



Interoperability of Bloombase StoreSafe Security Server and EMC Atmos for Transparent Cloud Storage Encryption Security

March, 2012



Executive Summary

EMC Atmos is the cloud storage platform that lets enterprises and service providers store, manage and protect globally distributed, unstructured content at scale. Atmos provides the essential building blocks to implement a private, public, or hybrid cloud storage environment. Bloombase StoreSafe Security Server provides application-transparent encryption security of enterprise storage systems from SAN, NAS, DAS, CAS to cloud, no exception for EMC Atmos. This document describes the steps carried out to test interoperability of EMC Atmos cloud storage with Bloombase StoreSafe Security Server running on VMware ESX as virtual appliance. The solution enables Atmos-aware enterprise applications to interact with Bloombase StoreSafe as-if virtual Atmos proxy such that no application change is required to access and retrieve Atmos encrypted objects as-if in plain-text

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

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

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

© 2012 Bloombase, Inc.

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

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

Document No.

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Bloombase StoreSafe Security Server Virtual Appliance.....	8
Cloud Storage / Object Store	9
Hosts	9
Configuration Overview	10
EMC ATMOS Service End Point Security	10
Encryption Key Configuration	11
Physical Storage Configuration.....	12
Virtual Storage Configuration	13
Validation Tests	15
Validation Testing.....	15
Test Scenarios	22
EMC Atmos Object Browser	22

Java JUnit Test Program	22
Result	23
EMC Atmos Object Browser	23
Java JUnit Test Program	24
Conclusion	25
Disclaimer	26
Technical Reference	27

Purpose and Scope

This document describes the steps necessary to transparently secure EMC Atmos cloud storage service objects by Bloomberg StoreSafe Security Server. Specifically, we cover the following topics:

- Preparing Bloomberg StoreSafe Security Server
- Interoperability testing on host systems including with Java applications via EMC Atmos API on Red Hat Linux and EMC Atmos Object Browser application on Microsoft Windows

Assumptions

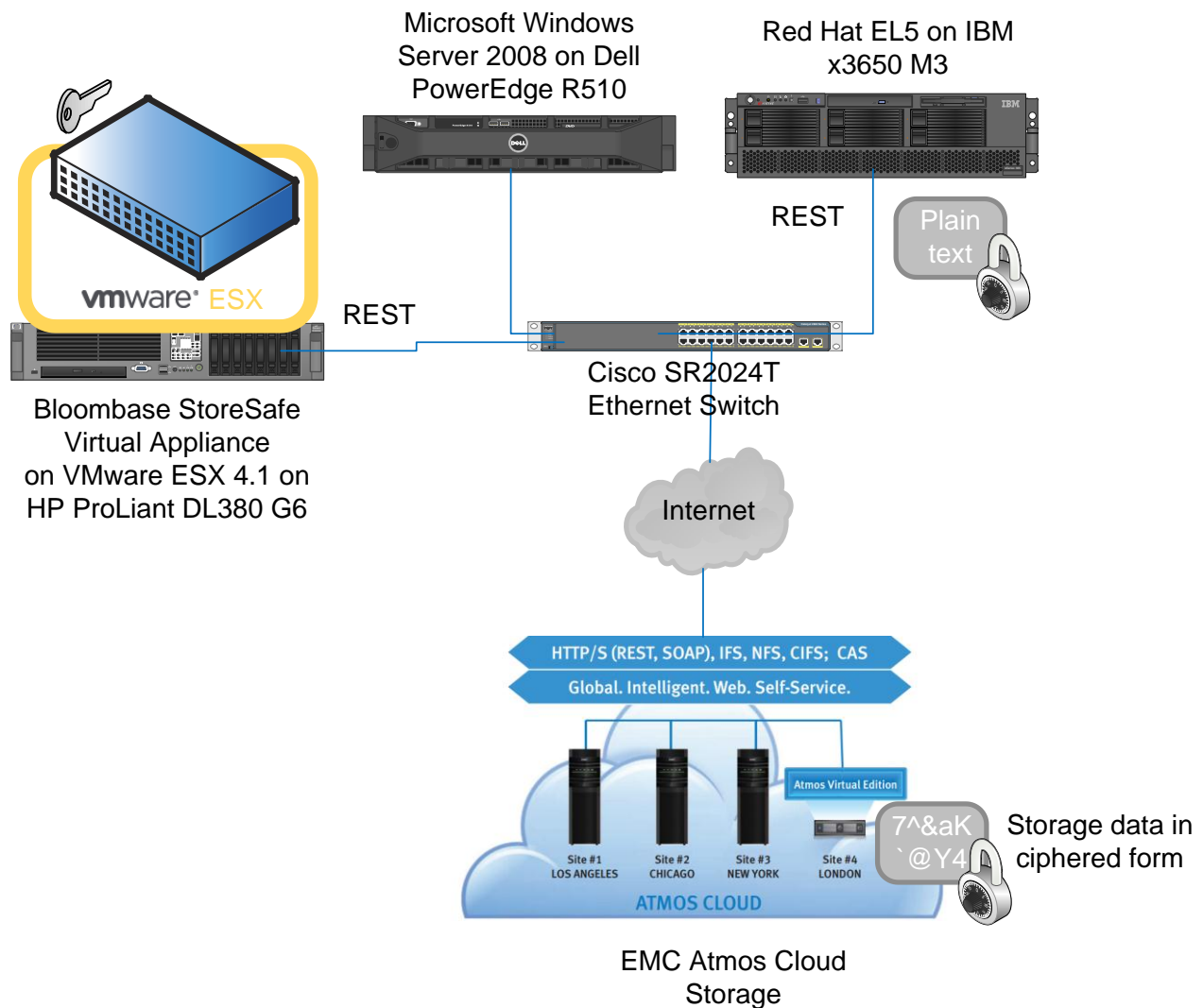
This document describes interoperability testing of Bloombase StoreSafe Security Server on EMC Atmos object storage service. Therefore, it is assumed that you are familiar with operation of storage systems and major operating systems including Linux and Windows. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of UNIX.

As EMC Atmos cloud storage service is proprietary technology of EMC, you are recommended to refer to software development kit and configuration guides of EMC Atmos and setup documentations of your EMC Atmos service provider. We assume you have basic knowledge of storage networking and information cryptography. For specific technical product information of StoreSafe, please refer to our website at <http://www.bloombase.com> or Bloombase SupPortal <http://supportal.bloombase.com>

Infrastructure

Setup

The validation testing environment is setup as in below figure



Bloomberg StoreSafe Security Server Virtual Appliance

Server	HP ProLiant DL380 G6
Processors	2 x Intel Xeon 5650 quad-core 2.66 GHz
Memory	8 GB
Hypervisor	VMware ESX 4.1
Operating System	Bloomberg SpitfireOS 5.5 – Hardened and customized OS based on Linux kernel version 2.6.26 64-bit
Storage Encryption Software	Bloomberg StoreSafe Security Server

Cloud Storage / Object Store

Storage	EMC Atmos Online
---------	------------------

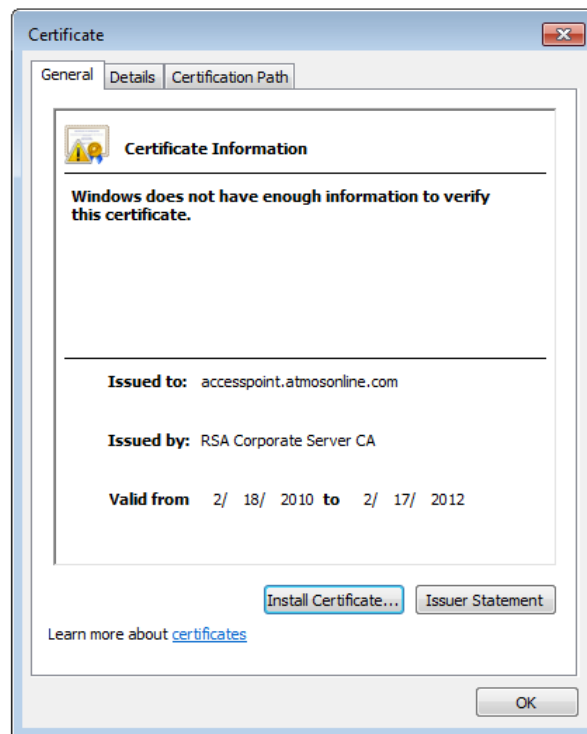
Hosts

Model	Dell PowerEdge R510	IBM x-Series x3650 M3
Operating System	Red Hat EL5	Microsoft Windows Server 2008

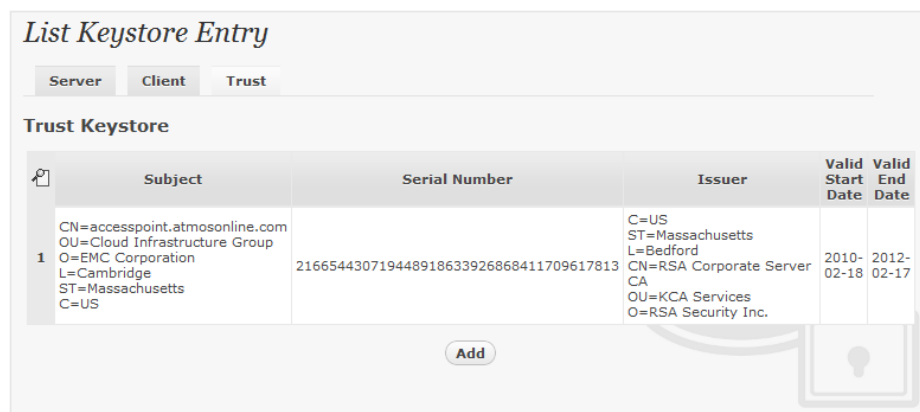
Configuration Overview

EMC ATMOS Service End Point Security

Download SSL certificate from EMC ATMOS Online



Import to Bloombase Spitfire Keystore Trust Store to establish trust between Bloombase Spitfire StoreSafe and EMC ATMOS Online



Encryption Key Configuration

Generate encryption key with name 'key' in bundled Spitfire KeyCastle key life-cycle management tool

Modify Key Wrapper

Key Wrapper

Upload Key Contents


Modify Key Source


CRLDP

OCSP

Permissions

Modify Key Wrapper

Name	<input type="text" value="key"/>
Active	<input checked="" type="checkbox"/>
Exportable	<input type="checkbox"/>
CA	<input type="checkbox"/>
Subject DN	CN=key
Serial Number	695376542685815571917364
Issuer DN	CN=key
Certificate	<input checked="" type="checkbox"/> 
Public Key	<input checked="" type="checkbox"/>
Private Key	<input checked="" type="checkbox"/>
Key Bit Length	1024
Effective Datetime	2011-02-18 22:26:36 +0800
Expiry Datetime	2021-02-15 22:26:36 +0800
Revocation Check Method Type	<input type="text" value=""/> ▼
Revoked	<input type="checkbox"/>
Key Usage	-
Extended Key Usage	-
Owner	admin
Last Update Datetime	-



Physical Storage Configuration

Configure physical storage namely 'atmos' to provision the EMC ATMOS object store to be encrypted by Spitfire StoreSafe. Select physical storage type as 'REST' and type as 'ATMOS'.


Specify service end-point URL in the configuration page for protocol as 'https', host as 'accesspoint.atmosonline.com' and port as '443'.

Modify Storage Configuration

Physical Storage Permissions

Physical Storage Configuration

Name	atmos
Description	
Physical Storage Type	REST
Type	ATMOS
Protocol	https
Host	accesspoint.atmosonline.com
Port	443
Owner	admin
Last Update Datetime	2012-01-04 14:14:25 +0800



Virtual Storage Configuration

Create virtual storage based on the actual service end-point sub-tenant ID namely 'ad3bab8bc95a4485997e6845e74ddd56' of type 'REST' and associate to physical storage 'atmos' for non-disruptive agentless encryption protection over REST.

Modify Virtual Storage


Virtual Storage Protection Access Control Permissions

Modify Virtual Storage

Name	ad3bab8bc95a4485997e6845
Status	<input checked="" type="checkbox"/>
Description	
Active	<input checked="" type="checkbox"/>
Mode	REST
Owner	admin
Last Update Datetime	2012-01-05 00:00:12 +0800

Physical Storage

Storage	atmos
Description	
Physical Storage Type	REST



Specify protection type as 'Privacy' and secure the EMC ATMOS sub-tenant contents using AES-XTS 256-bit encryption with encryption key 'key'

Modify Virtual Storage Handler

Virtual Storage Protection Access Control Permissions

Virtual Storage Protection

Protection Type Privacy ▾

Encryption Keys

	Key Name	Last Update Datetime
1	<input type="checkbox"/> Demo Valid 2	2012-01-05 15:20:45 +0800


Remove

Cryptographic Cipher

Cipher Algorithm AES ▾

Bit Length 256 ▾

Submit Close



Provision authorized EMC ATMOS user IDs or application IDs to 'Access Control' panel.

Modify Virtual Storage Access Control

Virtual Storage Protection **Access Control** Permissions


User Access Control

	User	Last Update Datetime
1	<input type="checkbox"/> A4854747110505f15082 ▾	2012-01-05 00:00:12 +0800
2	<input type="checkbox"/> A485474711da174e8437 ▾	2012-01-07 14:35:21 +0800
3	<input type="checkbox"/> A4854747117e925e4973 ▾	2012-01-11 12:50:04 +0800

Add Remove

▼ More Options

Submit Close



Validation Tests

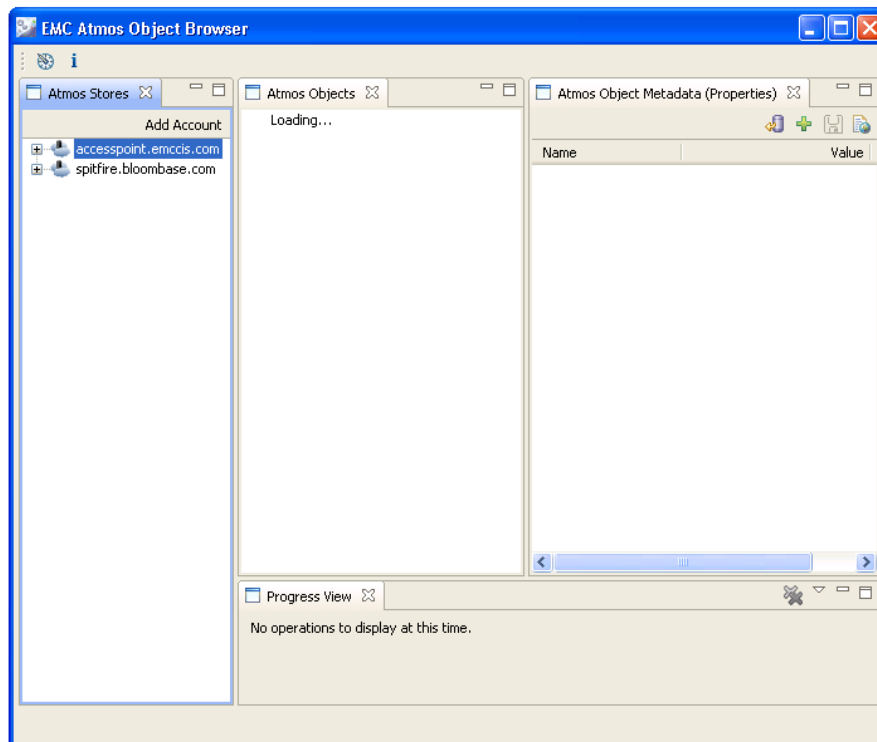
Validation Testing



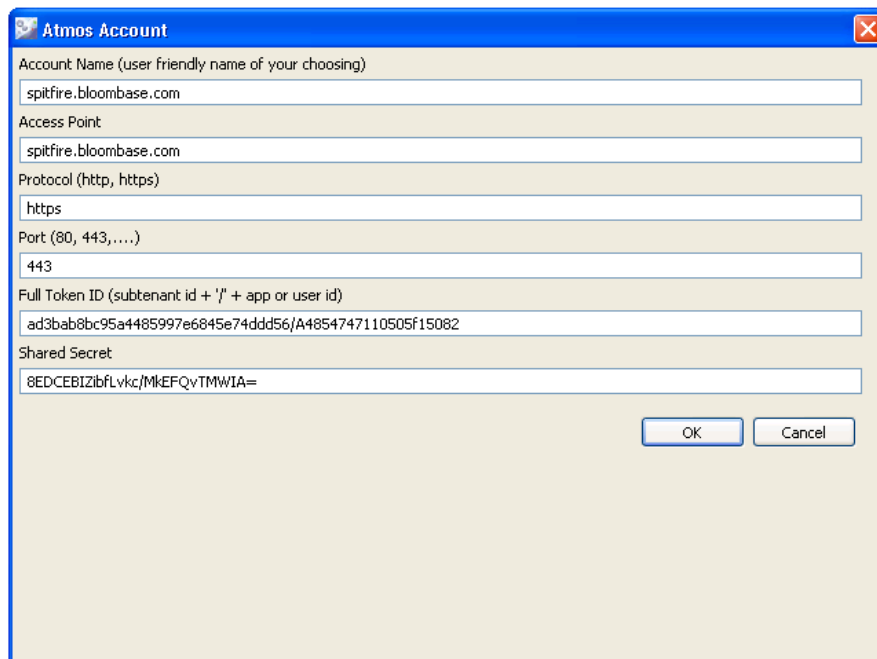
Double click to launch EMC ATMOS Object Browser



The main window is displayed

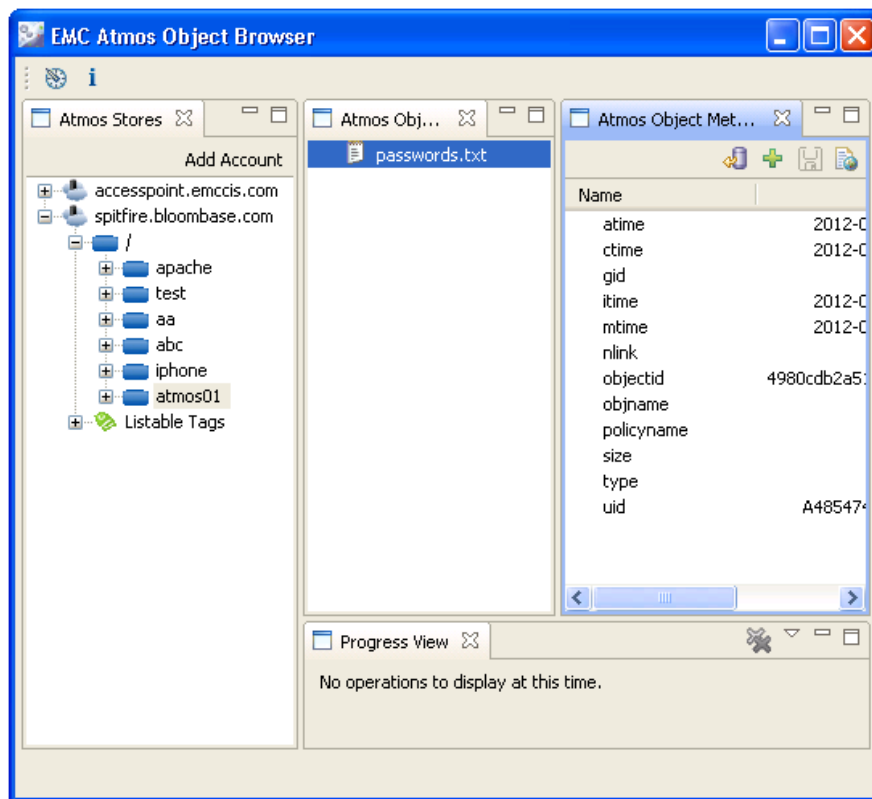


Provision Bloombase Spitfire StoreSafe RESTful EMC ATMOS object store endpoint 'ad3bab8bc95a4485997e6845e74ddd56' to EMC ATMOS object browser

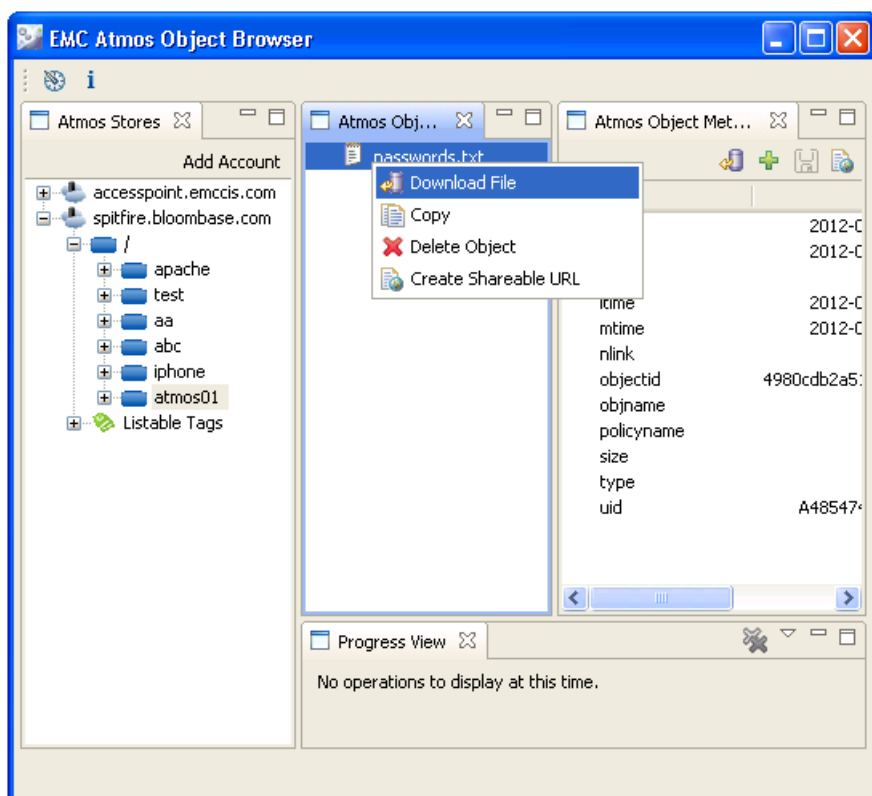


Press 'OK' to commit changes.

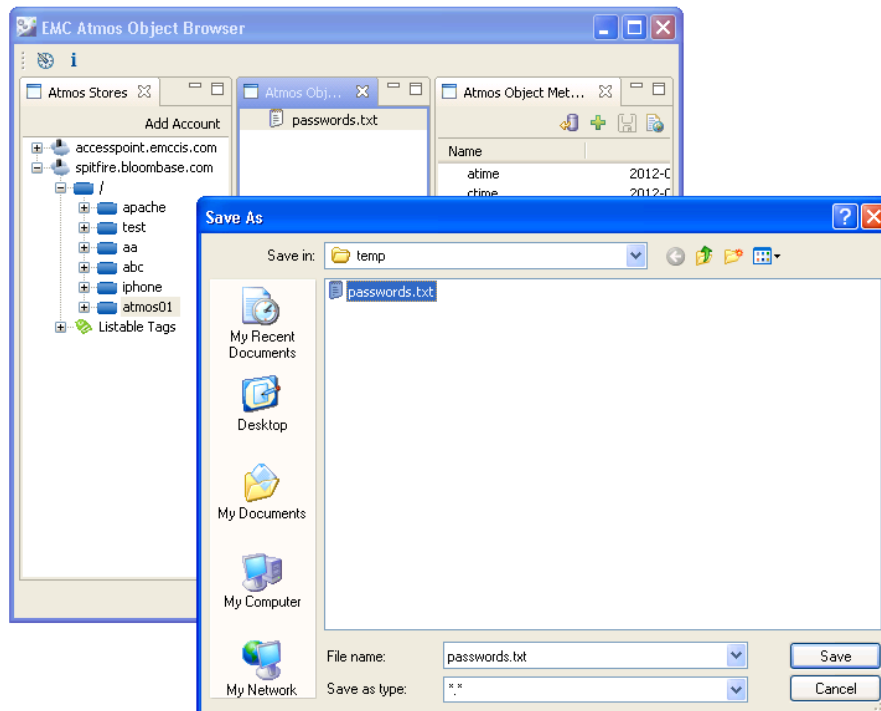
Double click Bloombase Spitfire StoreSafe virtual storage account to browse objects in EMC ATMOS.



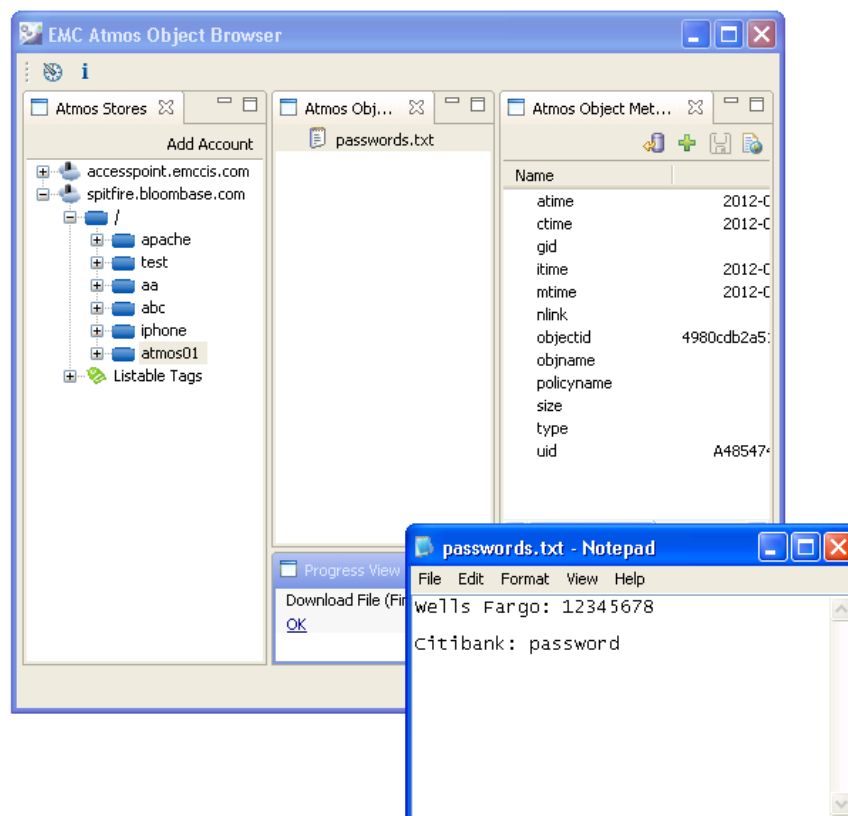
Right click contents to be downloaded and choose 'Download File' from popup menu.



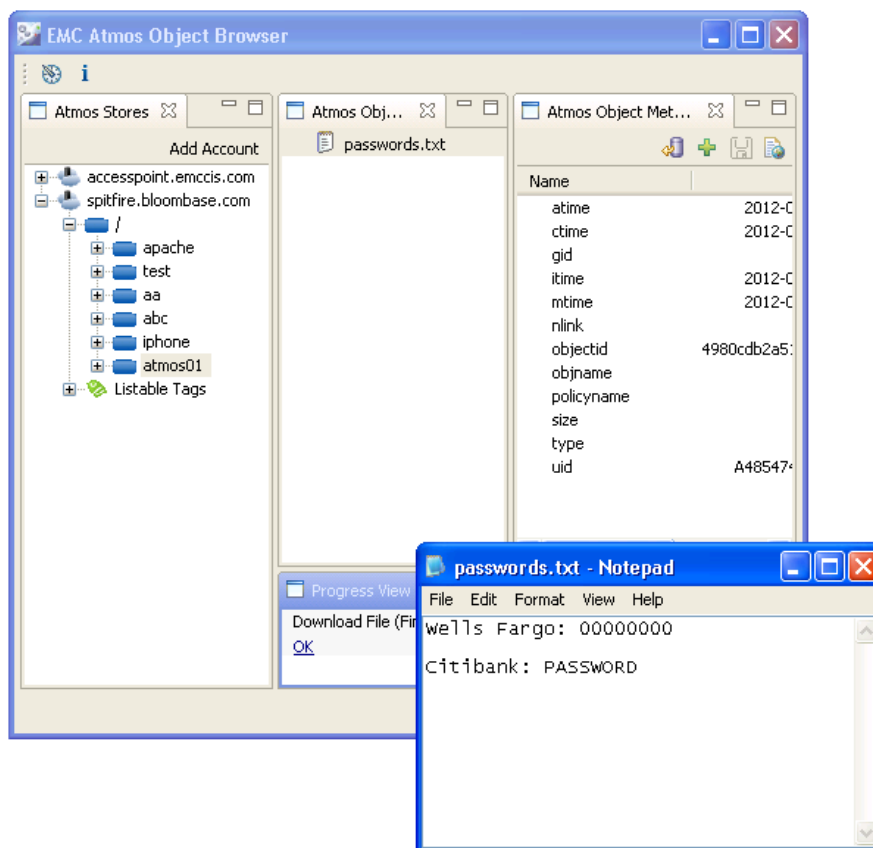
Choose destination where StoreSafe secured contents to be downloaded to locally



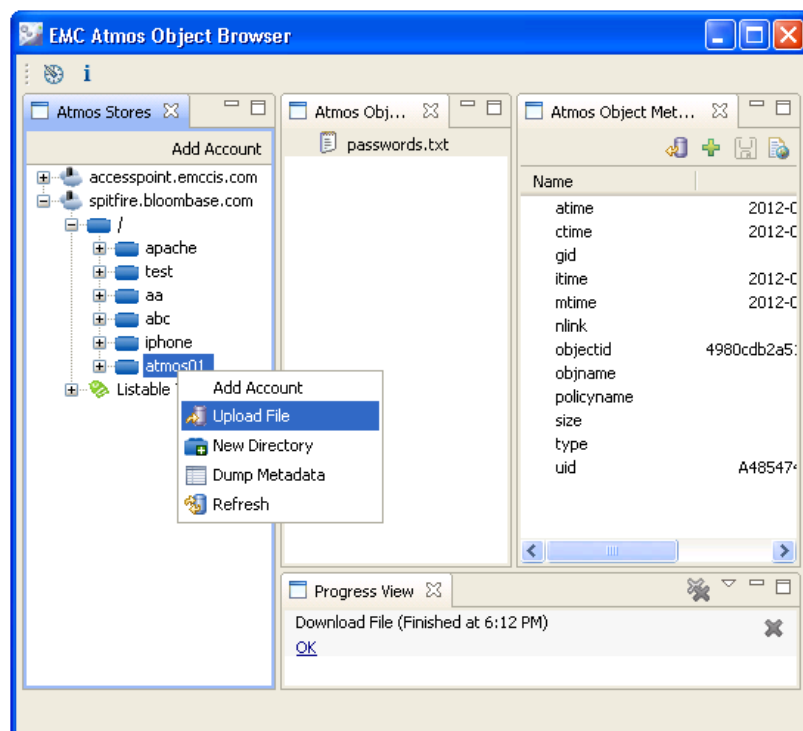
Click link to open downloaded secure ATMOS object.



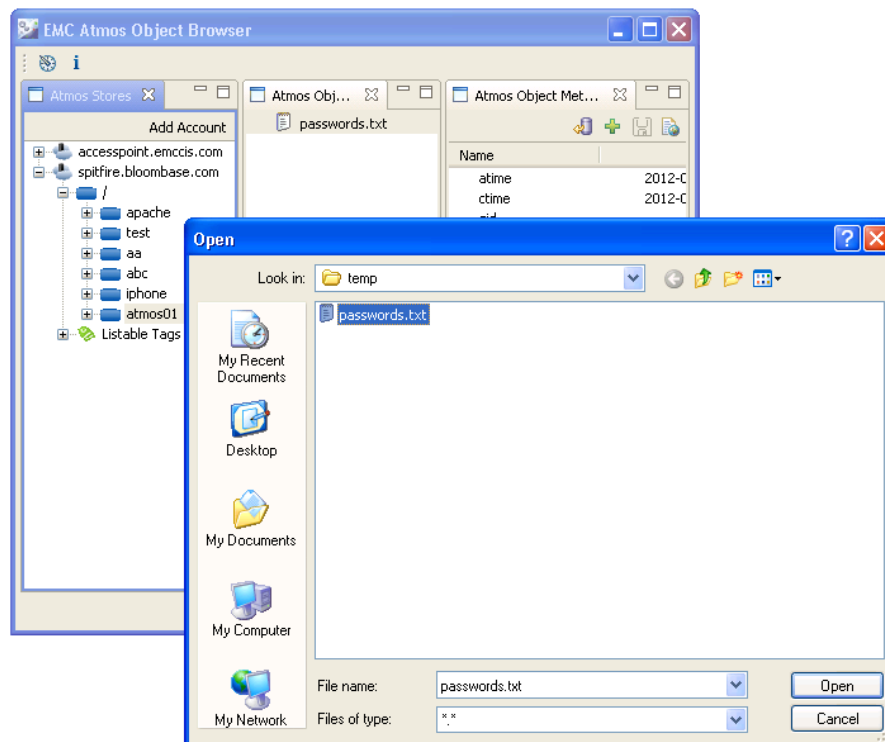
Modify secure contents



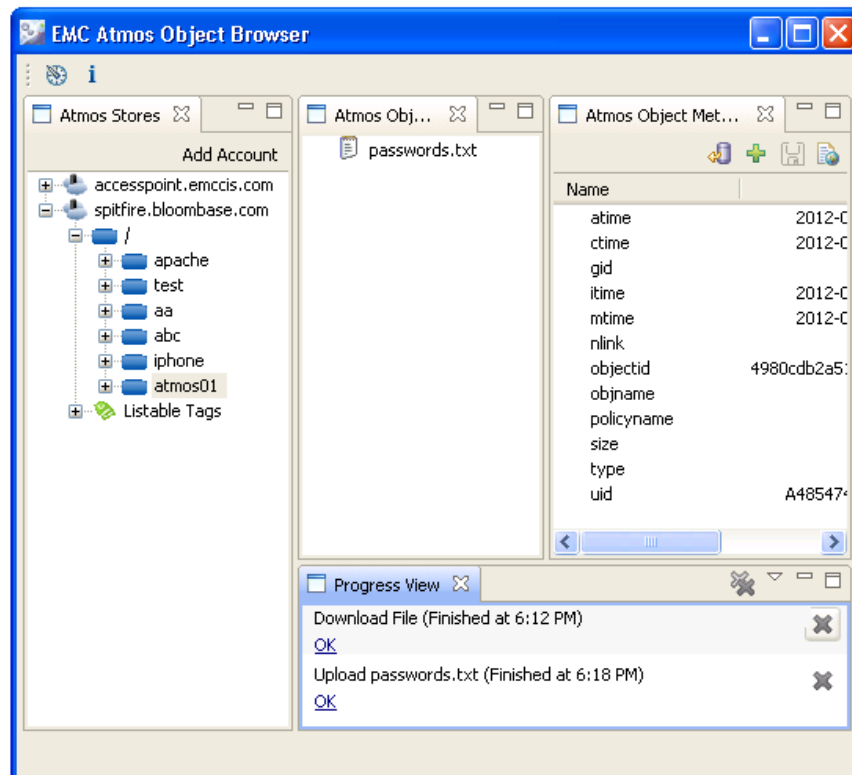
Put updated secure objects up on EMC ATMOS via Bloombase Spitfire StoreSafe virtual storage



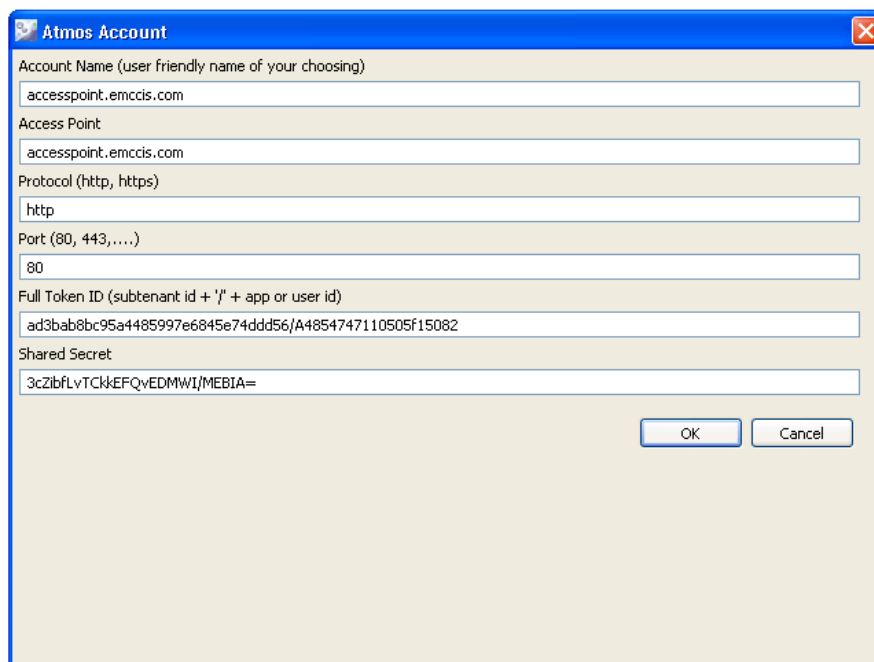
Choose file to be uploaded to Bloombase Spitfire StoreSafe EMC ATMOS object store proxy



Modified password.txt file is successfully encrypted by Spitfire StoreSafe and put to EMC ATMOS



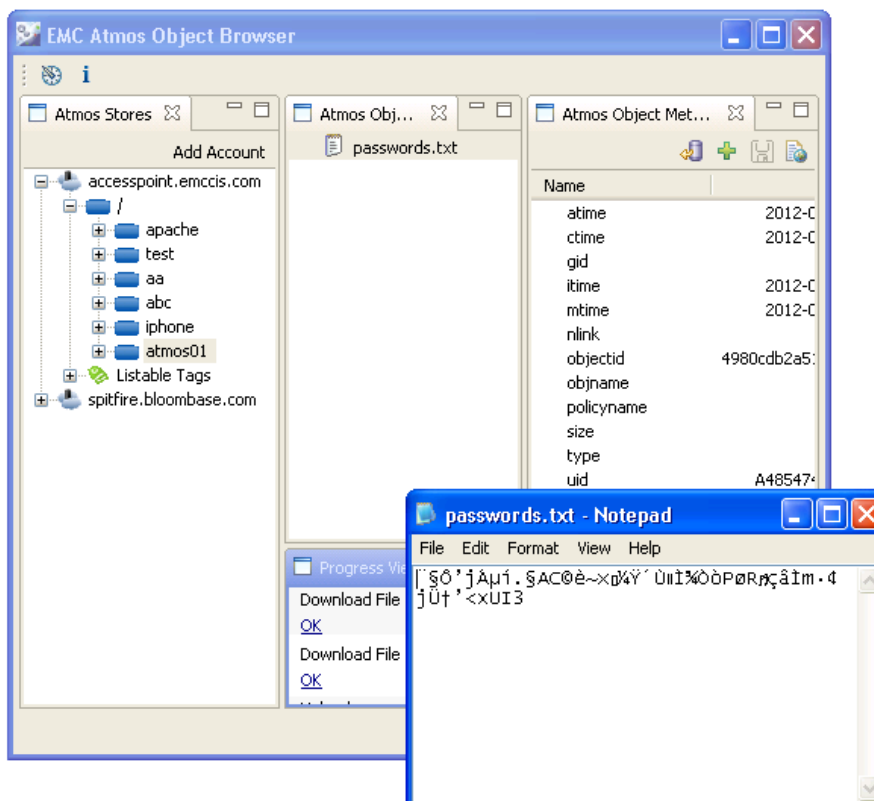
Provision actual/physical EMC ATMOS object store end-point



The 'Atmos Account' window is a configuration dialog for an Atmos account. It contains several text input fields and two buttons at the bottom right: 'OK' and 'Cancel'.

Field	Value
Account Name (user friendly name of your choosing)	accesspoint.emccis.com
Access Point	accesspoint.emccis.com
Protocol (http, https)	http
Port (80, 443, ...)	80
Full Token ID (subtenant id + '/' + app or user id)	ad3bab8bc95a4485997e6845e74ddd56/A4854747110505f15082
Shared Secret	3cZibfLvTCKeFQvEDMWI/MEBIA=

Examine physical contents persisted at actual EMC ATMOS repository by downloading 'passwords.txt' object



Test Scenarios

The following tests are carried out at storage hosts to access encrypted EMC Atmos cloud storage via Bloombase StoreSafe appliances by use of

- EMC Atmos Object Browser application
- Java JUnit test program using Atmos API

EMC Atmos Object Browser

Test	Description
User sign on	
List directories	Platform equivalence of UNIX's ls
List files	Platform equivalence of UNIX's ls
Change directory	Platform equivalence of UNIX's cd
Directory creation	Platform equivalence of UNIX's mkdir
Directory removal	Platform equivalence of UNIX's rm
File creation	Platform equivalence of UNIX's echo XXX ›
File read	Platform equivalence of UNIX's more XXX
File removal	Platform equivalence of UNIX's rm
File append – by character	Platform equivalence of UNIX's echo XXX ››
File append – by block	Platform equivalence of UNIX's echo XXX ››

Java JUnit Test Program

Test	Description
User sign on	
List directories	
List objects	

Change directory

Directory creation

Directory removal

Object creation

Object retrieve

Object removal

Object modify

Result

EMC Atmos Object Browser

Test	Validation Pass	Remarks
User sign on	✓	
List directories	✓	
List files	✓	
Change directory	✓	
Directory creation	✓	
Directory removal	✓	
File creation	✓	
File read	✓	
File removal	✓	
File append – by character	✓	
File append – by block	✓	

Java JUnit Test Program

Test	Validation Pass	Remarks
User sign on	✓	
List directories	✓	
List objects	✓	
Change directory	✓	
Directory creation	✓	
Directory removal	✓	
Object creation	✓	
Object retrieve	✓	
Object removal	✓	
Object modify	✓	

Conclusion

Bloombase StoreSafe Security Server passes all Bloombase interopLab's interoperability testing with EMC Atmos cloud storage on object access. It has also been validated that objects are stored encrypted at backend EMC Atmos cloud storage whereas on application access, the encrypted objects can be accessed as-if they are in plain, thus, application transparent encryption.

Bloombase Product	Operating System	Storage
Bloombase StoreSafe Security Server	Microsoft Windows Server 2008	EMC Atmos
	Java 1.6 on Red Hat Enterprise Linux 5	EMC Atmos

Disclaimer

The tests described in this paper were conducted in the Bloomberg InteropLab. Bloomberg 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 Spitfire StoreSafe Security Server Technical Specifications,
<http://www.bloombase.com/content/8936QA88Dh3lD3kYMKxe1VGb8UG4900eNL8Dj>
2. Bloombase Spitfire StoreSafe Security Server Compatibility Matrix,
<http://www.bloombase.com/content/e8Gzz281s480l2192FF4Btv5HOpb77vLpt1U8V>
3. EMC Atmos, <http://www.emc.com/storage/atmos/atmos.htm>
4. EMC Developer Network for Atmos, <https://community.emc.com/community/edn/atmos>