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.
Table of Contents
Table of Contents

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:
Microsoft Windows 11

\bloombase\smb01
\bloombase\nfs01
iqn.2012-07.com.bloombase:iscsi01

NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF,
WebDav, HTTP, REST, S3, etc

Bloombase StoreSafe

NFS, SMB, CIFS, iSCSI, FCP, NVMe-oF,
WebDav, HTTP, REST, S3, etc

\storage01\smb01
storage01:nfs01
iqn.1991-05.com.microsoft:iscsi01

^$8Yn
+=@~

Microsoft Storage Server on
Microsoft Windows Server 2022

KMIP

Read and Unencrypt

Write and Encrypt

Entrust KeyControl
## Key Management

| Key Manager | Entrust KeyControl 5.4 (b540001603) |

## Storage Encryption

<table>
<thead>
<tr>
<th>Storage Encryption</th>
<th>Bloombase StoreSafe Intelligent Storage Firewall Software Appliance v3.4.8.4-EA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>VMware Virtual Machine (VM) on VMware ESXi 6.0</td>
</tr>
<tr>
<td>Processor</td>
<td>4 x Virtual CPU (vCPU)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

## 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.
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 KMIP 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 KMIP > Client Certificates > Actions > Create Certificate > Upload CSR.
You may upload a CSR created by Bloombase StoreSafe, or create your own.
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

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
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).
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”. 
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](image)

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.

![Trust Certificate](image)
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.
Or if key already exists, simply choose from the dropdown box.
Ensure you import a key from the key manager before you submit the key wrapper.

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

<table>
<thead>
<tr>
<th>KMIP Attri</th>
<th>Custom Attri</th>
<th>Identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUID:</td>
<td>29b3e7ae-4e58-4d32-be5d-c20b4affb78e</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td>Not Set</td>
<td></td>
</tr>
<tr>
<td>CryptographicUsageMask:</td>
<td>UnwrapKey WrapKey</td>
<td></td>
</tr>
<tr>
<td>ActivationDate:</td>
<td>07/12/2021 8:06:02 PM</td>
<td></td>
</tr>
<tr>
<td>KeyFormatType:</td>
<td>Raw</td>
<td></td>
</tr>
<tr>
<td>CryptographicAlgorithm:</td>
<td>AES</td>
<td></td>
</tr>
<tr>
<td>Cryptographics.length:</td>
<td>256</td>
<td></td>
</tr>
</tbody>
</table>

**Data-at-Rest Encryption for SMB**

Physical storage namely

smb:01

is configured to be secured by Bloombase StoreSafe using encryption.
Virtual storage namely

<table>
<thead>
<tr>
<th>Physical Storage Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Physical Storage Type</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>Share Name</td>
</tr>
<tr>
<td>Read Size</td>
</tr>
<tr>
<td>Write Size</td>
</tr>
<tr>
<td>Mount Herd</td>
</tr>
<tr>
<td>User</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>Virtual Storage</td>
</tr>
<tr>
<td>Owner</td>
</tr>
<tr>
<td>Last Update Datetime</td>
</tr>
</tbody>
</table>

of type

File

is created to virtualize physical storage

smb01

for application transparent encryption protection over network file protocols including CIFS.
Protection type is specified as

Privacy

and secure the Microsoft Storage Server storage backend using

AES 256-bit

enetration and encryption key

keycontrol-key01

managed at Entrust KeyControl.
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.
Data-at-Rest Encryption for NFS

Physical storage namely

nfs01

is configured to be secured by Bloombase StoreSafe using encryption.
Virtual storage namely

nfs01

of type

File

is created to virtualize physical storage

nfs01

for application transparent encryption protection over network file protocols including NFS.
Protection type is specified as Privacy and secure the Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key keycontrol-key01 managed at Entrust KeyControl.
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`
Data-at-Rest Encryption for iSCSI

Physical storage namely

iscsi01
is configured to be secured by Bloombase StoreSafe using encryption.

<table>
<thead>
<tr>
<th>Physical Storage Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Physical Storage Type</strong></td>
</tr>
<tr>
<td><strong>Block I/O</strong></td>
</tr>
<tr>
<td><strong>Multipath</strong></td>
</tr>
<tr>
<td><strong>Device ID [max 8 chars]</strong></td>
</tr>
<tr>
<td><strong>Options</strong></td>
</tr>
<tr>
<td><strong>Device</strong></td>
</tr>
<tr>
<td><strong>Virtual Storage</strong></td>
</tr>
<tr>
<td><strong>Owner</strong></td>
</tr>
<tr>
<td><strong>Last Update Datetime</strong></td>
</tr>
</tbody>
</table>

Virtual storage namely

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

of type

```
isCSI
```

is created to virtualize physical storage

```
iscsi01
```

for application transparent encryption protection over network file protocols including iSCSI.
Protection type is specified as **Privacy** and secure the Microsoft Storage Server storage backend using **AES XTS 256-bit** encryption and encryption key **keycontrol-key01** managed at Entrust KeyControl.
iSCSI storage protocol relies mainly on CHAP, IQN, and networking for access control. In this test, the Bloombase StoreSafe secure storage resource

ign.2012-07.com.bloombase:iscsi01

is provisioned for initiator

**Modify Virtual Storage Access Control**

<table>
<thead>
<tr>
<th>Virtual Storage</th>
<th>Protection</th>
<th>Access Control</th>
<th>iSCSI</th>
<th>Permissions</th>
</tr>
</thead>
</table>

**Allowed Portal**

<table>
<thead>
<tr>
<th>Portal IP</th>
<th>Add</th>
<th>Remove</th>
</tr>
</thead>
</table>

**Incoming Users**

<table>
<thead>
<tr>
<th>User</th>
<th>Warning</th>
<th>Last Update Datetime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Initiators**

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Alias</th>
<th>Warning</th>
<th>Last Update Datetime</th>
</tr>
</thead>
</table>

**List initiators**

[Refresh] [Alias] [Submit] [Close]
Use Cases

Data-at-Rest Encryption for SMB

SMB 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 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.
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.
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 be added 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.
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.

<table>
<thead>
<tr>
<th>Bloombase Product</th>
<th>Application Components</th>
<th>Key Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bloombase StoreSafe Intelligent Storage Firewall</td>
<td>• Microsoft Storage Server</td>
<td>• Entrust KeyControl 5.4 (b540001603)</td>
</tr>
</tbody>
</table>
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

2. Bloombase StoreSafe Hardware Compatibility Matrix, https://www.bloombase.com/content/e8Gzz281
7. Bloombase is an Entrust nFinity Technology Partner, https://www.entrust.com/partner-directory/bloombase