iSCSI Permissions

Modify Virtual Storage

Name:

Status:

Description:

Active:

Mode: iSCSI

Tape Library:

ATS:

Cluster:

Vendor:

Model:

Revision:

Owner: admin

Last Update Datetime: 2021-07-23 11:54:59 -0700

Physical Storage

	Storage	Description	Device
1	<input type="checkbox"/> iscsi01		60003ff44dc75adc919e979aaaf58040

Protection type is specified as

Privacy

and secure the Microsoft Storage Server storage backend using

AES XTS 256-bit

encryption and encryption key

key01

managed at Entrust nShield 5c HSM.

Modify Virtual Storage Handler

Virtual Storage Protection Access Control iSCSI Permissions

Virtual Storage Protection

Protection Type **Privacy** ▾

Encryption Keys


	Key Name	Last Update Datetime
1 <input type="checkbox"/>	key01	

Remove

Cryptographic Cipher

Cipher Algorithm **AES XTS** ▾
Bit Length **256** ▾

Submit **Close**



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

Modify Virtual Storage Access Control

Virtual Storage | Protection | Access Control | iSCSI | Permissions

Allowed Portal

Portal IP

Add Remove

Incoming Users

User	Warning	Last Update Datetime

Add Remove

Initiators

Initiator	Alias	Warning	Last Update Datetime
1 <input type="checkbox"/> iqn.1991-05.com.microsoft:windows11			2021-07-23 12:19:08 -0700

Add Remove

▼ List Initiators

Refresh Alias Submit Close

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.

Modify Storage Configuration

Physical Storage | **Permissions**

Physical Storage Configuration

Name	<input type="text" value="nvme01"/>
Description	<input type="text"/>
Physical Storage Type	<input type="text" value="Block"/>
Device ID	<input type="text" value="1816d452-ac0d-49c2-9de0-d378f0cff5d6"/>
Options	<input type="text"/>
Device	d9395873-b937-4139-8911-07c347c447c0 🔍 🗑️
Virtual Storage	nqn.2022-06.io.storesafe:nvme01
Owner	admin
Last Update Datetime	2022-10-04 12:16:40 -0700

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

Modify Virtual Storage

Virtual Storage | Protection | Access Control | Permissions

Modify Virtual Storage

Name:

Status:

Description:

Active:

Mode: NVMe

Model:

Serial Number:

Owner: admin

Last Update Datetime: 2022-10-05 10:03:21 -0700

Physical Storage

	Storage	Description	Device
1	<input type="checkbox"/>	nvme01	d9395873-b937-4139-8911-07c347c447c0

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

Modify Virtual Storage Handler

Virtual Storage | **Protection** | Access Control | Permissions

Virtual Storage Protection

Protection Type:

Encryption Keys

	Key Name	Last Update Datetime
1	<input type="checkbox"/> key01	

Cryptographic Cipher

Cipher Algorithm:

Bit Length:

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

Modify Virtual Storage Access Control

Virtual Storage Protection Access Control Permissions

Initiators

	Initiator	Alias	Warning	Last Update Datetime
1	<input type="checkbox"/> nqn.2014-08.org.nvmexpress:uuid:cf2eae42-6537-4891-85c2-77bbff4598b8			2022-06-03 14:50:03 -0700
2	<input type="checkbox"/> nqn.2014-08.org.nvmexpress:uuid:98c22f42-0694-af6d-1b5b-6d7b4ea9944d			2022-07-13 12:20:18 -0700

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

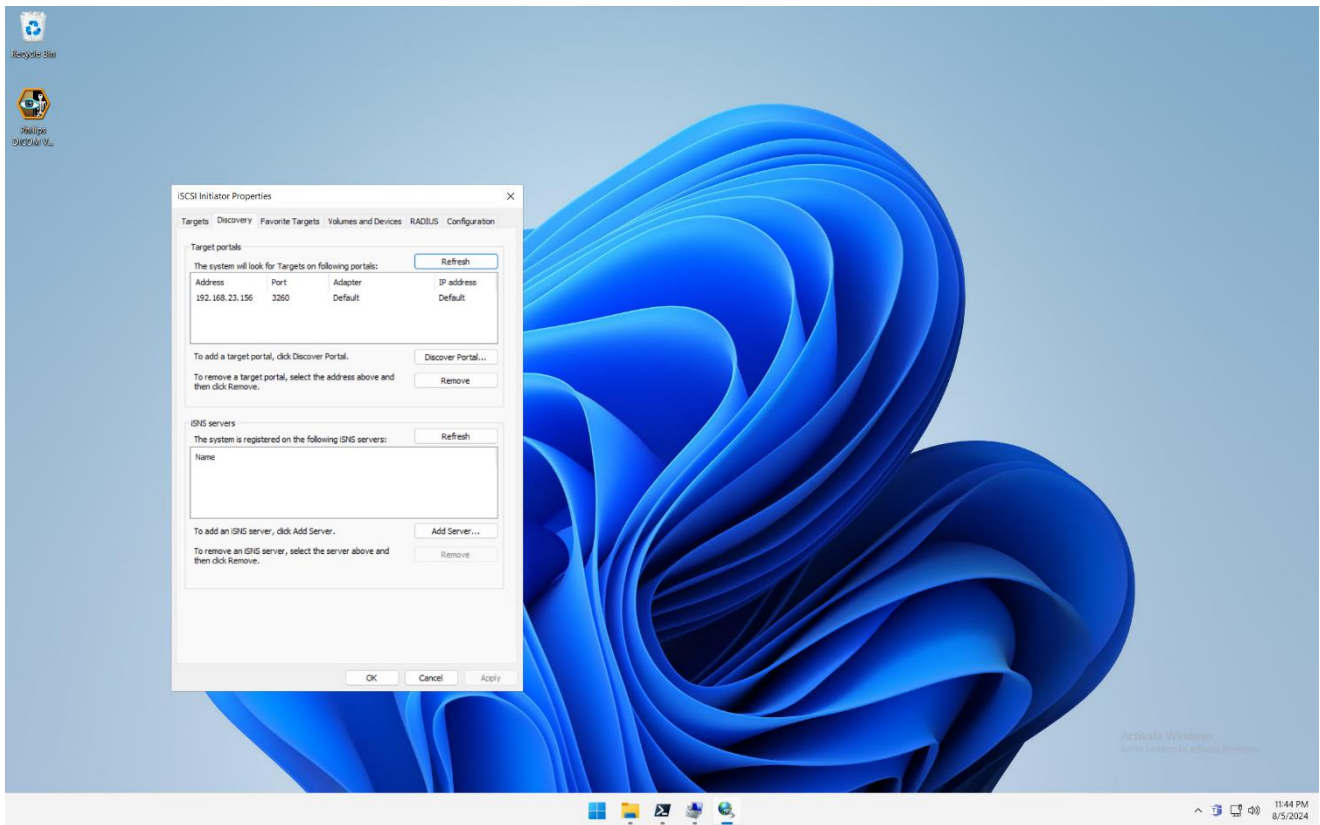
Share Name nqn.2022-06.io.storesafe:nvme01
Storage Type Unknown
Storage Path Target : nqn.2022-06.io.storesafe:nvme01
LUN 1:[_SS_nvme33n1_];
Sessions 2 🔑

Refresh Stop Start Close

Storage Clients

Microsoft Windows 11

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



Canonical Ubuntu 22.04 LTS

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

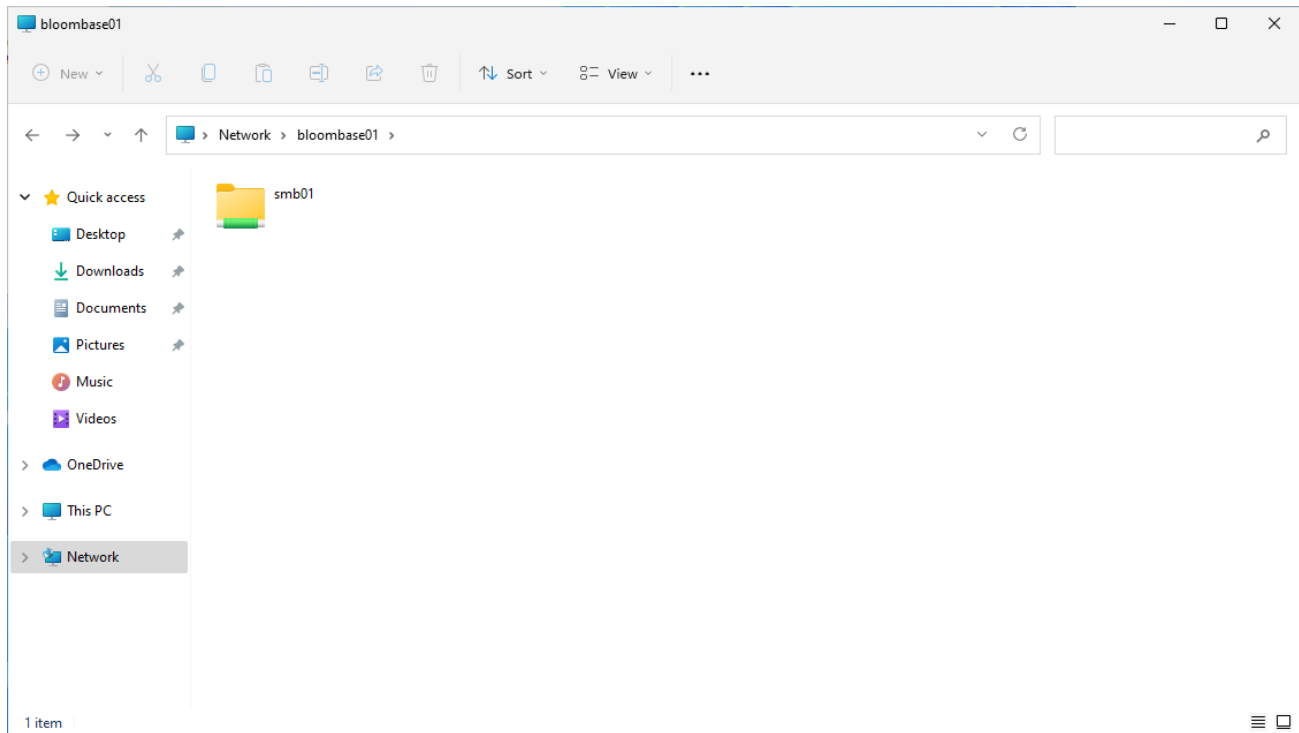
```
user@ubuntu68:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.2 LTS
Release:       22.04
Codename:      jammy
```

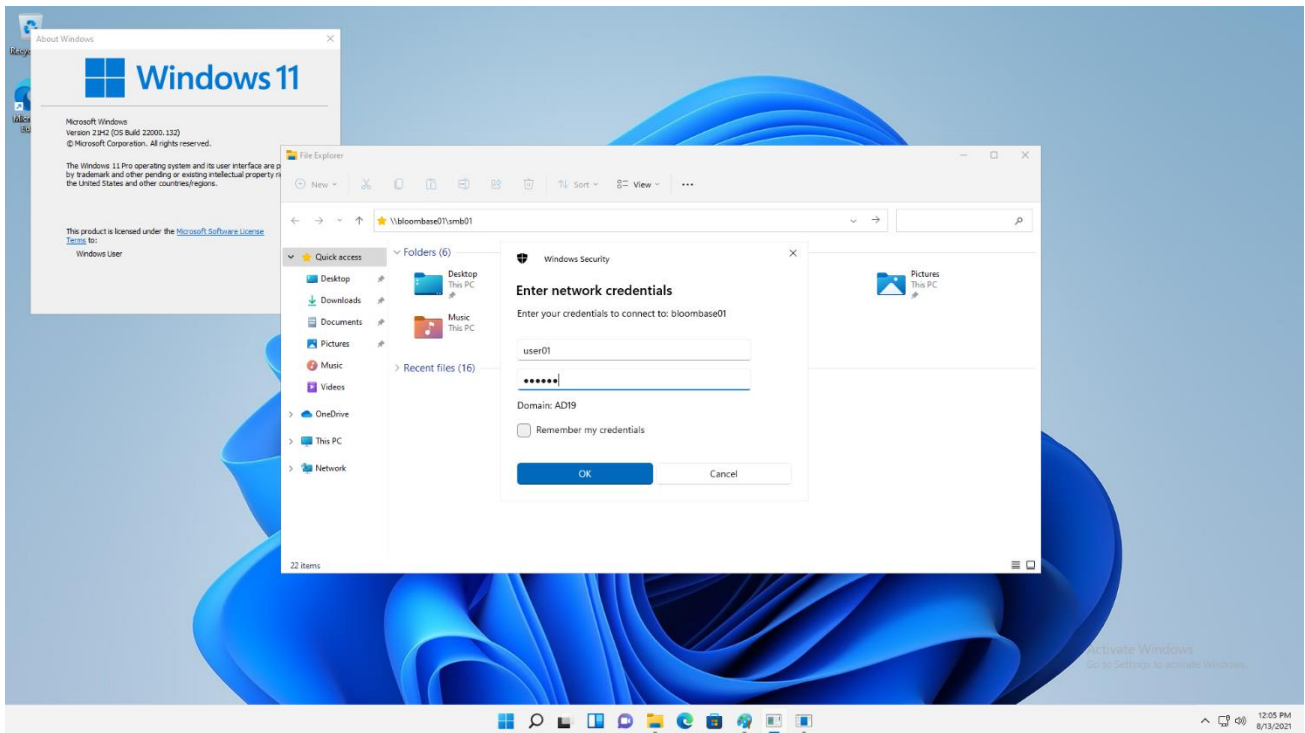
The client will need nvme initiator software installed.

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

Tests for Data-at-Rest Encryption over SMB/CIFS

SMB/CIFS shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Microsoft 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.

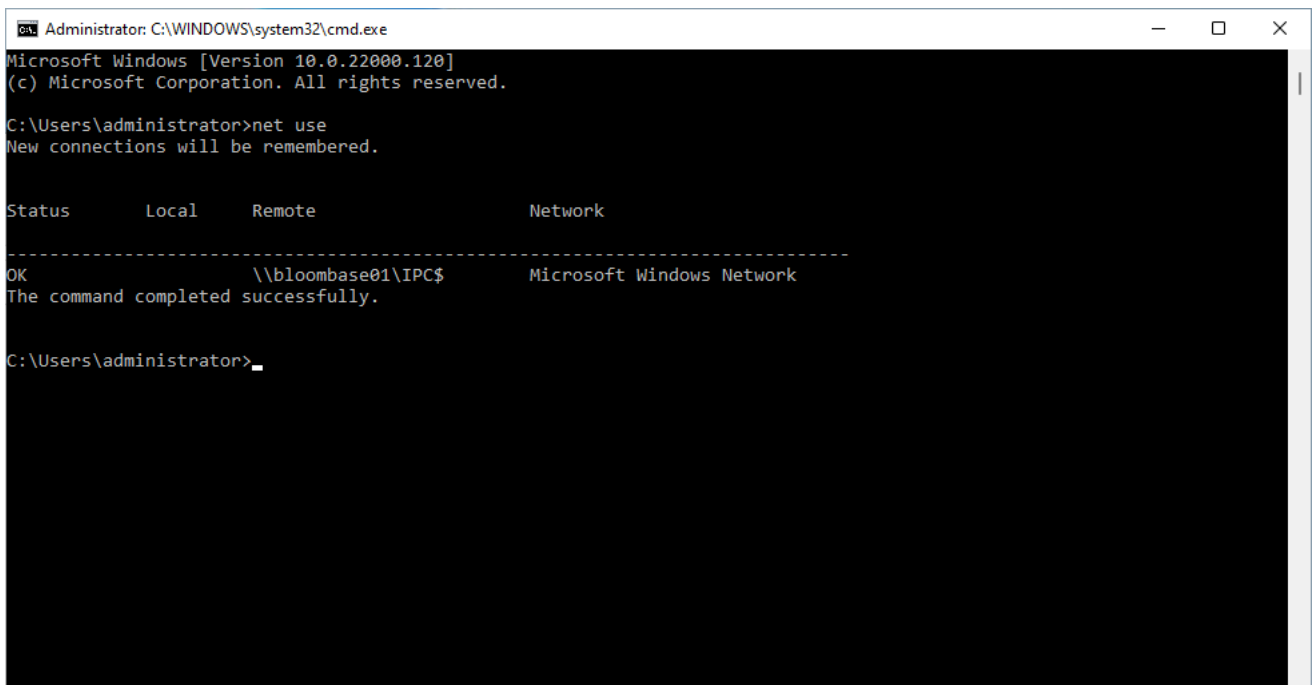




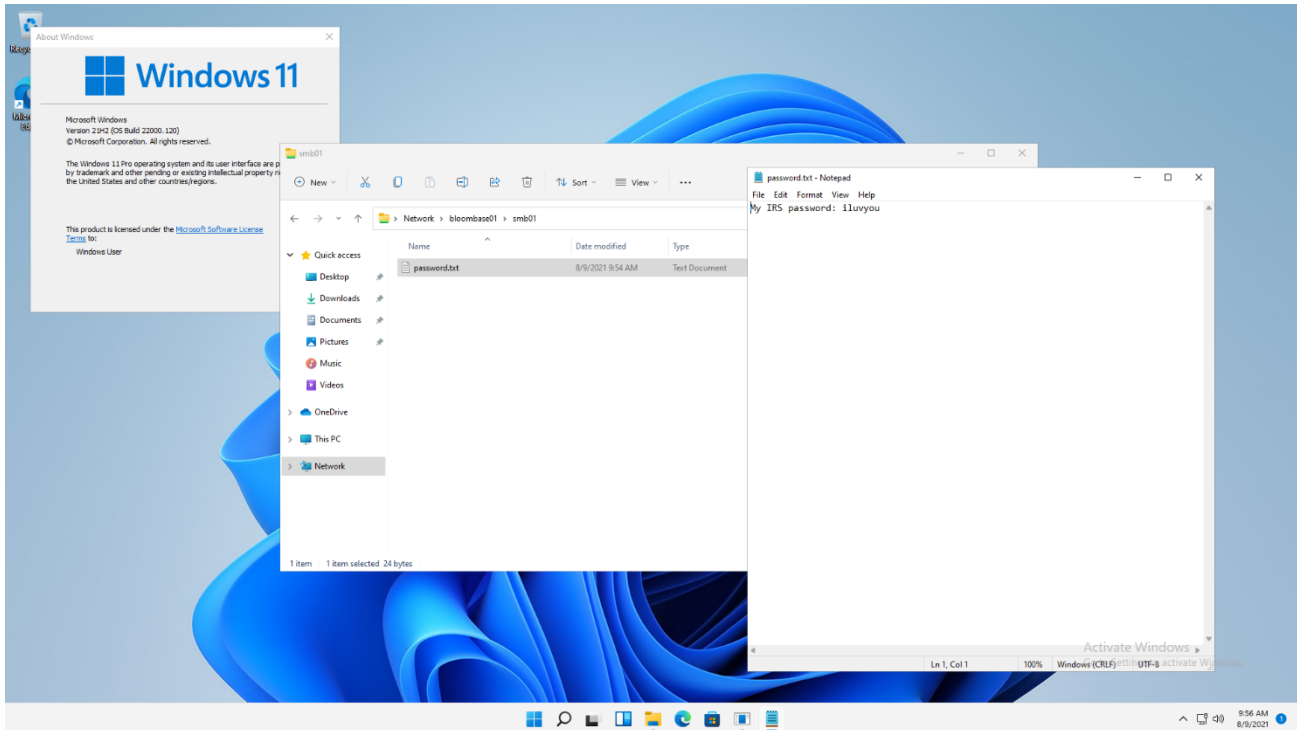
Microsoft Windows 11 clients can use the included network share on file manager to access the SMB share presented by Bloombase StoreSafe Intelligent Storage Firewall. Data owners can alternatively use the

`net use`

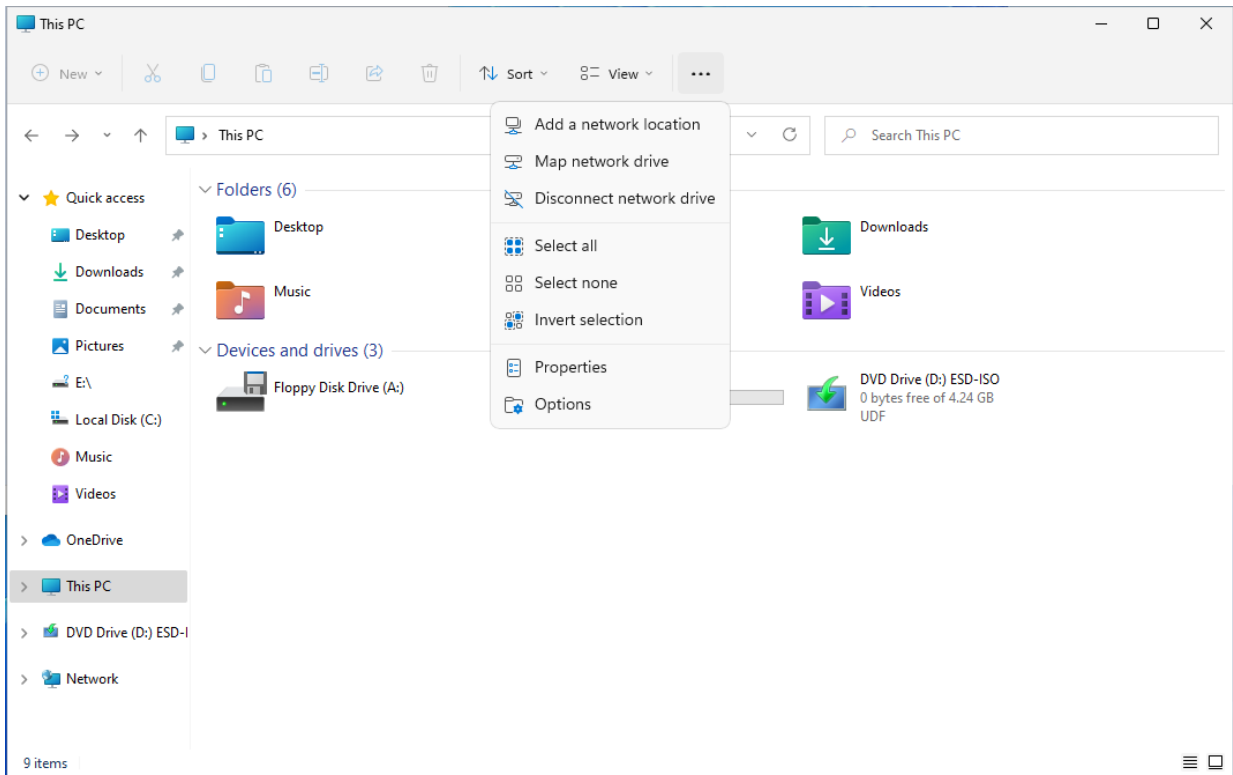
command to specify additional mounting options.

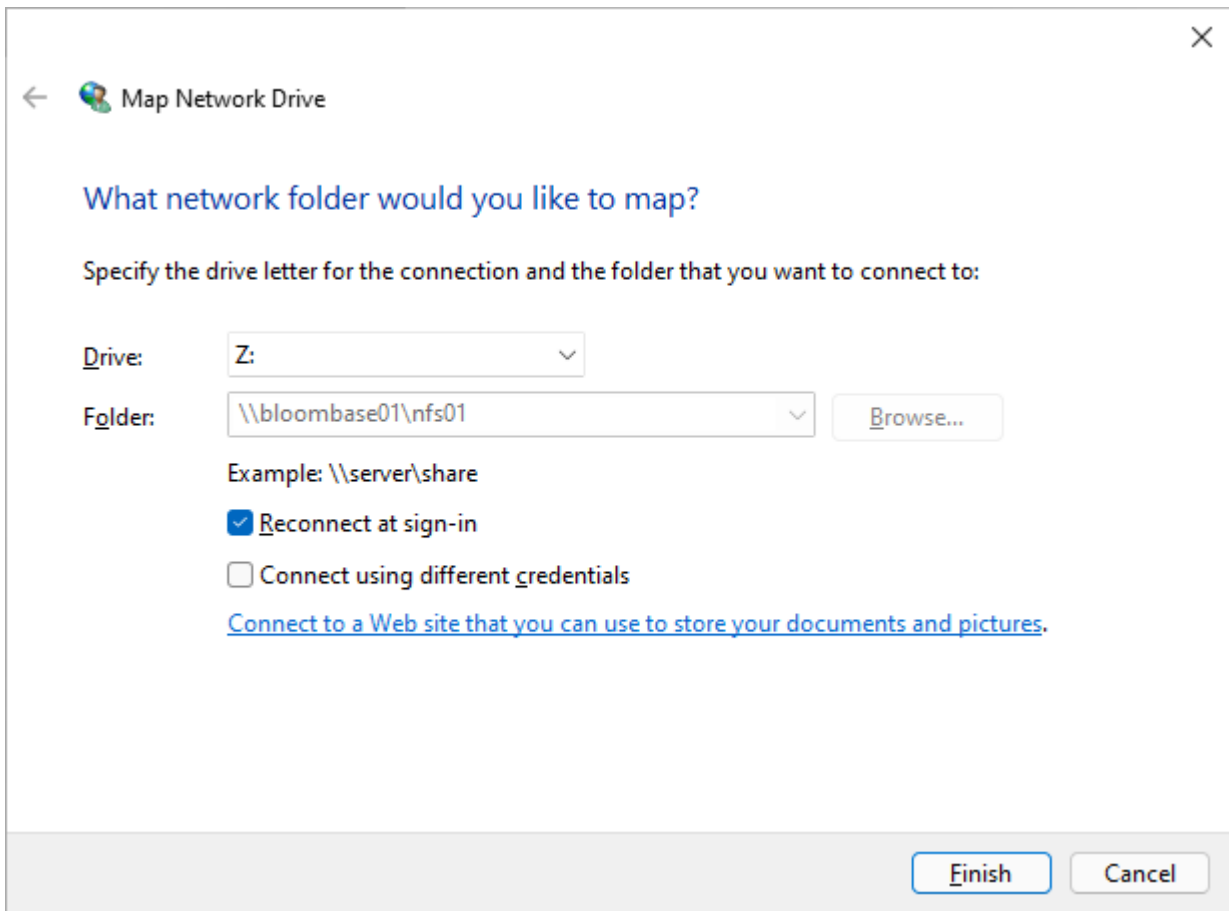


On the virtual encrypted SMB share, a sample plaintext file is created by the client and saved. The file is transparently encrypted by the Bloombase StoreSafe encryption engine with encryption keys managed by Entrust nShield 5c HSM and stored on the Microsoft Windows Server 2025 backend share.

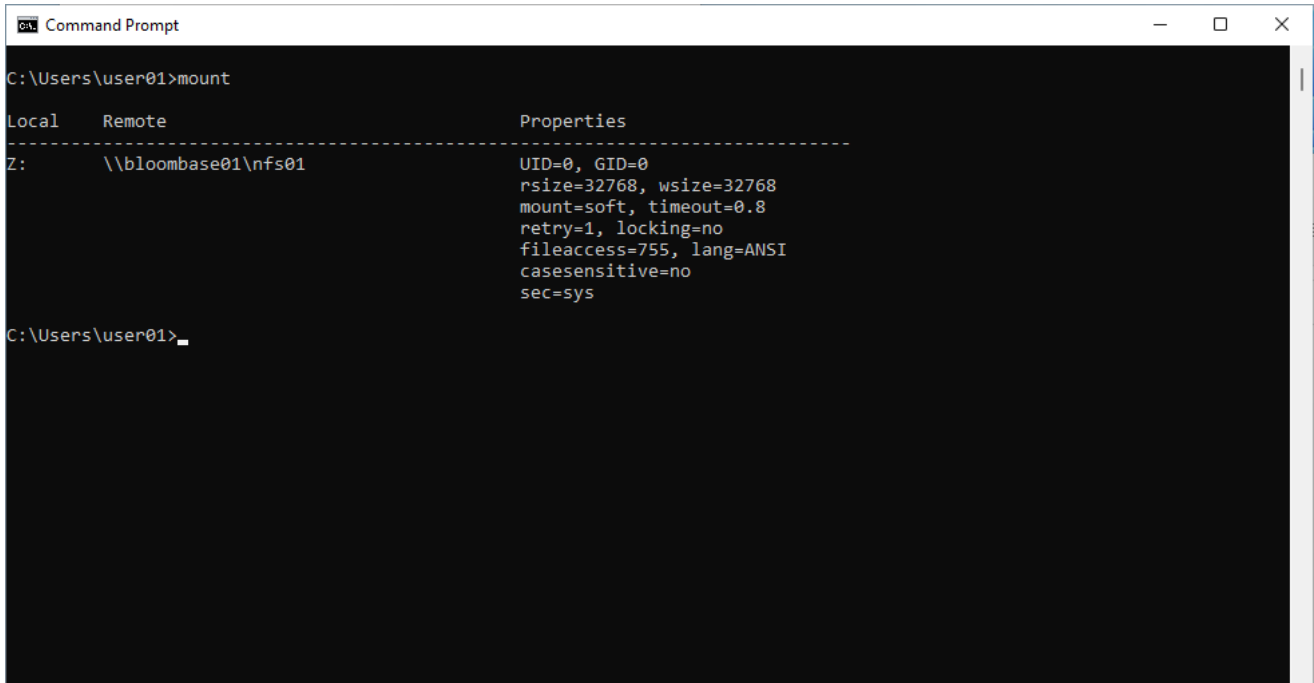


If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



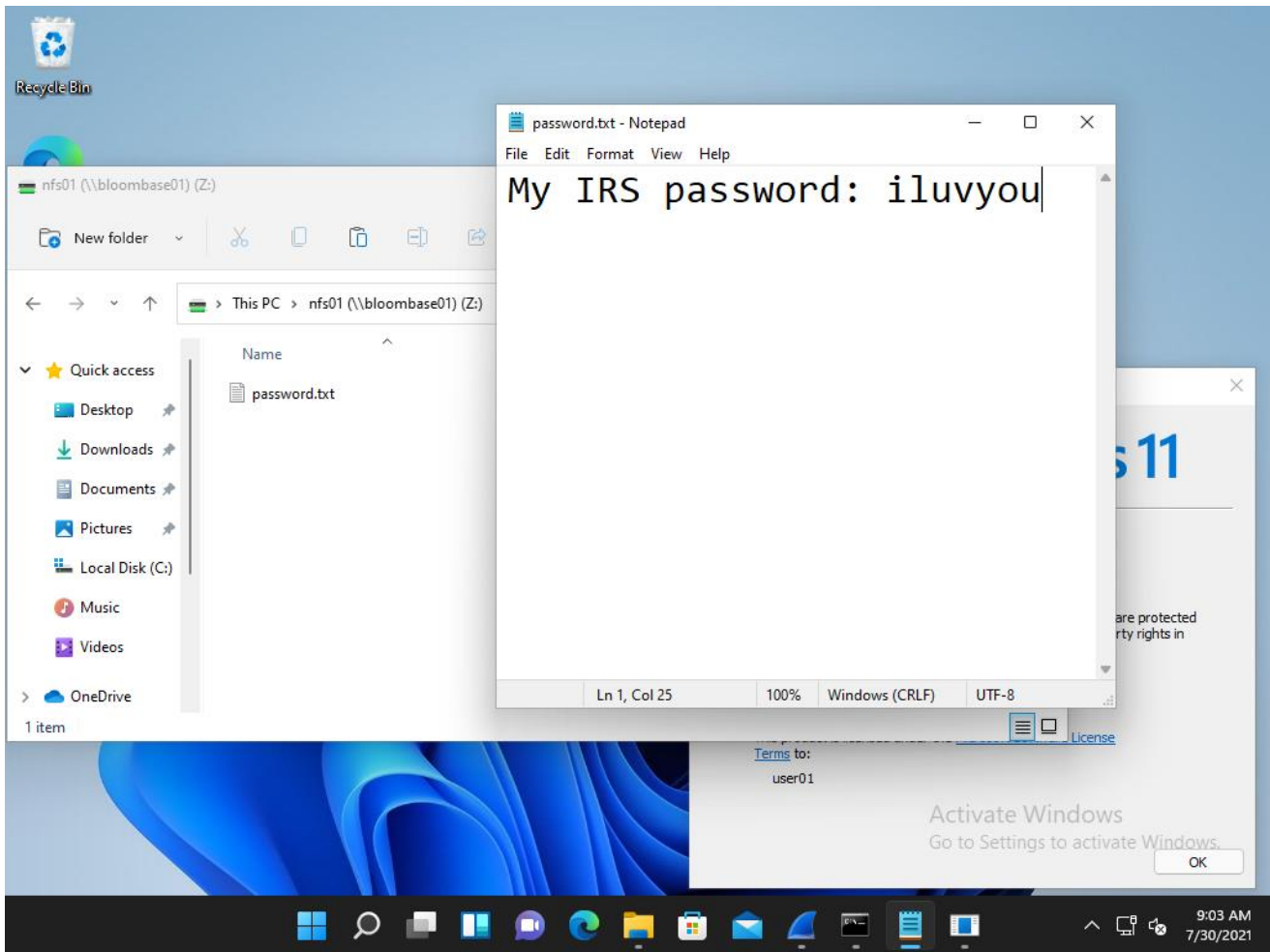


Microsoft Windows 11 clients can use the included map network drive option to add the NFS share presented by Bloombase StoreSafe Intelligent Storage Firewall with a drive letter. Data owners can alternatively use the mount command to specify additional mounting options.

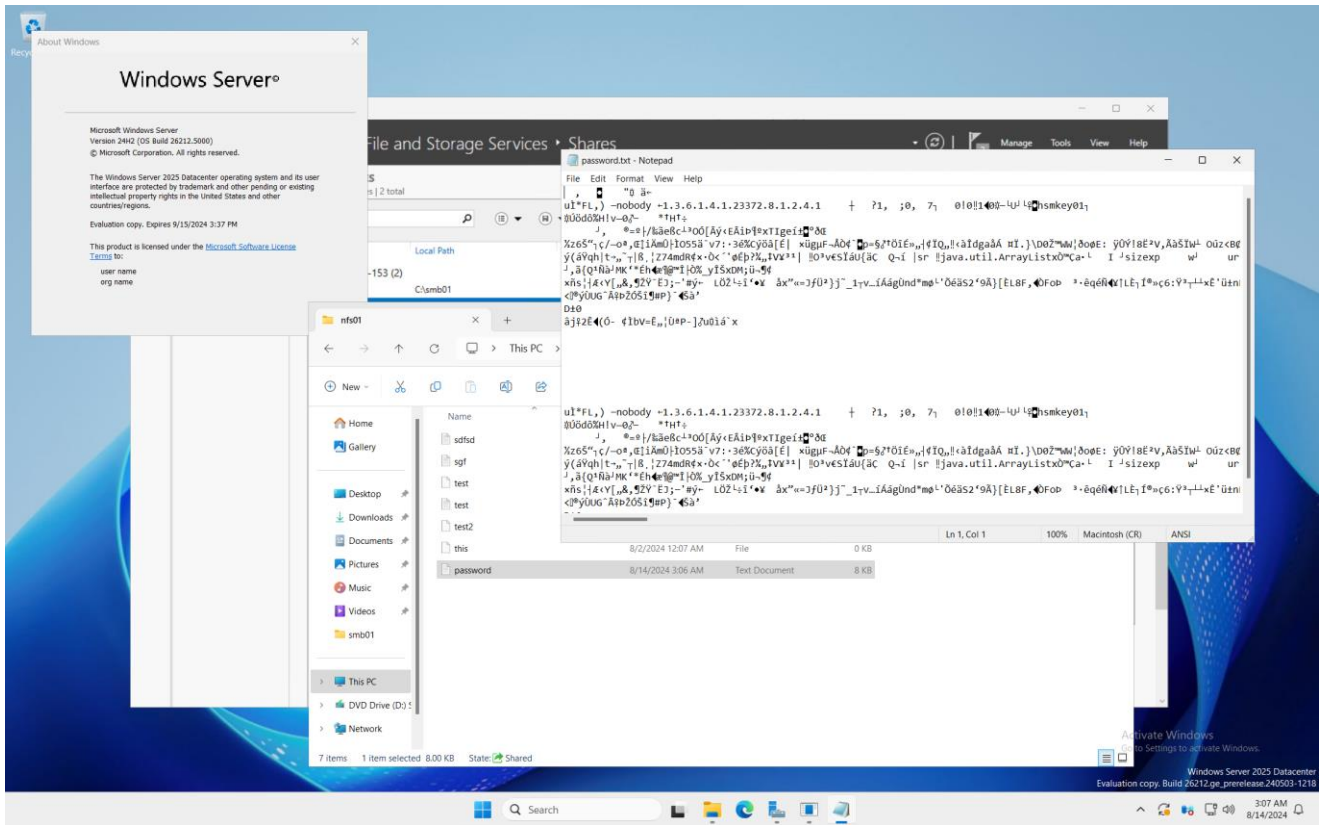


```
Command Prompt
C:\Users\user01>mount
Local      Remote      Properties
-----
Z:         \\bloombase01\nfs01  UID=0, GID=0
                                     rsize=32768, wsize=32768
                                     mount=soft, timeout=0.8
                                     retry=1, locking=no
                                     fileaccess=755, lang=ANSI
                                     casesensitive=no
                                     sec=sys
C:\Users\user01>
```

On the 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 with keys managed by Entrust nShield 5c HSM and stored on the Microsoft Windows Server 2025 backend share.

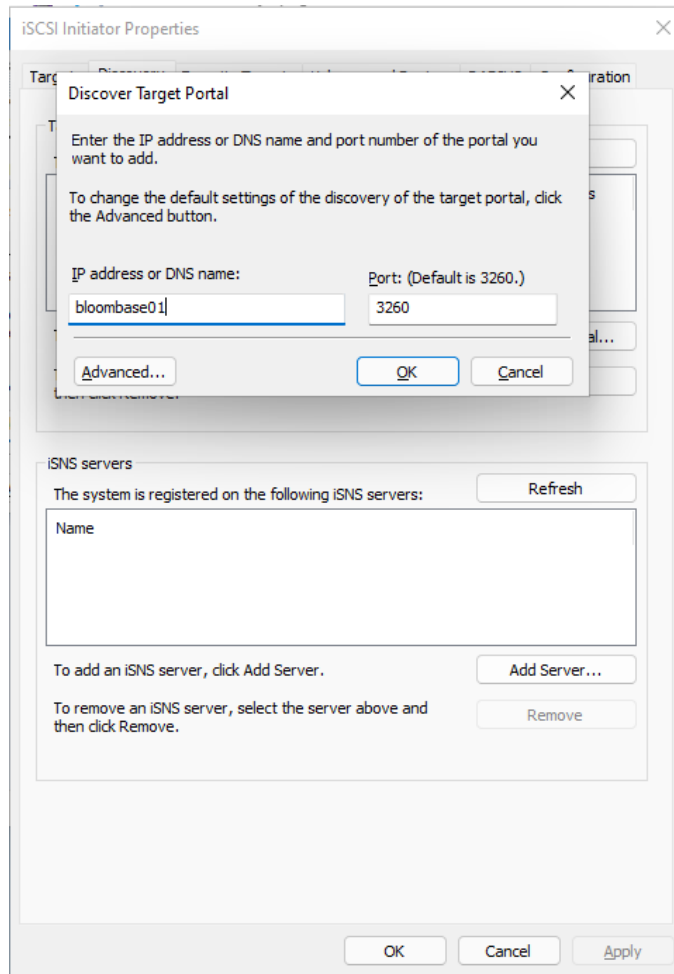


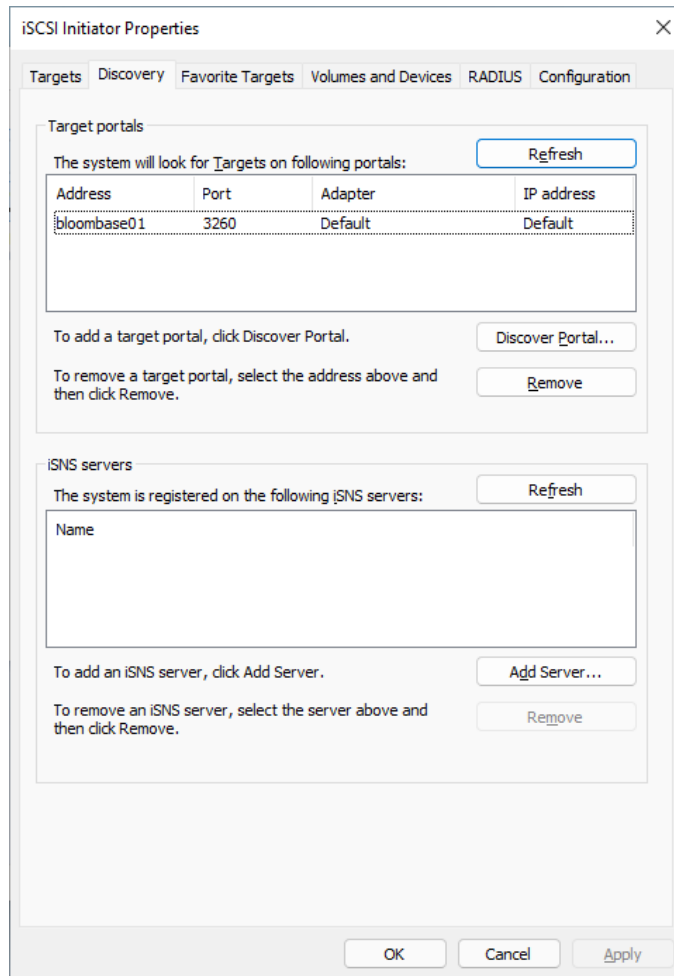
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



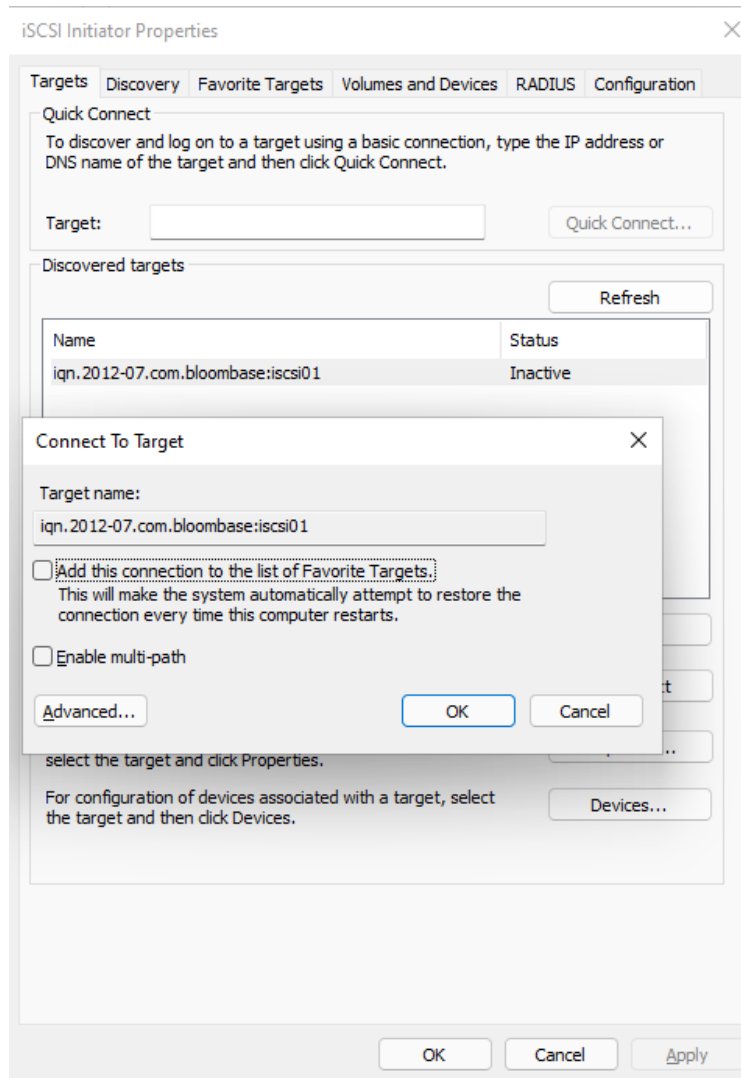
Tests for Data-at-Rest Encryption over iSCSI

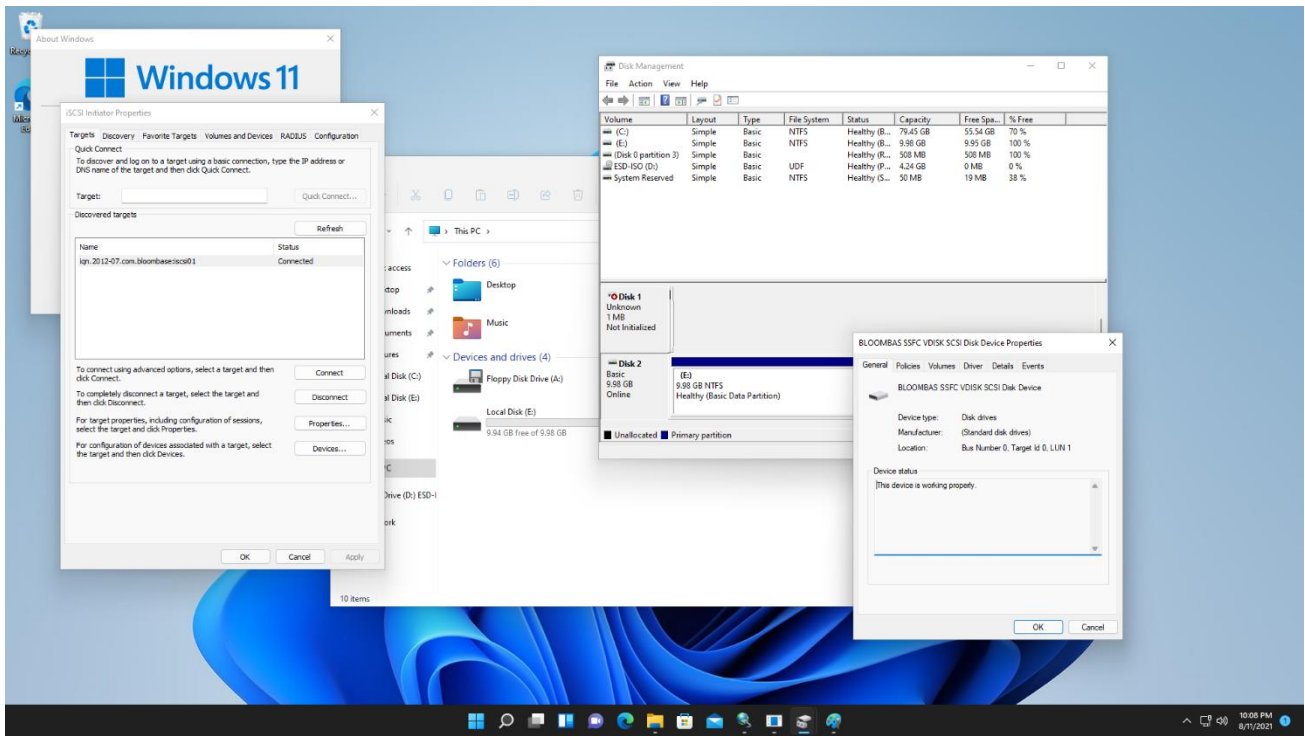
iSCSI targets are an example from the many protocols Bloombase StoreSafe supports for encryption. A target from a Microsoft Windows Server 2025 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname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



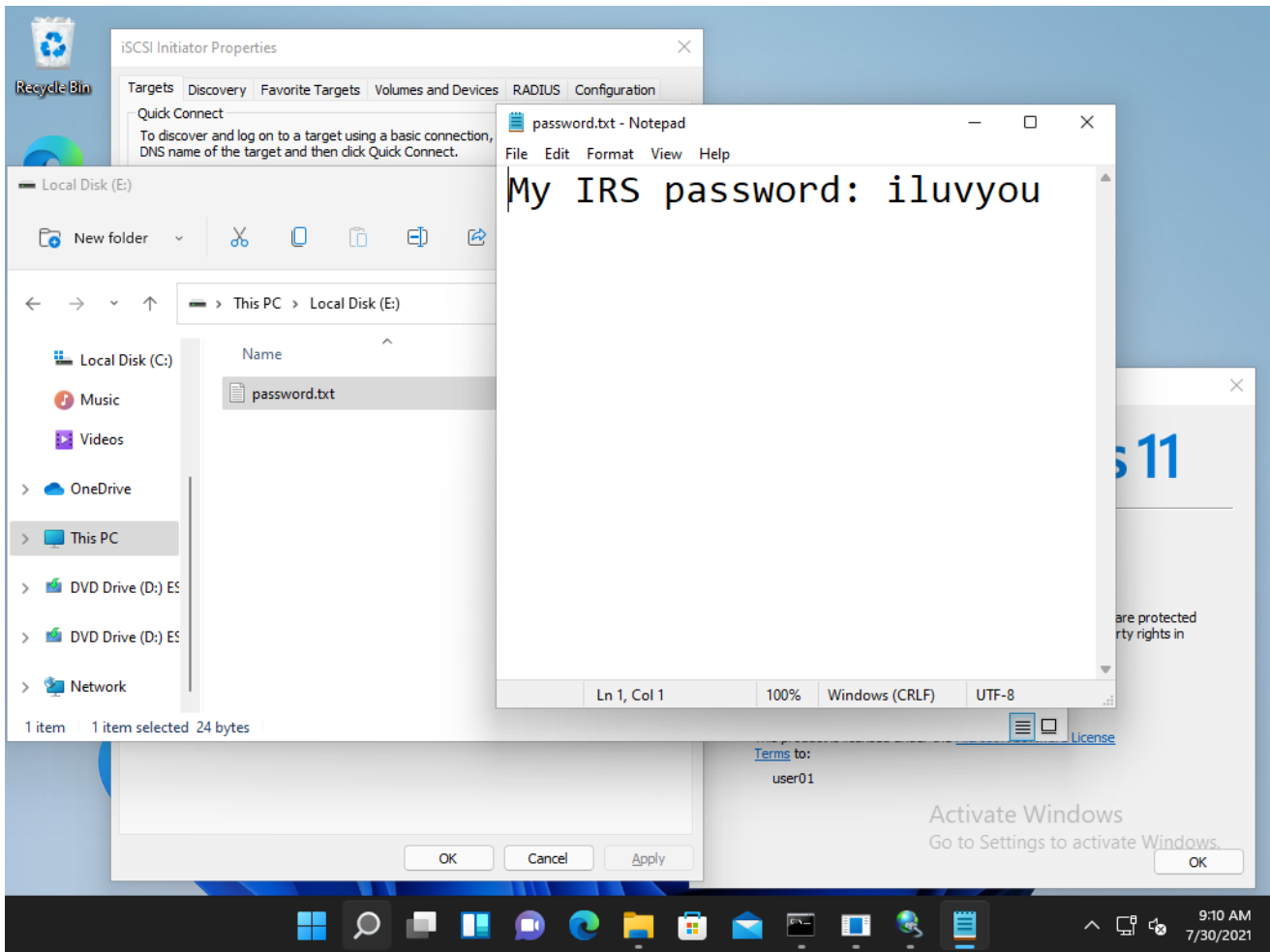


Microsoft Windows 11 clients can attach the virtual encrypted share with the default iSCSI initiator tool. Add the hostname and port to the discover tab, then connect to the iSCSI storage target presented by Bloombase StoreSafe Intelligent Storage Firewall. To access the Bloombase StoreSafe iSCSI disk,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





On the 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 with encryption keys managed by Entrust nShield 5c HSM 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.

```

Administrator: Command Prompt
C:\Users\administrator.AD19\Downloads>hexdump.exe \ISCSIVirtualDisks\iSCSI-disk01.vhdx
00000000: 76 68 64 78 66 69 6C 65 - 4D 00 69 00 63 00 72 00 |vhdxfileM i c r
00000010: 6F 00 73 00 6F 00 66 00 - 74 00 20 00 57 00 69 00 |o s o f t W i
00000020: 6E 00 64 00 6F 00 77 00 - 73 00 20 00 31 00 30 00 |n d o w s 1 0
00000030: 2E 00 30 00 2E 00 32 00 - 30 00 33 00 34 00 38 00 |. 0 . 2 0 3 4 8
00000040: 2E 00 30 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |. 0
00000050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |
*
00010000: 68 65 61 64 2A 71 DB FD - 0C 00 00 00 00 00 00 00 |head*q
00010010: 41 5E F1 A0 04 CF 84 4A - AA 33 4E 98 5B 15 1C A8 |A^ J 3N [
00010020: E7 E7 62 3E 18 A0 5B 40 - 9D 0A F9 B6 F2 9F FD ED |b> [ @
00010030: 3A E1 8B AB F1 CE FD 48 - A6 66 B3 85 27 CD 36 7E |: H f ' 6~
00010040: 00 00 01 00 00 00 10 00 - 00 00 10 00 00 00 00 00 |
00010050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |
*
00020000: 68 65 61 64 5D ED 23 7F - 0D 00 00 00 00 00 00 00 |head] #
00020010: 41 5E F1 A0 04 CF 84 4A - AA 33 4E 98 5B 15 1C A8 |A^ J 3N [
00020020: E7 E7 62 3E 18 A0 5B 40 - 9D 0A F9 B6 F2 9F FD ED |b> [ @
00020030: 3A E1 8B AB F1 CE FD 48 - A6 66 B3 85 27 CD 36 7E |: H f ' 6~
00020040: 00 00 01 00 00 00 10 00 - 00 00 10 00 00 00 00 00 |
00020050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |
*
00030000: 72 65 67 69 AE 8C 6B C6 - 02 00 00 00 00 00 00 00 |regi k
00030010: 66 77 C2 2D 23 F6 00 42 - 9D 64 11 5E 9B FD 4A 08 |fw -# B d ^ J
00030020: 00 00 30 00 00 00 00 00 - 00 00 10 00 01 00 00 00 |
00030030: 06 A2 7C 8B 90 47 9A 4B - B8 FE 57 5F 05 0F 88 6E | G K W_ n
00030040: 00 00 20 00 00 00 00 00 - 00 00 10 00 01 00 00 00 |
00030050: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |
*
    
```

```

Administrator: Command Prompt
01418fd0: 1E 18 73 08 4E FA 13 3D - 95 59 BA D0 22 2B 8A EC |s N = Y "+
01418fe0: FB 9C 8E 09 AA 4D B0 B6 - CF BE 6B D5 D2 77 87 30 |M k w 0
01418ff0: 43 93 80 6C 4A 79 19 F3 - A4 4F 35 E4 AE D0 E3 6E |C lJy 05 n
01419000: 4F 30 96 7C 32 4A 3B F1 - 58 F3 B8 E4 63 05 B4 26 |00 |2J; X c &
01419010: 50 8C 42 75 B6 B5 DA 9B - BE 57 3C 14 C6 C1 F1 DE |P Bu Wc
01419020: 1D 67 64 87 B7 AC A9 07 - 1F 1E EF DB 78 37 7F 98 |gd x7
01419030: 2F 3B 4B 1C 8E 67 7C 37 - 1B 0B C5 7A 9C 87 E4 47 |/;K g|7 z G
01419040: B0 E1 63 90 84 91 24 F5 - 8C 42 42 5F A1 8D B6 FF |c $ BB_
01419050: 8F F2 3D 10 E1 33 5F EB - EC E3 44 E9 19 32 E4 7A |= 3 D 2 z
01419060: FC DC 3D 63 4A 47 22 71 - D6 C4 F4 47 31 EE B2 2E |=cJG"q G1 .
01419070: 95 93 FF 79 A1 8F 16 AD - 65 B1 A8 FB 81 D1 7A C2 |y e z
01419080: 7E 79 83 AD F9 91 49 34 - 78 C2 7C 38 A2 27 8F B7 |~y I4x |8 '
01419090: 62 77 72 97 DA 1B 58 92 - E8 90 A5 54 69 73 32 A8 |bwr X Tis2
014190a0: 5E 45 35 02 EC 83 A0 86 - 93 F3 47 08 00 23 A6 F7 |^E5 G #
014190b0: EA F3 8C 4F 97 FA F3 18 - 39 EC A3 1A 7D 95 C5 49 |O 9 } I
014190c0: B4 CE 1E 93 D1 E6 3F 82 - 1C 5D 05 D7 50 9A 2C 98 |? ] P ,
014190d0: 6F F8 4F 59 3E 36 82 9B - 14 6D A3 D7 7A 33 92 91 |o OY>6 m z3
014190e0: 1D 63 8D 22 10 07 3B E9 - F6 72 1D 43 C2 47 5E 0D |c " ; r C G^
014190f0: 77 3F E2 CA 65 BB C6 47 - 43 76 E7 EB 69 77 16 C2 |w? e GCv iw
01419100: 66 30 1E 2D BD 3D FB A6 - 22 5B 19 5E D4 42 E1 F2 |f0 - = "[ ^ B
01419110: BD FC 54 CB A1 04 0B 21 - 81 35 7C 93 33 8E B4 7F |T ! 5| 3
01419120: 0D E5 5F 59 2C 93 99 3E - B2 42 C4 21 2B 29 2B 56 |_Y, > B !+)+V
01419130: C7 CB CD AC 14 81 4B C7 - 4D 59 64 47 BD EB 32 09 |K MYdG 2
01419140: 39 35 48 BD 4A 59 DF 4C - 83 C9 22 F4 F5 1D DE A5 |95H JY L "
01419150: 26 35 95 61 E1 39 7C A1 - 68 4A 47 D2 EA 89 EC B5 |&5 a 9| hJG
01419160: 40 A9 C7 3C 57 70 17 96 - 92 E4 67 93 BD 8E 6C 20 |@ <Wp g l
^C
C:\Users\administrator.AD19\Downloads>hexdump.exe \ISCSIVirtualDisks\iSCSI-disk01.vhdx | Findstr password
C:\Users\administrator.AD19\Downloads>_
    
```

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-over-Fabrics (NVMe-oF) protocols, in this case, NVMe/TCP.

```
[root@bb027 ~]# nvme discover -t tcp -a 192.168.211.24 -s 4420 -q nqn.2014-08.org.nvmexpress:uuid:cf2eae42-6537-4891-85c2-77bbff4598b8
```

```
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:cf2eae42-6537-4891-85c2-77bbff4598b8 -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 were in clear-text.

```

4/
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 with Entrust nShield 5c HSM centralized key management 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 were 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 with Entrust nShield 5c HSM 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 ~]#
```

Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall with Entrust nShield 5c Hardware Security Module (HSM) to deliver on-the-fly encryption of multiple storage protocols including SMB/CIFS, 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,

- Entrust nShield 5c Hardware Security Module (HSM) v13.2.4

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 Canonical Ubuntu 22.04 LTS.

Bloombase Product	Client Systems	Storage Backends	Key Management System
Bloombase StoreSafe Intelligent Storage Firewall 4.0	<ul style="list-style-type: none"> • Microsoft Windows 11 • Canonical Ubuntu 22.04 LTS 	<ul style="list-style-type: none"> • Microsoft Windows Server 2025 • Rocky Linux 9 	Entrust nShield 5c Hardware Security Module (HSM) v13.2.4

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.

Acknowledgement

Bloombase InteropLab would like to thank Entrust team for supporting the integration of Bloombase StoreSafe with Entrust nShield 5c Hardware Security Module (HSM).

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 Broadcom VMware, <https://marketplace.cloud.vmware.com/vsx/solutions/bloombase-storesafe-security-server>
4. Entrust nShield 5c Hardware Security Module (HSM), <https://www.entrust.com/products/hsm/nshield-5c>
5. Bloombase StoreSafe for Entrust, <https://www.entrust.com/partners/directory/bloombase>
6. OASIS PKCS#11, <https://www.oasis-open.org/committees/pkcs11>
7. Post-Quantum Cryptography (PQC), <https://csrc.nist.gov/Projects/post-quantum-cryptography>
8. NVIDIA ConnectX NICs, <https://www.nvidia.com/en-us/networking/ethernet-adapters/>
9. Rocky Linux, <https://rockylinux.org>
10. Canonical Ubuntu Linux, <https://ubuntu.com>
11. NVM Express community, <https://nvmexpress.org/about/membership-list/>
12. PCI-SIG community, <https://pcisig.com/bloombase>

13. Bloombase StoreSafe Intelligent Storage Firewall for Dell PowerEdge servers, <https://infohub.delltechnologies.com/en-us/p/bloombase-storesafe>
14. Bloombase StoreSafe AI-Powered Threat Detection and PQC Encryption for Intel Xeon 6 processors, <https://www.intel.com/content/www/us/en/content-details/858867/bloombase-delivers-ai-powered-threat-detection-and-pqc-encryption.html>
15. Bloombase StoreSafe for 5th Gen Intel Xeon Scalable processors, <https://www.intel.com/content/www/us/en/content-details/839465/bloombase-storesafe-optimization-with-5th-gen-intel-xeon-scalable-processors.html>
16. Bloombase StoreSafe for Intel, <https://builders.intel.com/solutionslibrary/bloombase-storesafe-intelligent-storage-firewall>
17. Bloombase StoreSafe for NVIDIA, <https://resources.nvidia.com/en-us-accelerated-networking-resource-library/bluefield-and-doca-bloombase>
18. Bloombase StoreSafe for Red Hat, <https://catalog.redhat.com/software/container-stacks/detail/5e9874cb3f398525a0ceb024>
19. Bloombase StoreSafe for Microsoft, https://azuremarketplace.microsoft.com/en-us/marketplace/apps/bloombase.bloombase-storesafe-3_4_7_0_el7_x86_64