interopLab

# Interoperability of Bloombase StoreSafe and Gemalto SafeNet KeySecure for Data-at-Rest Encryption

April 2016

BLOOMBASE®

## Executive Summary

Gemalto SafeNet KeySecure Key Management System is validated by Bloombase InteropLab to run with Bloombase StoreSafe data-at-rest encryption security solution. This document describes the steps carried out to test interoperability of Gemalto SafeNet KeySecure Key Management System with Bloombase StoreSafe software appliance on VMware ESXi. Client host systems on Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Sun Solaris, IBM AIX and HP-UX are tested with Gemalto SafeNet KeySecure powered Bloombase StoreSafe with NetApp FAS unified storage system as backend storage.

Document No.: BLBS-TN-Bloombase-StoreSafe-Gemalto-SafeNet-KeySecure-Interoperability-USLET-EN-R0.92

# Table of Contents

# Purpose and Scope

This document describes the steps necessary to integrate Gemalto SafeNet KeySecure Key Management System with Bloombase StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Gemalto SafeNet KeySecure
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

# Assumptions

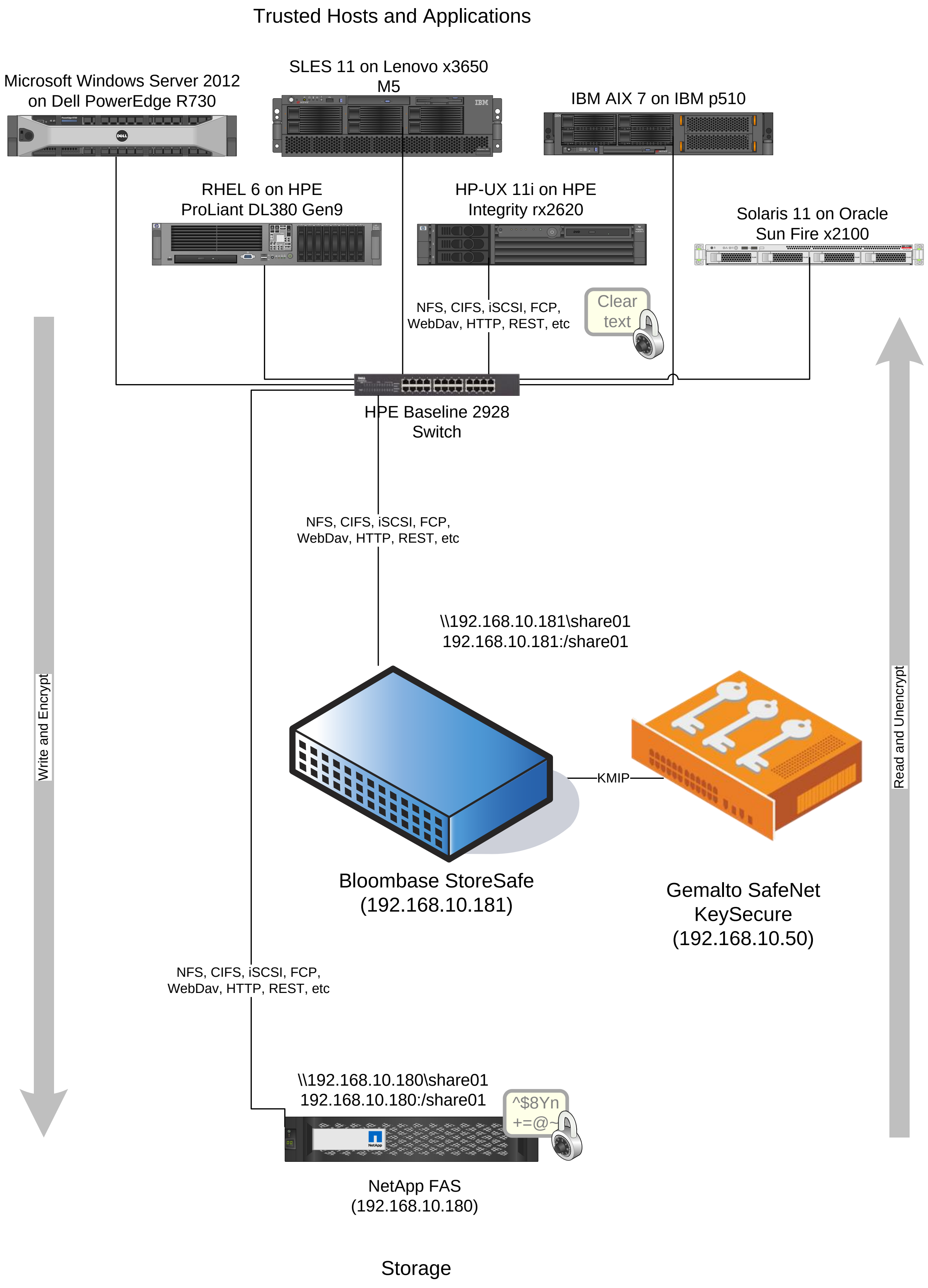
This document describes interoperability testing of Gemalto SafeNet KeySecure with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Gemalto SafeNet KeySecure, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that the reader possesses basic UNIX administration skill-set. The examples provided may require modifications before they could be run in reader's IT environment.

As Gemalto SafeNet KeySecure is a third party hardware option to Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model of Gemalto SafeNet KeySecure for the actual use case. We assume the reader has basic knowledge of storage networking and information cryptography. For specific technical product information of Bloombase StoreSafe, please refer to our website at http://www.bloombase.com and Bloombase SupPortal http://supportal.bloombase.com.

# Infrastructure

## Setup

The validation testing environment is set up as in below diagram:


Trusted Hosts and Applications
Microsoft Windows Server 2012 on Dell PowerEdge R730
SLES 11 on Lenovo x3650 M5
IBM AIX 7 on IBM p510
RHEL 6 on HPE ProLiant DL380 Gen9
HP-UX 11i on HPE Integrity rx2620
Solaris 11 on Oracle Sun Fire x2100
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
Clear text
HPE Baseline 2928 Switch
Write and Encrypt
Read and Unencrypt
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.181\share01
192.168.10.181:/share01
KMIP
Bloombase StoreSafe (192.168.10.181)
Gemalto SafeNet KeySecure (192.168.10.50)
NFS, CIFS, iSCSI, FCP, WebDav, HTTP, REST, etc
\\192.168.10.180\share01
192.168.10.180:/share01
^$8Yn +=@~
NetApp FAS (192.168.10.180)
Storage

# Key Management System

| | |
|---|---|
| **Key Management System** | Gemalto SafeNet KeySecure |

# Bloombase StoreSafe

| | |
|---|---|
| **Bloombase StoreSafe** | Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 7 |
| **Server** | VMware Virtual Machine (VM) on VMware ESXi 5.5 |
| **Processor** | 4 x Virtual CPU (vCPU) |
| **Memory** | 8 GB |

# Storage System

| | |
|---|---|
| **Storage System** | NetApp FAS Simulator |

# Client Hosts

| | | | | | | |
|---|---|---|---|---|---|---|
| **Model** | Dell PowerEdge R730 | HPE ProLiant DL380 Gen9 | Lenovo System x3650 M5 | HPE Integrity rx2620 | IBM System p5 510 | Oracle Sun Fire x2100 |
| **Operating System** | Microsoft Windows Server 2012 | Red Hat Enterprise Linux 6 | SUSE Linux Enterprise 11 | HP-UX 11i | IBM AIX 7 | Oracle Solaris 11 |

# Configuration Overview

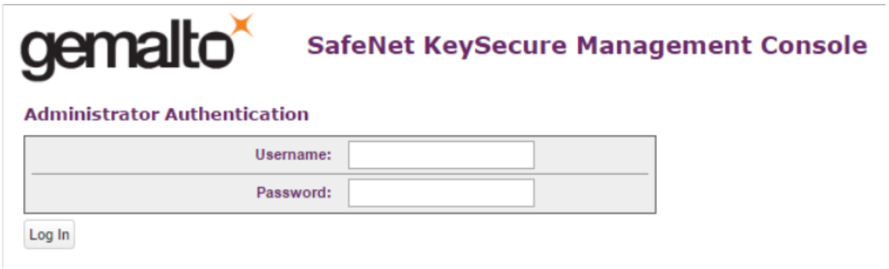
## Gemalto SafeNet KeySecure

Gemalto SafeNet KeySecure is a centralized key management platform, and is available as a hardware appliance or hardened virtual security appliance. By utilizing Gemalto SafeNet KeySecure, organizations benefit from its flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments. It includes integration API that supports the industry standards (KMIP 1.1, PKCS #11, JCE, MS-CAPI, ICAPI, and .NET) which are used in many application scenarios, e.g., Enterprise PKI application and database encryption. The Gemalto SafeNet KeySecure is available as a hardware appliance or hardened virtual security appliance with a hardware root of trust using SafeNet Network Hardware Security Modules or Amazon CloudHSM service. The key management and cryptographic functionalities provided by Gemalto SafeNet KeySecure are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

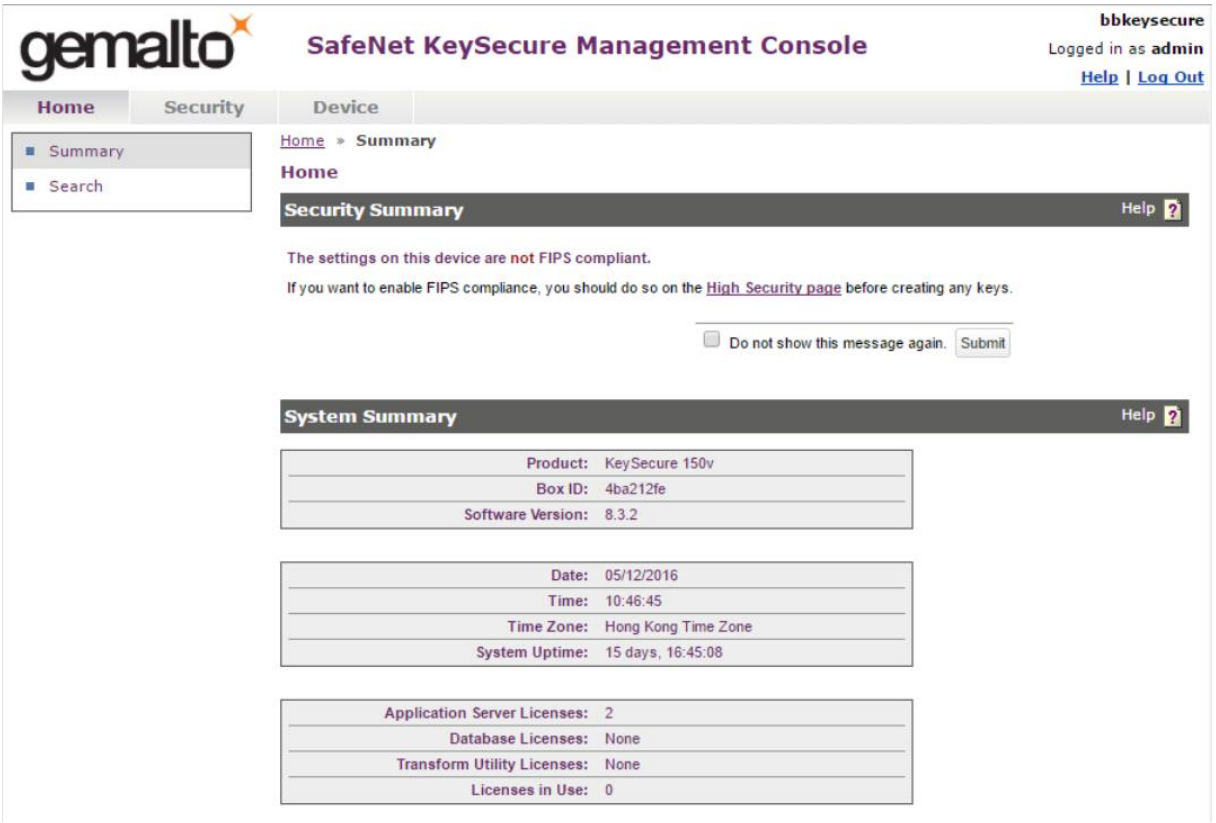
## Gemalto SafeNet KeySecure Configurations

Assume Gemalto SafeNet KeySecure is installed and configured as a network attached appliance with IP address 192.168.10.50.

Gemalto SafeNet KeySecure can be managed remotely via web-based management console.


gemalto
SafeNet KeySecure Management Console
Administrator Authentication
Username:
Password:
Log In

Once logged in, basic information of Gemalto SafeNet KeySecure is shown.



The settings on this device are not FIPS compliant.

If you want to enable FIPS compliance, you should do so on the High Security page before creating any keys.

□ Do not show this message again. Submit

| | |
|---|---|
| Product: | KeySecure 150v |
| Box ID: | 4ba212fe |
| Software Version: | 8.3.2 |

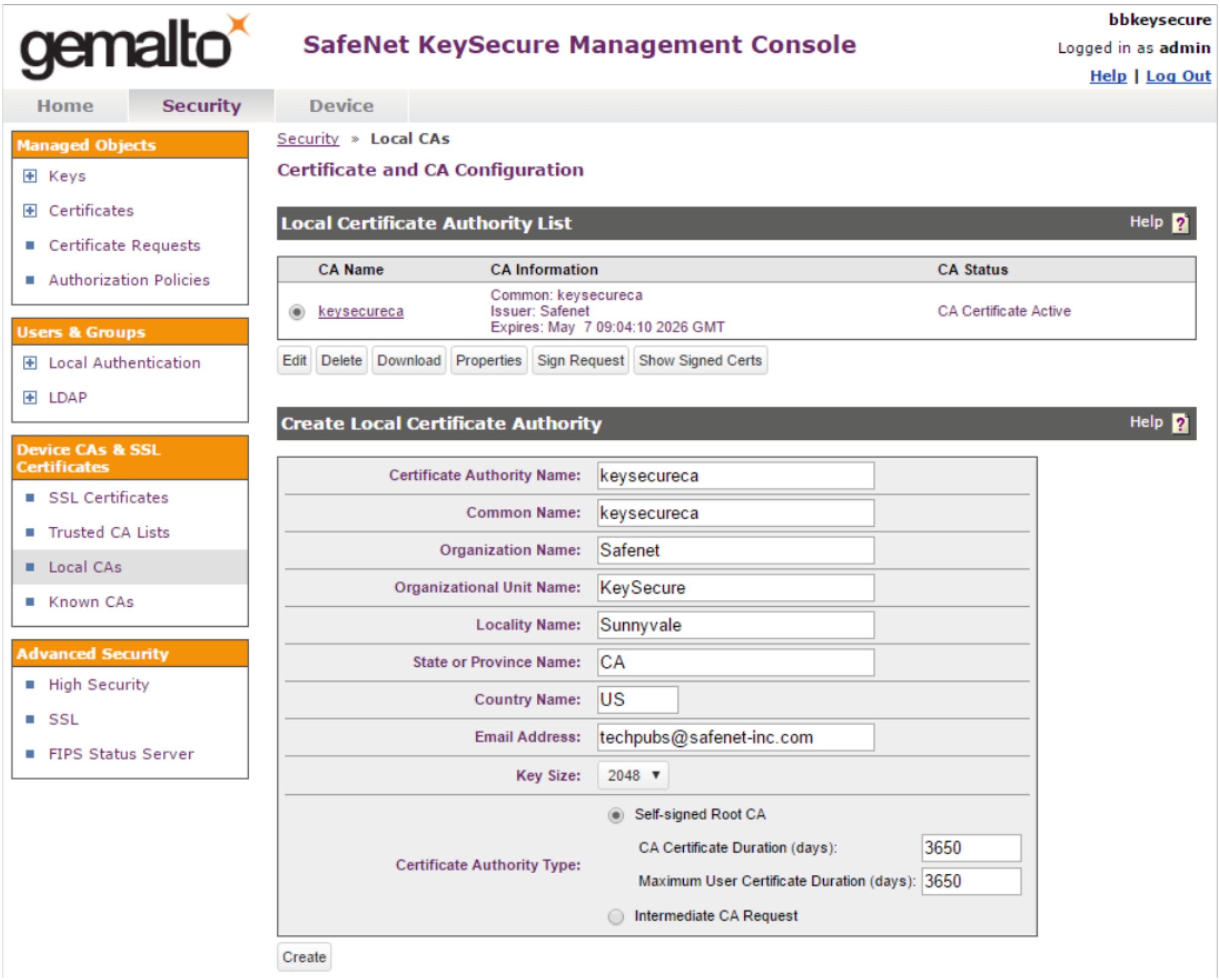
| | |
|---|---|
| Date: | 05/12/2016 |
| Time: | 10:46:45 |
| Time Zone: | Hong Kong Time Zone |
| System Uptime: | 15 days, 16:45:08 |

| | |
|---|---|
| Application Server Licenses: | 2 |
| Database Licenses: | None |
| Transform Utility Licenses: | None |
| Licenses in Use: | 0 |

Gemalto SafeNet KeySecure can be configured to support a hardware root of trust using SafeNet Network HSM or the Amazon CloudHSM service to achieve FIPS compliant.

To authenticate the communication between Gemalto SafeNet KeySecure and Bloombase StoreSafe, signed certificates need to be created and stored in the Gemalto SafeNet KeySecure and the Bloombase StoreSafe. In the Gemalto SafeNet KeySecure, this is done as follows.

A Self-signed Local Root CA is first created in “Local CAs” of the Gemalto SafeNet KeySecure under the Security tab.



Certificate and CA Configuration

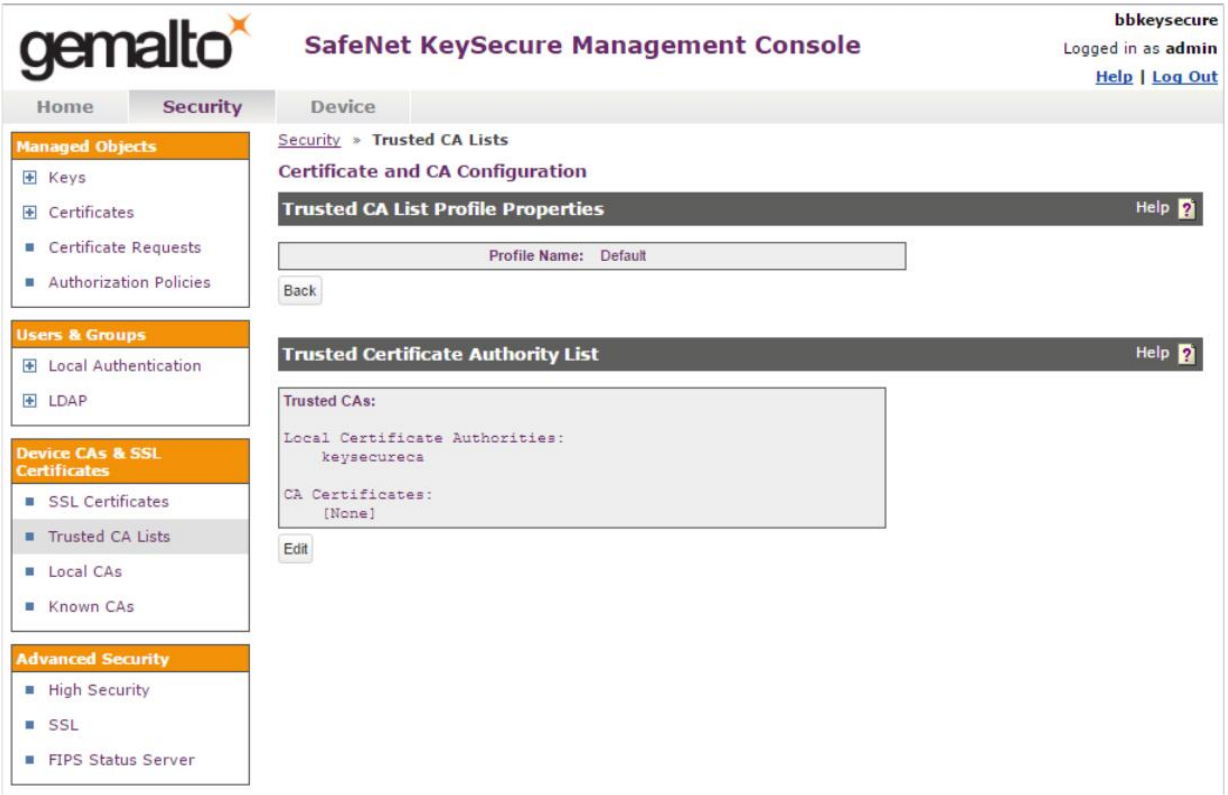
Local Certificate Authority List

| | CA Name | CA Information | CA Status |
|---|---|---|---|
| ● | keysecureca | Common: keysecureca<br>Issuer: Safenet<br>Expires: May 7 09:04:10 2026 GMT | CA Certificate Active |

Create Local Certificate Authority

| | |
|---|---|
| Certificate Authority Name: | keysecureca |
| Common Name: | keysecureca |
| Organization Name: | Safenet |
| Organizational Unit Name: | KeySecure |
| Locality Name: | Sunnyvale |
| State or Province Name: | CA |
| Country Name: | US |
| Email Address: | techpubs@safenet-inc.com |
| Key Size: | 2048 ▼ |
| Certificate Authority Type: | ● Self-signed Root CA<br>CA Certificate Duration (days): 3650<br>Maximum User Certificate Duration (days): 3650<br>○ Intermediate CA Request |

The newly created Local CA is then added to the “Default” trusted CA lists.



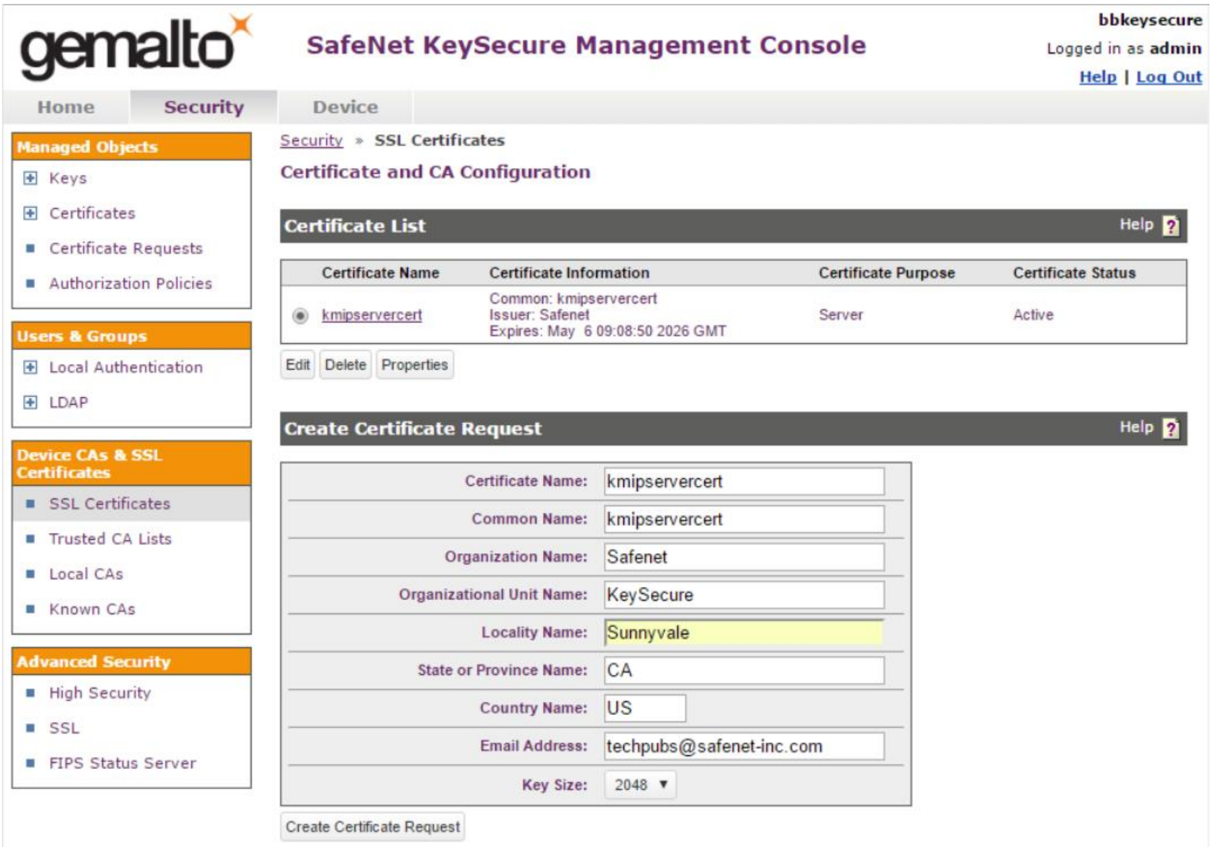
Profile Name: Default

Trusted CAs:

```
Local Certificate Authorities:
    keysecureca

CA Certificates:
    [None]
```

A signed certificate is created for the Gemalto SafeNet KeySecure. This is done by “Create Certificate Request” under “SSL Certificates”.



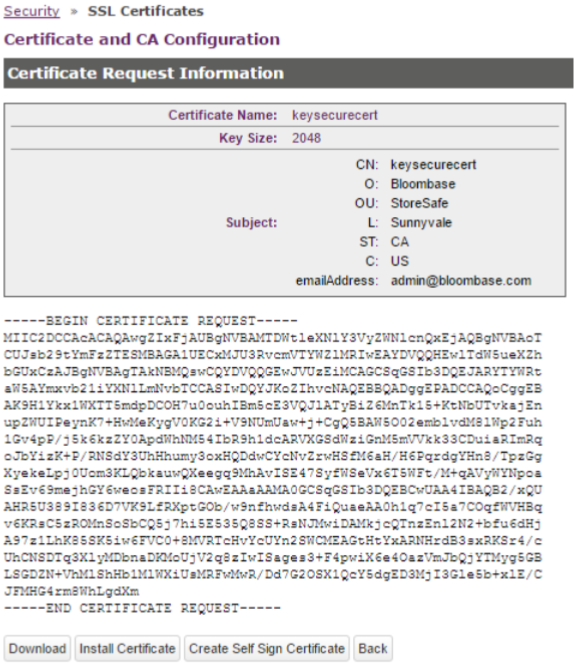
Certificate and CA Configuration

**Certificate List**

| | Certificate Name | Certificate Information | Certificate Purpose | Certificate Status |
|---|---|---|---|---|
| ● | kmipservercert | Common: kmipservercert<br>Issuer: Safenet<br>Expires: May 6 09:08:50 2026 GMT | Server | Active |

**Create Certificate Request**

| | |
|---|---|
| Certificate Name: | kmipservercert |
| Common Name: | kmipservercert |
| Organization Name: | Safenet |
| Organizational Unit Name: | KeySecure |
| Locality Name: | Sunnyvale |
| State or Province Name: | CA |
| Country Name: | US |
| Email Address: | techpubs@safenet-inc.com |
| Key Size: | 2048 ▼ |



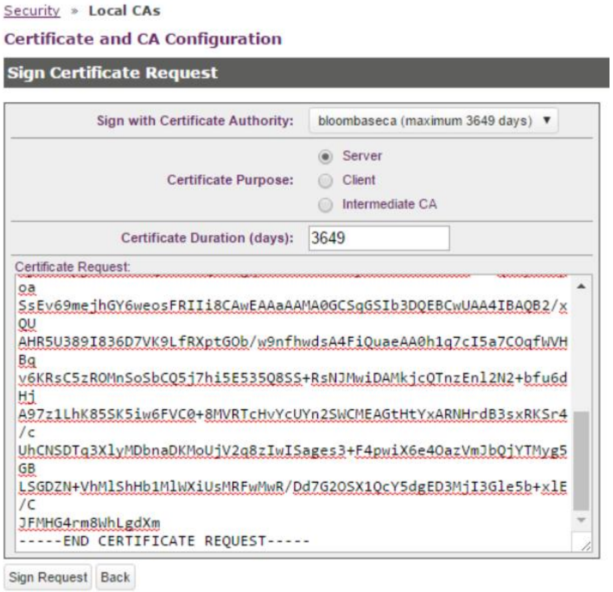
Certificate and CA Configuration

**Certificate Request Information**

| | |
|---|---|
| Certificate Name: | keysecurecert |
| Key Size: | 2048 |
| Subject: | CN: keysecurecert<br>O: Bloombase<br>OU: StoreSafe<br>L: Sunnyvale<br>ST: CA<br>C: US<br>emailAddress: admin@bloombase.com |

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC2DCCAcACAQAwgZIxFjAUBgNVBAMTDWtleXNlY3VyZWNlcnQxEjAQBgNVBAoT
CUJsb29tYmFzZTESMBAGA1UECxMJU3RvcmVTYWZlMRIwEAYDVQQHEwlTdW5ueXZh
bGUxCzAJBgNVBAgTAkNBMQswCQYDVQQGEwJVUzEiMCAGCSqGSIb3DQEJARYTYWRt
aW5AYmxvb21iYXNlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AK9H1Ykx1WXTT5mdpDCOH7u0ouhIBm5cE3VQJ1ATyBiZ6MnTk15+KtNbUTvkajEn
upZWUIPeynK7+HwMeKygV0KG2i+V9NUmUaw+j+CgQ5BAW5O02emblvdM81Wp2Fuh
1Gv4pP/j5k6kzZY0ApdWhNM54IbR9h1dcARVXGSdWziGnM5mVVkk33CDuiaRImRq
oJbYizK+P/RNSdY3UhHhumy3oxHQDdwCYcNvZrwHSfM6aH/H6PqrdgYHn8/TpzGg
XyekeLpj0Uom3KLQbkauwQXeegq9MhAvISE47SyfWSeVx6T5WFt/M+qAVyWYNpoa
SsEv69mejhGY6weosFRIIi8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQB2/xQU
AHR5U389I836D7VK9LfRXptGOb/w9nfhwdsA4FiQuaeAA0h1q7cI5a7COqfWVHBq
v6KRsC5zROMnSoSbCQ5j7hi5E535Q8SS+RsNJMwiDAMkjcQTnzEn12N2+bfu6dHj
A97z1LhK85SK5iw6FVC0+8MVRTcHvYcUYn2SWCMEAGtHtYxARNHrdB3sxRKSr4/c
UhCNSDTq3XlyMDbnaDKMoUjV2q8zIwISages3+F4pwiX6e4OazVmJbQjYTMyg5GB
LSGDZN+VhMlShHb1MlWXiUsMRFwMwR/Dd7G2OSX1QcY5dgED3MjI3Gle5b+x1E/C
JFMHG4rm8WhLgdXm
-----END CERTIFICATE REQUEST-----
```

And then use the created Local CA to sign the request.



Security » Local CAs

Certificate and CA Configuration

Sign Certificate Request

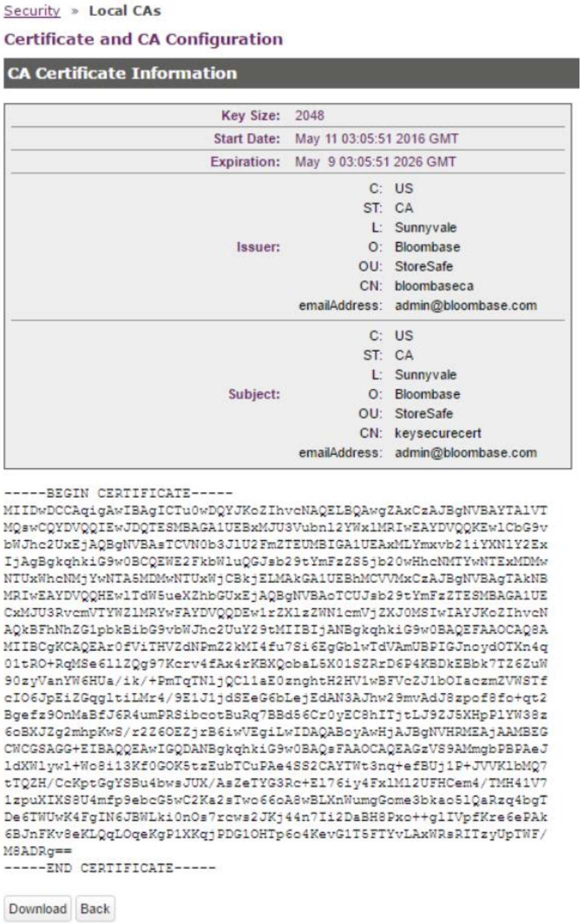
Sign with Certificate Authority: bloombaseca (maximum 3649 days) ▼

Certificate Purpose: ● Server ○ Client ○ Intermediate CA

Certificate Duration (days): 3649

Certificate Request:

```
oa
SsEv69mejhGY6weosFRIIi8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQB2/x
QU
AHR5U389I836D7VK9LfRXptGOb/w9nfhwdsA4FiQuaeAA0h1q7cI5a7COqfWVH
Bq
v6KRsC5zROMnSoSbCQ5j7hi5E535Q8SS+RsNJMwiDAMkjcQTnzEnl2N2+bfu6d
Hj
A97z1LhK85SK5iw6FVC0+8MVRTcHvYcUYn2SWCMEAGtHtYxARNHrdB3sxRKSr4
/c
UhCNSDTq3XlyMDbnaDKMoUjV2q8zIwISages3+F4pwiX6e4OazVmJbQjYTMyg5
GB
LSGDZN+VhMlShHb1MlWXiUsMRFwMwR/Dd7G2OSX1QcY5dgED3MjI3Gle5b+xlE
/C
JFMHG4rm8WhLgdXm
-----END CERTIFICATE REQUEST-----
```



Security » Local CAs

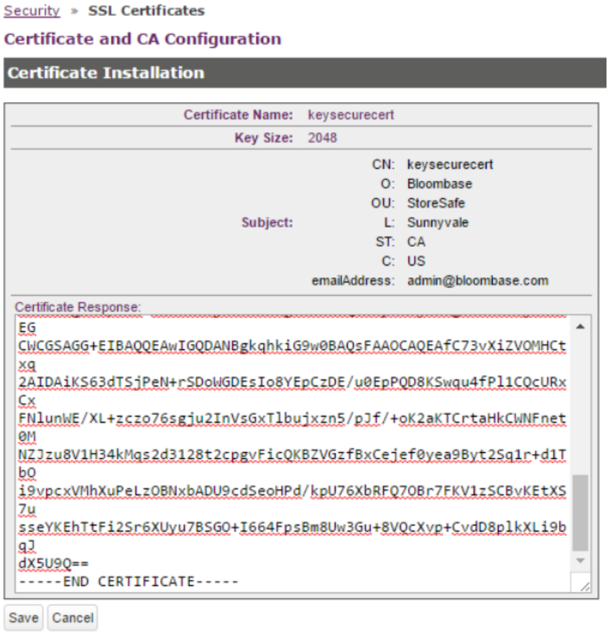
Certificate and CA Configuration

CA Certificate Information

| | | |
|---|---|---|
| Key Size: | 2048 | |
| Start Date: | May 11 03:05:51 2016 GMT | |
| Expiration: | May 9 03:05:51 2026 GMT | |
| Issuer: | C: | US |
| | ST: | CA |
| | L: | Sunnyvale |
| | O: | Bloombase |
| | OU: | StoreSafe |
| | CN: | bloombaseca |
| | emailAddress: | admin@bloombase.com |
| Subject: | C: | US |
| | ST: | CA |
| | L: | Sunnyvale |
| | O: | Bloombase |
| | OU: | StoreSafe |
| | CN: | keysecurecert |
| | emailAddress: | admin@bloombase.com |

```
-----BEGIN CERTIFICATE-----
MIIDwDCCAqigAwIBAgICTu0wDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJDQTESMBAGA1UEBxMJU3Vubnl2YWxlMRIwEAYDVQQKEwlCbG9v
bWJhc2UxEjAQBgNVBAsTCVN0b3JlU2FmZTEUMBIGA1UEAxMLYmxvb21iYXNlY2Ex
IjAgBgkqhkiG9w0BCQEWE2FkbWluQGJsb29tYmFzZS5jb20wHhcNMTYwNTExMDMw
NTUxWhcNMjYwNTA5MDMwNTUxWjCBkjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNB
MRIwEAYDVQQHEwlTdW5ueXZhbGUxEjAQBgNVBAoTCUJsb29tYmFzZTESMBAGA1UE
CxMJU3RvcmVTYWZlMRYwFAYDVQQDEw1rZXlzZWN1cmVjZXJ0MSIwIAYJKoZIhvcN
AQkBFhNhZG1pbkBibG9vbWJhc2UuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAr0fViTHVZdNPmZ2kMI4fu7Si6EgGblwTdVAmUBPIGJnoydOTXn4q
01tRO+RqMSe6llZQg97Kcrv4fAx4rKBXQobaL5X01SZRrD6P4KBDkEBbk7TZ6ZuW
90zyVanYW6HUa/ik/+PmTqTNljQCl1aE0znghtH2HV1wBFVcZJ1bOIaczmZVWSTf
cIO6JpEiZGqgltiLMr4/9E1J1jdSEeG6bLejEdAN3AJhw29mvAdJ8zpof8fo+qt2
Bgefz9OnMaBfJ6R4umPRSibcotBuRq7BBd56Cr0yEC8hITjtLJ9ZJ5XHpPlYW38z
6oBXJZg2mhpKwS/r2Z6OEZjrB6iwVEgiLwIDAQABoyAwHjAJBgNVHRMEAjAAMBEG
CWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEAGzVS9AMmgbPBPAeJ
ldXWlywl+Wo8i13Kf0GOK5tzEubTCuPAe4SS2CAYTWt3nq+efBUj1P+JVVKlbMQ7
tTQZH/CcKptGgYSBu4bwsJUX/AsZeTYG3Rc+El76iy4FxlMl2UFHCem4/TMH41V7
1zpuXIXS8U4mfp9ebcG5wC2Ka2sTwo66oA8wBLXnWumgGome3bkao51QaRzq4bgT
De6TWUwK4FgIN6JBWLki0nOs7rcws2JKj44n7Ii2DaBH8Pxo++glIVpfKre6ePAk
6BJnFKv8eKLQqLOqeKgPlXKqjPDG1OHTp6o4KevG1T5FTYvLAxWRsRITzyUpTWF/
M8ADRg==
-----END CERTIFICATE-----
```

And have the signed certificate saved under the Certificate List.



Certificate Name: keysecurecert

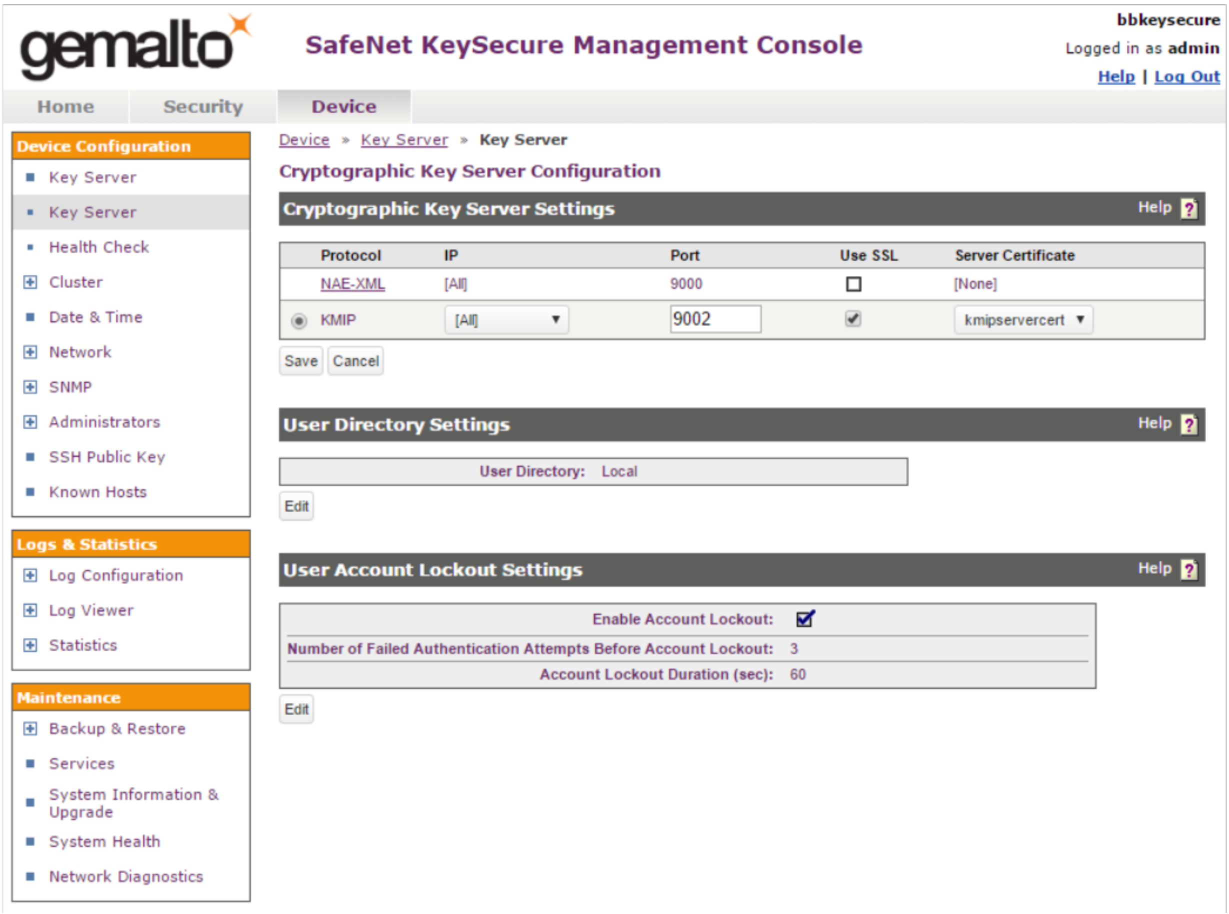
Key Size: 2048

Subject:
CN: keysecurecert
O: Bloombase
OU: StoreSafe
L: Sunnyvale
ST: CA
C: US
emailAddress: admin@bloombase.com

Certificate Response:

```
EG
CWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQsFAAOCAQEAfC73vXiZVOMHCt
xq
2AIDAiKS63dTSjPeN+rSDoWGDEsIo8YEpCzDE/u0EpPQD8KSwqu4fPl1CQcURx
Cx
FNlunWE/XL+zczo76sgju2InVsGxTlbujxzn5/pJf/+oK2aKTCrtaHkCWNFnet
0M
NZJzu8V1H34kMqs2d3128t2cpgvFicQKBZVGzfBxCejef0yea9Byt2Sq1r+d1T
bO
i9vpcxVMhXuPeLzOBNxbADU9cdSeoHPd/kpU76XbRFQ7OBr7FKV1zSCBvKEtXS
7u
sseYKEhTtFi2Sr6XUyu7BSGO+I664FpsBm8Uw3Gu+8VQcXvp+CvdD8plkXLi9b
qJ
dX5U9Q==
-----END CERTIFICATE-----
```

We can then configure the Gemalto SafeNet KeySecure to enable KMIP with the newly created signed server cert.



Cryptographic Key Server Configuration

Cryptographic Key Server Settings

| | Protocol | IP | Port | Use SSL | Server Certificate |
|---|---|---|---|---|---|
| | NAE-XML | [All] | 9000 | □ | [None] |
| ● | KMIP | [All] ▼ | 9002 | ☑ | kmipservercert ▼ |

Save Cancel

User Directory Settings

User Directory: Local

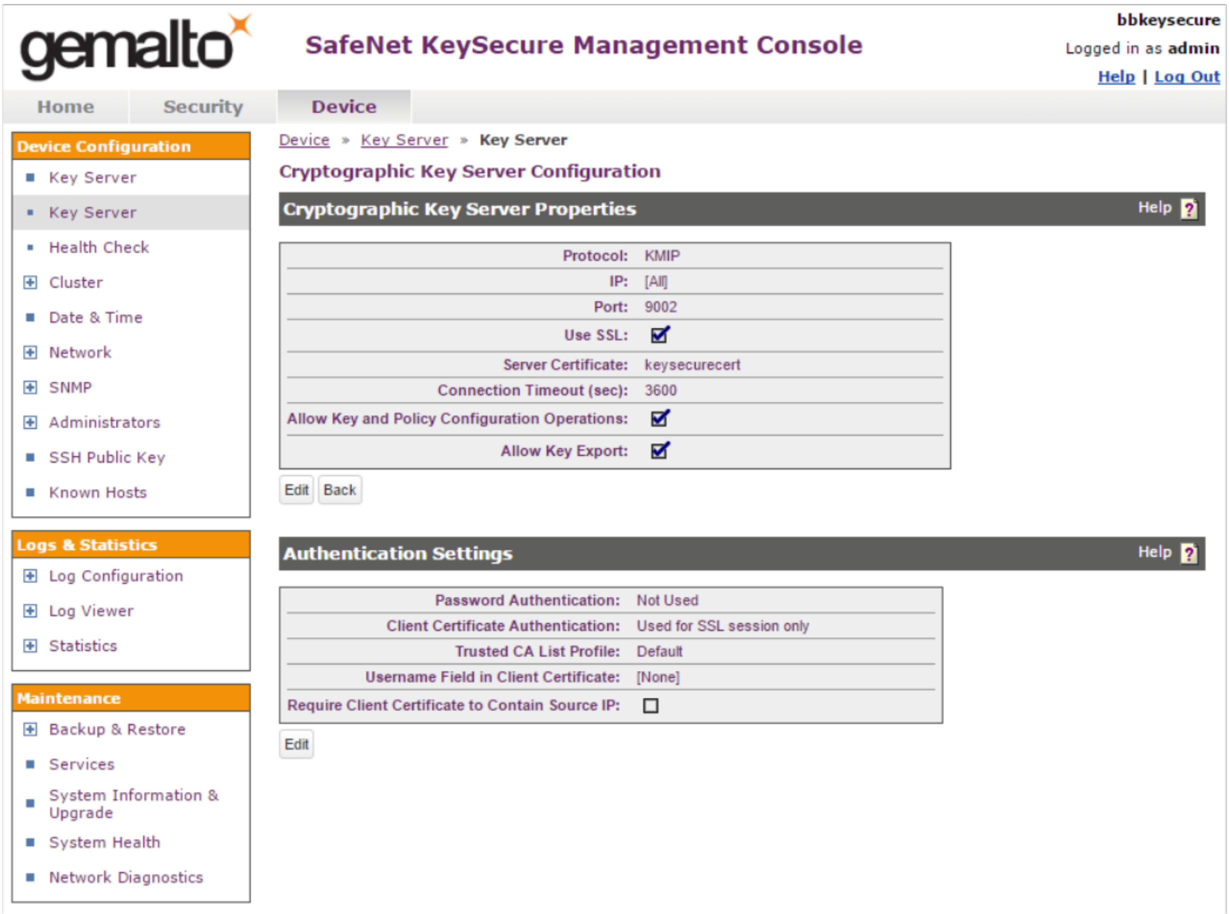
Edit

User Account Lockout Settings

| | |
|---|---|
| Enable Account Lockout: | ☑ |
| Number of Failed Authentication Attempts Before Account Lockout: | 3 |
| Account Lockout Duration (sec): | 60 |

Edit

Edit the authentication settings of the Cryptographic Key Server Settings, “Client Certificate Authentication” to be “Used for SSL session only” and “Trusted CA List Profile” as “Default”.



Cryptographic Key Server Configuration

Cryptographic Key Server Properties

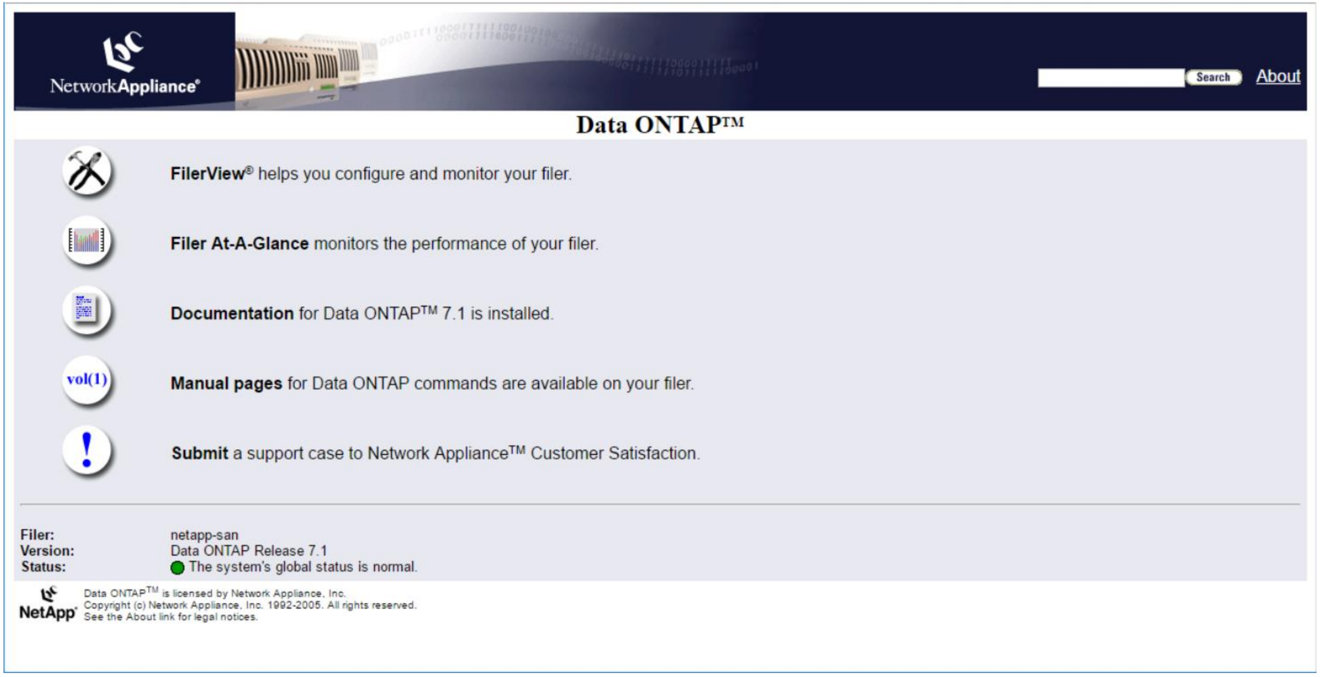
| | |
|---|---|
| Protocol: | KMIP |
| IP: | [All] |
| Port: | 9002 |
| Use SSL: | ☑ |
| Server Certificate: | keysecurecert |
| Connection Timeout (sec): | 3600 |
| Allow Key and Policy Configuration Operations: | ☑ |
| Allow Key Export: | ☑ |

Authentication Settings

| | |
|---|---|
| Password Authentication: | Not Used |
| Client Certificate Authentication: | Used for SSL session only |
| Trusted CA List Profile: | Default |
| Username Field in Client Certificate: | [None] |
| Require Client Certificate to Contain Source IP: | □ |

# NetApp FAS Storage

NetApp FAS virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.



Data ONTAP™

**FilerView**® helps you configure and monitor your filer.

**Filer At-A-Glance** monitors the performance of your filer.

**Documentation** for Data ONTAP™ 7.1 is installed.

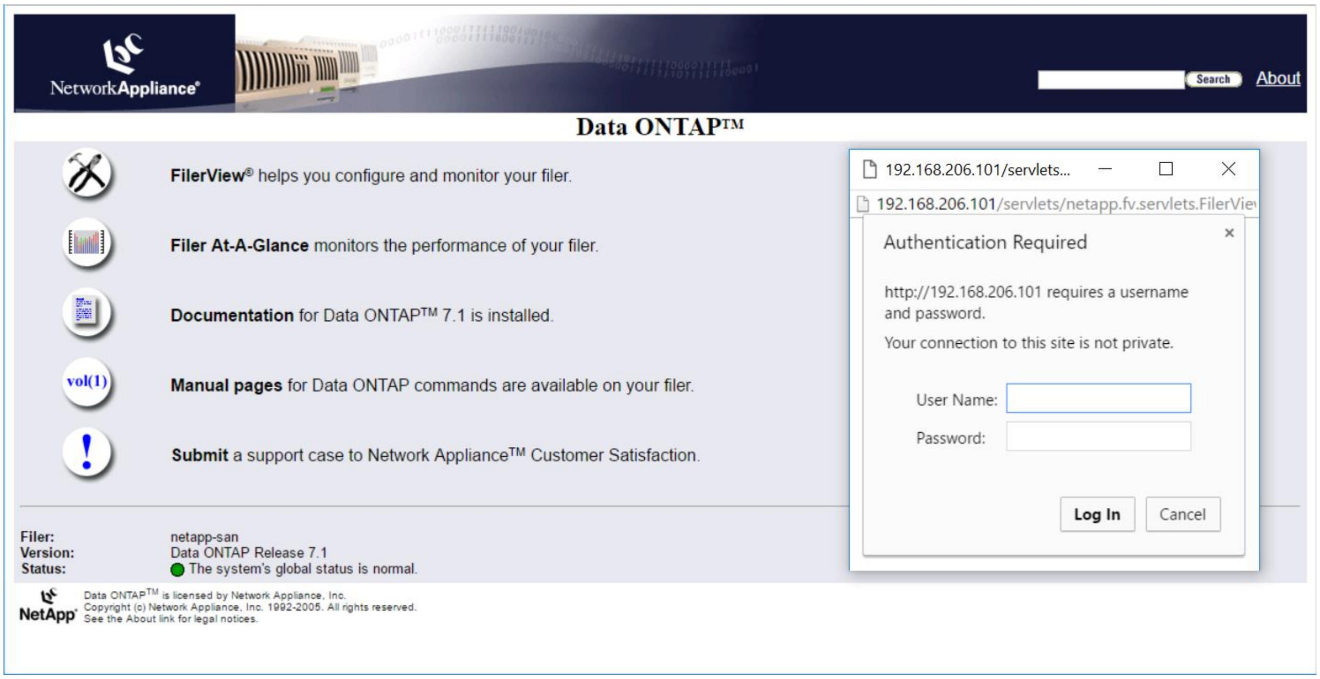
**Manual pages** for Data ONTAP commands are available on your filer.

**Submit** a support case to Network Appliance™ Customer Satisfaction.

| | |
|---|---|
| **Filer:** | netapp-san |
| **Version:** | Data ONTAP Release 7.1 |
| **Status:** | ● The system's global status is normal. |

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc.
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.
See the About link for legal notices.

NetApp FAS is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FC, FCoE, iSCSI, etc.



Data ONTAP™

**FilerView**® helps you configure and monitor your filer.

**Filer At-A-Glance** monitors the performance of your filer.

**Documentation** for Data ONTAP™ 7.1 is installed.

**Manual pages** for Data ONTAP commands are available on your filer.

**Submit** a support case to Network Appliance™ Customer Satisfaction.

| | |
|---|---|
| **Filer:** | netapp-san |
| **Version:** | Data ONTAP Release 7.1 |
| **Status:** | ● The system's global status is normal. |

NetApp® Data ONTAP™ is licensed by Network Appliance, Inc.
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.
See the About link for legal notices.

192.168.206.101/servlets...

192.168.206.101/servlets/netapp.fv.servlets.FilerVie

Authentication Required

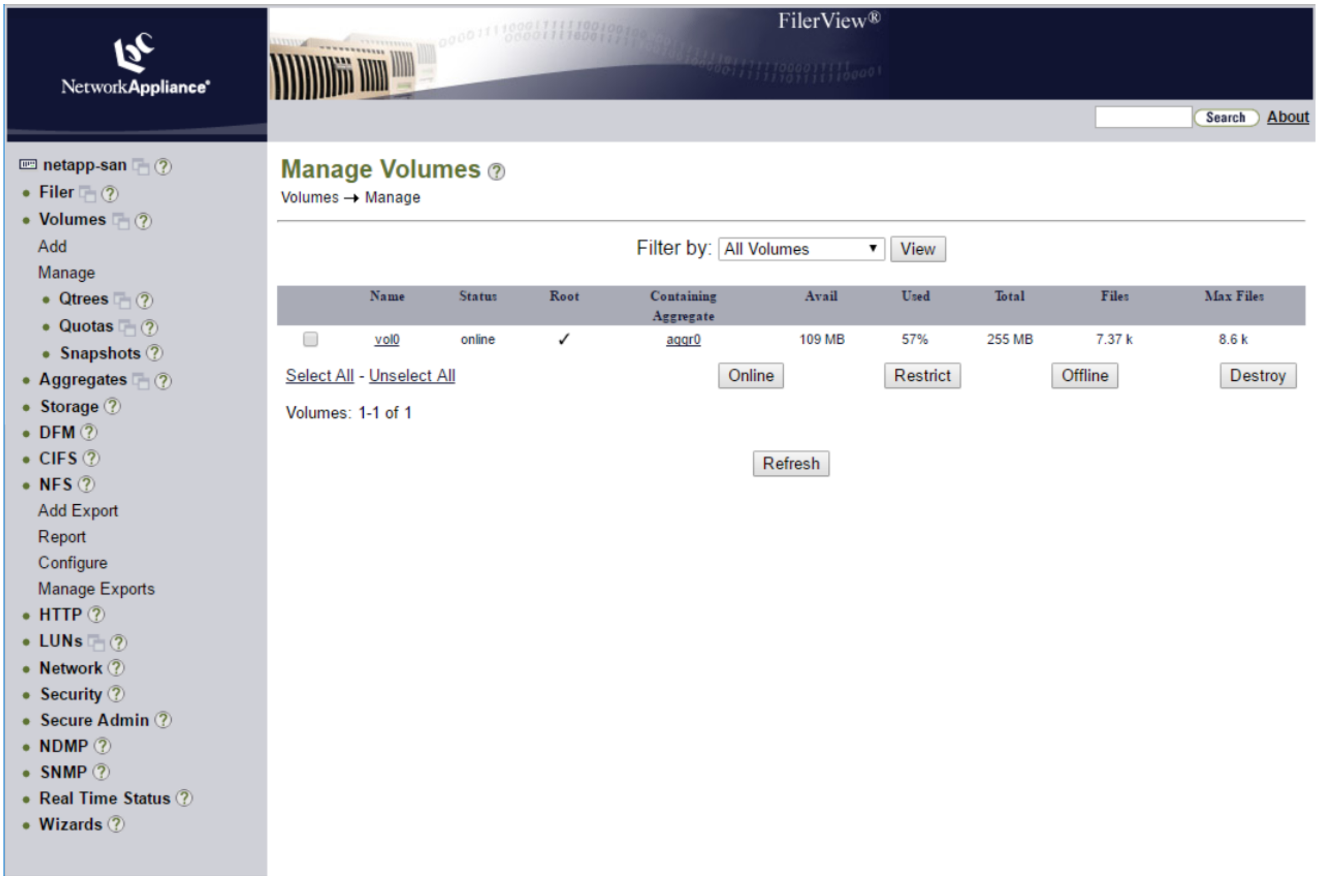
http://192.168.206.101 requires a username and password.

Your connection to this site is not private.

User Name:

Password:

CIFS and NFS storage resources are provisioned on NetApp FAS to be used in this testing.



Manage Volumes

Volumes → Manage

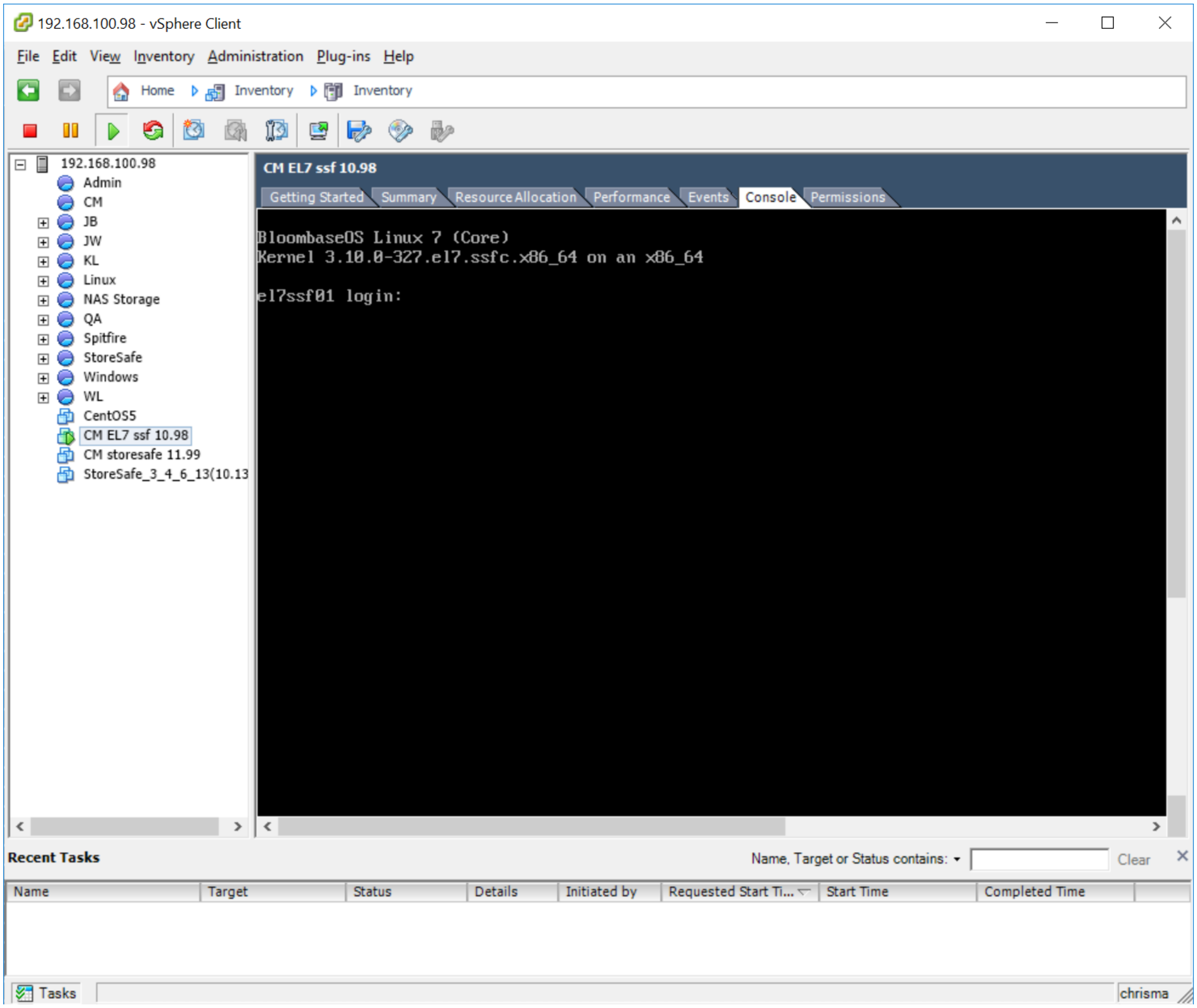
Filter by: All Volumes

| | Name | Status | Root | Containing Aggregate | Avail | Used | Total | Files | Max Files |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | vol0 | online | ✓ | aggr0 | 109 MB | 57% | 255 MB | 7.37 k | 8.6 k |

Volumes: 1-1 of 1

# Bloombase StoreSafe

Bloombase StoreSafe delivers unified data-at-rest encryption security of block storage volumes, files, objects, sequential storage devices, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Gemalto SafeNet KeySecure.



```
BloombaseOS Linux 7 (Core)
Kernel 3.10.0-327.el7.ssfc.x86_64 on an x86_64

el7ssf01 login:
```

Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware ESXi.

## Network Security, Trust and Authentication Configuration

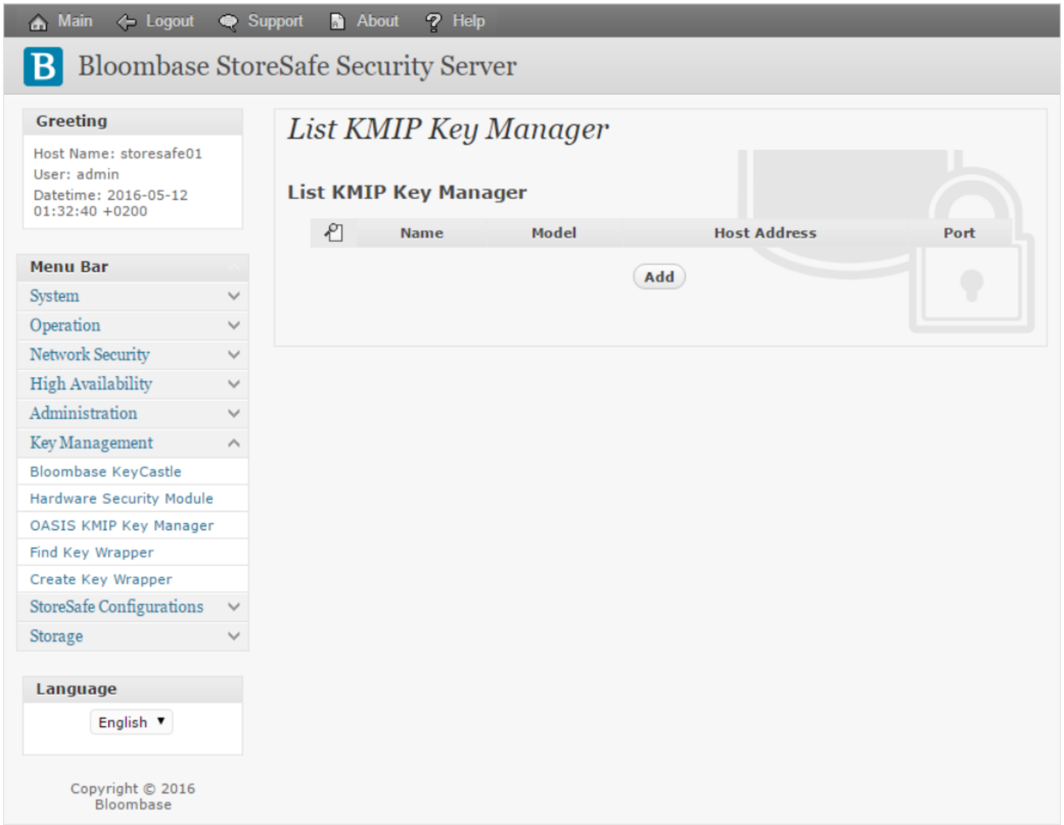
In this interoperability test effort, Bloombase StoreSafe serves as the user of Gemalto SafeNet KeySecure for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Gemalto SafeNet KeySecure is done with signed certificates through SSL communications.

## Gemalto SafeNet KeySecure and Bloombase KeyCastle Integration

Bloombase supports Gemalto SafeNet KeySecure out of the box due to the fact that both support OASIS Key Management Interoperability Protocol (KMIP).

X.509 key pair “CN=bloombaseca, OU=StoreSafe, O=Bloombase, L=Sunnyvale, ST=CA, C=US” is created, signed by the newly created local root CA in the Gemalto SafeNet KeySecure, and assigned as the authentication key pair for Bloombase StoreSafe.

To enable the built-in Bloombase KeyCastle to utilize keys managed in the network attached Gemalto SafeNet KeySecure, 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”.



Greeting

Host Name: storesafe01
User: admin
Datetime: 2016-05-12 01:32:40 +0200

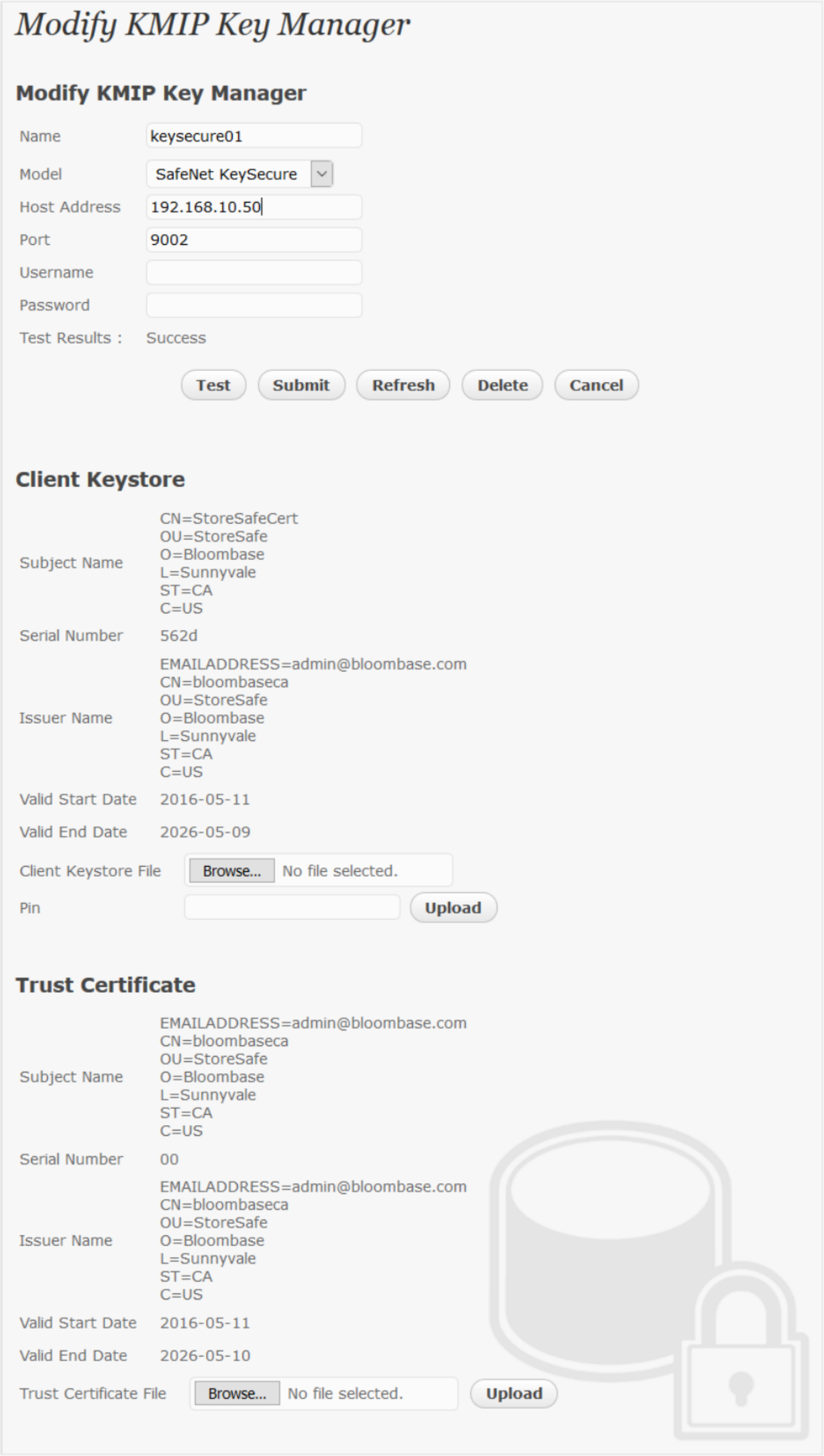
List KMIP Key Manager

List KMIP Key Manager

| | Name | Model | Host Address | Port |
|---|---|---|---|---|

Copyright © 2016 Bloombase

Input a name for the Gemalto SafeNet KeySecure, and select Model as 'SafeNet KeySecure'. Input also the host address and port to access the SafeNet KeySecure, and import the signed X.509 key pair as "Client Keystore", the certificate of the local root CA on Gemalto SafeNet KeySecure as "Trust Certificate".



*Modify KMIP Key Manager*

**Modify KMIP Key Manager**

| | |
|---|---|
| Name | keysecure01 |
| Model | SafeNet KeySecure |
| Host Address | 192.168.10.50 |
| Port | 9002 |
| Username | |
| Password | |
| Test Results : | Success |

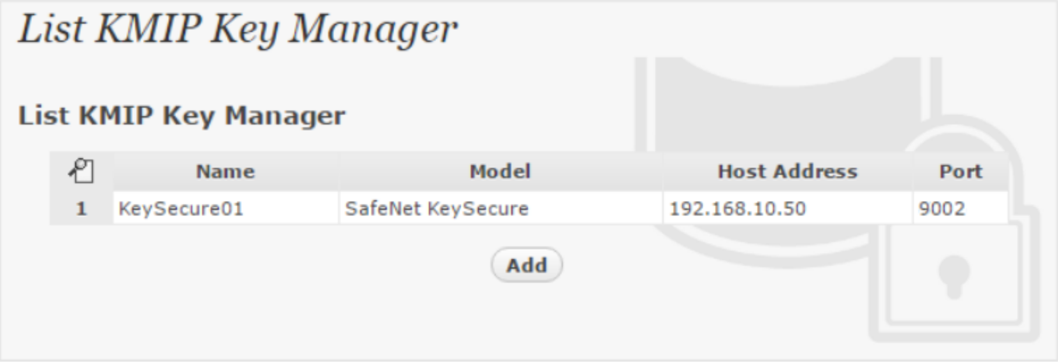
**Client Keystore**

| | |
|---|---|
| Subject Name | CN=StoreSafeCert<br>OU=StoreSafe<br>O=Bloombase<br>L=Sunnyvale<br>ST=CA<br>C=US |
| Serial Number | 562d |
| Issuer Name | EMAILADDRESS=admin@bloombase.com<br>CN=bloombaseca<br>OU=StoreSafe<br>O=Bloombase<br>L=Sunnyvale<br>ST=CA<br>C=US |
| Valid Start Date | 2016-05-11 |
| Valid End Date | 2026-05-09 |
| Client Keystore File | Browse... No file selected. |
| Pin | |

**Trust Certificate**

| | |
|---|---|
| Subject Name | EMAILADDRESS=admin@bloombase.com<br>CN=bloombaseca<br>OU=StoreSafe<br>O=Bloombase<br>L=Sunnyvale<br>ST=CA<br>C=US |
| Serial Number | 00 |
| Issuer Name | EMAILADDRESS=admin@bloombase.com<br>CN=bloombaseca<br>OU=StoreSafe<br>O=Bloombase<br>L=Sunnyvale<br>ST=CA<br>C=US |
| Valid Start Date | 2016-05-11 |
| Valid End Date | 2026-05-10 |
| Trust Certificate File | Browse... No file selected. |

Click ‘Submit’ to commit the configuration. If the certificates are setup properly, “test results” of the KMIP Key Manager would return “Success”.



List KMIP Key Manager

List KMIP Key Manager

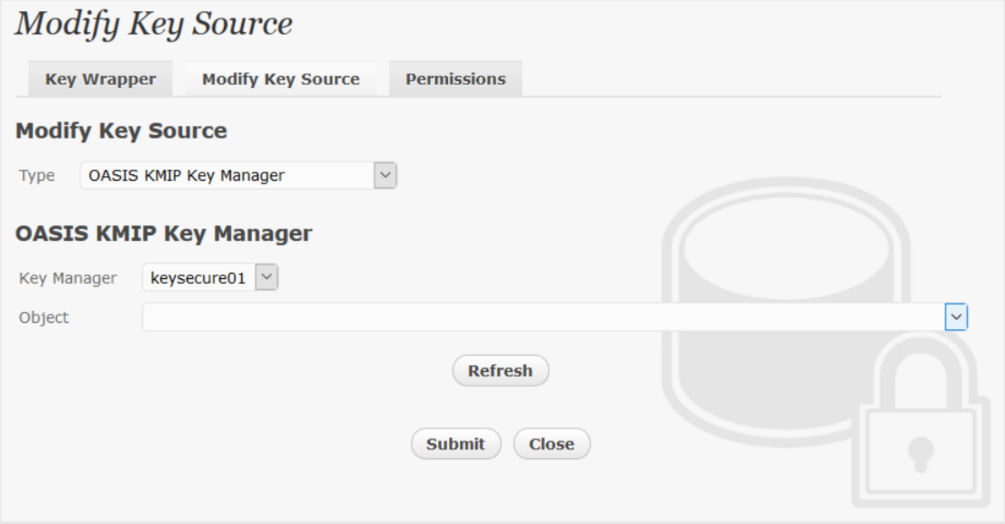
| | Name | Model | Host Address | Port |
|---|---|---|---|---|
| 1 | KeySecure01 | SafeNet KeySecure | 192.168.10.50 | 9002 |

## Encryption Key Provisioning

Generate encryption key with name ‘key01’ in bundled Bloombase KeyCastle key life-cycle management tool.

First configure the key source of the wrapping key as “OASIS KMIP Key Manager” with Gemalto SafeNet KeySecure as the “Key Manager”.

If the encryption key is present in the Gemalto SafeNet KeySecure, select it from the dropdown menu of “Object” and click “submit”.



Modify Key Source

Modify Key Source

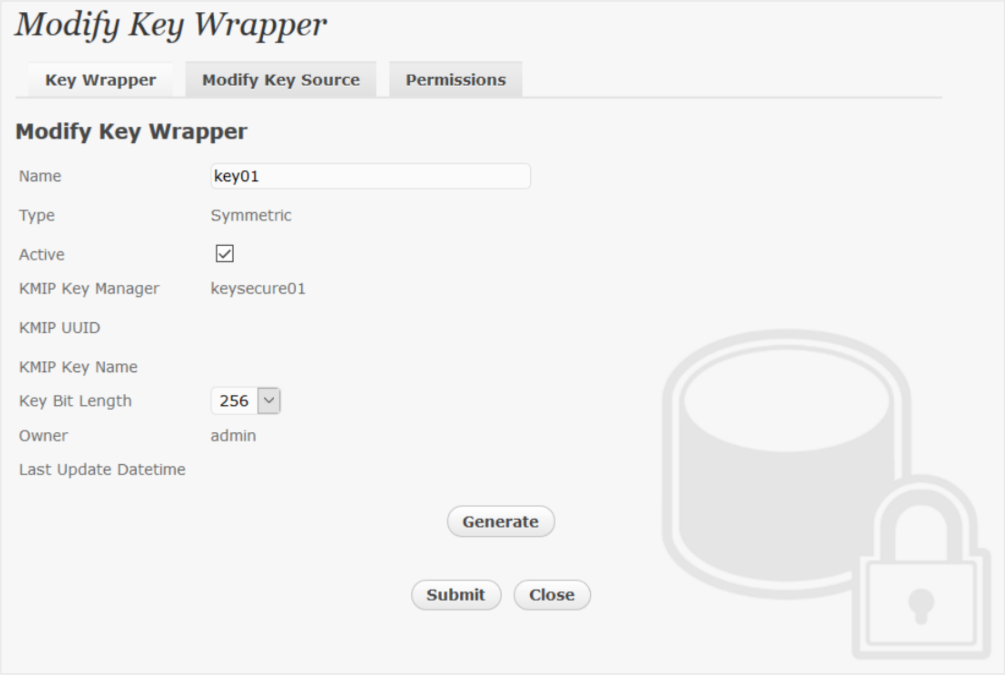
Type: OASIS KMIP Key Manager

OASIS KMIP Key Manager

Key Manager: keysecure01

Object:

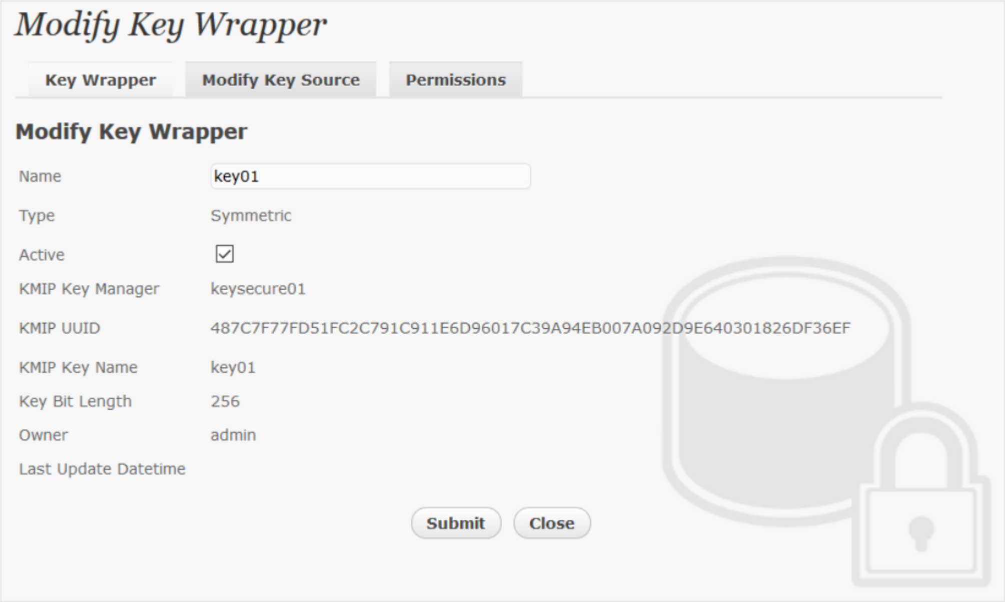
Otherwise, in order to generate the key in the attached Gemalto SafeNet KeySecure, leave the "Object" field as empty and turn to the "Key Wrapper" tab to input the name of the key and click 'Generate'.



Modify Key Wrapper

| | |
|---|---|
| Name | key01 |
| Type | Symmetric |
| Active | ☑ |
| KMIP Key Manager | keysecure01 |
| KMIP UUID | |
| KMIP Key Name | |
| Key Bit Length | 256 |
| Owner | admin |
| Last Update Datetime | |

The key is then generated in the attached Gemalto SafeNet KeySecure.



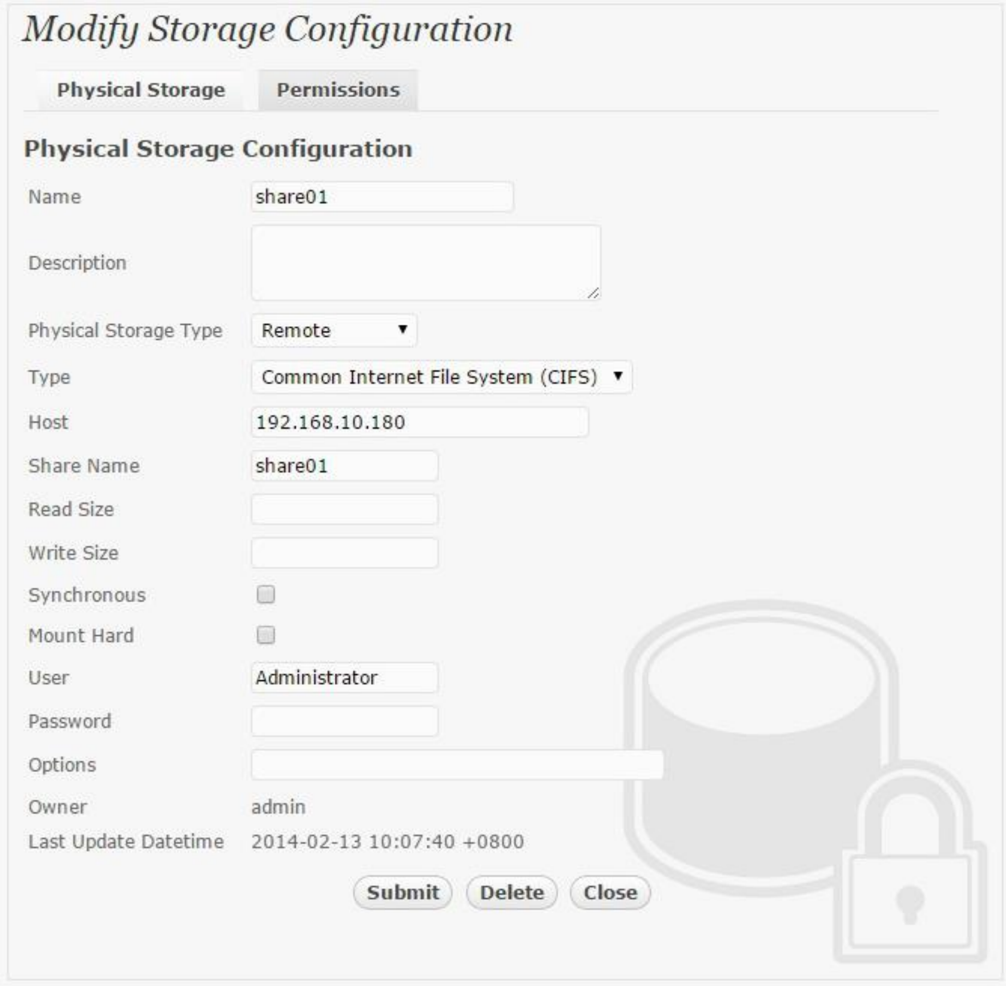
Modify Key Wrapper

| | |
|---|---|
| Name | key01 |
| Type | Symmetric |
| Active | ☑ |
| KMIP Key Manager | keysecure01 |
| KMIP UUID | 487C7F77FD51FC2C791C911E6D96017C39A94EB007A092D9E640301826DF36EF |
| KMIP Key Name | key01 |
| Key Bit Length | 256 |
| Owner | admin |
| Last Update Datetime | |

Notice that only symmetric keys are generated and accessed through KMIP Key Managers.

## Backend Physical Storage Configuration

Physical storage namely ‘share01’ is configured to be secured by Bloombase StoreSafe using encryption.



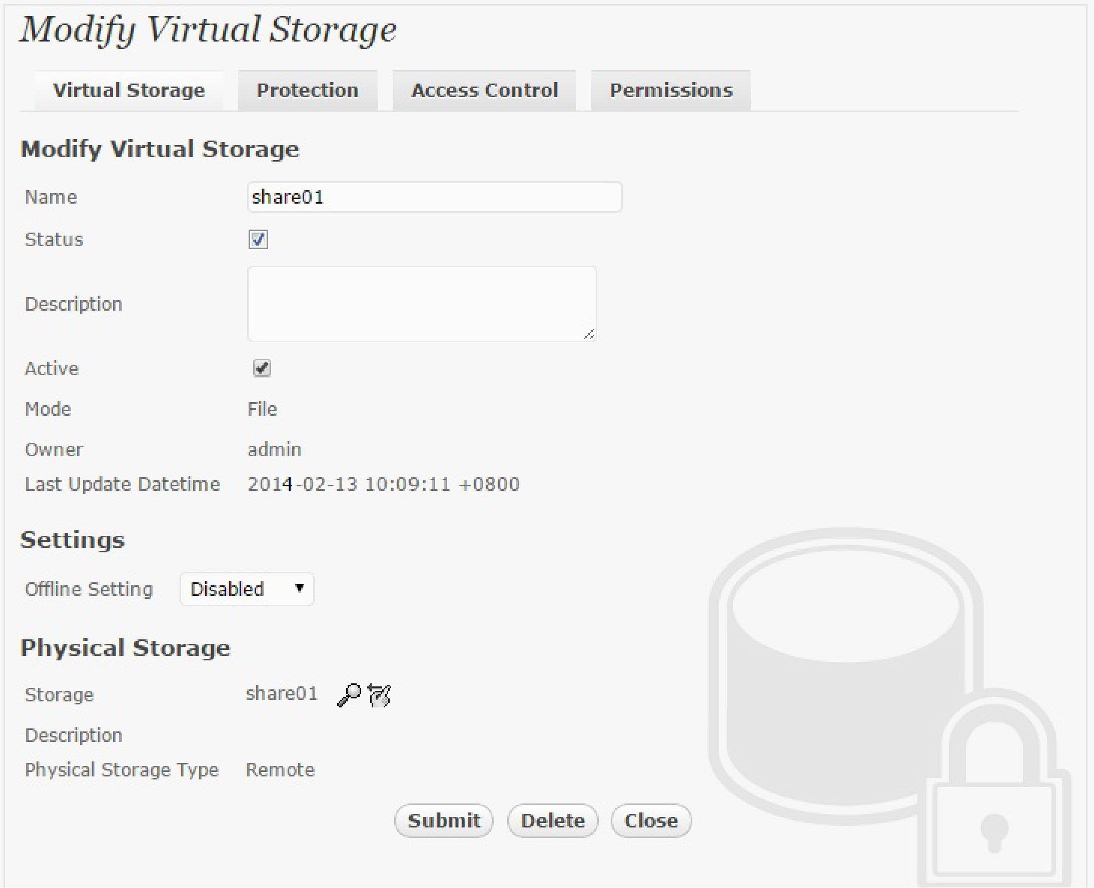
*Modify Storage Configuration*

**Physical Storage Configuration**

| | |
|---|---|
| Name | share01 |
| Description | |
| Physical Storage Type | Remote ▼ |
| Type | Common Internet File System (CIFS) ▼ |
| Host | 192.168.10.180 |
| Share Name | share01 |
| Read Size | |
| Write Size | |
| Synchronous | □ |
| Mount Hard | □ |
| User | Administrator |
| Password | |
| Options | |
| Owner | admin |
| Last Update Datetime | 2014-02-13 10:07:40 +0800 |

## Secure Storage Configuration

Virtual storage namely ‘share01’ of type ‘File’ is created to virtualize physical storage ‘share01’ for application transparent encryption protection over network file protocols including CIFS and NFS.


*Modify Virtual Storage*

**Modify Virtual Storage**

| | |
|---|---|
| Name | share01 |
| Status | ☑ |
| Description | |
| Active | ☑ |
| Mode | File |
| Owner | admin |
| Last Update Datetime | 2014-02-13 10:09:11 +0800 |

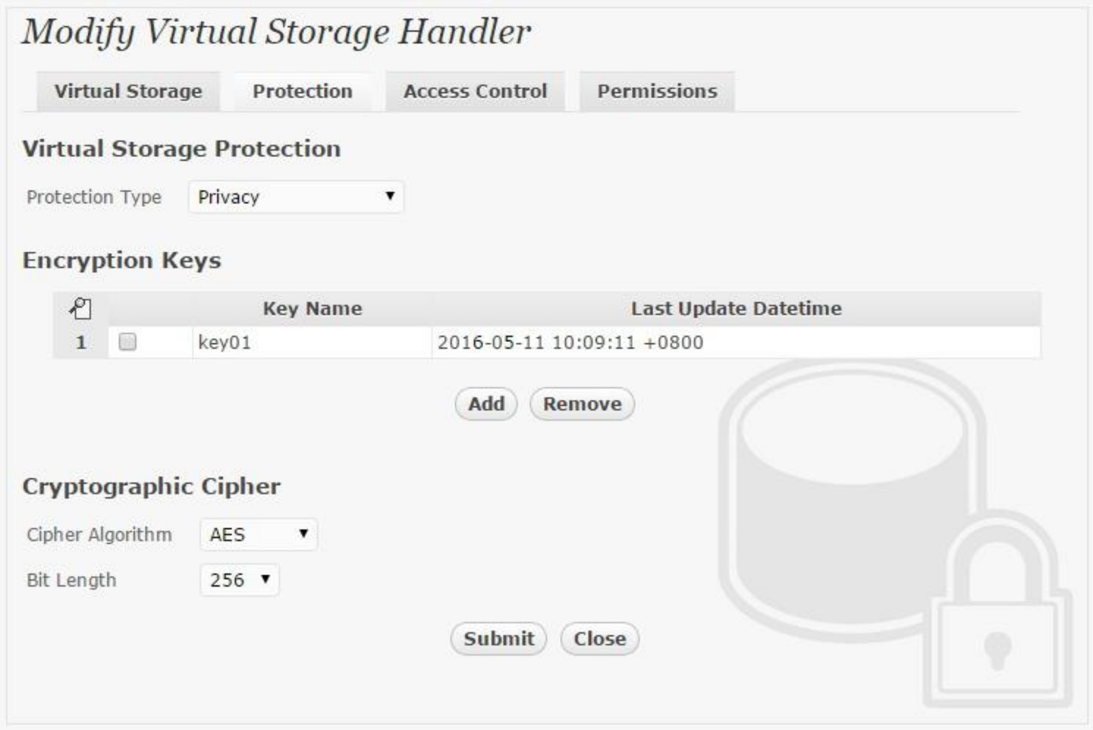
**Settings**

| | |
|---|---|
| Offline Setting | Disabled ▾ |

**Physical Storage**

| | |
|---|---|
| Storage | share01 |
| Description | |
| Physical Storage Type | Remote |

Protection type is specified as ‘Privacy’ and secure the backend EMC VNX storage using AES 256-bit encryption and encryption key ‘key01’ managed at Gemalto SafeNet KeySecure.



*Modify Virtual Storage Handler*

**Virtual Storage Protection**

Protection Type: Privacy

**Encryption Keys**

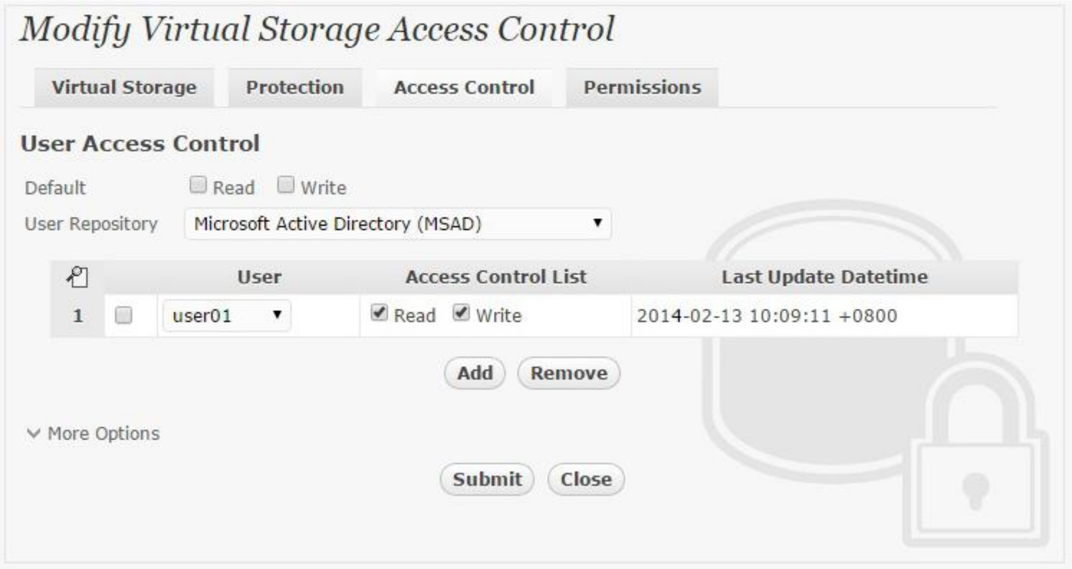
|  |  | Key Name | Last Update Datetime |
|---|---|---|---|
| 1 | □ | key01 | 2016-05-11 10:09:11 +0800 |

**Cryptographic Cipher**

Cipher Algorithm: AES

Bit Length: 256

CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource ‘share01’ is provisioned for user ‘user01’ with Microsoft Active Directory integration for user-password authentication and single sign-on.



*Modify Virtual Storage Access Control*

**User Access Control**

Default □ Read □ Write

User Repository: Microsoft Active Directory (MSAD)

|  |  | User | Access Control List | Last Update Datetime |
|---|---|---|---|---|
| 1 | □ | user01 | ☑ Read ☑ Write | 2014-02-13 10:09:11 +0800 |

# Conclusion

Key management system

- Gemalto SafeNet KeySecure

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

| Bloombase Product | Operating System | Hardware Security Module |
|---|---|---|
| Bloombase StoreSafe | Microsoft Windows Server | • Gemalto SafeNet KeySecure |
| | Red Hat Enterprise Linux (RHEL) | • Gemalto SafeNet KeySecure |
| | SUSE Linux Enterprise Server (SLES) | • Gemalto SafeNet KeySecure |
| | Oracle Solaris | • Gemalto SafeNet KeySecure |
| | IBM AIX | • Gemalto SafeNet KeySecure |
| | HP-UX | • Gemalto SafeNet KeySecure |

# Disclaimer

The tests 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 differences 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.

# Technical Reference

1. Bloombase StoreSafe Technical Specifications, http://www.bloombase.com/content/8936QA88

2. Bloombase StoreSafe Hardware Compatibility Matrix, http://www.bloombase.com/content/e8Gzz281

3. Gemalto SafeNet KeySecure, http://www.safenet-inc.com/data-encryption/enterprise-key-management/key-secure/