High Level Use Case Document

Current Version	**1.0**
Approved By	**Jianwen Yin**
Approval Date	**06/14/2013**

Dell FS7610 (EqualLogic) and FS8600 (Compellent) Platform – Use Cases & Certification: Bloombase (UCC)

Table of Contents

1 Document Revision History

Revision	Date	Revised By	Comments
0.1	05/11/2013	Dell	Initial Draft For Discussion
0.2	05/13/2013	Bloombase	Template details for Bloombase applications
0.3	05/15/2013	Bloombase	Case details
0.4	05/15/2013	Dell	Comments and updates
0.5	06/14/2013	Bloombase	Graphics updates
1.0	06/14/2013	Dell	Final Editing and Approval

2 Introduction

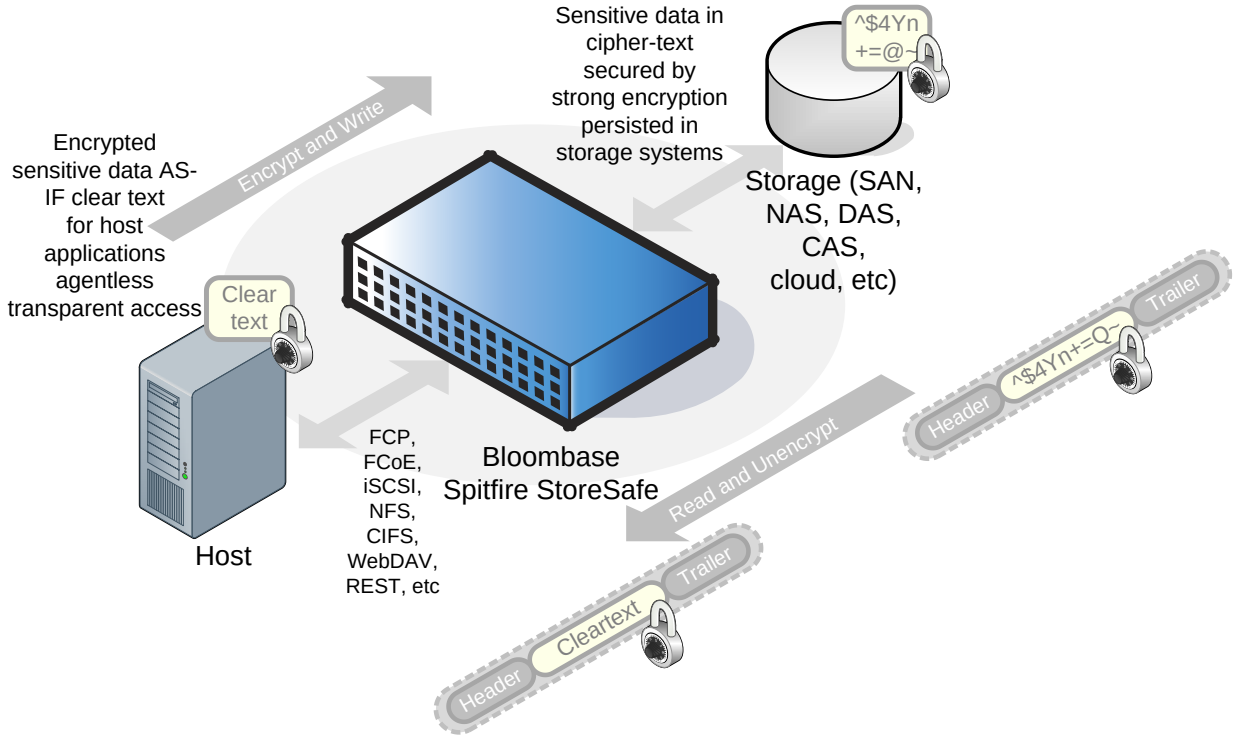
This document outlines the use case scenarios of implementing Bloombase Non-Disruptive Transparent Storage Encryption solution on Dell PowerEdge server and Dell Fluid File System Storage Devices including FS7610 (EqualLogic) and FS8600 (Compellent) system.

Traditional IT security measures regard outsiders as origins of cyber-attacks. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), content filters, anti-virus, anti-malware, anti-spyware, SSL-VPN, Unified Threat Management (UTM), etc all sits at the frontline defending core IT infrastructure at the perimeter only.

As unknown attacks, insider threats and targeted attacks are on the rise, sensitive and invaluable business data residing on core enterprise storage sub-systems in plain leaves business automation in huge vulnerabilities. Encryption of at-rest data is generally perceived as the last line of defense as inked in numerous industry best practices. Nevertheless, enterprises adopting application-specific encryption usually have to pay tremendous efforts on implementation and push the mission-critical applications in performance degradation and risks. The demand for application transparent data at-rest encryption solution and the drive for various information regulatory compliance which has to be high performance, easy to deploy, effortless integration, extensive infrastructure support, sustainable, scalable and fast to deployment as a turnkey solution drives the creation of Bloombase.

Bloombase is the Next Generation Data Security company. Bloombase's mission is to transform all critical business data from plain-text to encrypted cipher-text.

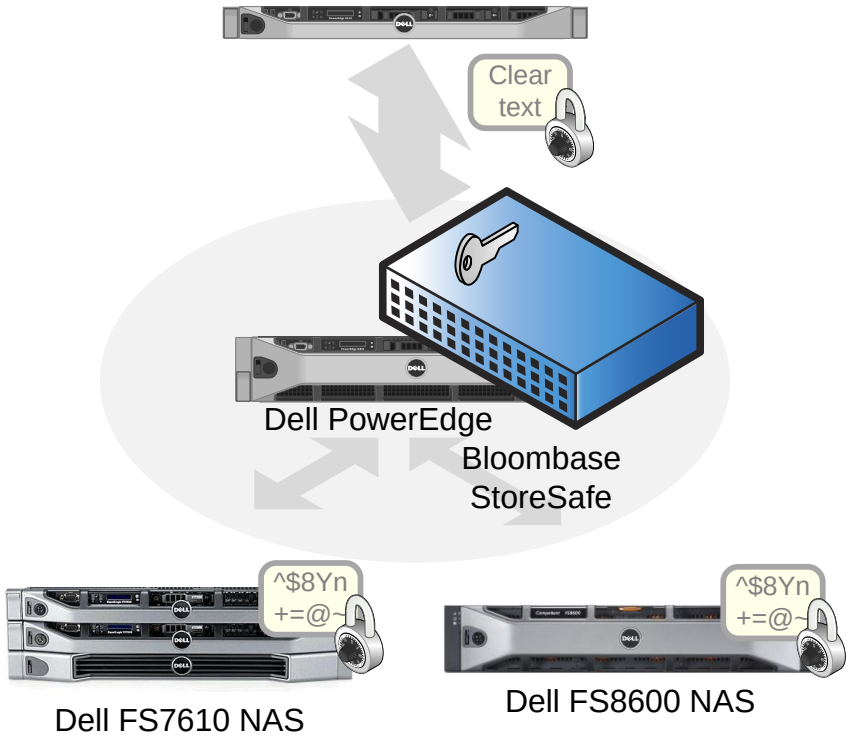
Essentially Bloombase StoreSafe agentless unified storage encryption security solution acts as a storage proxy providing transparent encryption and un-encryption of contents stored in enterprise Network Attached Storage (NAS), Storage Area Network (SAN) and RESTful object stores for authorized hosts and applications.



Unlike traditional data at-rest encryption offerings in the market, such as proprietary hardware appliances, Bloombase takes a transformative approach to provide real-time encryption of enterprise storage systems by a software-only implementation. Bloombase StoreSafe is ready to deploy on any x86-architecture hardware server appliance. Extending to the virtual data center space, Bloombase StoreSafe offers the capability to run as virtual appliance on any QEMU-compliant virtual hypervisor securing virtual machine data and virtual storage systems.

Dell offers a complete hardware solution from server computing, network connectivity, storage connectivity, object, file, and block storage infrastructure powering mission critical applications for enterprises of all sizes.

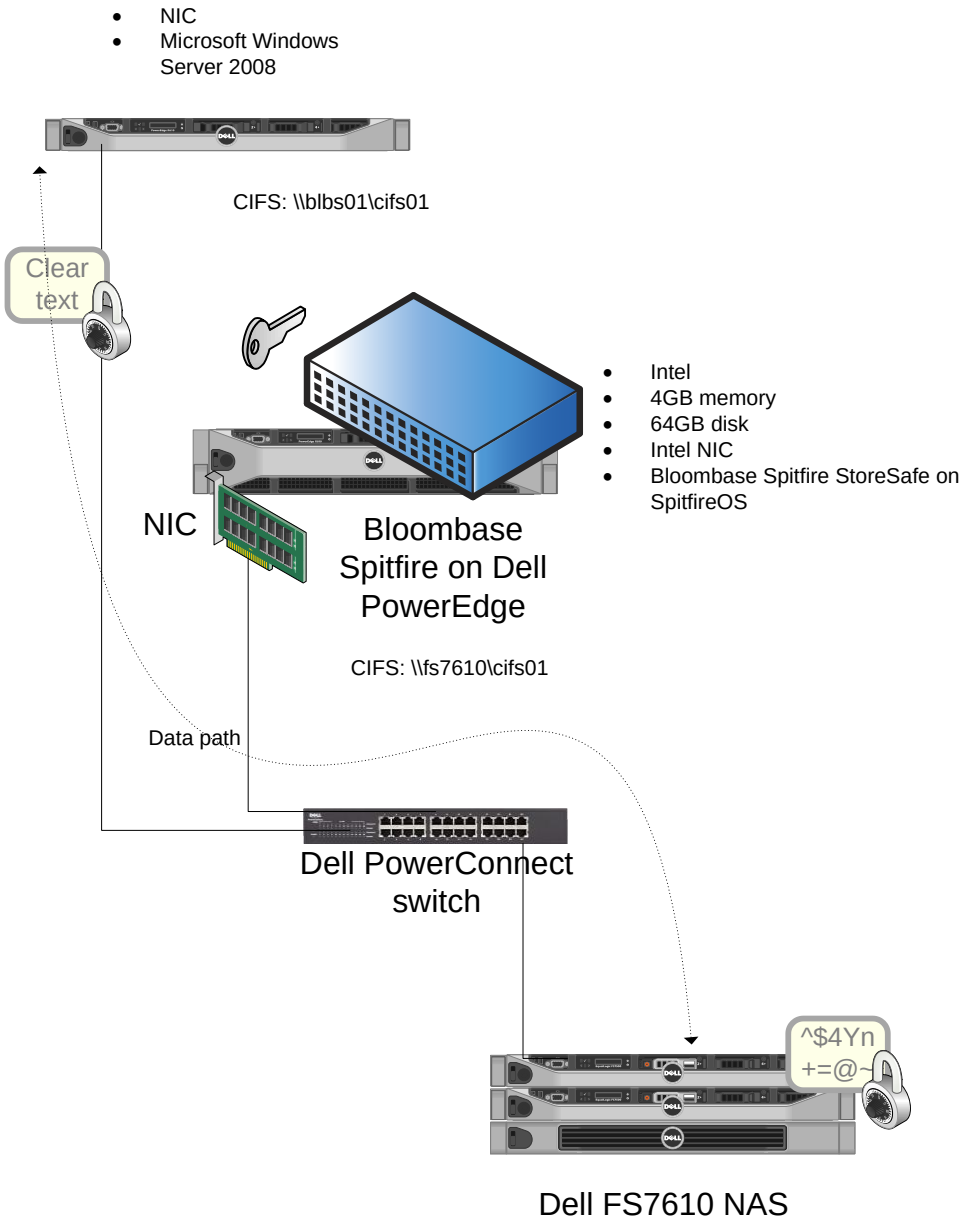
Enter Bloombase data at rest security software solution, Dell does not only provide the high-performance and highly scalable PowerEdge servers which Bloombase StoreSafe encryption software runs on, Dell also houses business critical information on their Compellent, and EqualLogic in which business secrets and sensitive data are kept away from unauthorized access by Bloombase encryption.



The following use cases will cover all encryption capabilities achieved by the Bloombase solution.

1.1 Use Cases for FS7610 (EqualLogic) as the storage device for CIFS security

The Use Cases for supporting FS7610 (EqualLogic) as the storage system for CIFS security with PowerEdge server for Bloombase solution.



1.1.1 CIFS user authentication access control

User authentication at Windows Server 2008 by Bloombase StoreSafe CIFS virtual storage will be supported.

Example Use Case: Access Bloombase StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 where the correct user name and password combination yields access to the Bloombase StoreSafe CIFS virtual storage. Incorrect user name and password combination should yield request for retry.

1.1.2 Host network access control

Only authorized hosts are allowed to access Bloombase StoreSafe CIFS virtual storage.

Example Use Case: Accessing Bloombase StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 with authorized IP network address with correct user authentication credentials yields successful connection to Bloombase StoreSafe CIFS virtual storage. Otherwise, access denied.

1.1.3 Connect to Bloombase StoreSafe CIFS virtual storage

When a connection is established between Windows Server 2008 and Bloombase StoreSafe CIFS virtual storage, the host applications should be able to use it as a normal CIFS network share.

Example Use Case: User presents correct combination of username and password at the authorized Windows Server 2008 host and successfully connects to Bloombase StoreSafe CIFS virtual storage \\blbs01\cifs01 with Windows Explorer.

1.1.4 List of Bloombase StoreSafe CIFS virtual storage

When connection is established to Bloombase StoreSafe CIFS virtual storage, its contents should be viewable in Windows Explorer.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, the user should be able to list files and folders in Windows Explorer.

1.1.5 Write and encrypt files to Bloombase StoreSafe CIFS virtual storage

Files created on or copied to Bloombase StoreSafe CIFS virtual storage are encrypted and saved in cipher text at Dell FS7610.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, the user creates and copies files to the Bloombase StoreSafe CIFS virtual storage successfully. The physical file in cipher-text can be examined at \\fs8600\cifs01.

1.1.6 Read and unencrypt files from Bloombase StoreSafe CIFS virtual storage

Access and open encrypted files at Bloombase StoreSafe CIFS virtual storage and obtain virtual, as-if-plain-text contents.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens and reads virtual-plain text of encrypted files physically stored at Dell EqualLogic \\fs7610\cifs01 via Bloombase StoreSafe.

1.1.7 Update files in Bloombase StoreSafe CIFS virtual storage

Update contents of files in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens encrypted files at \\fs7610\cifs01 via Bloombase StoreSafe. Any updates or alterations to existing files are automatically encrypted by Bloombase StoreSafe and saved as cipher text to Dell FS7610.

1.1.8 Delete files from Bloombase StoreSafe CIFS virtual storage

Delete files from Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes a file in Bloombase StoreSafe CIFS virtual storage, resulting in the file being deleted from FS7610.

1.1.9 Create folders in Bloombase StoreSafe CIFS virtual storage

Create folder in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user creates a folder on Bloombase StoreSafe using Windows Explorer and the same folder is created at Dell FS7610 \\fs7610\cifs01.

1.1.10 Open folder in Bloombase StoreSafe CIFS virtual storage

Access and open folders at Bloombase StoreSafe CIFS virtual storage

as normal folders.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens folders on Bloombase StoreSafe CIFS virtual storage via Windows Explorer.

1.1.11 Delete folders in Bloombase StoreSafe CIFS virtual storage

Delete folders in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes folders under Bloombase StoreSafe CIFS virtual storage via Windows Explorer, resulting in the actual folder stored at Dell FS7610 \\fs7610\cifs01 also being deleted.

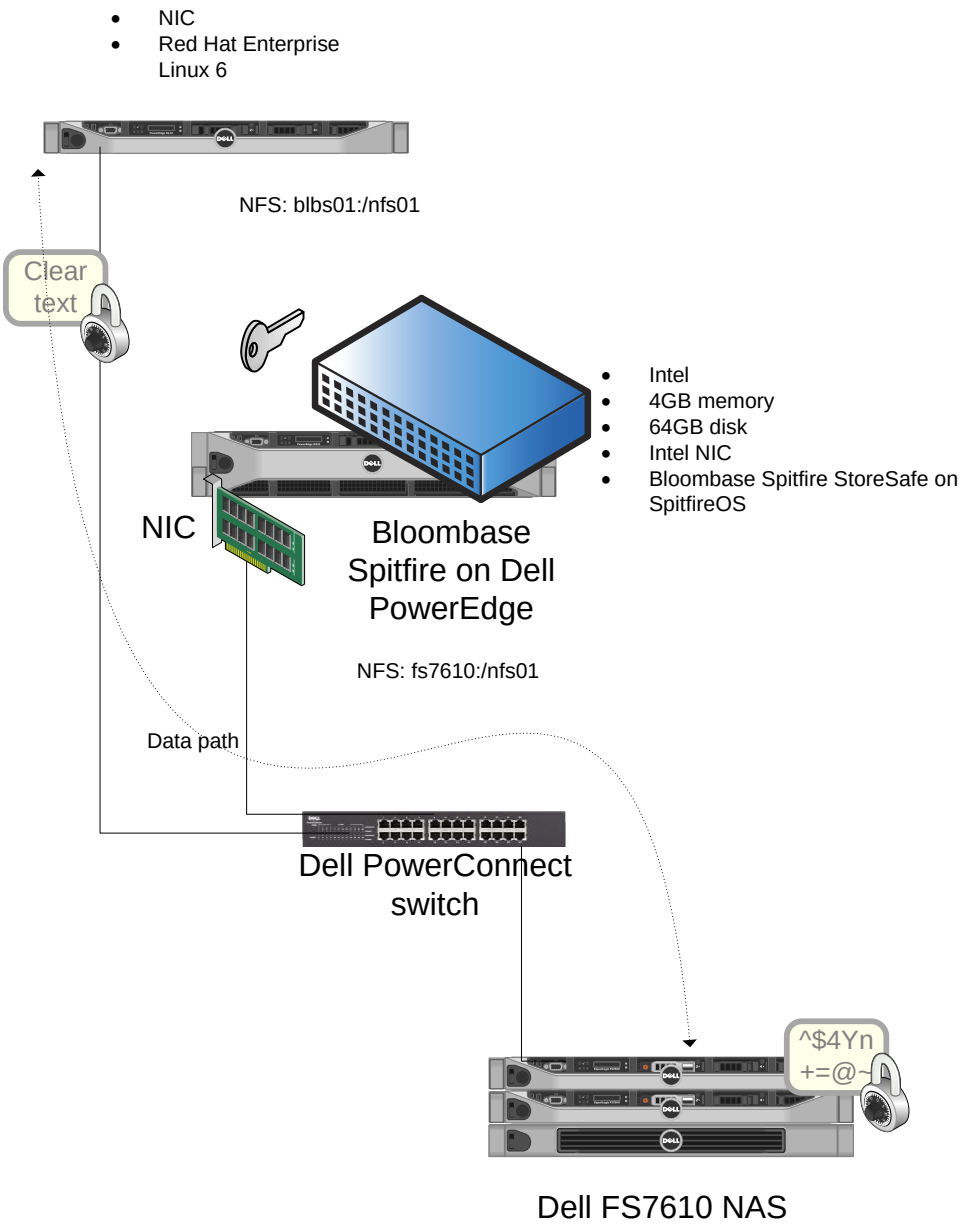
1.1.12 Write-once-read-many (WORM) in Bloombase StoreSafe CIFS virtual storage

Bloombase StoreSafe CIFS virtual storage behave as a logic write-once-read-many (WORM) for secure archival use

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user copies or moves files to Bloombase StoreSafe CIFS WORM virtual storages, resulting in the files being encrypted and saved on Dell EqualLogic at \\fs7610\cifs01. The file(s) are read-only, any alteration of the files on Bloombase StoreSafe CIFS virtual storage, ensuring for long term secure retention. If any intruder attempts to alter the contents at FS7610, the files saved via Bloombase StoreSafe will be seen as tampered with and corrupted yielding I/O errors as proof of tampering.

1.2 Use Cases for FS7610 (EqualLogic) as the storage device for NFS security

The Use Cases for supporting FS7610(EqualLogic) as the storage system for NFS security with PowerEdge server for Bloombase solution.



1.2.1 Host network access control

Only authorized hosts are allowed to access Bloombase StoreSafe NFS virtual storage.

Example Use Case: Access Bloombase StoreSafe CIFS virtual storage from Red Hat Enterprise Linux shell blbs01:/nfs01 with authorized IP network address to connect successfully to Bloombase StoreSafe NFS virtual storage. Otherwise, access is denied.

1.2.2 Connect to Bloombase StoreSafe NFS virtual storage

With connection established from Red Hat Enterprise Linux to Bloombase StoreSafe NFS virtual storage the host applications can connect and access the share as a normal NFS network share/mount point.

Example Use Case: The administrator of an authorized Red Hat Enterprise Linux server mounts the NFS share at blbs01:/nfs01 and successfully connects to Bloombase StoreSafe NFS virtual storage.

1.2.3 List of Bloombase StoreSafe NFS virtual storage

The contents of a Bloombase StoreSafe NFS virtual storage can be listed and viewed as a normal NFS share.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator should be able to list files and folders using the ls command.

1.2.4 Write and encrypt files to Bloombase StoreSafe NFS virtual storage

Files created on or copied to Bloombase StoreSafe NFS virtual storage are encrypted and stored as cipher text on Dell EqualLogic.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator creates or copies files to folders on Bloombase StoreSafe NFS virtual storage, resulting in the files being encrypted and stored on Dell EqualLogic. The encrypted, physical files can be examined at fs7610:/nfs01.

1.2.5 Read and un-encrypt files in Bloombase StoreSafe NFS virtual storage

Access and open encrypted files in Bloombase StoreSafe NFS virtual storage and obtain virtual, as-if-plain-text contents.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator opens and reads the virtual, as-if-

plain-text contents of the encrypted files physically stored at Dell EqualLogic fs7610:/nfs01.

1.2.6 Update files from Bloombase StoreSafe NFS virtual storage

Update contents of files in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the Bloombase StoreSafe unencrypts the files at fs7610:/nfs01 and presents the virtual, as-if-plain-text contents. The administrator uses Vim to alter/update file contents, and the changes are automatically encrypted by Bloombase StoreSafe and saved to Dell FS7610.

1.2.7 Delete files in Bloombase StoreSafe NFS virtual storage

Delete files from Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator deletes a file on Bloombase StoreSafe virtual storage using the rm command, resulting in the physical file on Dell FS7610 being deleted.

1.2.8 Create folders in Bloombase StoreSafe NFS virtual storage

Create folders in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator creates a folder on Bloombase StoreSafe virtual storage using the mkdir command, resulting in the folder being created on Dell FS7610 at fs7610:/nfs01.

1.2.9 Open folder in Bloombase StoreSafe NFS virtual storage

Access and view folders in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator can navigate through the folders in Bloombase StoreSafe NFS virtual storage in the shell using the cd command.

1.2.10 Delete folders in Bloombase StoreSafe NFS virtual storage

Delete folders at Bloombase StoreSafe NFS virtual storage

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, and the administrator deletes folders in Bloombase StoreSafe NFS virtual storage using rmdir command, it results in the actual folders stored at Dell FS7610 fs7610:/nfs01 being deleted.

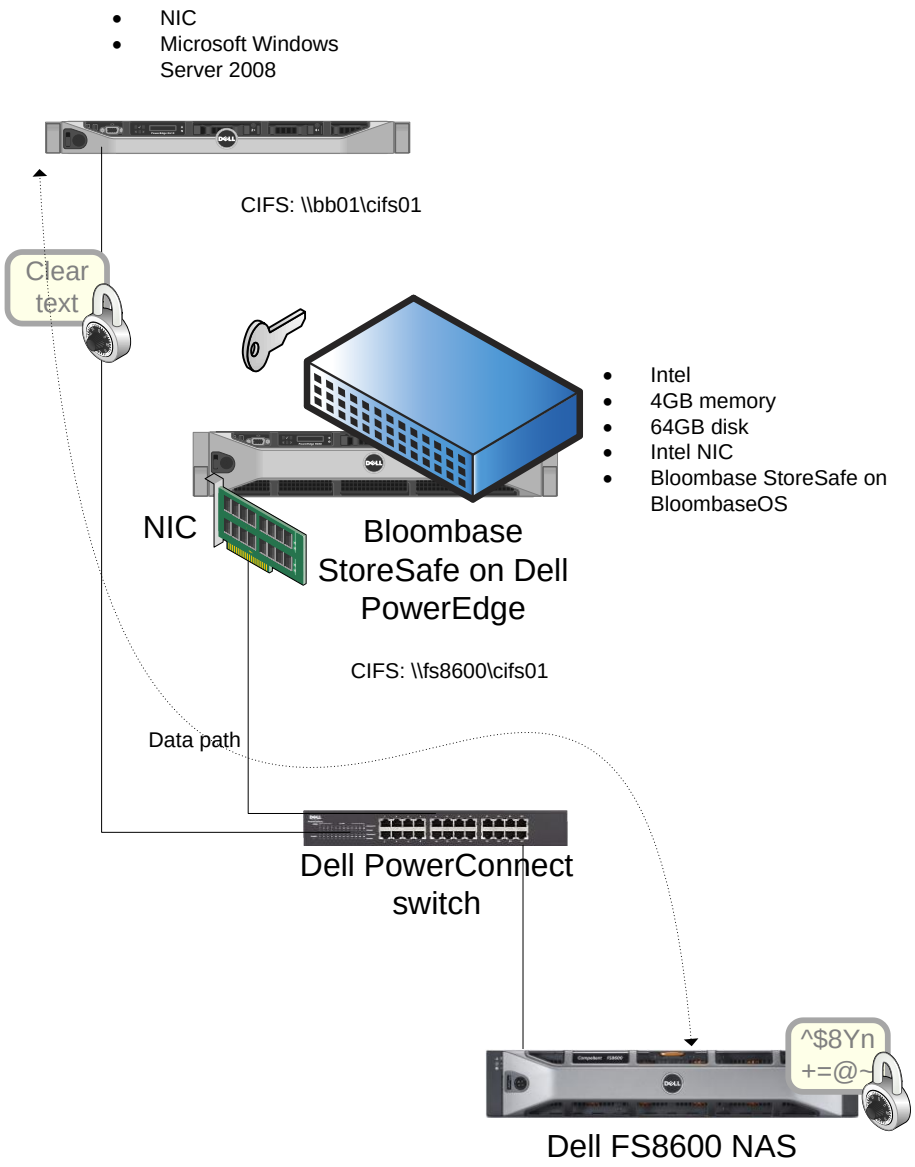
1.2.11 Write-once-read-many (WORM) in Bloombase StoreSafe NFS virtual storage

Bloombase StoreSafe NFS virtual storage behaves as a logic write-once-read-many (WORM) for secure archival use.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, and the administrator copies or moves files to Bloombase StoreSafe NFS WORM virtual storage the files are encrypted and saved at Dell EqualLogic at fs7610:/nfs01. The file(s) are read-only, preventing any rewrite via Bloombase StoreSafe NFS virtual storage and ensures long term secure retention. If intruders alter the contents at Dell EqualLogic, the files saved via Bloombase StoreSafe will be corrupted yielding I/O errors as proof of tampering.

1.3 Use Cases for FS8600 (Compellent) as the storage device for CIFS security

The Use Cases for supporting FS8600 (Compellent) as the storage system for CIFS with PowerEdge server and Bloombase security solution.



1.3.1 CIFS user authentication access control

User authentication at Windows Server 2008 by Bloombase StoreSafe CIFS virtual storage will be supported.

Example Use Case: Accessing Bloombase StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 requires the correct user name and password. Incorrect user name and password combination should yield request for retry.

1.3.2 Host network access control

Only authorized hosts are allowed to access Bloombase StoreSafe CIFS virtual storage.

Example Use Case: Accessing Bloombase StoreSafe CIFS virtual storage at Windows Server 2008 Windows Explorer \\blbs01\cifs01 with authorized IP network address with correct user authentication credentials yields successful connection to Bloombase StoreSafe CIFS virtual storage. Otherwise, access denied.

1.3.3 Connect to Bloombase StoreSafe CIFS virtual storage

When a connection is established between Windows Server 2008 and Bloombase StoreSafe CIFS virtual storage, the host applications should be able to use it as a normal CIFS network share.

Example Use Case: User presents correct combination of username and password at the authorized Windows Server 2008 host and successfully connects to Bloombase StoreSafe CIFS virtual storage \\blbs01\cifs01 with Windows Explorer.

1.3.4 List of Bloombase StoreSafe CIFS virtual storage

When connection is established to Bloombase StoreSafe CIFS virtual storage, its contents should be viewable in Windows Explorer.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, the user should be able to list files and folders in Windows Explorer.

1.3.5 Write and encrypt files to Bloombase StoreSafe CIFS virtual storage

Create or copy files to Bloombase StoreSafe CIFS virtual storage and contents get encrypted

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, the user creates and copies files to the Bloombase StoreSafe CIFS virtual storage successfully. The physical file in cipher-text can be examined at \\fs8600\cifs01.

1.3.6 Read and unencrypt files from Bloombase StoreSafe CIFS virtual storage

Access and open encrypted files at Bloombase StoreSafe CIFS virtual storage and obtain virtual-plain contents

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens and read virtual-plain text of encrypted files physically stored at Dell Compellent \\fs8600\cifs01 via Bloombase StoreSafe.

1.3.7 Update files from Bloombase StoreSafe CIFS virtual storage

Update contents of files in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens encrypted files at \\fs7610\cifs01 via Bloombase StoreSafe. Any updates or alterations to existing files are automatically encrypted by Bloombase StoreSafe and saved as cipher text to Dell FS8600.

1.3.8 Delete files from Bloombase StoreSafe CIFS virtual storage

Delete files from Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes a file in Bloombase StoreSafe CIFS virtual storage, resulting in the file being deleted from Dell FS8600.

1.3.9 Create folders on Bloombase StoreSafe CIFS virtual storage

Create folder in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user creates a folder on Bloombase StoreSafe using Windows Explorer and the same folder is created at Dell FS8600 at \\fs7610\cifs01.

1.3.10 Open folder in Bloombase StoreSafe CIFS virtual storage

Access and open folders at Bloombase StoreSafe CIFS virtual storage

as normal folders.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user opens folders under Bloombase StoreSafe CIFS virtual storage via Windows Explorer.

1.3.11 Delete folders in Bloombase StoreSafe CIFS virtual storage

Delete folders in Bloombase StoreSafe CIFS virtual storage.

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user deletes folders under Bloombase StoreSafe CIFS virtual storage via Windows Explorer, resulting in the folder at Dell FS8600 \\fs7610\cifs01 being deleted.

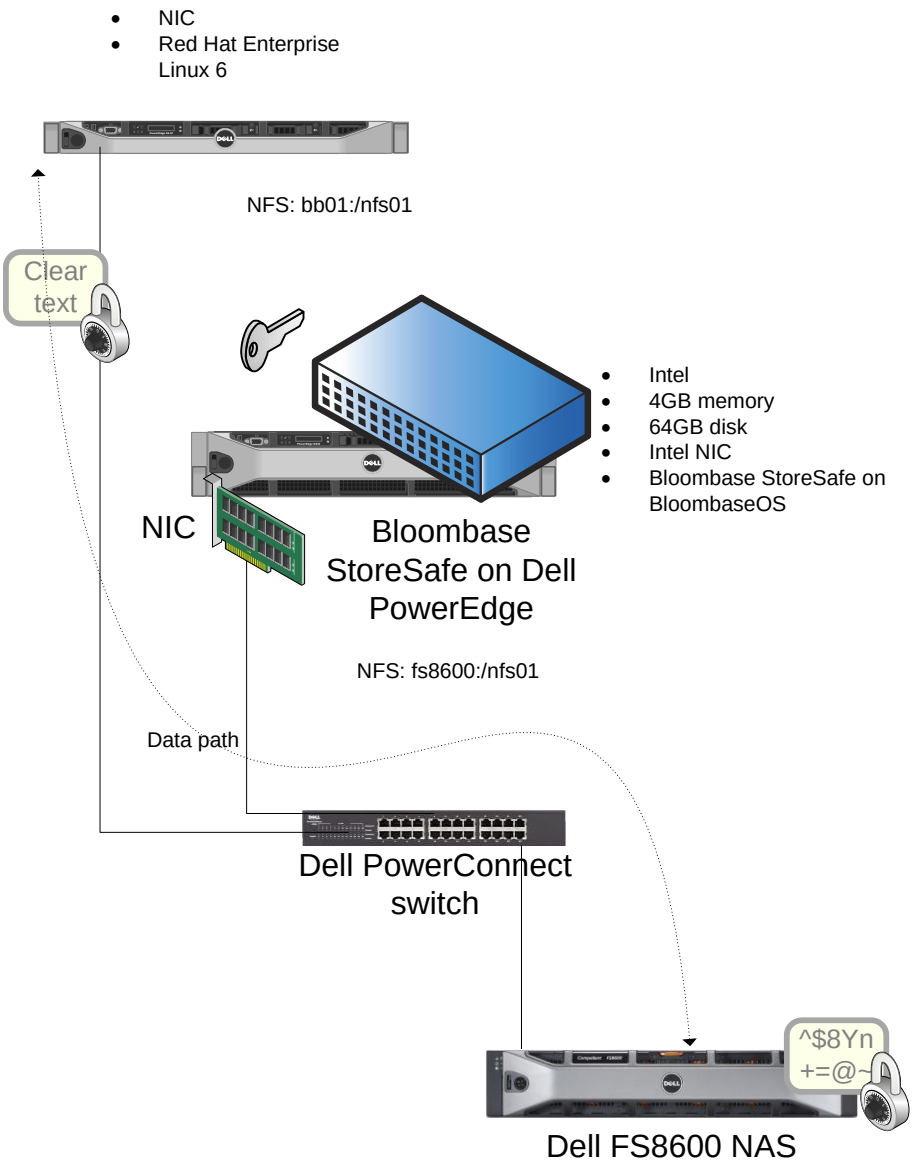
1.3.12 Write-once-read-many (WORM) in Bloombase StoreSafe CIFS virtual storage

Bloombase StoreSafe CIFS virtual storage behave as a logic write-once-read-many (WORM) for secure archival use

Example Use Case: On granted user and host access from Windows Server 2008 to Bloombase StoreSafe CIFS virtual storage at \\blbs01\cifs01, user copies or moves files to Bloombase StoreSafe CIFS WORM virtual storages, resulting in the files being encrypted and saved on Dell Compellent at \\fs7610\cifs01. The file(s) are read-only, any alteration of the files on Bloombase StoreSafe CIFS virtual storage, ensuring for long term secure retention. If any intruder attempts to alter the contents at Dell FS8600, the files saved via Bloombase StoreSafe will be seen as tampered with and corrupted yielding I/O errors as proof of tampering.

1.4 Use Cases for FS8600 (Compellent)as the storage device for NFS security

The Use Cases for supporting FS8600 (Compellent) as the storage system for NFS security with PowerEdge server for Bloombase solution.



1.4.1 Host network access control

Only authorized hosts are allowed to access Bloombase StoreSafe NFS virtual storage.

Example Use Case: Access Bloombase StoreSafe CIFS virtual storage from Red Hat Enterprise Linux shell blbs01:/nfs01 with authorized IP network address to connect successfully to Bloombase StoreSafe NFS virtual storage. Otherwise, access is denied.

1.4.2 Connect to Bloombase StoreSafe NFS virtual storage

With connection established from Red Hat Enterprise Linux to Bloombase StoreSafe NFS virtual storage the host applications can connect and access the share as a normal NFS network share/mount point.

Example Use Case: The administrator of an authorized Red Hat Enterprise Linux server mounts the NFS share at blbs01:/nfs01 and successfully connects to Bloombase StoreSafe NFS virtual storage.

1.4.3 List of Bloombase StoreSafe NFS virtual storage

The contents of a Bloombase StoreSafe NFS virtual storage can be listed and viewed as a normal NFS share.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator should be able to list files and folders using the ls command.

1.4.4 Write and encrypt files to Bloombase StoreSafe NFS virtual storage

Files created on or copied to Bloombase StoreSafe NFS virtual storage are encrypted and stored as cipher text on Dell EqualLogic.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator creates or copy files to base or subfolders of Bloombase StoreSafe NFS virtual storage successfully. The encrypted file contents on Dell FS8600 can be examined at fs8600:/nfs01.

1.4.5 Read and un-encrypt files from Bloombase StoreSafe NFS virtual storage

Access and open encrypted files at Bloombase StoreSafe NFS virtual storage and obtain virtual, as-if-plain-text contents.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator opens and reads the virtual, as-if-plain-text contents of the encrypted files physically stored at Dell

Compellent fs8600:/nfs01.

1.4.6 Update files from Bloombase StoreSafe NFS virtual storage

Update contents of encrypted files in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator opens encrypted files at fs8600:/nfs01 via Bloombase StoreSafe virtual storage using Vim and alters/updates file contents. The changes are automatically encrypted by Bloombase StoreSafe and saved as cipher text to Dell FS8600.

1.4.7 Delete files from Bloombase StoreSafe NFS virtual storage

Delete files from Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator deletes a file on Bloombase StoreSafe virtual storage using the rm command, resulting in the actual file on Dell Compellent also being deleted.

1.4.8 Create folders in Bloombase StoreSafe NFS virtual storage

Create folders in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, administrator creates a folder via Bloombase StoreSafe using the mkdir command, resulting in the same folder being created at Dell FS8600 fs8600:/nfs01.

1.4.9 Open folder in Bloombase StoreSafe NFS virtual storage

Access and open folders at Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, the administrator navigates through the folders in Bloombase StoreSafe NFS virtual storage using the cd command.

1.4.10 Delete folders in Bloombase StoreSafe CIFS virtual storage

Delete folders in Bloombase StoreSafe NFS virtual storage.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, and the administrator deletes folders in Bloombase StoreSafe NFS virtual storage using rmdir command, it results in the actual folders stored on Dell FS8600 at fs8600:/nfs01 being deleted.

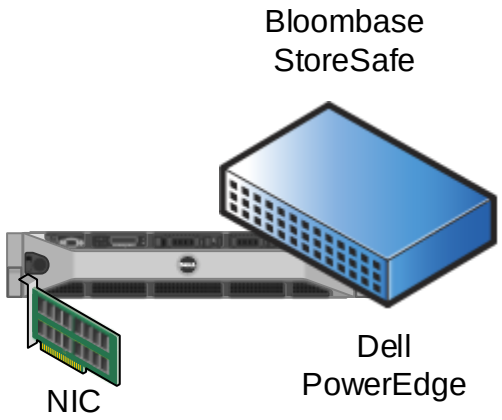
1.4.11 Write-once-read-many (WORM) in Bloombase StoreSafe NFS virtual storage

Bloombase StoreSafe NFS virtual storage behaves as a logic write-once-read-many (WORM) for secure archival use.

Example Use Case: When a Red Hat Enterprise Linux Server is granted access to Bloombase StoreSafe NFS virtual storage at blbs01:/nfs01, and the administrator copies or moves files to Bloombase StoreSafe NFS WORM virtual storage the files are encrypted and saved on Dell Compellent at fs8600:/nfs01. The file(s) are read-only, preventing any re-write via Bloombase StoreSafe NFS virtual storage and ensures long term secure retention. If intruders alter the contents at Dell FS8600, the files saved via Bloombase StoreSafe will be corrupted yielding I/O errors as proof of tampering.

1.5 The Bloombase solution Configuration

This section covers the configuration of the solution with detailed hardware requirement and set up, and GUI for any required configuration.



Bloombase StoreSafe 3.4.5 ISO is to be installed at Dell PowerEdge server, providing agentless, non-disruptive, file-, block- and object-based encryption of data at rest managed by Dell FS7610 and Dell FS8600.

For NAS applications with Dell FS7610 (EqualLogic) and FS8600 (Compellent), only network interface cards (NIC) are required.

1.5.1 Parameters for configuration

Bloombase StoreSafe Network Configuration

- Host name: blbs01
- IP address: 10.10.10.141

Bloombase StoreSafe NAS Server Configuration

- SMB server name: blbs01

Bloombase StoreSafe SAN Server Configuration

- Targets: <WWNs of HBAs which act as target>

Bloombase StoreSafe Key Management

- Key name: key01
- Bit length: 2048

Bloombase StoreSafe CIFS Configuration

- Virtual storage name: cifs01
- Type: File/Share
- Physical storage: \\fs7610\cifs01
- Protection: Privacy
- Key: key01
- Cipher algorithm: AES
- Key length: 256
- User access control: user01/123456
- Host access control: 10.10.10.140

Bloombase StoreSafe NFS Configuration

- Virtual storage name: nfs01
- Type: File/Share
- Physical storage: fs7610:/nfs01
- Protection: Privacy
- Key: key01

- Cipher algorithm: AES
- Key length: 256
- Host access control: 10.10.10.140

1.5.2 Configuration Screens

Installation

Bloombase Spitfire Server ISO images can be directly mounted as virtual disk drive on VMware Server or ESX for virtual appliance installation.
Installation CD/DVDs are also available for installation directly from disk drives.

Bloombase SpitfireOS installer will guide you through the rest of the installation process.

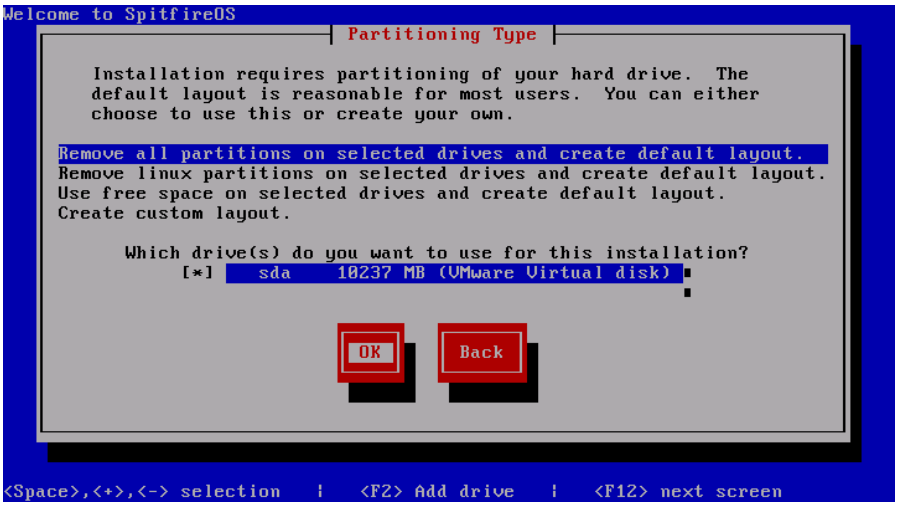
Keyboard Configuration

Choose the type of keyboard attached to the physical or virtual appliance on which Bloombase StoreSafe Server is installed. As a default option, the keyboard type is ‘us’.

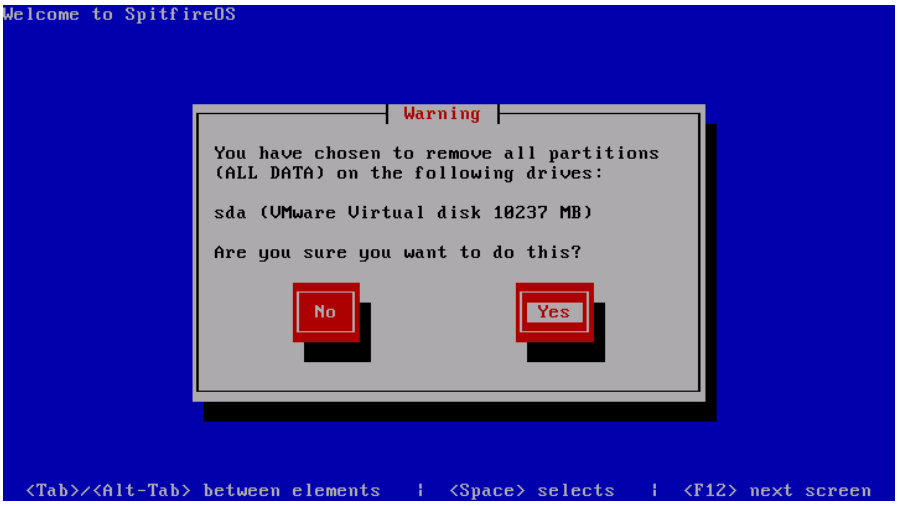
Disk Partitioning

Attached hard-drive partition table has to be erased before Bloombase StoreSafeOS installation can begin.
Choose ‘Yes’ to confirm that the partition table can be erased. Note that **all data** on the drive **will be erased**.

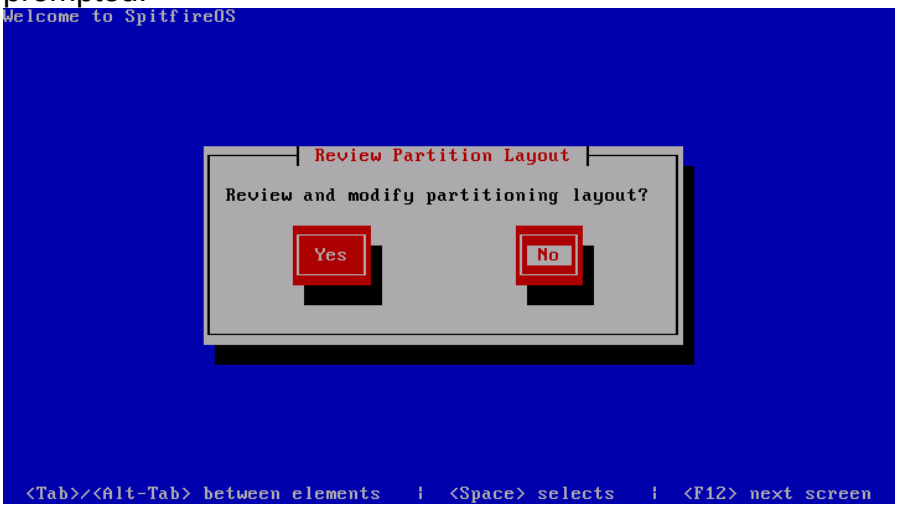
Specify the layout of disk partitioning for the installation of Bloombase StoreSafe Server.
Select the partition where Bloombase StoreSafeOS is to be installed.
Choose ‘OK’ to continue.



The installation prompts again for confirmation to install Bloombase SpitfireOS on the specified hard drive partition.
Choose ‘Yes’ to confirm.

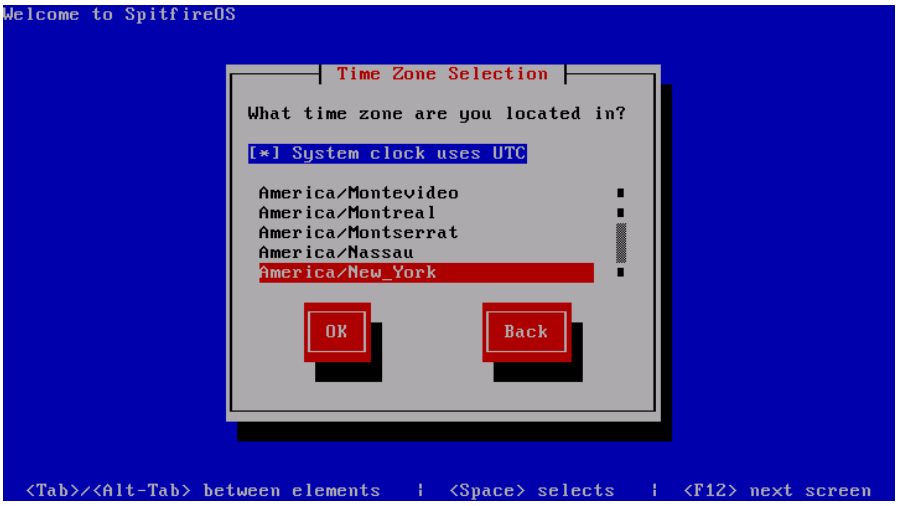


Bloombase SpifireOS prompts to review partition table and if any modifications are required.
If you are sure about the partitioning settings, choose ‘No’ when prompted.



System Time Zone Configuration

Specify Bloombase StoreSafeOS to use UTC for system clock and configure the location where Bloombase StoreSafe Server is located. This step is particularly important for time sensitive applications.



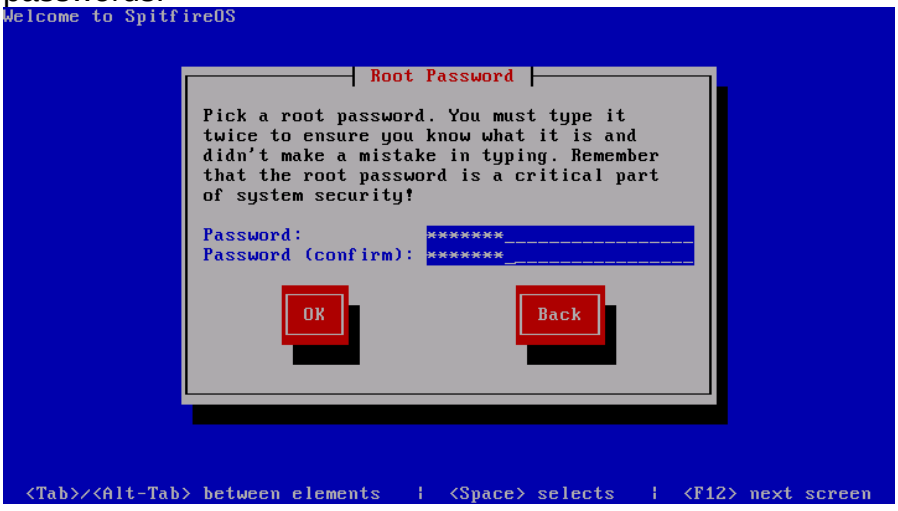
Bloombase SpitfireOS Super User Configuration

For normal usage, customers do not need to access to SpitfireOS. Administrators, operators, and users can simply utilize the command line interface (CLI) console and web management console for administration and management.

For circumstances where unsupported or special hardware needs to be added or system parameters changed, administrators may need super user/root access to SpitfireOS.

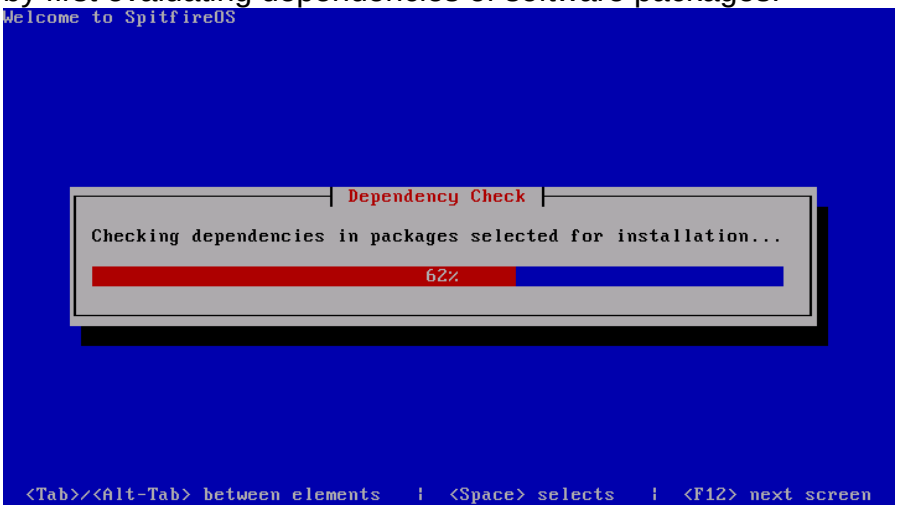
Specify a SpitfireOS root password when prompted.

IMPORTANT: SpitfireOS super user password empowers the administrator to gain system root access to SpitfireOS. Customers should handle SpitfireOS super user password with the same care and secrecy as their CLI and web management console passwords.

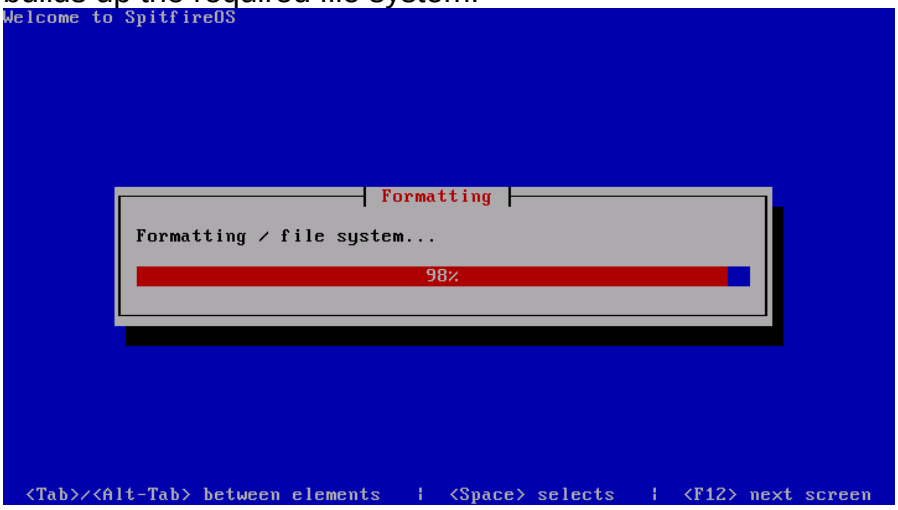


SpitfireOS Operating System Installation

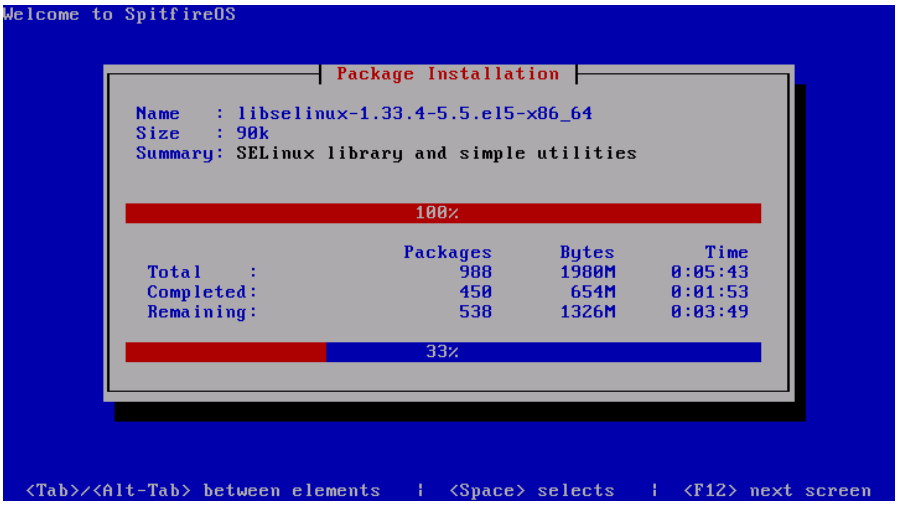
SpitfireOS automatic installer deploys the software on the system by first evaluating dependencies of software packages.



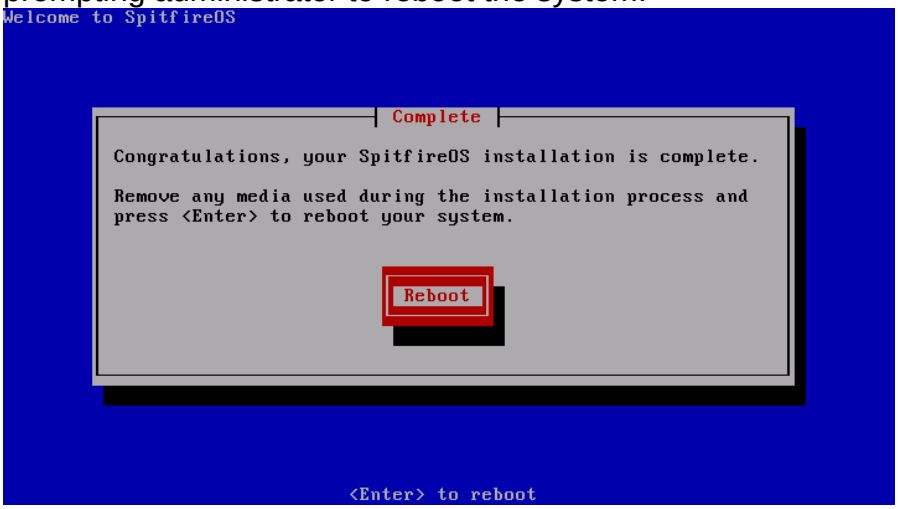
SpitfireOS starts to format the specified hard drive location and builds up the required file system.



SpitfireOS delivers baseline software packages to the operating system that is required to power application specific Spitfire servers.

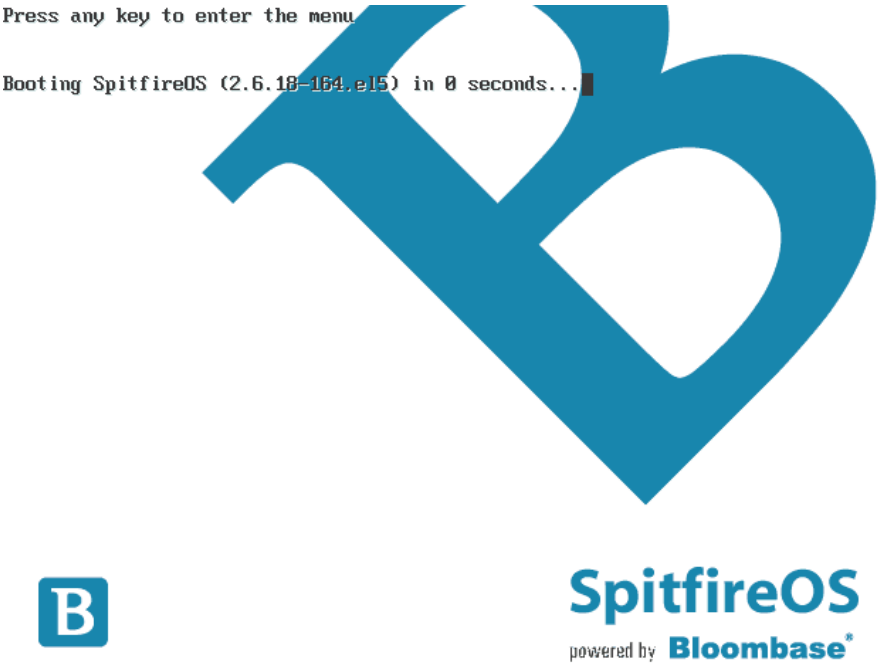


Once SpitfireOS successfully deploys, a dialog will be shown prompting administrator to reboot the system.

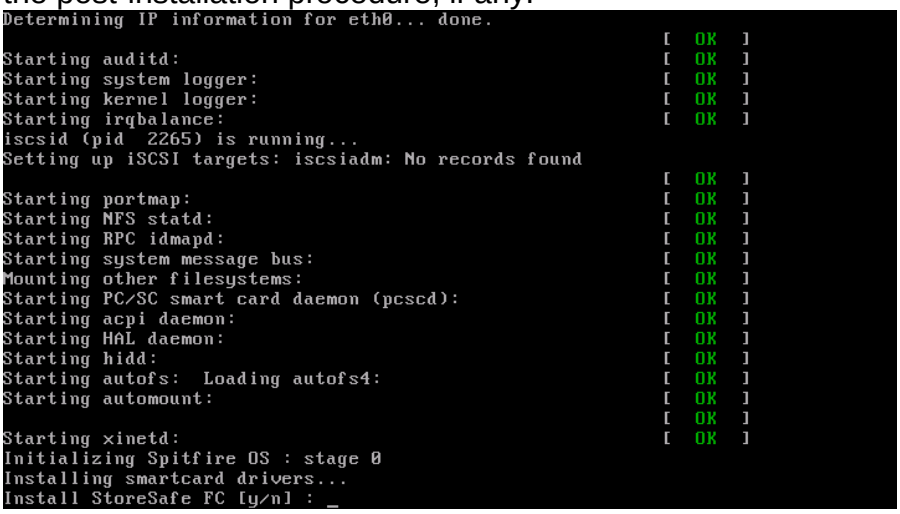


Follow the instructions to restart the newly installed system.

Post Installation Procedures

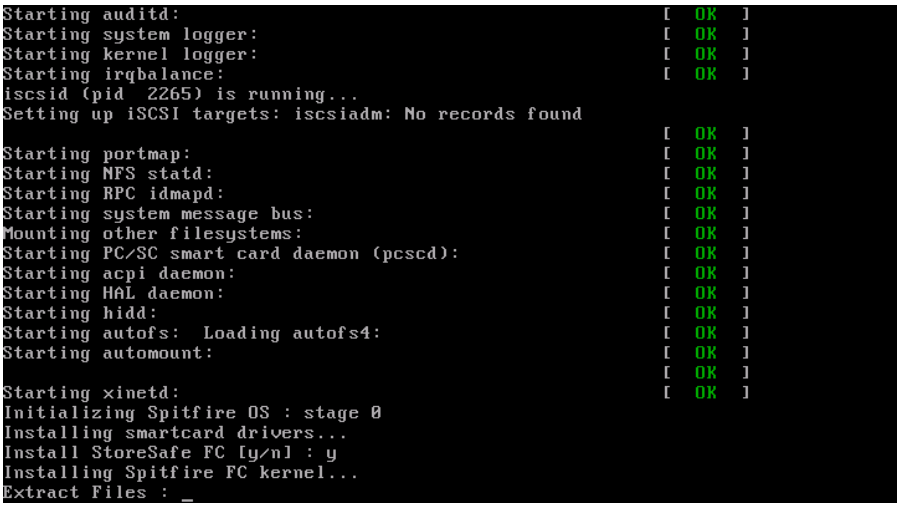


Bloombase SpitfireOS will boot up for the first time and complete the post-installation procedure, if any.

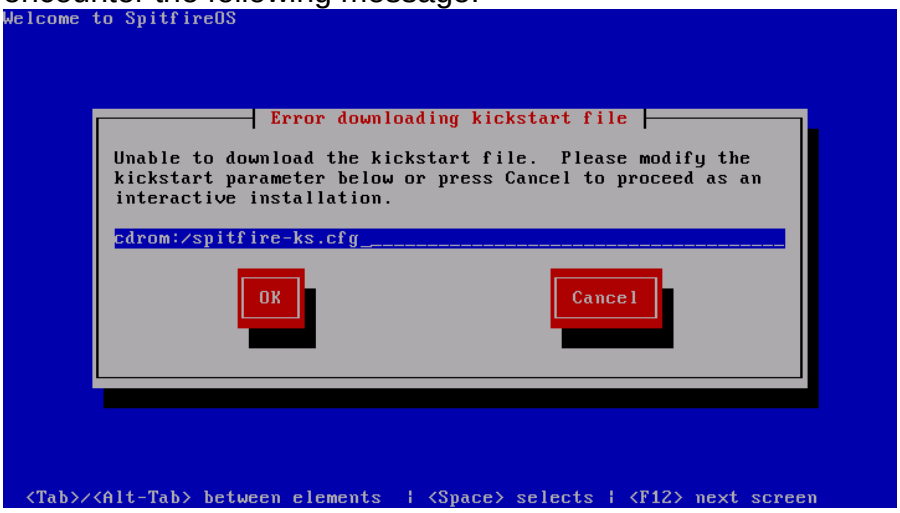


You will be prompted to install additional components and software modules as required by Spitfire Server, answer ‘y’ to start the rest of software installation.

If FC functionality is required, this must be specified and installed during the first startup, as seen in the screen capture below:



In case the path to the Spitfire kickstart file location is incorrect, or the device name of CD ROM is not the default ‘cdrom’, you may encounter the following message:



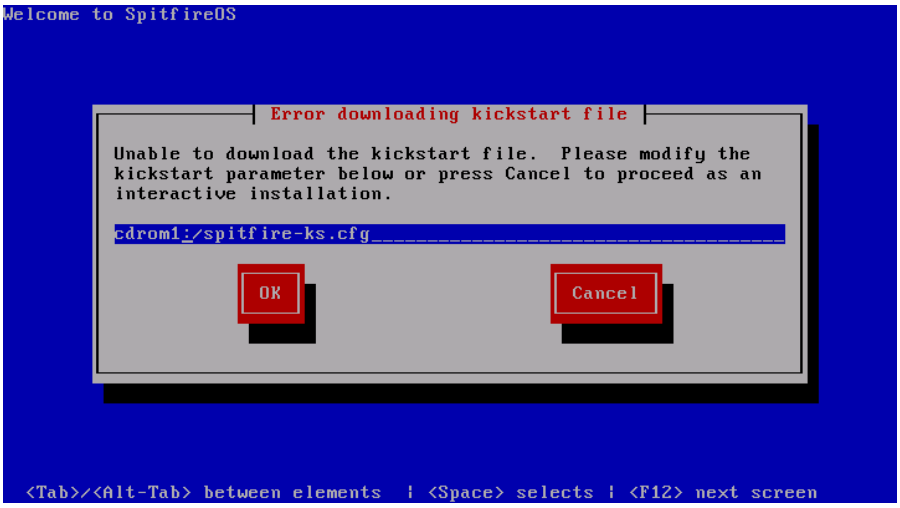
In this case, alter the path from

cdrom:/spitfire-ks.cfg

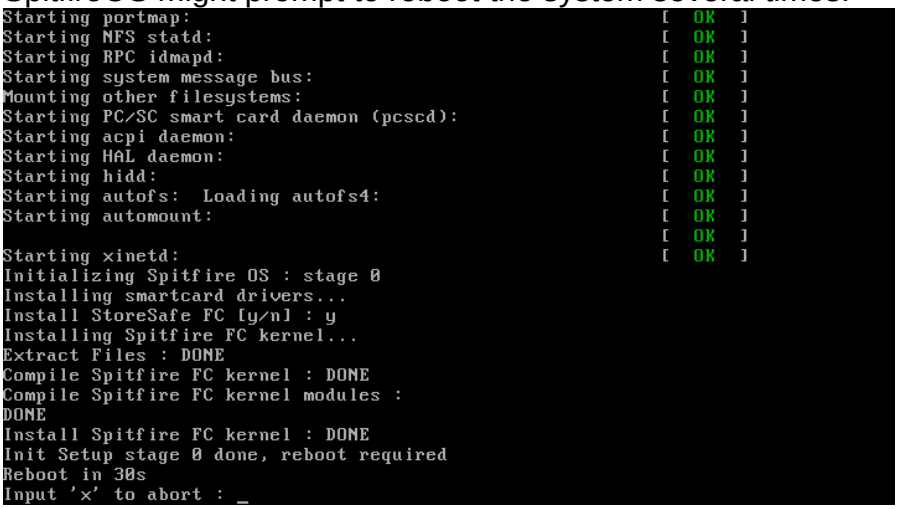
to

cdrom1:/spitfire-ks.cfg

If the message persists, try cdrom2, cdrom3, etc, until the installer can proceed with the installation.

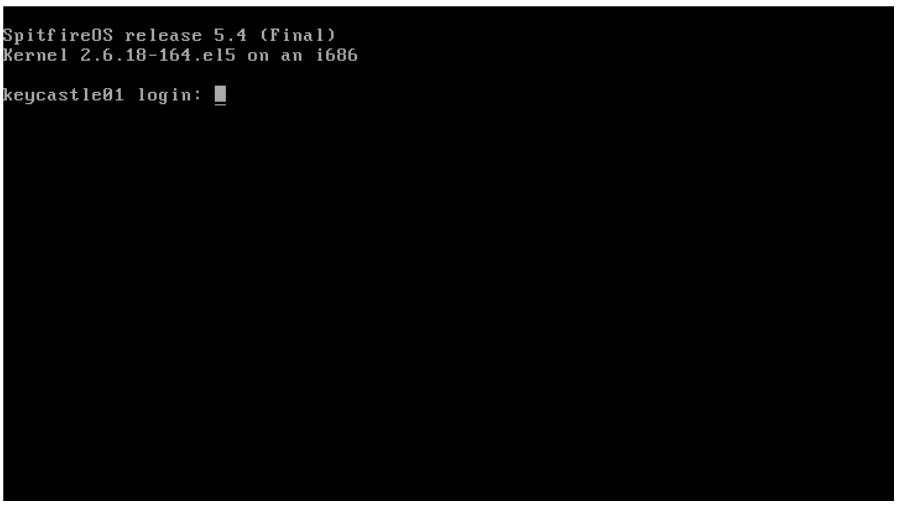


On completion of the SpitfireOS installation, Spitfire server installer will start deploying Spitfire server binaries to install and set up application specific Spitfire servers and related components.
SpitfireOS might prompt to reboot the system several times.



Once Spitfire Server completes installation, after reboot you will see the login prompt to the Spitfire CLI console.

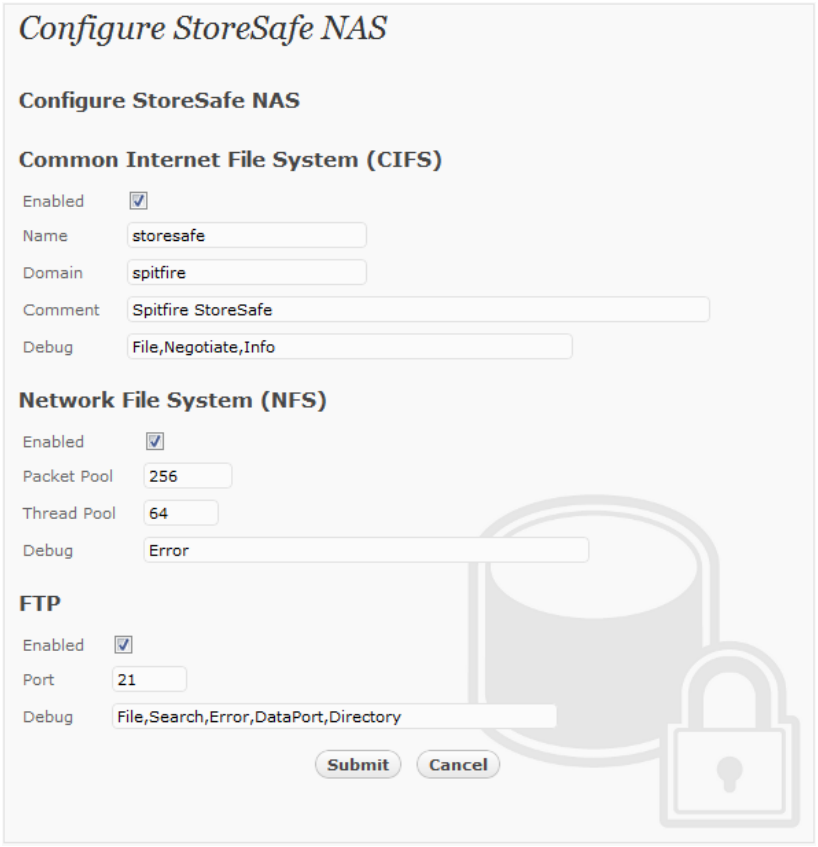
The Bloombase SpitfireOS Server is ready for configuration.



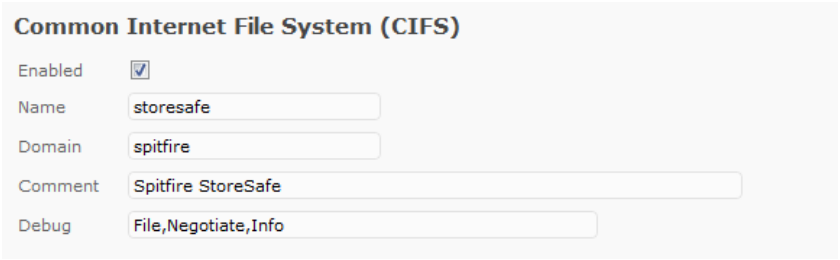
Log in for the first time using the default username admin and password admin. Change the password to prevent unauthorized access to the system.

NAS Server Configuration

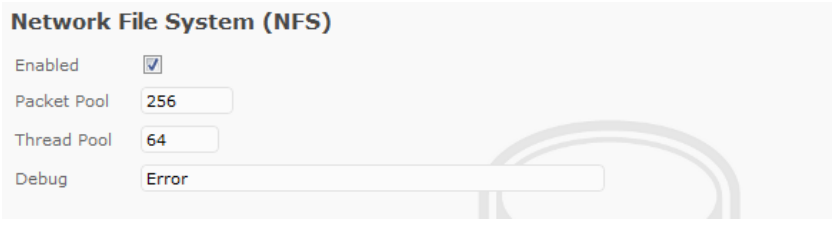
To configure StoreSafe NAS service components, the StoreSafe administrator can sign on to the StoreSafe web-based management console. Expand ‘Storage’ menu and launch ‘Configure StoreSafe NAS’ tool.



For CIFS



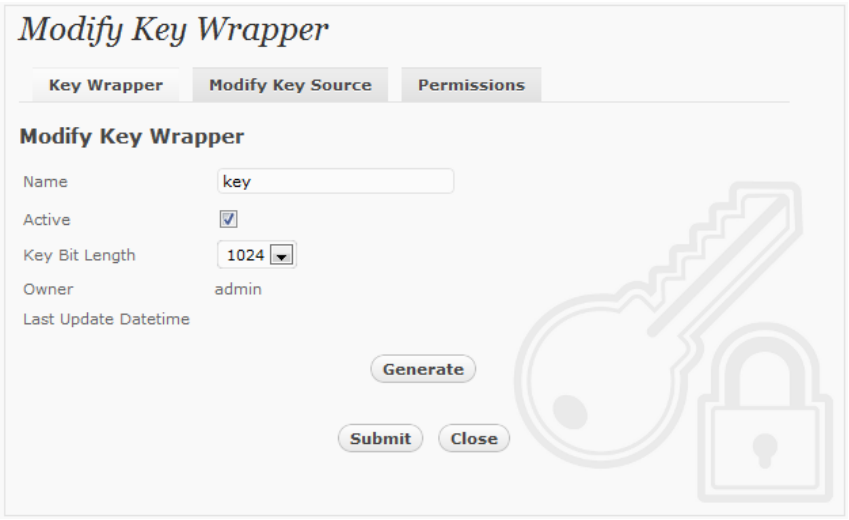
For NFS



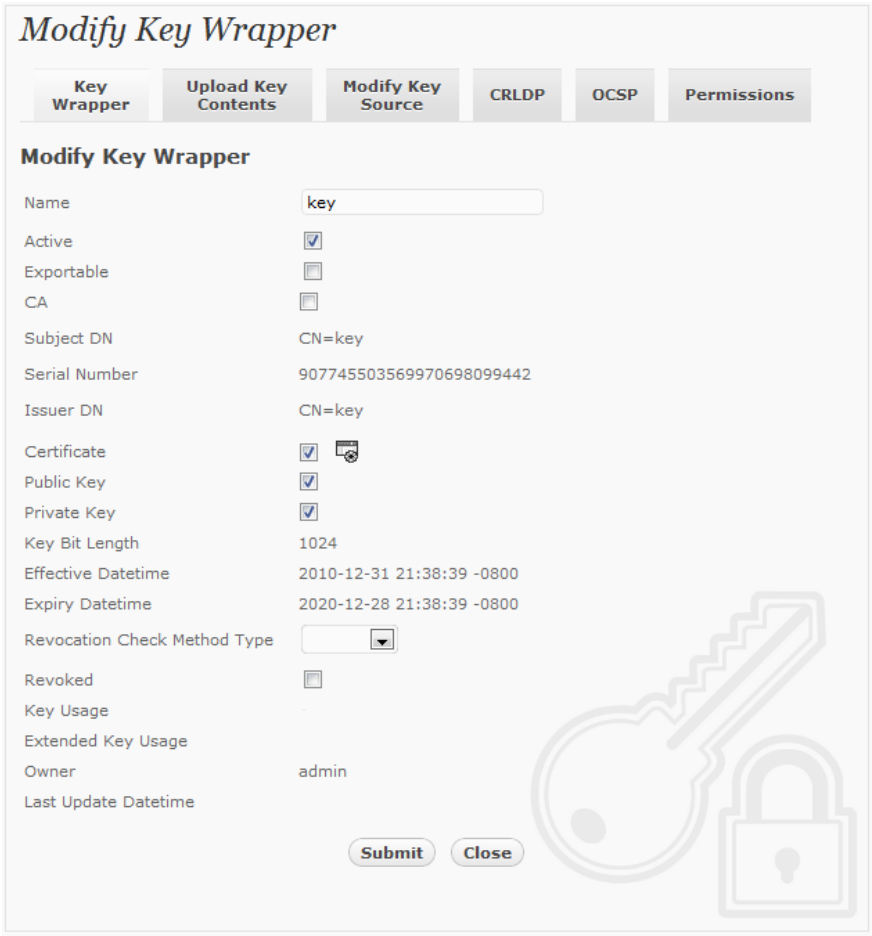
SAN Server Configuration

Navigate to the ‘Storage’ menu and click ‘Configure StoreSafe SAN’ tool to enter the list of fiber channel SAN targets provided by StoreSafe SAN module for servers equipped with compatible fiber channel host bus adapters (HBA).

Key Management

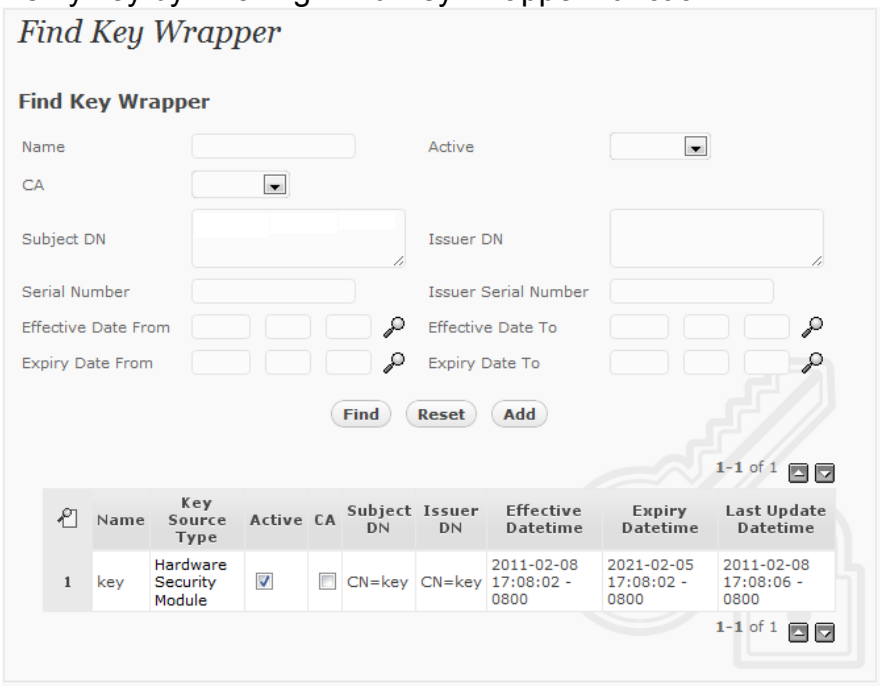


Push ‘Generate’ button to create a key.



Review the key details and choose ‘Submit’ to commit the changes.

Verify key by invoking ‘Find Key Wrapper’ function.



CIFS Virtual Storage Configuration

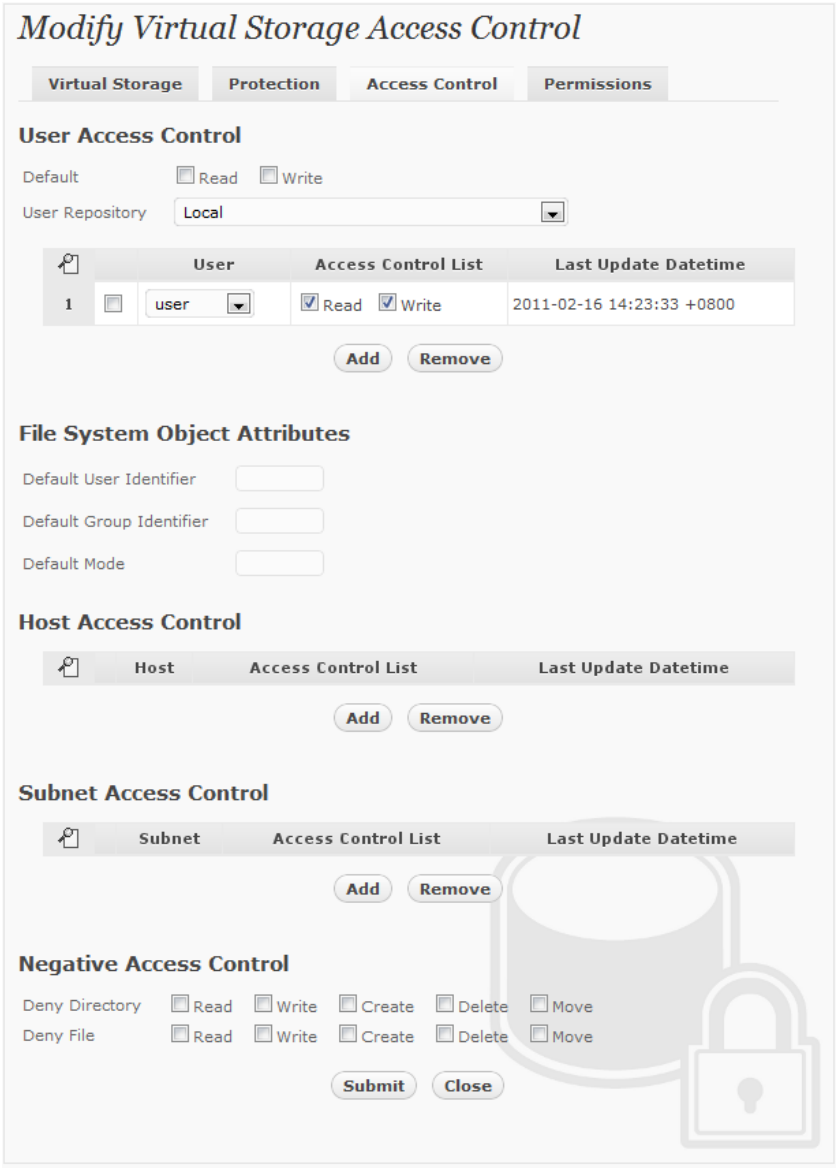
Navigate to the Storage menu and click 'Virtual Storage'. Click the 'Add' button to create virtual storage. Name the virtual storage as ‘cifs01'.

Select virtual storage mode 'File' or ‘Share’ for file-based protection. File-based protection provides a more fine-grained and tighter security, whereas share-based protection allows effective deduplication and compression.

Choose 'cifs01' as physical storage. Virtual storage 'cifs01' will be created as a network share to be accessed by a Windows client.

Turn to 'Virtual Storage Handler' tab and specify protection as 'Privacy' which means encryption has to be applied onto the virtual storage resources.

Secure files in cifs01 with AES-256 bit cipher encrypted with 'key01' previously generated.



Go to the 'Storage Access Control' tab and allow all hosts in the same network to access the StoreSafe secured storage, grant 'user01' the privilege to be able to access and write to the virtual storage.

Push 'Submit' button to commit changes.

NFS Virtual Storage Configuration

Navigate to the Storage menu and click 'Virtual Storage' tool. Click 'Add' to create a virtual storage. Name the virtual storage as 'nfs01'.

Select virtual storage mode as 'File' or 'Share'.

Choose 'nfs01' as physical storage. Virtual storage 'nfs01' will be created as a network share to be accessed by a Linux client.

Turn to 'Virtual Storage Handler' tab and specify protection as 'Privacy' which means encryption has to be applied onto the virtual storage resources.

Secure files inside nfs01 with AES-256 bit cipher encrypted by 'key01' previously generated.

Click the 'Storage Access Control' tab and allow host IP the privilege to be able to access and write to the virtual storage.

Push 'Submit' button to commit changes.

3 Dell Storage Platform Certification

Certification of the Bloombase solution with the Dell Storage Platform including EqualLogic FS7610 and Compellent FS8600 will be deemed complete and accepted by Dell when the Use Case designs in this document are demonstrated on a releasable version of the Bloombase solution.

An Exit Form document for each storage platform will be co-developed to capture the detailed test scenarios for Certification.