



Bloombase StoreSafe and Entrust KeyControl Integration Guide for Data-at-Rest Encryption

June 2021



Executive Summary

Entrust KeyControl has been validated by Bloombase InteropLab to run with Bloombase StoreSafe Intelligent Storage Firewall. This document describes the steps carried out to integrate Entrust KeyControl with Bloombase StoreSafe software appliance on VMware ESXi to deliver high bandwidth transparent storage encryption for mission critical applications. Client host system Microsoft Windows 11 has been tested with Entrust KeyControl and Bloombase StoreSafe data-at-rest encryption solution to secure Microsoft Storage Server 2022 storage backend.

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.

© 2021 Bloombase, Inc.

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

Entrust KeyControl is trademark of Entrust Corporation 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 KeyControl Integration Guide - USLET-EN-Ro.99

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Key Management	9
Storage Encryption	9
Storage System	9
Application Client	9
Configuration Overview	10
Entrust KeyControl	10
Entrust KeyControl Configurations	10
Entrust KeyControl Client Enrollment	12
Microsoft Storage Server on Microsoft Windows Server 2022	15
SMB Services Configuration	16
NFS Services Configuration	18
iSCSI Services Configuration	20
Bloombase StoreSafe Intelligent Storage Firewall	20
Entrust KeyControl and Bloombase StoreSafe Integration	21
Encryption Key Provisioning	23
Data-at-Rest Encryption for SMB	25
Data-at-Rest Encryption for NFS	29
Data-at-Rest Encryption for iSCSI	33
Use Cases	38
Data-at-Rest Encryption for SMB	38
Data-at-Rest Encryption for NFS	41
Data-at-Rest Encryption for iSCSI	46
Conclusion	53
Disclaimer	55
Acknowledgement	56
Reference	57

Purpose and Scope

This document describes the steps necessary to integrate Entrust KeyControl 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 topics:

- Install and configure Bloombase StoreSafe software appliance
- Integrate Bloombase StoreSafe with Entrust KeyControl
- Integrate application components Microsoft Windows 11 client host system and Microsoft Storage Server 2022 with Bloombase StoreSafe and Entrust KeyControl to demonstrate how high-bandwidth, agentless, application-transparent data encryption could be achieved for multiple network storage protocols namely SMB, NFS and iSCSI

Assumptions

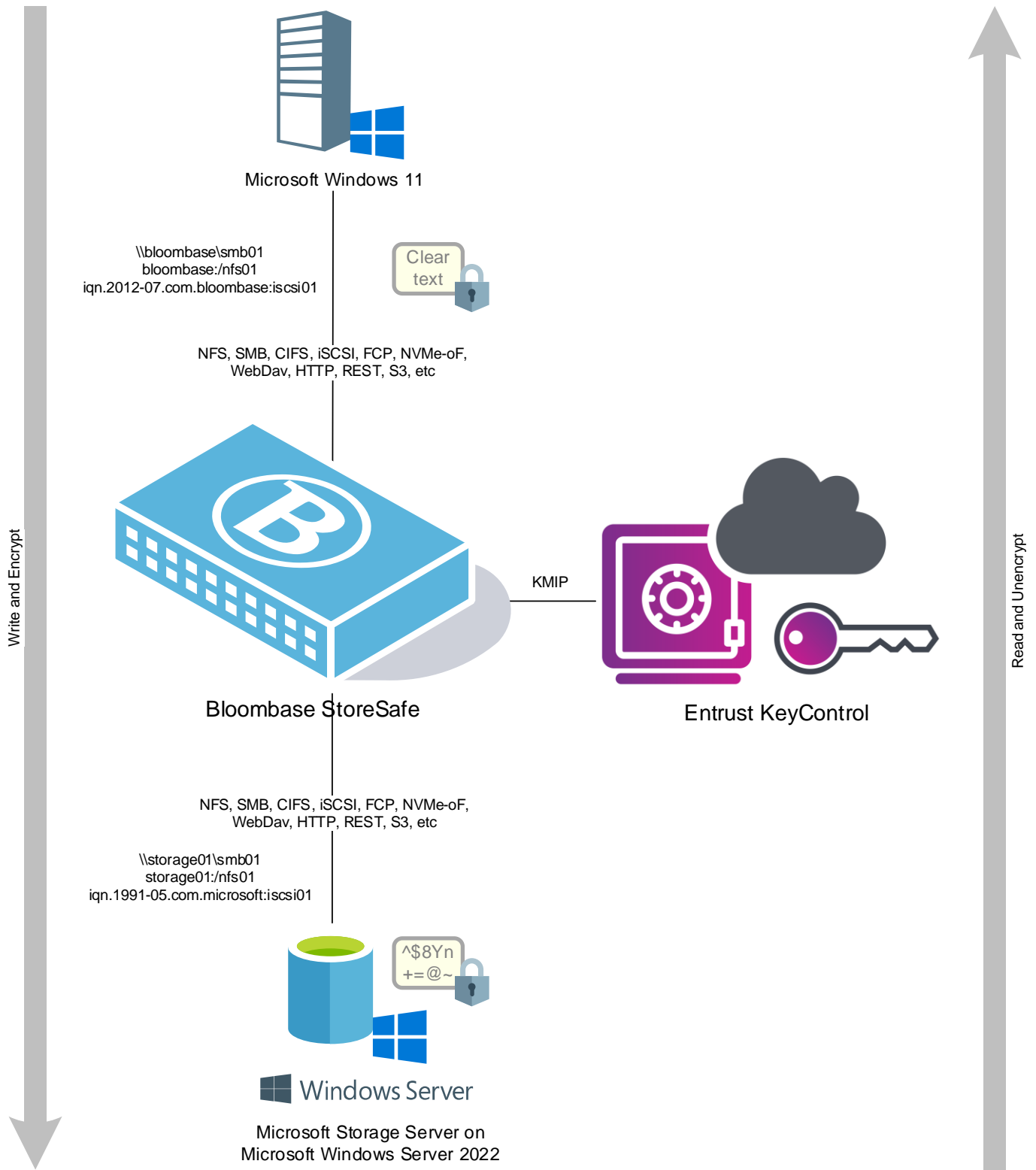
This document describes the integration of Entrust KeyControl with Bloombase StoreSafe. It is assumed that you are familiar with operation of Entrust KeyControl, storage systems, and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed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



Key Management

Key Manager	Entrust KeyControl 5.4 (b540001603)
--------------------	-------------------------------------

Storage Encryption

Storage Encryption	Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.8.4-EA2
Server	VMware Virtual Machine (VM) on VMware ESXi 6.0
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	Microsoft Storage Server on Microsoft Windows Server 2022 on VMware ESXi 6.0
-----------------------	--

Application Client

Client Host	Microsoft Windows 11 on VMware ESXi 6.0
--------------------	---

Configuration Overview

Entrust KeyControl

Entrust KeyControl is a VMware-certified, scalable, and feature rich KMIP server. KeyControl manages the encryption keys for all of your virtual machines and encrypted data stores and can scale to support thousands of encrypted workloads in large deployments.

The KeyControl provides central management and secure storage of encryption keys, including those generated by Bloombase StoreSafe products, and KMIP-compliant cloud vendors. It provides intuitive web-based console, and APIs for managing of encryption keys.

The KMIP services provided by Entrust KeyControl are used by Bloombase StoreSafe for encryption protection of data-at-rest use cases.

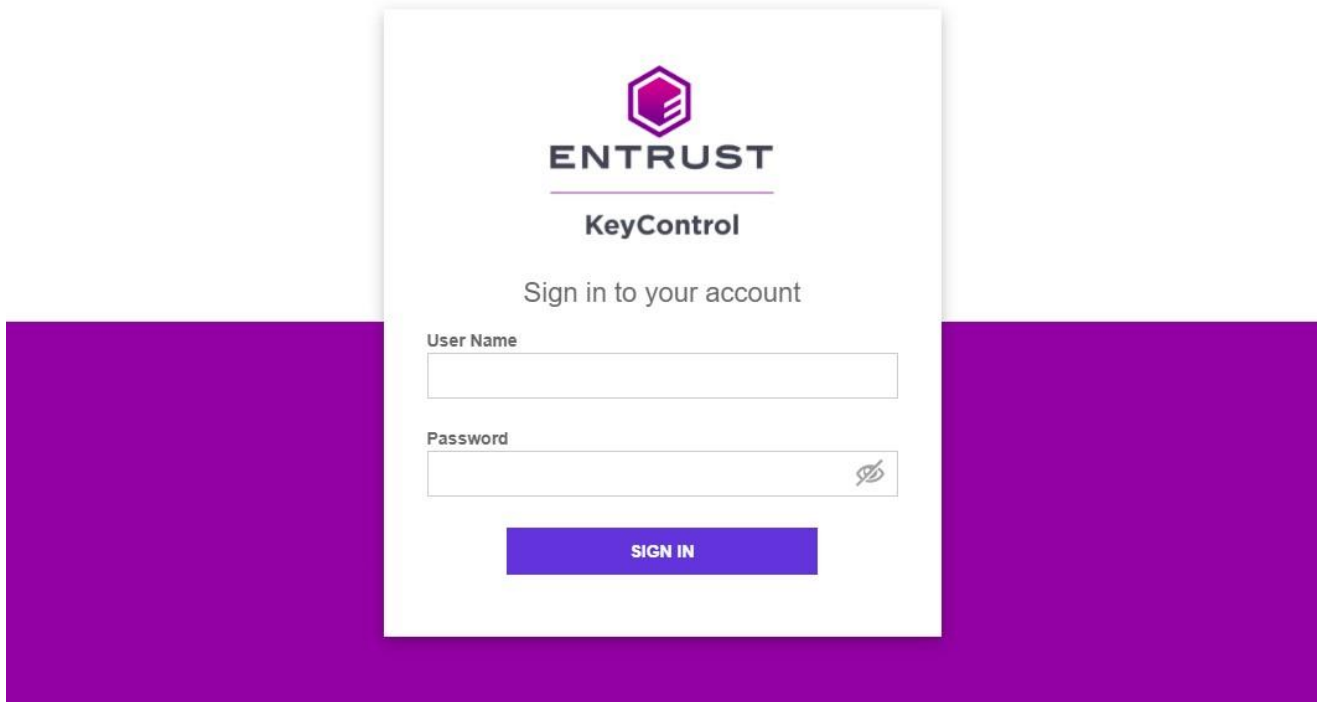
Entrust KeyControl Configurations

Assume Entrust KeyControl is installed and configured as a network attached appliance with IP address

192.168.23.249

Entrust KeyControl can be managed remotely via web-based management console at URL

<https://192.168.23.249>



Once logged in, the dashboard of the Entrust KeyControl is shown.

The screenshot shows the Entrust KeyControl dashboard with the Security tab selected. The navigation bar includes icons for Dashboard, Security, Cluster, Cloud, BYOK, Vault, Audit Log, Alerts, KMP, and Settings. Below the navigation bar, there are tabs for 'KeyControl Managed Users', 'Active Directory Users', and 'Groups'. A table displays the following data:

Name	Login Name	Status	Authenticati.:	Last Login	Two-Factor Aut.:	Securit.:	Domai.:	Cloud:
Security Adminis...	secroot	Enabled	Local	Wed Jul 28 2021 21:37:35 G...		✓	✓	✓

Please make a selection to see details.

Entrust KeyControl Client Enrollment

To authenticate the communication between Entrust KeyControl and Bloombase StoreSafe, signed certificates need to be created and stored in the Entrust KeyControl and the Bloombase StoreSafe. In the Entrust KeyControl, this can be configured as follows.

Enable the KMP feature, with the network port and any other configuration.

Provision the authorized client which key management services are to be delivered, in this case, the Bloombase StoreSafe server instance namely `storesafe-cert` by navigating to KMP > Client Certificates > Actions > Create Certificate > Upload CSR

ENTRUST | KeyControl | DASHBOARD | SECURITY | CLUSTER | CLOUD | BYOK | VAULT | AUDIT LOG | ALERTS | KMIP | SETTINGS

Actions ▾ Basic Client Certificates Objects Multi-Select: Refresh

Actions	Valid From	Expiration	Expires In (days)
Create Certificate Delete All Certificates	<input type="text"/>	<input type="text"/>	<input type="text"/>
storesafe-cert	Thu Jul 29 2021 02:58:16 GMT-0700 (Pacific...)	Fri Jul 29 2022 02:58:16 GMT-0700 (Pacific ...)	359

Please make a selection to see details.

©2021 Entrust Corporation. All Rights Reserved.

You may upload a CSR created by Bloombase StoreSafe, or create your own.

ENTRUST | KeyControl | DASHBOARD | SECURITY | CLUSTER | CLOUD | BYOK | VAULT | AUDIT LOG | ALERTS | KMIP | SETTINGS

Actions ▾ Basic Client Certificates Objects Multi-Select: Refresh

Certificate Name

Certificate Expiration

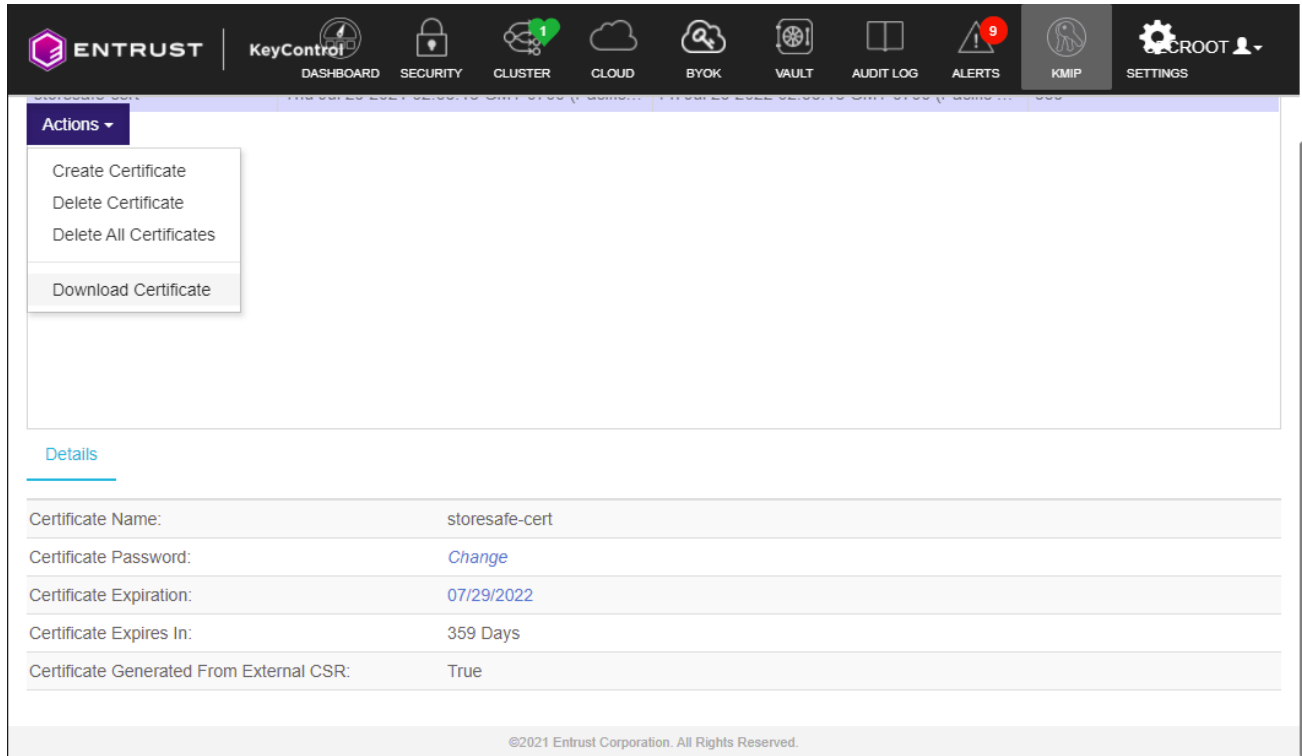
Certificate Signing Request (CSR)

CSR needs to be in base64 encoded PKCS#10.

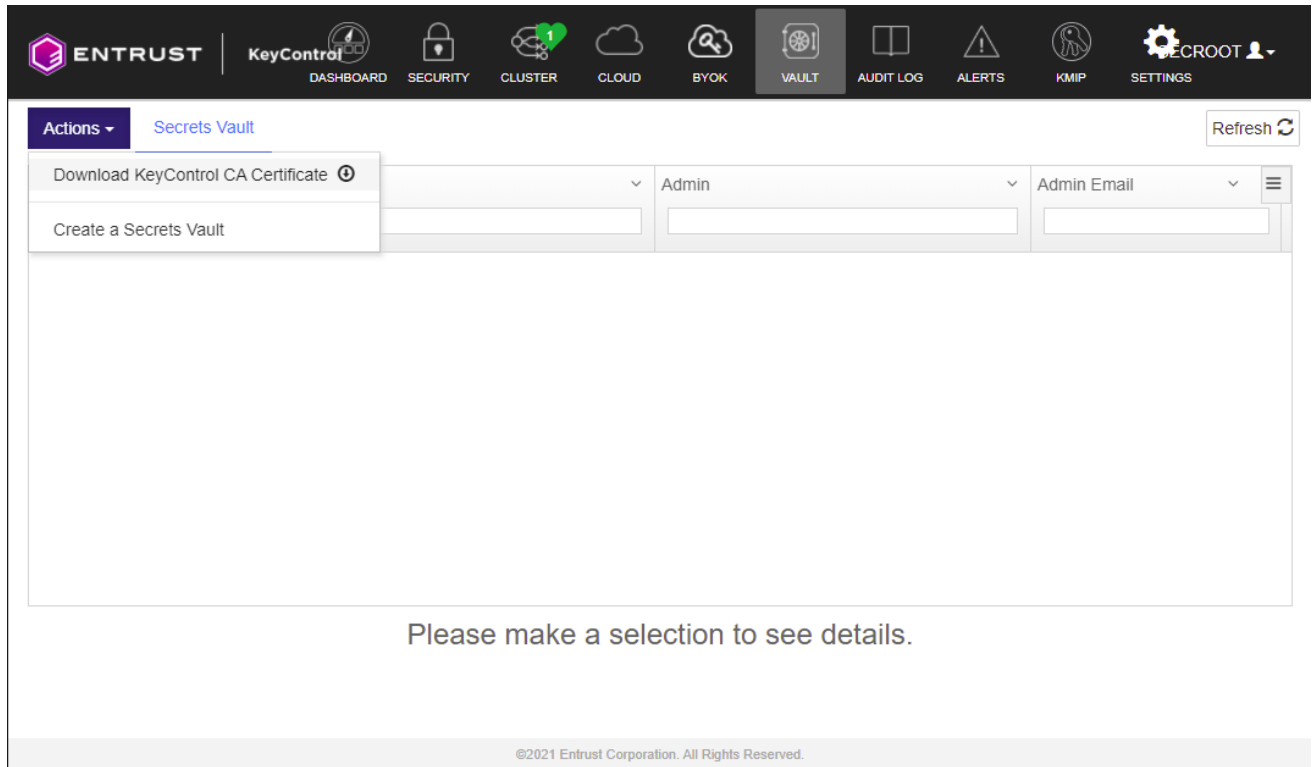
Certificate Password

Confirm Password

KMIP client certificate is generated and imported to KeyControl host configuration. Download the Certificate to upload to Bloombase StoreSafe client configuration.



Also, download the Entrust KeyControl CA certificate which will be needed for the Bloombase StoreSafe



Microsoft Storage Server on Microsoft Windows Server 2022

Microsoft Storage Server on Microsoft Windows Server 2022 running on VMware ESXi is used in this interoperability test which is able to provide storage services over network storage protocols including NVMe-oF, FCP, iSCSI, NFS, SMB, CIFS, REST, etc.

Microsoft Windows Server 2022 is deployed as a virtual appliance (VA) on VMware ESXi.

SMB Services Configuration

The screenshot displays the Windows Server Manager interface. The left-hand navigation pane shows the following options: Servers, Volumes, Disks, Storage Pools, Shares (selected), iSCSI, and Work Folders. The main area is titled "Server Manager > File and Storage Services > Shares".

The "SHARES" section shows "All shares | 2 total". A table lists the shares:

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

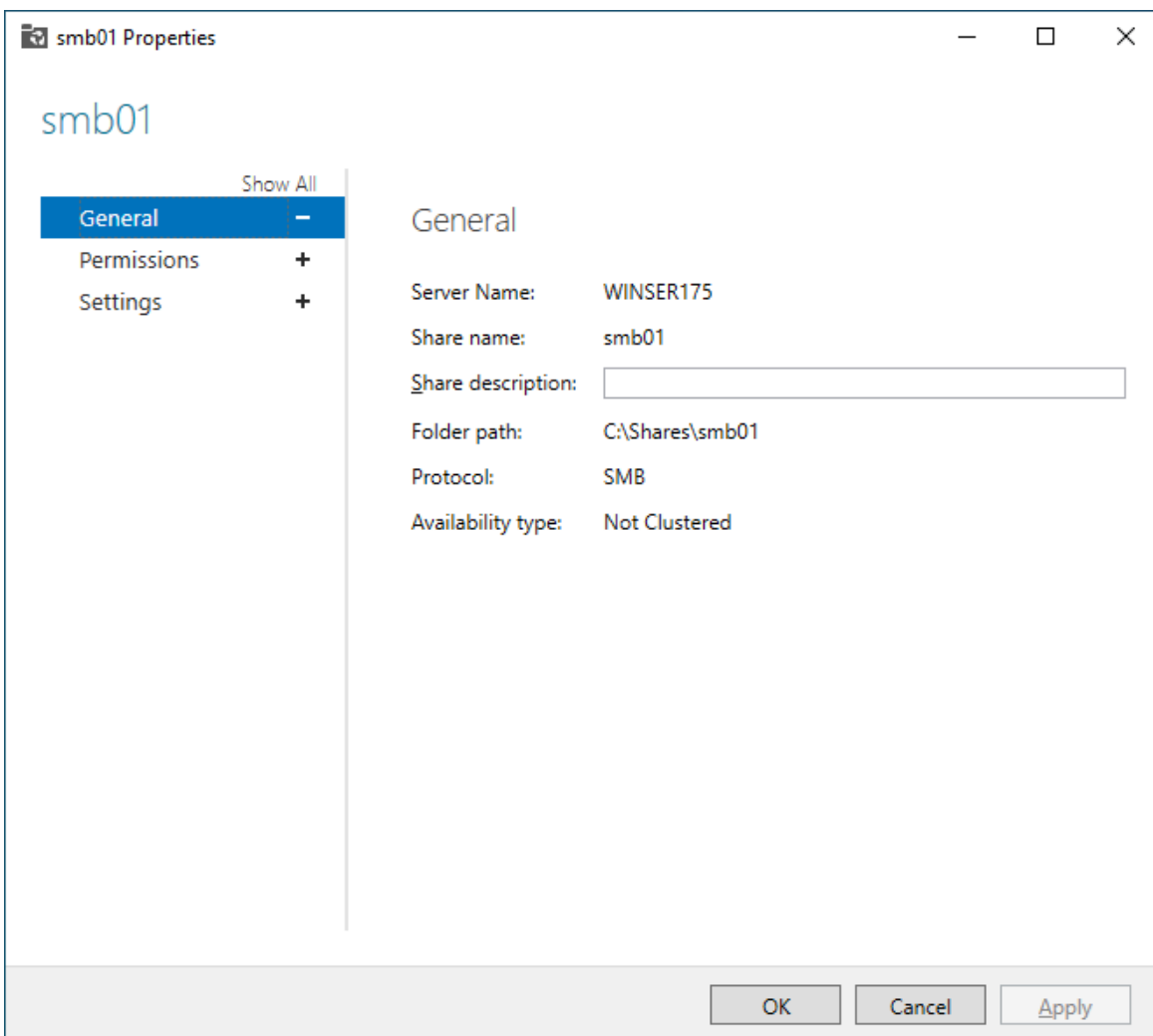
The "VOLUME" section shows "smb01 on WINSER175". It displays a progress bar for the C: drive with the following information:

- Capacity: 99.4 GB
- 18% Used
- 17.9 GB Used Space
- 81.5 GB Free Space

Below the volume information, there is a "QUOTA" section for "smb01 on WINSER175" with the following instructions:

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 2022 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. The left-hand navigation pane shows the hierarchy: Servers > File and Storage Services > Shares. The main area is divided into two panes. The left pane, titled 'SHARES', shows a table of shares for the server 'WINSER175 (2)'. The right pane, titled 'VOLUME', shows details for the volume 'smb01 on WINSER175', including its capacity and usage. Below the volume details is a 'QUOTA' section with instructions on how to install File Server Resource Manager.

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

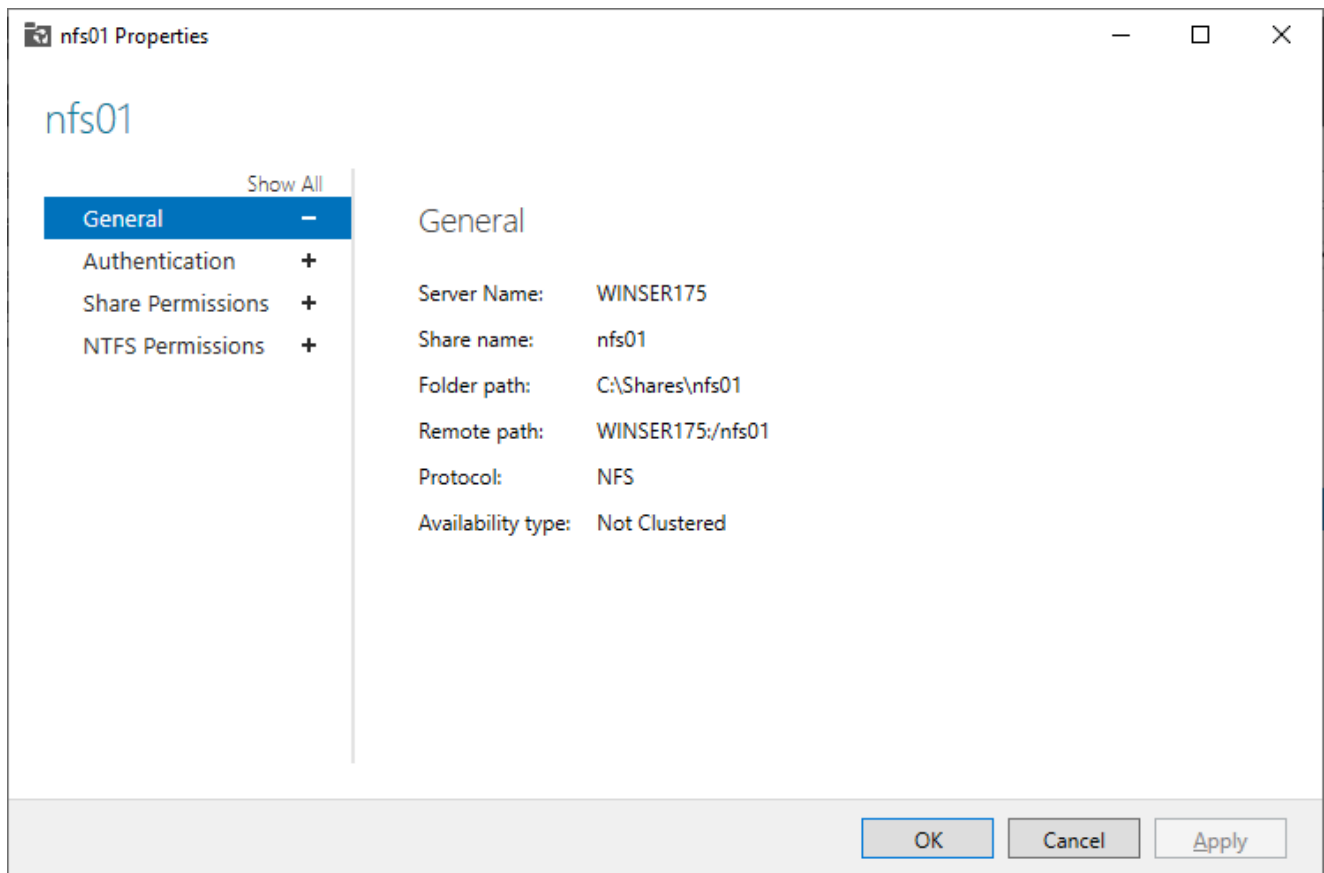
18% Used 17.9 GB Used Space
81.5 GB Free Space

[Go to Volumes Overview >](#)

QUOTA
smb01 on WINSER175

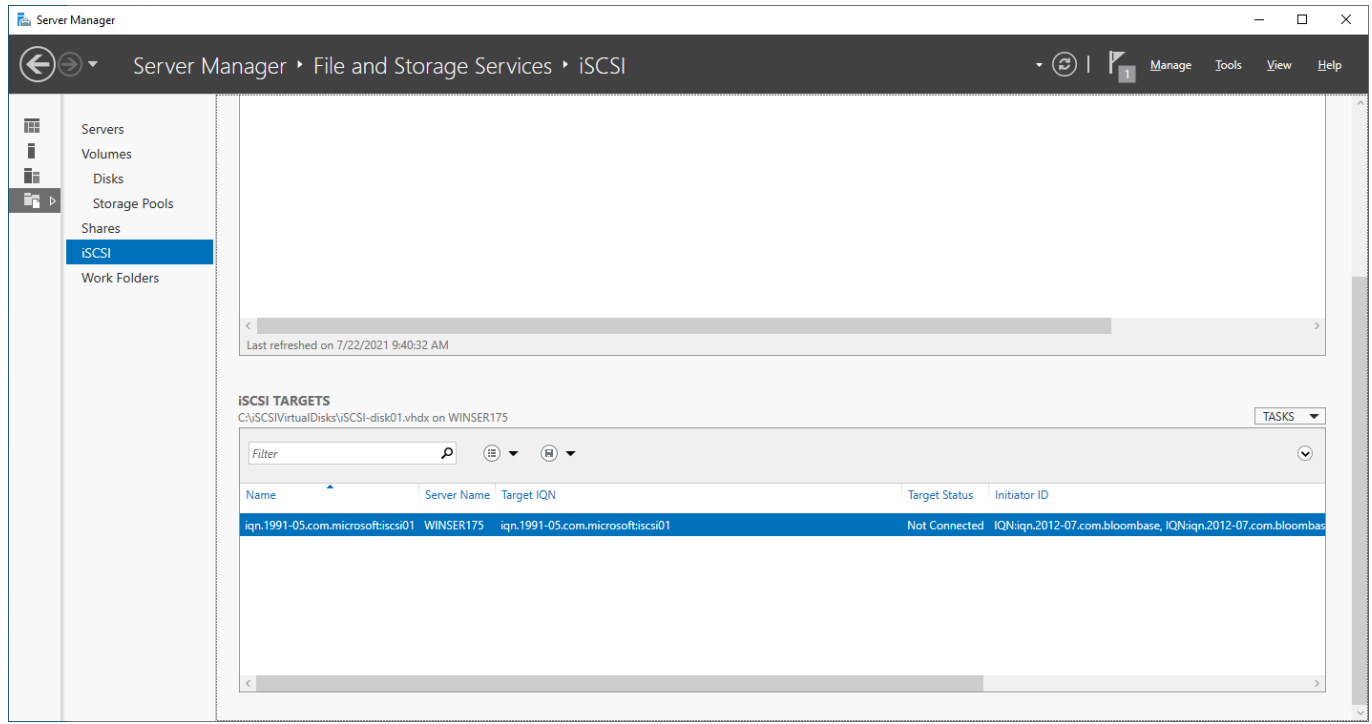
To use quotas, File Server Resource Manager must be installed.

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



NFS storage service is provisioned on Microsoft Windows Server 2022 to be used in this integration testing.

iSCSI Services Configuration



iSCSI storage service is also provisioned on Microsoft Windows Server 2022 to be used in this integration testing.

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 KeyControl.

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

Bloombase StoreSafe Security Server

Greeting
 Host Name: bloombase01
 User: admin
 Datetime: 2021-08-03 01:19:10 -0700

Menu Bar
 System
 Operation
 High Availability
 Administration
 Key Management
 StoreSafe Configurations
 Storage

Language
 English

Main

System Information

Product Name	Bloombase StoreSafe Security Server	Version	3.4.8.4-EA2
Host Name	bloombase01 / bloombase01	System Up Since	2021-07-29 00:54:08 -0700
Host Addresses	1 ens192 fe80:0:0:0:250:56ff:feaf:3b55, 192.168.23.87		
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	Total Memory	536,870,912
Memory Utilization	2%	Free Memory	421,181,440
Max Memory	4,294,967,296	Total Disk Space	14,371,782,656
Disk Space Utilization	18%	Free Disk Space	11,718,811,648
Used Disk Space	2,652,971,008		

Application Status

Application Status:

Last Shutdown Time
 Last Standby Time: 2021-07-29 00:54:14 -0700
 Last Startup Time: 2021-07-29 01:00:57 -0700

Entrust KeyControl and Bloombase StoreSafe Integration

Bloombase supports Entrust KeyControl out of the box due to the fact that both products support OASIS Key Management Interoperability Protocol (KMIP).

To enable the built-in Bloombase KeyCastle to utilize keys managed in the network attached Entrust KeyControl, the KMIP service configuration at Bloombase web management console has to be set up. This is done by clicking “OASIS KMIP Key Manager” under “Key Management”.

List KMIP Key Manager

Name	Model	Host Address	Port
Add			

Input a name for the Entrust KeyControl, and select Model as `Entrust KeyControl`. Input also the host address and port to access the Entrust KeyControl, and import the signed X.509 key pair as “Client Keystore”, the certificate of the local root CA on Entrust KeyControl as “Trust Certificate”.

Client Keystore

Subject Name	CN=storesafe O=Bloombase L=Redwood City ST=CA C=United States
Serial Number	00f9e7e683
Issuer Name	CN=HyTrust KeyControl Certificate Authority O=HyTrust Inc. C=US
Certificate	
Valid Start Date	2021-07-29
Valid End Date	2022-07-29


Client Key/ Certificate No file chosen

Pin

Trust Certificate

Subject Name	CN=HyTrust KeyControl Certificate Authority O=HyTrust Inc. C=US
Serial Number	60e7e67e
Issuer Name	CN=HyTrust KeyControl Certificate Authority O=HyTrust Inc. C=US
Valid Start Date	2011-05-31
Valid End Date	2049-12-31

Trust Certificate File No file chosen



X.509 key pair CN=storesafe is generated and signed by the root CA in the Entrust KeyControl, and assigned as the client authentication key pair for Bloombase StoreSafe.

Modify KMIP Key Manager

Modify KMIP Key Manager

Name:

Model:

Host Addresses:

Port:

Timeout: ms

Retry Count:

Retry Wait Time: ms

Username:

Password:

Test Results :
192.168.23.249 : Success Vendor ID : cryptsoft.com

Click 'Submit' to commit the configuration. If the certificates are setup properly, "test results" of the KMIP Key Manager would return "Success".

Encryption Key Provisioning

To generate key in attached Entrust KeyControl, select Key Source Type as

OASIS KMIP Key Manager

and the assigned Key Manager label, in this case

keycontrol


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" value="keycontrol-key01"/>
Key Source	OASIS KMIP Key Manager
Type	Symmetric
Active	<input checked="" type="checkbox"/>
KMIP Key Manager	keycontrol
KMIP UUID	
KMIP Key Name	
KMIP Key State	
Key Bit Length	<input type="text" value="256"/>
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	<input type="text" value="OASIS KMIP Key Manager"/>
Key Manager	<input type="text" value="keycontrol"/>
Object	<input type="text" value="keycontrol-key01 [29b3e7ae-4e58-4d32-be6d-c2084affb78e]"/>



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

Find Key Wrapper

Find Key Wrapper

Name Type **Symmetric** Active **Active** CA

▼ More Options

Find **Reset** **Add**

1-1 of 1

Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1 keycontrol-key01	Symmetric	OASIS KMIP Key Manager	<input checked="" type="checkbox"/>			UUID=29b3e7ae-4e58-4d32-be6d-c2084affb78e	KMIP=keycontrol			2021-07-12 05:16:33 -0700

1-1 of 1

The new key can be found on the KeyControl management console.

KMIP Attrs Custom Attrs Identifiers

UUID:	29b3e7ae-4e58-4d32-be6d-c2084affb78e
Description:	Not Set
CryptographicUsageMask:	UnwrapKey WrapKey
ActivationDate:	07/12/2021 8:06:02 PM
KeyFormatType:	Raw
CryptographicAlgorithm:	AES
CryptographicLength:	256

Data-at-Rest Encryption for SMB

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 ▾
Type	Common Internet File System (CIFS) ▾
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 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

keycontrol-key01

managed at Entrust KeyControl.

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"/>	keycontrol-key01	2021-07-22 04:33:45 -0700

Header

Protected

Cryptographic Cipher

Cipher Algorithm

Bit Length

CTR Mode



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.

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

Data-at-Rest Encryption for NFS

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

keycontrol-key01

managed at Entrust KeyControl.

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"/>	keycontrol-key01	2021-07-22 04:33:45 -0700

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

192.168.12.242

Modify Virtual Storage Access Control

Virtual Storage | Protection | Access Control | Permissions

User Access Control

Everybody Read Write

NFS File System Object Attributes

Native File Permission
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="checkbox"/>	192.168.12.242	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	sys ▼	<input type="text"/>	2021-07-23 12:17:54 -0700

Subnet Access Control

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

▼ More Options



Data-at-Rest Encryption for iSCSI

Physical storage namely

iscsi01

is configured to be secured by Bloombase StoreSafe using encryption.

Modify Storage Configuration

Physical Storage | Permissions

Physical Storage Configuration

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

Submit Delete Close

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

keycontrol-key01

managed at Entrust KeyControl.

Modify Virtual Storage Handler

Virtual Storage Protection Access Control iSCSI Permissions

Virtual Storage Protection

Protection Type

Encryption Keys

	Key Name	Last Update Datetime
1 <input type="checkbox"/>	keycontrol-key01	2021-07-23 11:54:59 -0700

Cryptographic Cipher

Cipher Algorithm

Bit Length



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
<input type="text"/>

Incoming Users

User	Warning	Last Update Datetime
<input type="text"/>	<input type="text"/>	<input type="text"/>

Initiators

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

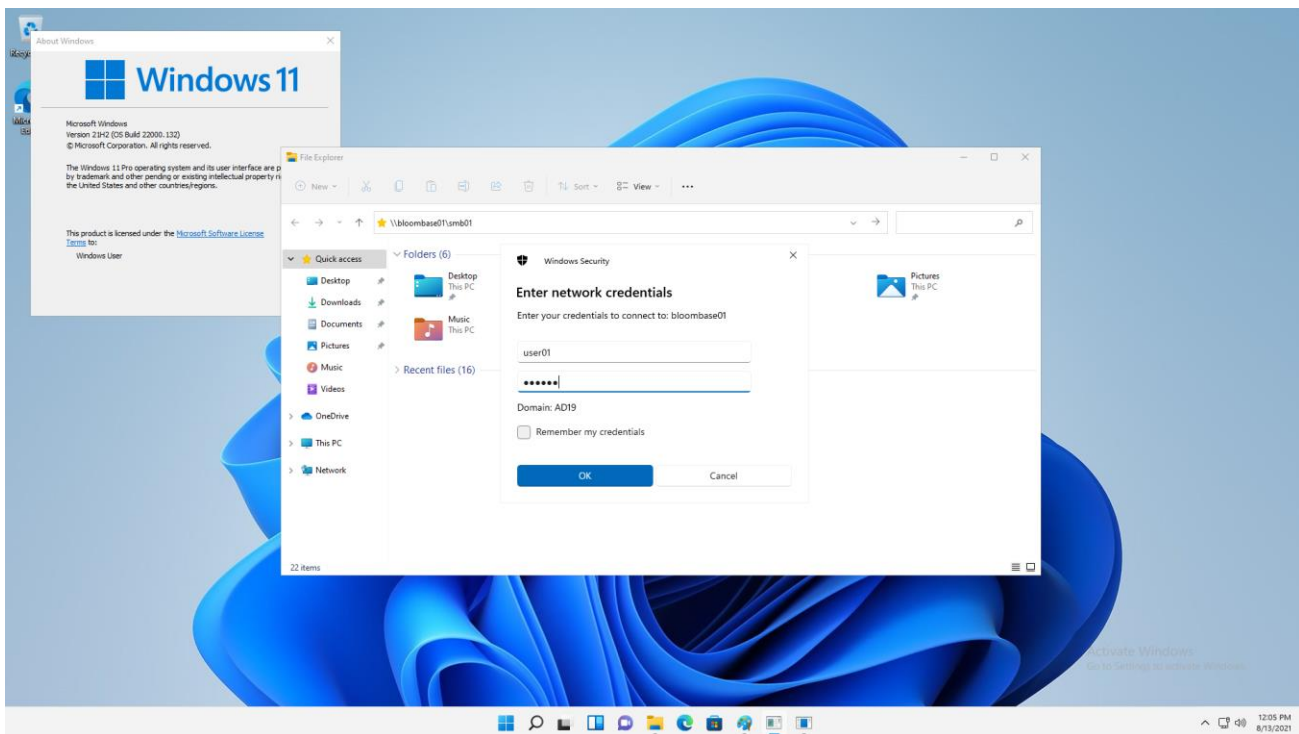
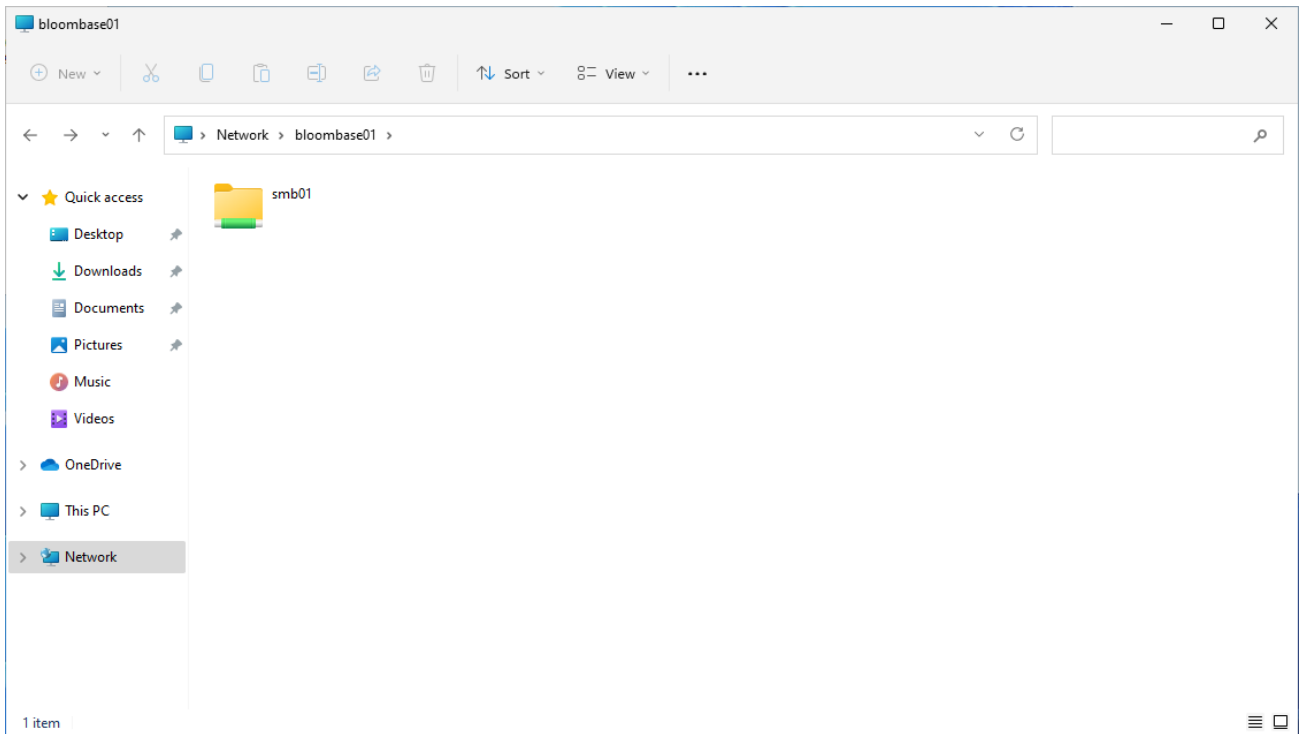
▼ List Initiators

-
-
-
-

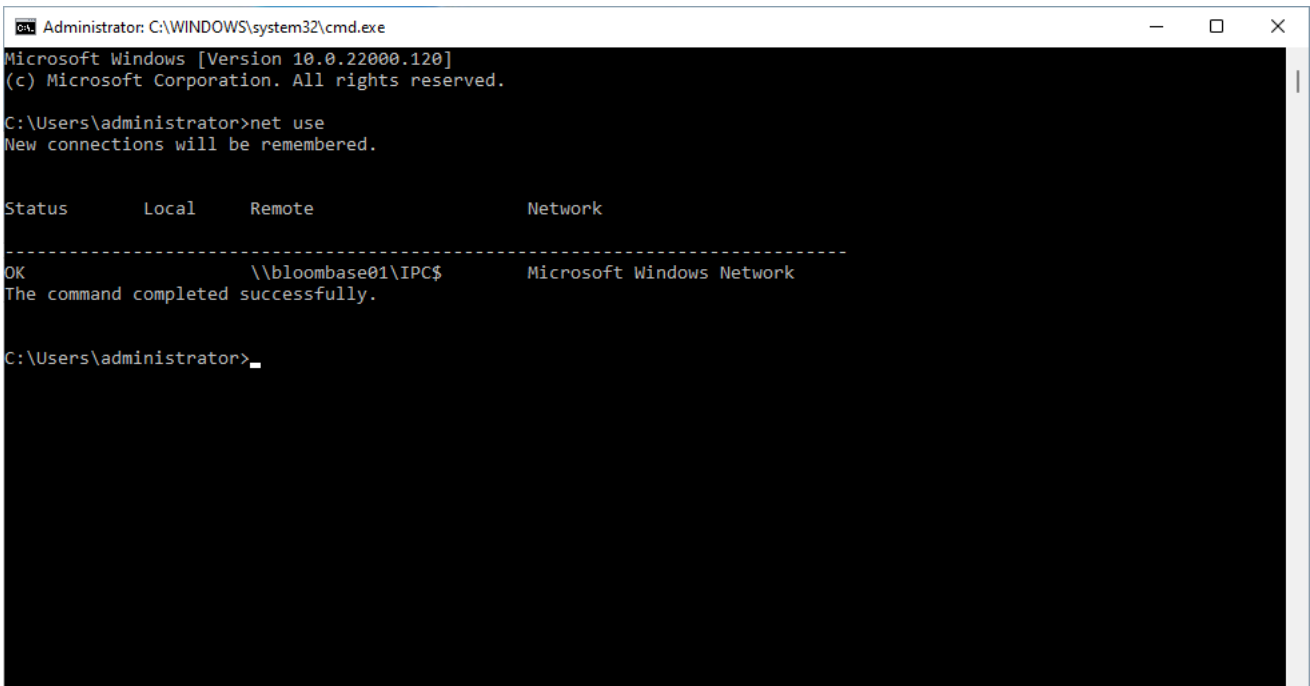
Use Cases

Data-at-Rest Encryption for SMB

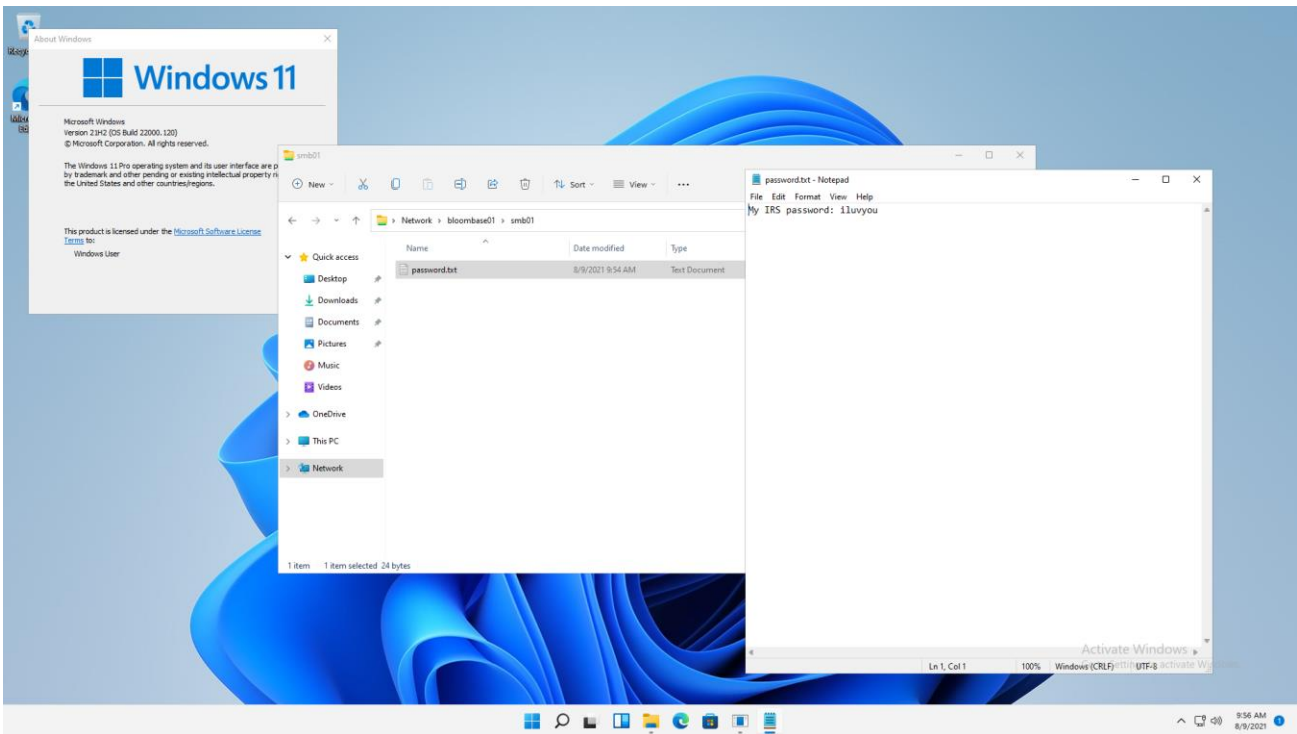
SMB shares are an example from the many protocols Bloomberg StoreSafe supports for encryption. A share from a Windows Server 2022 system that is accessible by domain users is created to act as backend storage. Bloomberg StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.



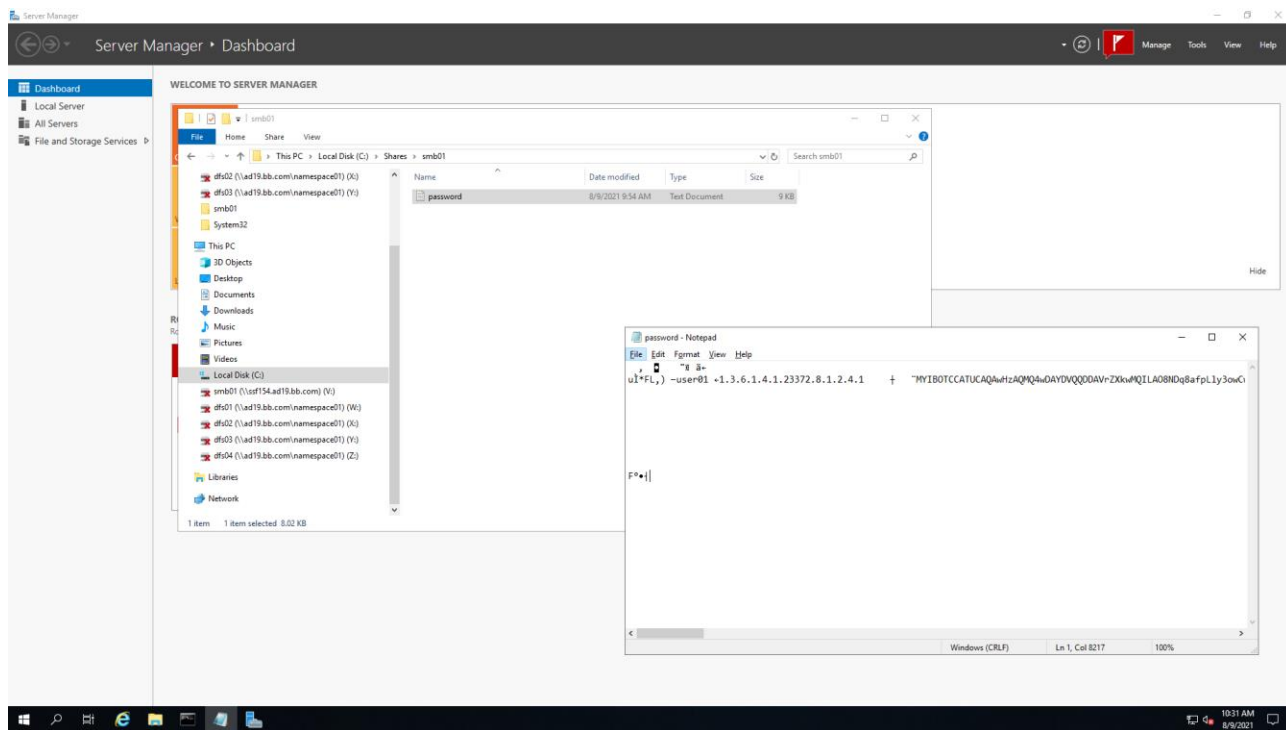
Windows 11 clients can use the included network share on file manager to access the SMB share. Data owners can alternatively use the Net Use command to specify additional mounting options.



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 2022 backend share.

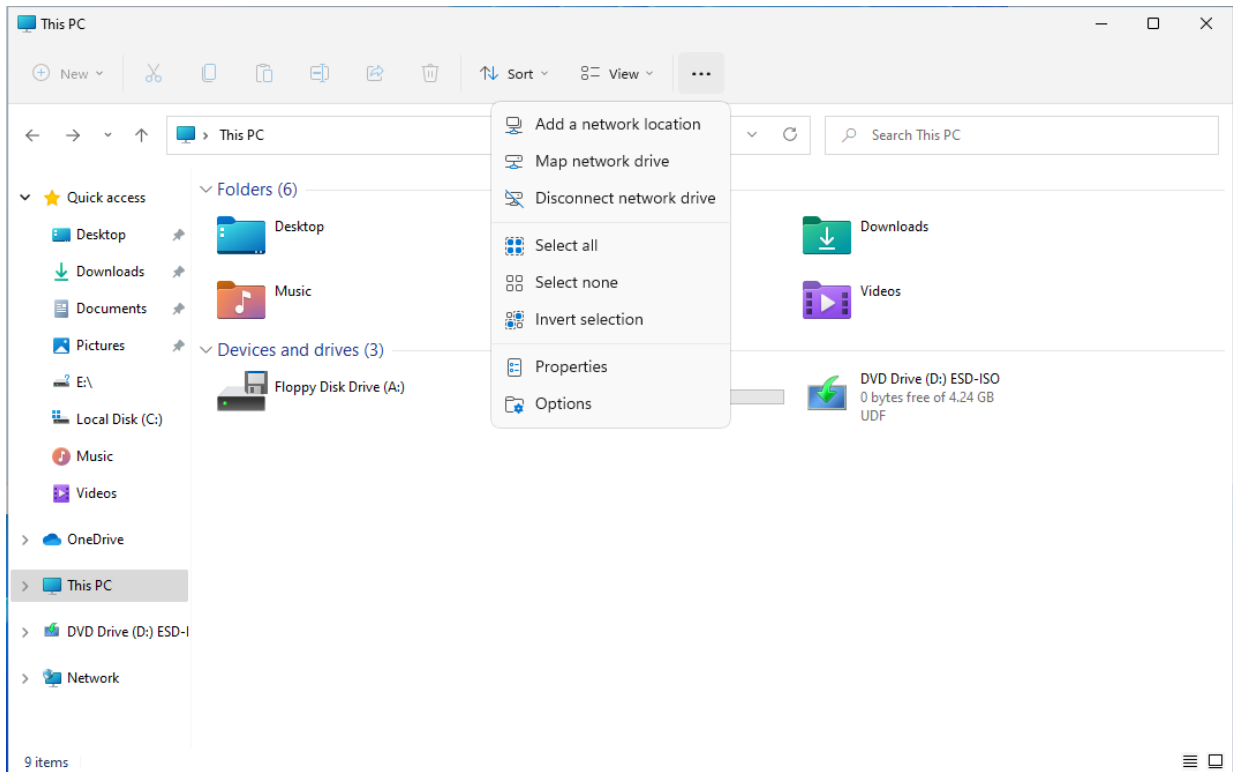


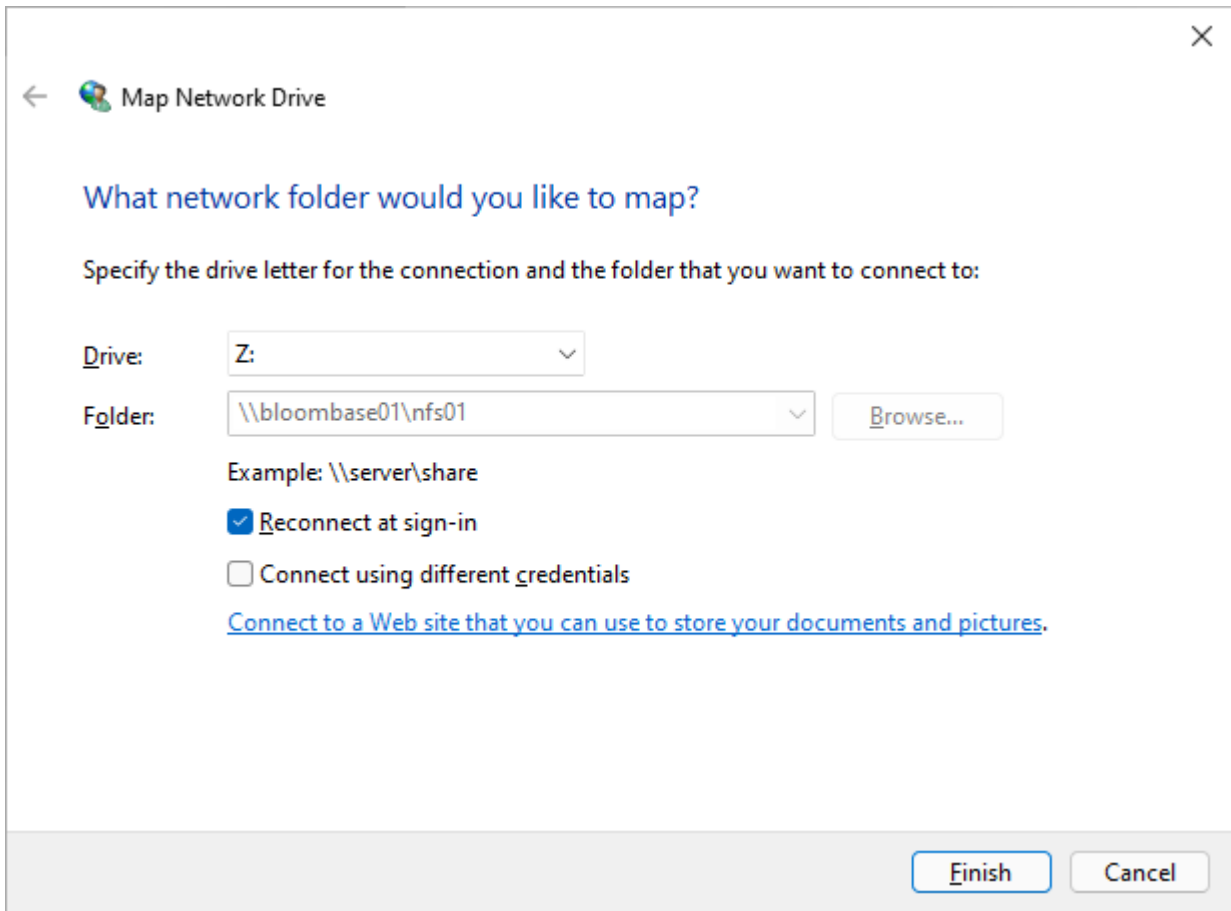
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



Data-at-Rest Encryption for NFS

NFS shares are an example from the many protocols Bloombase StoreSafe supports for encryption. A share from a Windows Server 2022 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.





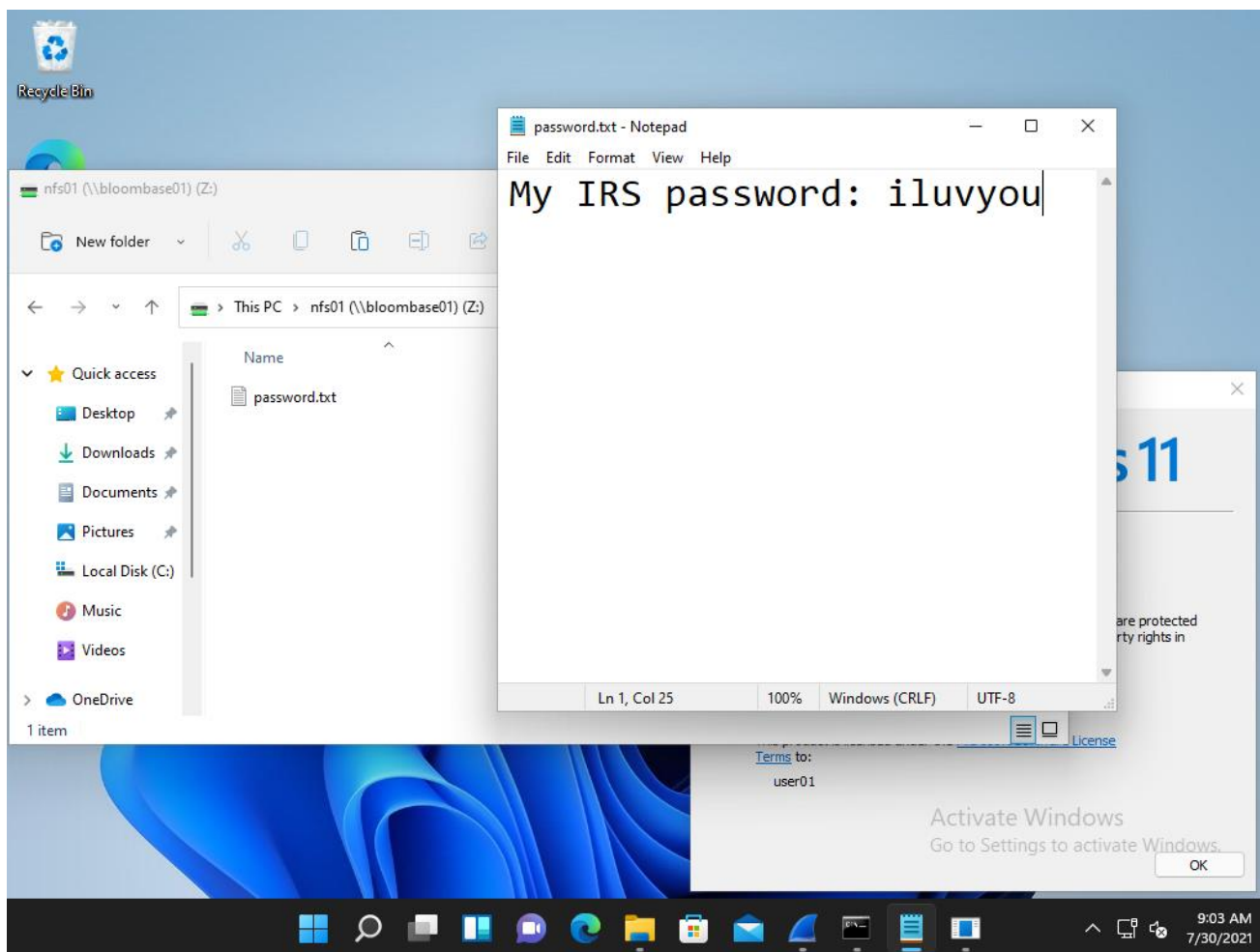
Windows 11 clients can use the included map network drive option to add the NFS share with a drive letter. Data owners can alternatively use the mount command to specify additional mounting options.

```
Command Prompt
C:\Users\user01>mount

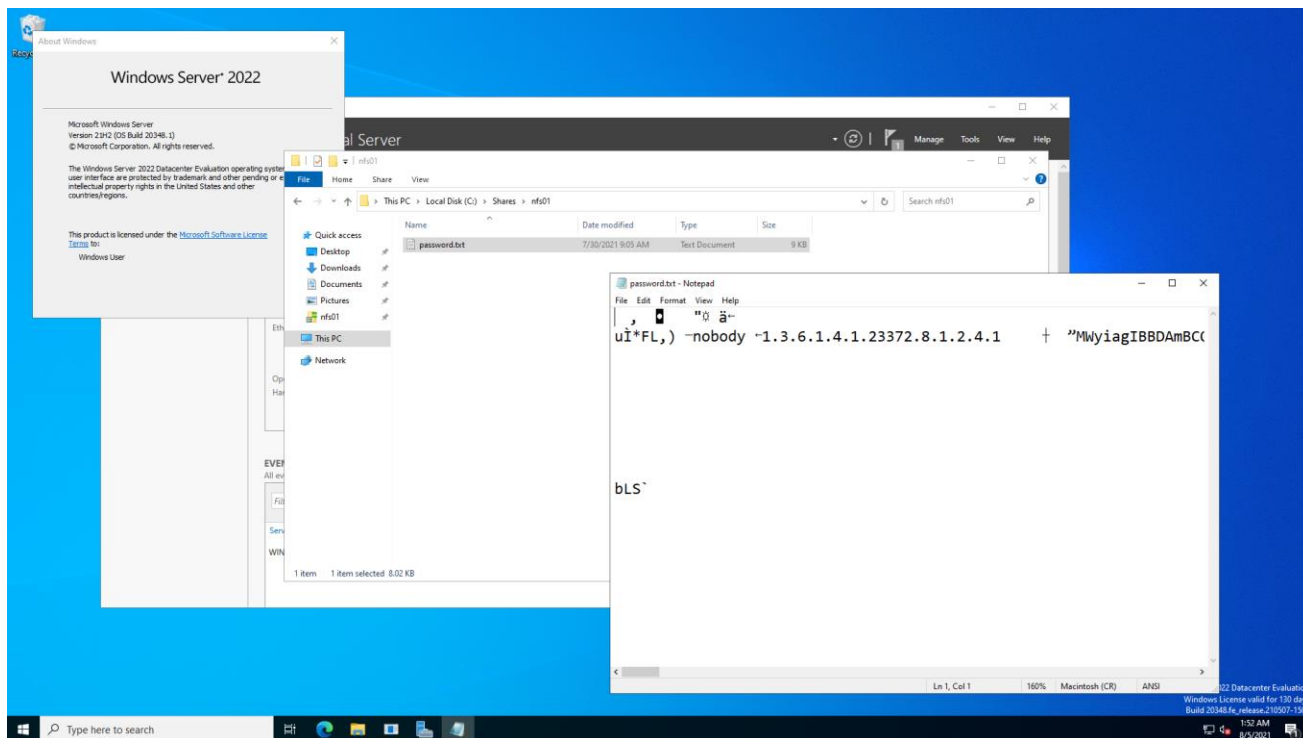
Local      Remote                                     Properties
-----
Z:         \\bloombase01\nfs01                       UID=0, GID=0
                                                rsize=32768, wsize=32768
                                                mount=soft, timeout=0.8
                  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

C:\Users\user01>
```

On the 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 Windows Server 2022 backend share.

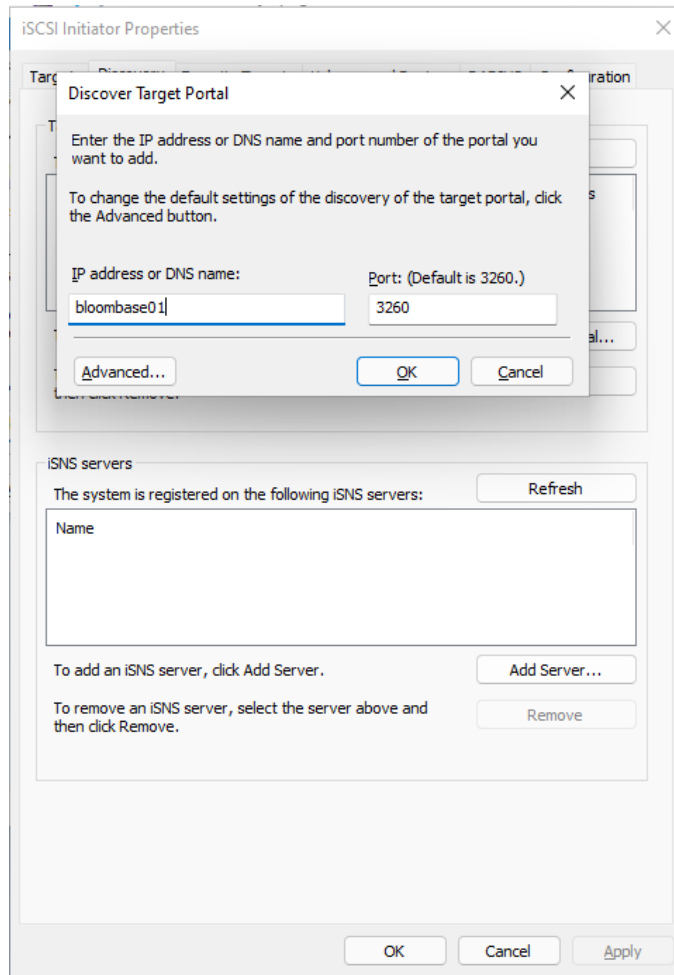


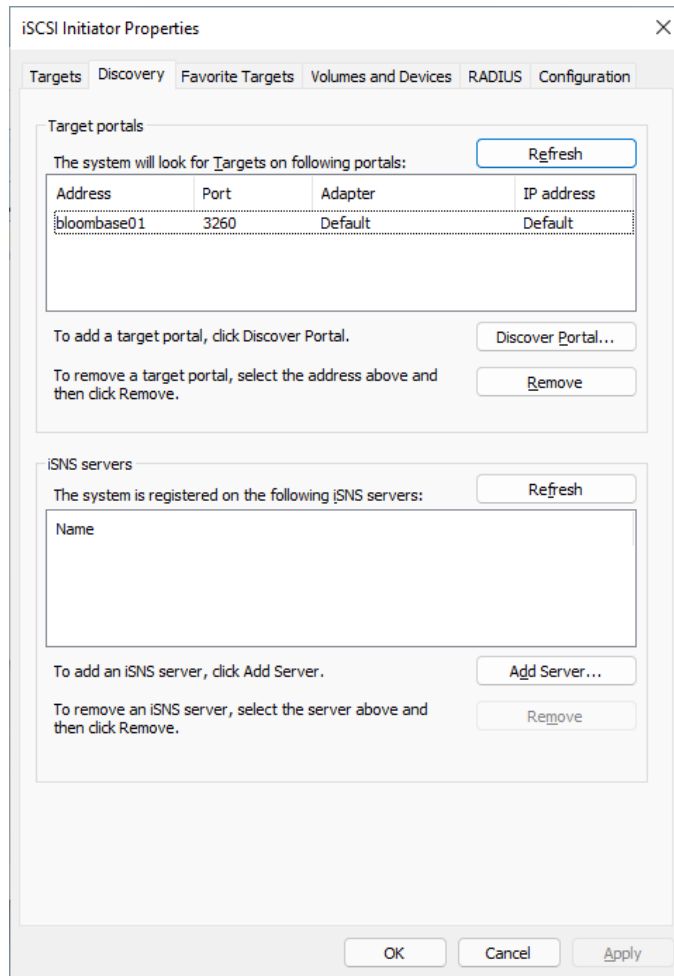
If the application data is attempted to be accessed directly on the backend without going through the Bloombase StoreSafe encryption engine, only ciphertext can be read as expected.



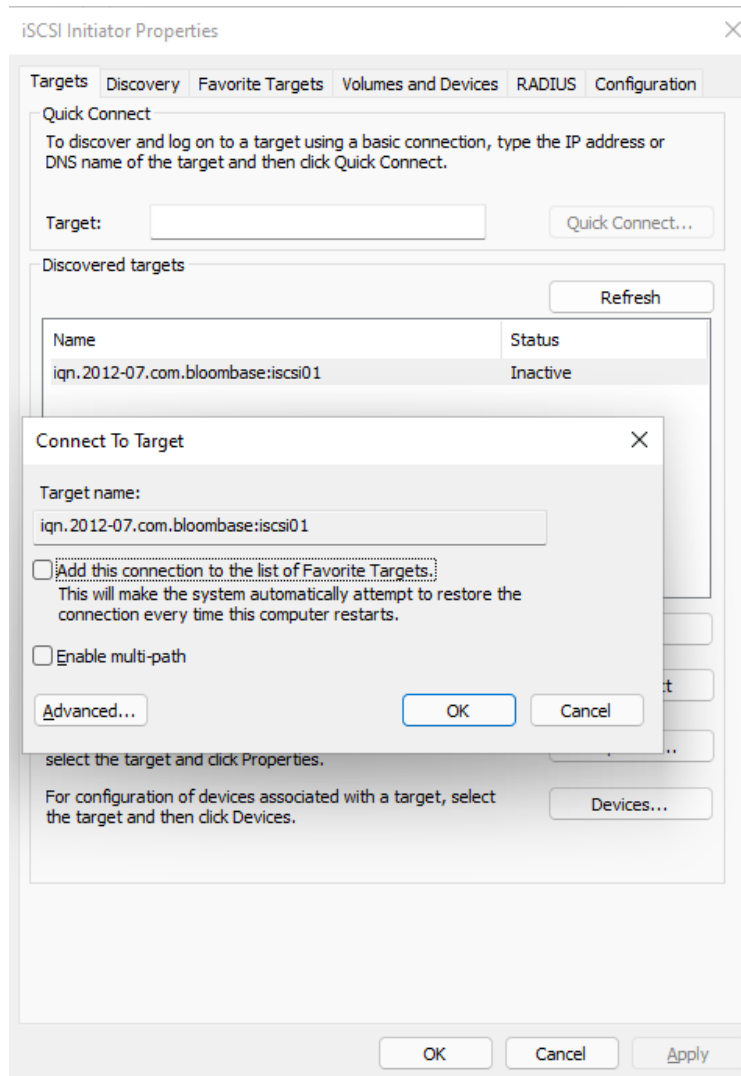
Data-at-Rest Encryption for iSCSI

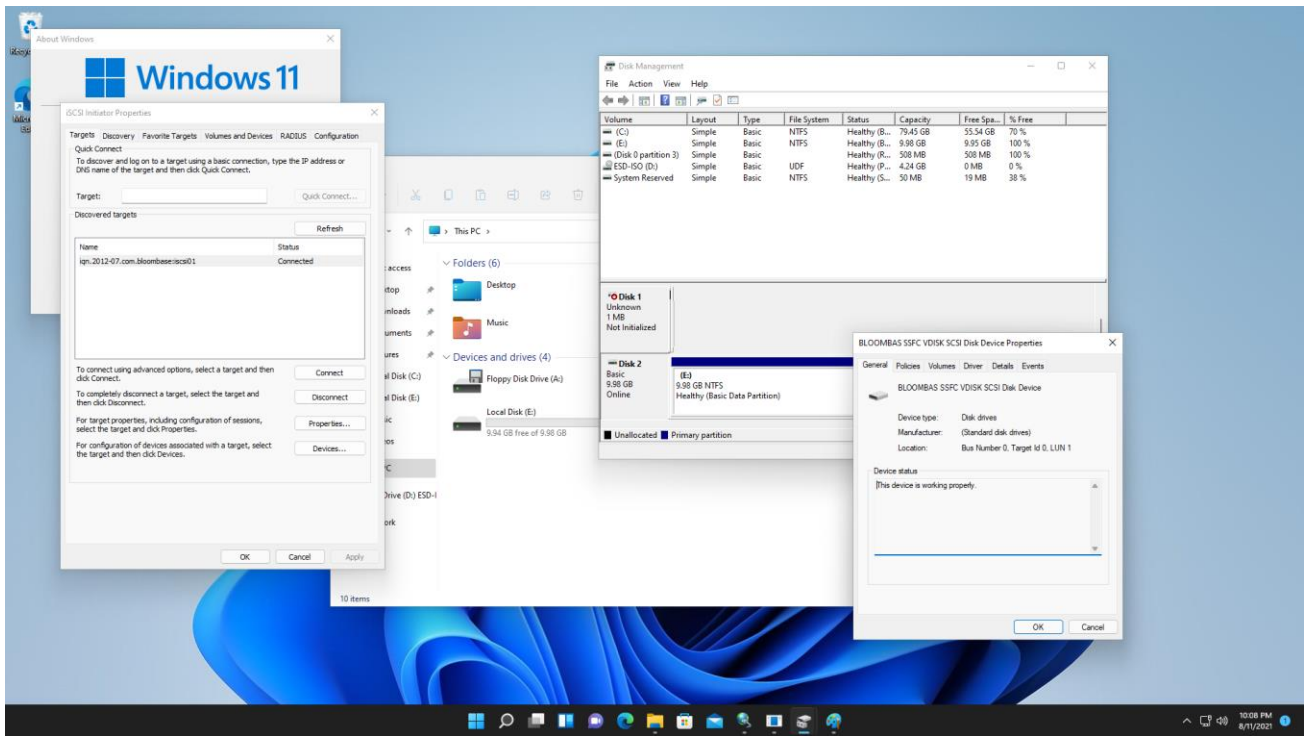
iSCSI targets are an example from the many protocols Bloombase StoreSafe supports for encryption. A target from a Windows Server 2022 system that is accessible by configure clients is created to act as backend storage. Bloombase StoreSafe creates a virtual encrypted share on its own hostname path that is accessed from a client software system.



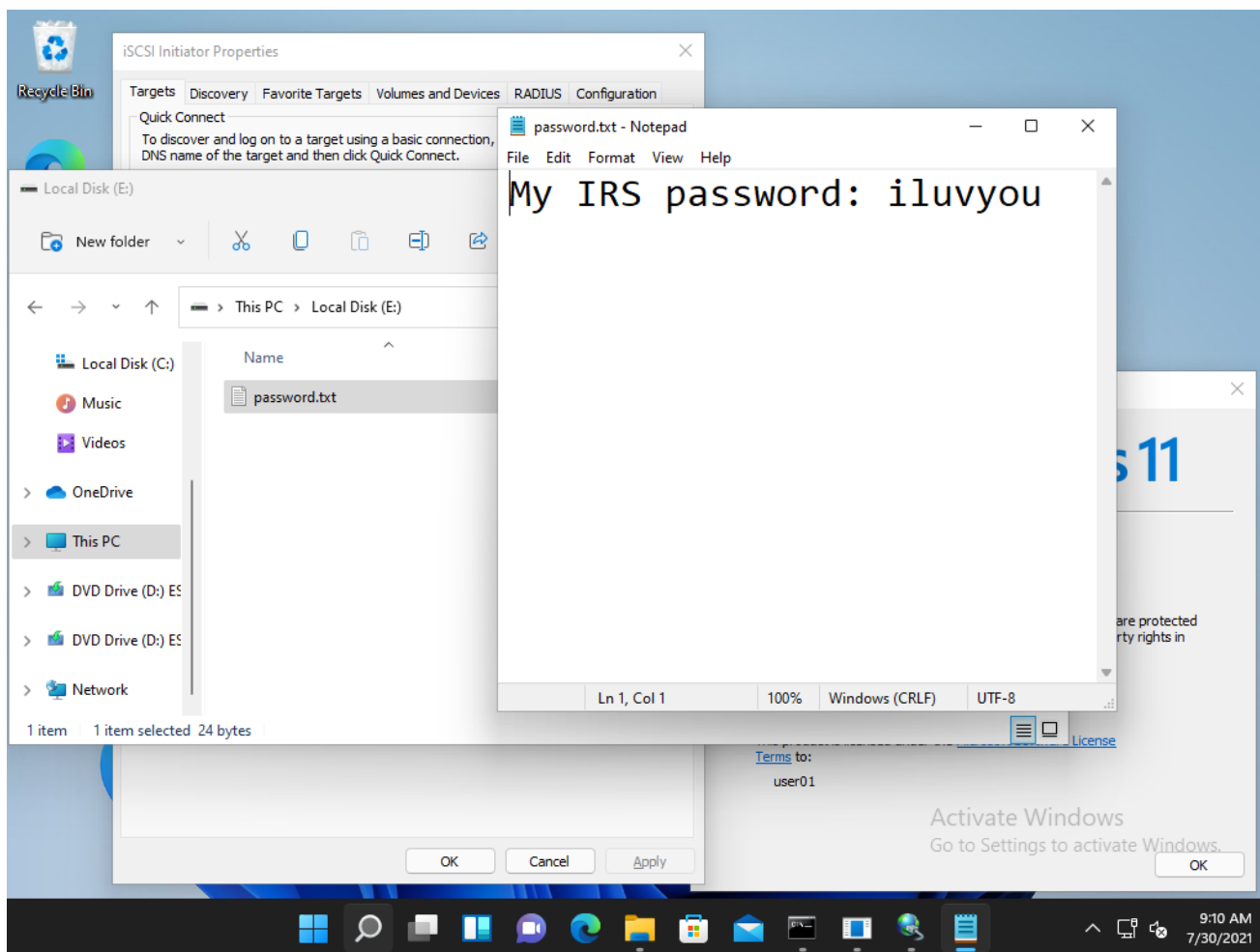


Windows 11 clients can attach the virtual encrypted share with the default iSCSI initiator tool. Add the hostname and port to the discover tab, then connect to the Bloombase StoreSafe target. To access the iSCSI disk, make sure the client IQN is added to the Bloombase StoreSafe configuration. The disk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





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 Windows Server 2022 backend target.



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 | 0 |
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 W< |
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 | 0 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>_

```

Conclusion

In this integration guide, we have shown how to set up Bloombase StoreSafe Intelligent Storage Firewall with Entrust KeyControl to deliver on-the-fly encryption of multiple storage protocols including SMB, NFS and iSCSI. 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 KeyControl

has been integrated with Bloombase StoreSafe Intelligent Storage Firewall to deliver encryption security of Microsoft Storage Server on Microsoft Windows Server 2022 over SMB/CIFS, NFS and iSCSI network storage protocols for software applications running on Microsoft Windows Server 2022 and Windows 11.

Bloombase Product	Application Components	Key Manager
Bloombase StoreSafe Intelligent Storage Firewall	<ul style="list-style-type: none"> ● Microsoft Storage Server ● Microsoft Windows Server 2022 ● Microsoft Windows 11 	<ul style="list-style-type: none"> ● Entrust KeyControl 5.4 (b540001603)

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 KeyControl.

Reference

1. Bloomberg StoreSafe Technical Specifications, <https://www.bloomberg.com/content/8936QA88>
2. Bloomberg StoreSafe Hardware Compatibility Matrix, <https://www.bloomberg.com/content/e8Gzz281>
3. Entrust KeyControl, <https://www.entrust.com/digital-security/key-management/keycontrol>
4. Entrust nShield family of general purpose HSMs, <https://www.entrust.com/digital-security/hsm/products/nshield-hsms>
5. Entrust nShield-as-a-Service (nSaaS), <https://www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-as-a-service>
6. OASIS KMIP, http://oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
7. Bloomberg is an Entrust nFinity Technology Partner, <https://www.entrust.com/partner-directory/bloomberg>