EMC Corporation®
Atmos™ v2.0.1

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.14

Prepared for:

EMC Corporation
171 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 508 435 1000
Email: info@emc.com
http://www.emc.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is EMC Atmos v2.0.1, and will hereafter be referred to as the TOE throughout this document. The TOE is a software only multi-petabyte offering for information storage and distribution, referred to as Cloud Optimized Storage (COS). It provides cloud storage, combining scalability with automated data placement to deliver content information services.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) - Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	EMC Corporation® Atmos™ v2.0.1 Security Target
ST Version	Version 0.14
ST Author	Corsec Security, Inc
ST Publication Date	2/2/2012
TOE Reference	EMC® Atmos v2.0.1.67681
FIPS[1] 140-2 Status	N/A
Keywords	Cloud Computing, Sensitive Data Protection, Security Management

[1] FIPS = Federal Information Processing Standard

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

EMC Atmos is a multi-petabyte server system for information storage and distribution. Atmos serves as the infrastructure for building cloud storage solutions, combining scalability with automated data placement to help customers efficiently deliver content, and information services distributed globally.

The major features of Atmos are:

- Massive scale: supports many petabytes of storage capacity and billions of objects.
- Globally distributed: servers can be distributed around the world, but share one global namespace.
- Multi-tenancy: many different users and groups of users can use the cloud without data leakage between users. Supports a hierarchy of Tenants[2], Sub-Tenants[3] (which belong to a Tenant), and Users (which belong to a Sub-Tenant).
- Business objectives achieved via policy: storage policies are defined and enforced automatically for each tenant, sub-tenant, user, and type of data (based on the data object's metadata).
- Standards-based data access: provides web-based (SOAP[4], REST[5]) and file system-based (CIFS[6], NFS[7], IFS[8]) object access.
- Internal LDAP server

Although Atmos can be used simply as a high-capacity, redundant, distributed storage device, the true power of the product is utilized by creating policies that enforce business logic based on object metadata. For example, consider an Atmos deployment that consists of three Atmos servers distributed in three locations: one in Boston, devoted to financial data; one in London, devoted to engineering data; and one in Tokyo, devoted to providing backup for the other two sites. When a data object is added to the cloud, its metadata is analyzed; if the metadata identifies it as financial data, then the data will be stored on the Boston-based Atmos server but not the London-based server, and it will also be stored in the Tokyo-based server to provide backup. Although this is a very simplistic example, Atmos is capable of implementing very complicated business logic via its robust policy enforcement engine. Policies are analyzed and triggered by events within the cloud, such as when data is created, read, deleted, etc.

Atmos divides objects (or files) into two parts: user data and metadata. User data is application data, such as Word files, text files, movies, or MP3[9] files. Metadata is information about user data. Metadata is further divided into system metadata and user metadata. System metadata includes the filename, file size, modification date, creation date, access-control lists, and object ID. In addition, metadata includes arbitrary, custom, name-value pairs such as the artist name for MP3 (e.g., for MP3 data) or customer type.

---

[2] Tenant = A conceptual subset of the storage resources within an Atmos system. Associated with a tenant are specific storage resources, security control, storage policies, and access to the data stored on that tenant's resources. Each tenant has a name that is unique system-wide.

[3] Sub-Tenants = A logical subset of a tenant that group together selected policies, data access (i.e., file-system or Web-service namespaces), and reporting capabilities. When the SysAdmin creates a tenant, the system automatically creates one corresponding subtenant (which is identical to the tenant). SysAdmins can choose to create additional subtenants within each tenant.

[4] SOAP = Simple Object Access Protocol

[5] REST = Representational State Transfer

[6] CIFS = Common Internet File System

[7] NFS = Network File System

[8] IFS = Installable File System

[9] MP3 = MPEG-1 Audio Layer 3

Multiple Atmos servers can operate as a single entity, and the use of metadata and business policy ensures that the correct data is automatically delivered to the correct location at the correct time. These qualities combine to increase customers' operational efficiency, reduce management complexity, and ultimately reduce operational costs. EMC offers two Atmos product lines: "EMC Atmos"and "EMC Atmos Virtual Edition (VE)". "EMC Atmos" is a series of stand-alone servers that can be purchased by end-users to build their own storage cloud. Atmos VE is a software only version of Atmos that runs on VMWare's ESX and can be used to build an Atmos storage system on ESX supported compute and storage hardware. Atmos is also accessible through "EMC Atmos Online", a service offering from EMC wherein EMC provides storage on a pre-existing Atmos cloud for partner integration and validation. Both the stand-alone Atmos product and Atmos VE are being evaluated in the Common Criteria evaluation. Atmos VE is sold as a virtual appliance consisting of the Atmos software and the rPath Linux v2 operating system (OS) only. The stand-alone servers are sold as appliances consisting of the Atmos software, rPath Linux v2, and hardware. There are currently three server models in the Atmos product line:

- WS-120: designed for low power consumption and provides 120 terabytes of storage.
- WS-240: designed for high performance (but not low power consumption) and provides 240 terabytes of storage.
- WS-360: designed for high capacity (but not high performance), providing 360 terabytes of storage.

EMC Atmos provides a single web based GUI[10], called the Atmos System management GUI, for system administration. This includes:

- Managing, monitoring, and controlling hardware resources
- Managing network resources (IP address allocation and service)
- Controlling the software that each Atmos server also known as a node runs
- Configuring (at a low level) each service on each node
- Controlling Atmos behavior
- Setting alerts for abnormal conditions and faults
- Restoring nodes and system resources

System management tools enable administrators to obtain operational data for Atmos hardware, software, and the network. This operational data can be accessed through both the System management GUI and standard network-management tools, like SNMP[11].

[10] GUI = Graphical User Interface

[11] SNMP = Simple Network Management Protocol

The minimum system requirements for Atmos are shown in Table 2 below. It should be noted that Atmos can be installed on a hardware appliance or can be installed on VMware ESX.

Table 2 – Atmos Minimum Requirements for all Platforms

Product Component	Type of Required Software	Requirement
Software Requirements		
Atmos Installable File System (IFS):	Operating System Add-ons considered to be Third Party Software	• Linux RHEL[12] 5 client (32-bit and 64-bit) version 5 or higher with the following installed: ○ FUSE 2.7.4 or higher ○ RHEL5 developer kit ○ SAMBA (required if you want to export the file system to a Windows client) version 3.4.5 ○ NFS (required if you want to export the file system to a Linux client) version 3
Atmos System management GUI	Third Party Software	Internet Explorer 6 or 7
Authenticate CIFS access to Atmos nodes with Active Directory	Third Party Software	Active Directory 2008
VMware Environments		
Atmos Server	Third Party Software	ESX v4.0

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is software only and includes the rPath Linux v2 Operating System and Atmos Software. It is considered a Cloud Optimized Storage (COS) product in the cloud computing space. EMC Atmos is a COS platform that combines massive scale, global distribution, and optimized object storage and retrieval via a policy-based approach that will scale on a petabyte capacity level. At the same time, it provides a single System management GUI for administering the TOE.

Architecturally, Atmos is an object store, although it can be expressed as a traditional file system. All stored objects have both data (the "content" of the object) and metadata (information about the content).

[12] RHEL = Red Hat Enterprise Linux

Figure 1 shows the details of a simple sample deployment configuration of the TOE:

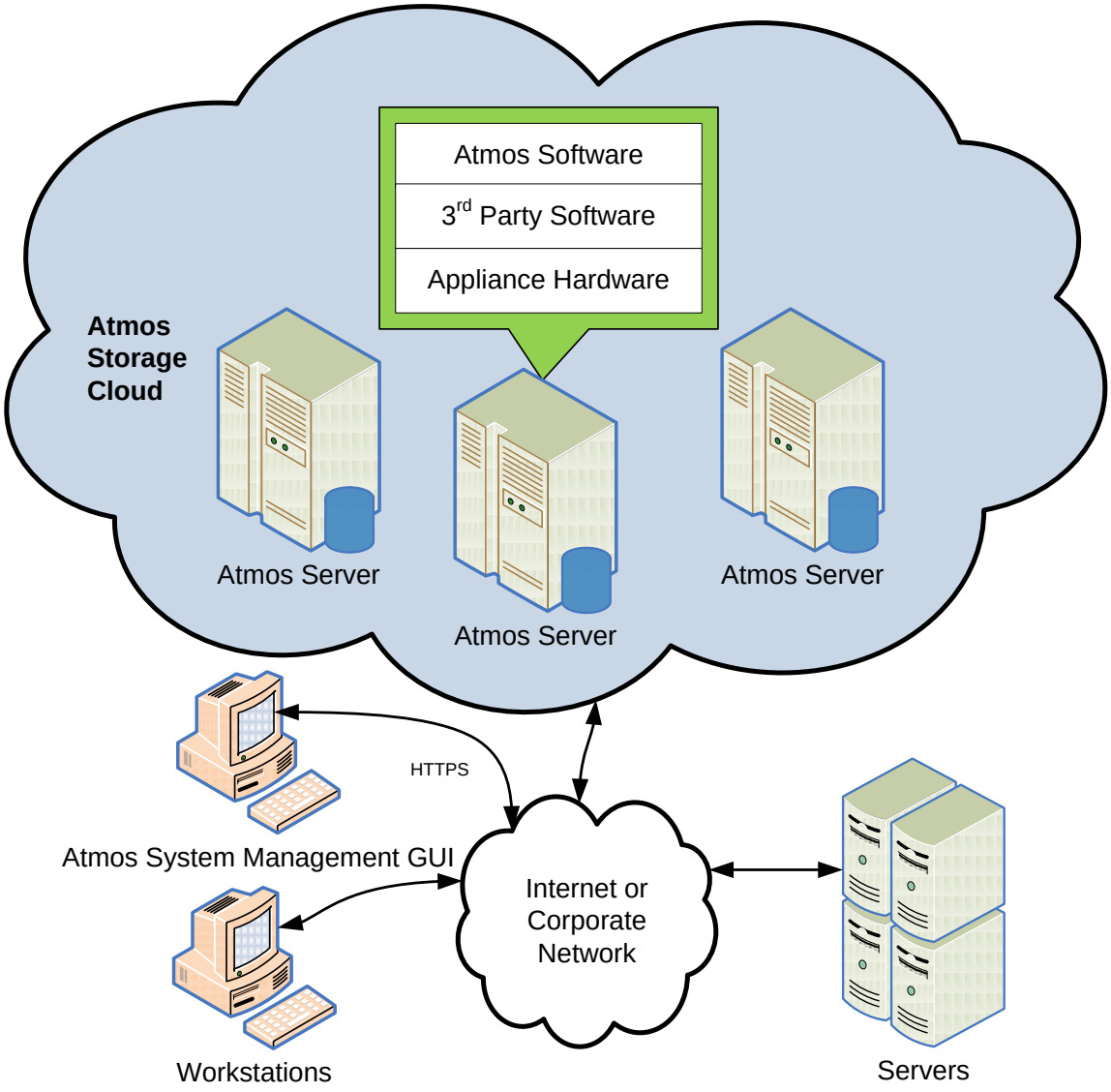

Figure 1 - Deployment Configuration of the TOE

The "System management GUI" is a web-based GUI used to manage the TOE security functions. The "Workstations" are a representation of the end user machines that are accessing the Atmos cloud in order to access their stored data. The "Servers" are customer servers that operate within a company's infrastructure such as LDAP[13] servers, SMTP[14] servers, and SNMP network management servers. These are external to the TOE and are optional.

[13] LDAP = Lightweight Directory Access Protocol
[14] SMTP = Simple Mail Transfer Protocol

1.4.1 Brief Description of the Components of the TOE

The Atmos server software, also referred to as a "node", is the TOE. Logically, the Atmos server software is separated into two components: the Atmos software and the rPath Linux v2 OS.

1.4.1.1 Atmos software

The Atmos software provides the core functionality of Atmos. The Atmos server software provides an authorized administrator of the TOE a web based GUI[15] interface to easily manage the security functions of the TOE. Through the System management GUI, accessible via web browser, an authorized administrator can configure Atmos server configuration parameters, provision new users, and assign roles as necessary. The Atmos software provides a collection of Atmos storage features including replication, de-duplication, compression, retention and deletion.

1.4.1.2 rPath Linux v2 OS

The rPath Linux v2 OS provides the operating system functionality for the TOE. The OS provides identification and authentication of local login accounts for performing installation, configuration, and maintenance tasks via a command line interface (CLI).

Since it is bundled with the installation media for the Atmos Software and the installation is transparent to the user, the OS is considered to be part of the TOE.

1.4.2 TOE Environment

It is assumed that there will be no un-trusted users or software on the Atmos server host. In addition, the Atmos server is intended to be deployed in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

The Atmos server software relies upon the underlying hardware platform or virtual hypervisor to provide protection and execution of the TOE software, disk storage, and reliable timestamps. A listing of third party software relied upon by the Atmos server is given in column 2 ('Type of Required Software') in Table 2, labeled as 'Third Party Software'.

The Atmos server relies upon an external NTP[16] server to provide the Atmos server with a reliable timestamp. This ensures that both application servers and Atmos nodes are synchronized. Atmos validates timestamps on requests and rejects any that are out of sync more than five minutes.

[15] GUI = Graphical User Interface
[16] NTP = Network Time Protocol

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and shows all of the components of the TOE and the constituents of the TOE Environment together. The TOE is software only. Table 3 details the TOE components and its Environment's minimum requirements.

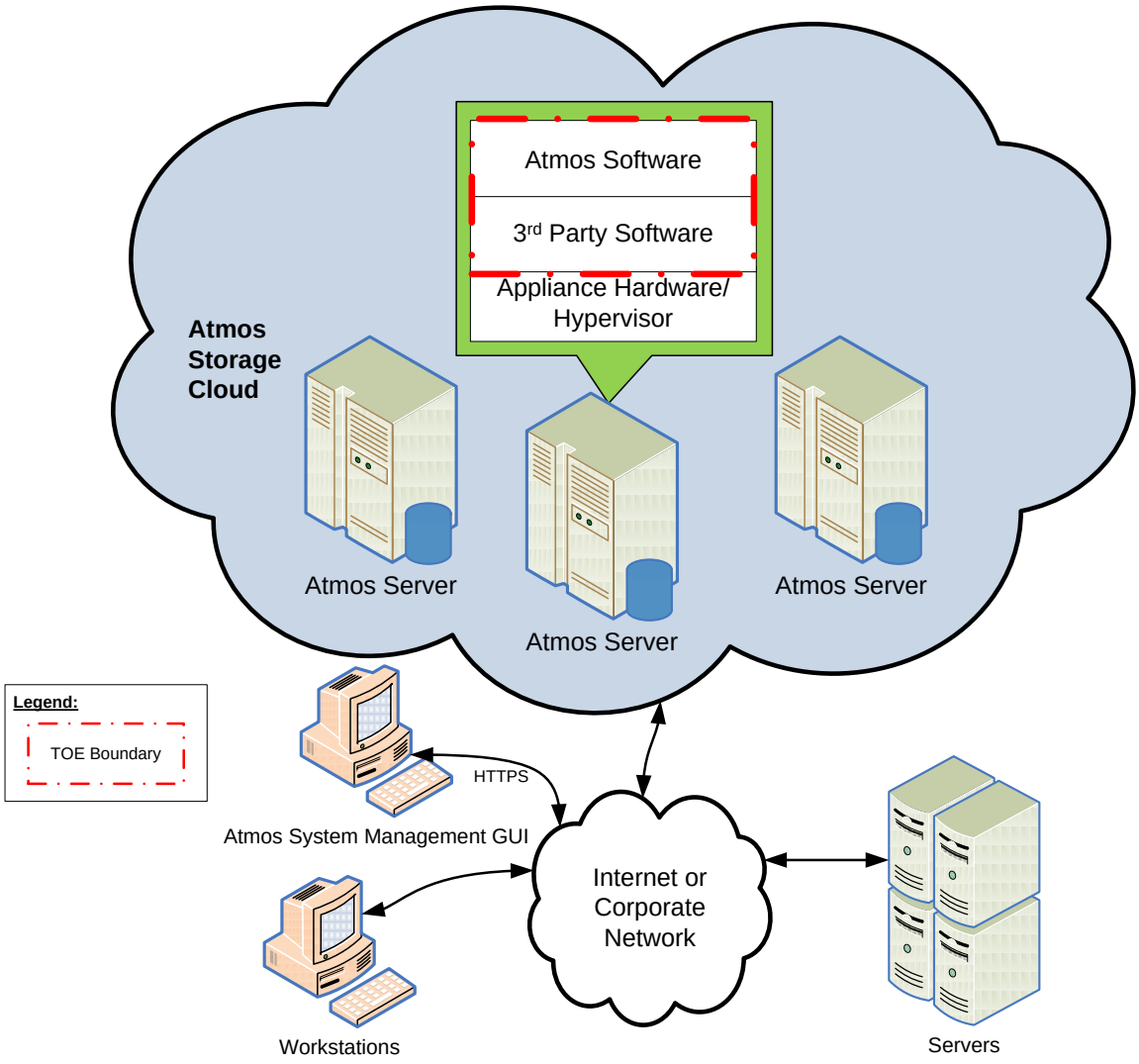

Figure 2 - Physical TOE Boundary

The TOE Boundary includes all the EMC-developed parts of the Atmos product. Any third party source code or software that EMC has modified is considered to be TOE Software. This includes the rPath Linux v2 OS which is bundled with the Atmos Software and installation is transparent to the user. As a result, the Linux OS is not listed as a separate component.

The TOE Boundary specifically does not include any of the third party software that the TOE relies upon as described in section 1.4.2 of the ST and Table 3 below. In addition, the API interface will be outside the TOE Boundary.

In order to provide customers multiple identification and authentication options, Atmos provides the ability for an external LDAP or AD[17] server to be used for administrative authentication. Neither external LDAP nor Active Directory is included in the TOE.

[17] AD = Active Directory

Table 3 – Components of the TOE and TOE Environment

Component	TOE	TOE Environment	Requirement
Atmos Software v2.0.1	✓		All EMC developed software, and bundled open source and third party software.
rPath Linux v2 OS	✓		The rPath OS provides a platform for software vendors to create and maintain software appliances. A major feature of rPath is Conary, a software package management and configuration program that allows rollbacks, incremental ("changeset") updates, and distributed downloading.
Linux RHEL[18] 5 client (32-bit and 64-bit) installed version 5 or higher developer kit with FUSE 2.7.4 or higher[19]		✓	RHEL developer kit is required because the FUSE installation requires a C compiler. If Atmos is intended to provide Atmos file system access of Atmos storage to Microsoft Windows systems, then Linux RHEL 5 client with FUSE must be installed on the Atmos Server.
Internet Explorer 6 or 7		✓	Used with the Atmos system management GUI.
Active Directory 2008		✓	In order to authenticate CIFS access to Atmos nodes with Active Directory
TOE appliance hardware		✓	Provides Atmos with physical layer 1 components. This includes the chassis, networking hardware, and interfaces and ports.
TOE virtual appliance hypervisor		✓	Provides the Atmos VE with the virtual environment necessary for its execution, including networking adapters, storage, and other virtual resources.
SMTP server		✓	The Atmos server relies upon an external SMTP server to deliver alert messages and forgotten passwords for administrative users.
NTP server		✓	The external NTP server provides a reliable time stamp to the OS.

1.5.1.1 Guidance Documentation

The following guides provide additional information and are considered to be part of the TOE:

- EMC Atmos v2.0 Administrator's Guide
- EMC Atmos v2.0 Programmer's Guide
- EMC Atmos v2.0 Security Configuration Guide
- EMC Atmos v2.0 Non-EMC Software License Agreements
- EMC Atmos v2.0.1 Physical Hardware Installation Procedures
- EMC Atmos v2.0.1 Virtual Edition Installation Procedures
- EMC Atmos v2.0.1 Release Notes

[18] RHEL = Red Hat Enterprise Linux
[19] This is a developer kit and add-on to the OS.

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Functions:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF[20]
- Resource utilization

1.5.2.1 Security Audit

The Atmos Server software generates audit records for the security relevant actions of all authorized administrators. The Atmos Server software makes sure that only authorized administrators are allowed to view the audit records.

1.5.2.2 User Data Protection

Atmos controls access to its user data and metadata by enforcing the Atmos Discretionary Access Control policy. Access to Atmos user data and metadata is controlled by the user's assigned role and object ACLs[21] and UIDs[22].

1.5.2.3 Identification and Authentication

Atmos identifies and authenticates all administrative users before they are allowed access to the System management GUI. In addition, Atmos authenticates end user accessing Atmos via a Web browser also known as "Web-services users" with user name and shared secret..

1.5.2.4 Security Management

Atmos provides a web-based System management GUI for the management of TSF data, which is the data for the operation of the TOE upon which the enforcement of the SFRs relies. Atmos controls security for administrative tasks through role-based access control. It includes roles for managing the system, tenants, and subtenants. The System management GUI allows authorized administrators to manage the TSF data of Atmos.

1.5.2.5 Protection of the TSF

Atmos protects its programs and data from unauthorized access through its own interfaces. Atmos preserves a secure state when the following failures occur: operational failure of a single Server Node when set up in a multi-node configuration, or a transaction is interrupted by machine error.

1.5.2.6 Resource Utilization

Atmos maintains full TOE functionality if one Atmos server goes offline when set up in a multi-node configuration. Atmos allows for data to be replicated across multiple nodes based on user defined policy.

[20] TSF = TOE Security Functionality
[21] ACL = Access Control List
[22] UID = User Identification

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Most features and functionality of EMC Atmos 2.0.1 are part of the evaluated configuration of the TOE. The Admin API will be excluded from the TOE Boundary.

The hardware components of the Atmos appliances are excluded from the evaluation. The external LDAP and AD servers used for authentication are excluded from the TOE.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 6/16/2010 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[23] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[24] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives. The following threats are applicable:

Table 5 - Threats

Name	Description
T.ACCOUNT	The security relevant actions of users may go undetected which could lead to a misconfiguration of the TOE or loss of data being unaccounted for.
T.ACCESS	An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE to access and use security functions and/or other functionality provided by the TOE.
T.TOEFAIL	The failure of a TOE server may result in a failure to meet the TSF.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

[23] IT – Information Technology
[24] TSF – TOE Security Functionality

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 - Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware with the recommended third party software.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 7 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.ACCESS	The TOE will allow authorized TOE users to access only authorized TOE functions and data.
O.AUDIT	The TOE must record audit records for use of the TOE functions.
O.AUTHEN	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.SAFEFAIL	The TOE must protect the TSF in the event of failure of a single TOE server in a redundant pair configuration.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 - IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 - Non-IT Security Objectives

Name	Description
OE.MANAGE	Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PROTECT	Those responsible for the TOE must ensure that the physical environment must be suitable for supporting a computing device in a secure setting.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with the Product Documentation.

5 Extended Components

There are no TOE Extended Components.

5.1 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

Name	Description	S	A	R	I
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.1	Degraded fault tolerance		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events, for the [not specified] level of audit; and

c) [*the specifically defined auditable events as listed in Table 11* -

Table 11 - Auditable Events

Atmos Server
Creation of a Resource Management Group (RMG)
Creation of a Subtenant
Assignment of the Subtenant admin role to a user
Removal of a subtenant admin role from a user
Creation of a Tenant
Assignment of the Tenant admin role to a user
Removal of the Tenant admin role from a user
Assignment of a storage placement policy to a subtenant
Modification of the default storage policy for a subtenant
Modification of the LDAP key store configuration
Administrative user changed password
Administrative user modified profile information (email, phone)
Administrator issued a log collection operation
Administrator issued a request to generate a system report (Configuration snap shot)
Administrator configured a remote MDS replica
Administrator configured SNMP (RMG or System level)
Administrator acknowledge an alert (or all alerts)
Administrator created a UID for application (i.e. REST access)
Administrator disables/enables UID
Administrator modified UID contact information
Administrator deleted an alert (or all alerts)
Administrator created a placement policy
Administrator deleted a placement policy
Administrator modified a placement policy
Administrator delete a policy sector

Atmos Server
Administrator modified the SMTP configuration
Removal of the system administrator role from a user
Rename of a Tenant
Generation of temporary password for admin user
Upgrade operation started
Update the software serial number
Administrator successfully authenticated

].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorised administrator*] with the capability to read [*audit events*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control policy*] on [*all subjects (users and user applications), all DBMS-controlled objects (data, metadata) and all operations among them*].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Discretionary Access Control policy*] to objects based on the following: [
Subjects: processes acting on behalf of users and user applications
Subject security attributes: Roles
Objects: data, metadata
Object security attributes: ACLs, UIDs
].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) If the authorized user or user application associated with the subject is the owner of the object, then the requested access is allowed; or
b) If the authorized user or user application associated with the subject has the object access right for the requested access to the object, then the requested access is allowed; or
c) Otherwise, the access is denied].

FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the [*none*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users: [*user name, password, role*].
Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
FIA_UAU.5.1
The TSF shall provide [*the following multiple authentication mechanisms:*
[

- *User name and password for users*
- *Registered applications authenticated with unique User ID and shared secret.*

] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*internally stored identity and credential information*.].

Dependencies: No dependencies

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control policy*] to restrict the ability to [query, modify [*none*] the security attributes [*access control*] to [*the authorised administrator roles and owner of the object*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Discretionary Access Control policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*SysAdmin*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [change_default, query, modify, delete, clear, [*and other operations as defined in column 'Operation'* of *Table 12*]] the [*TSF data as defined in column 'TSF Data' of Table 12* to [*the authorized identified roles as defined in column 'Authorized Role' of Table 12*].

Table 12 - Management of TSF Data

Operation	TSF Data	Authorized Role
Configure	NTP[25] server parameters	SysAdmin
Configure	Federation target	SysAdmin
Configure	SSL certificates	SysAdmin
Configure	MDS[26] remote replication	SysAdmin
Configure	Installation Segments	SysAdmin
List, create, rename	Tenant	SysAdmin
Add node to a Tenant	node	SysAdmin
List, create, modify, delete	subtenant	TenantAdmin
Define	Policy	TenantAdmin
Confirm, delete	Alert	SysAdmin

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [*management of TSF data, management of security attributes*].
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*SysAdmin, TenantAdmin, and SubtenantAdmin*].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*operational failure of a single Server Node when in a multi-TOE configuration.*].
Dependencies: No dependencies.

[25] NTP = Network Time Protocol
[26] MDS = Metadata Service

6.2.6 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance
Hierarchical to: No other components.
FRU_FLT.1.1

The TSF shall ensure the operation of [*maintain full TOE functionality*] when the following failures occur: [

- *any failure of a single non-master node when in a multi-node configuration.*].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 13 - Assurance Requirements summarizes the requirements.

Table 13 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 14 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.1	Degraded fault tolerance

7.1.1 Security Audit

Atmos provides audit logging capabilities. Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who (i.e., which user) is responsible for those activities.

Atmos provides non-configurable full auditing of specified administrative actions done through the System management GUI. Audit records are stored internally within the internal database. The ability to review audit records is only available to authorized administrative users.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1.

7.1.2 User Data Protection

The user data protection function implements a Discretionary Access Control policy for users and user applications accessing user data and metadata that is stored within Atmos. The TOE enforces the Discretionary Access Control policy on all access requests to access the end user's and user application's stored data which includes both the user data and metadata stored within Atmos.

The *Discretionary Access Control policy* controls authorized user access to objects within the TOE's Scope of Control. The *Discretionary Access Control policy* supports a set of user privileges based on roles and object-level permissions based on ACLs and UIDs that determine what operations a user and user application can perform on a particular object.

The ACL element specifies the access-control permissions assigned to an object. Only the object owner can assign or modify permissions of an object. The permissions that can be assigned to an object are as follows:

- Read
- Write
- Full Control
- None

.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1.

7.1.3 Identification and Authentication

Atmos maintains the following security attributes for users that are created within the internal LDAP directory: user name, password, and role.

Atmos offers multiple authentication mechanisms. Atmos identifies and authenticates administrative users logging in at the System management GUI as well as web-services users. Web services applications must authenticate to their assigned node with a shared secret. For a more detailed explanation of these identification and authentication mechanisms see sections 7.1.3.1,7.1.3.2,7.1.3.3 below.

7.1.3.1 Administrative Users

Each administrative user must be identified and authenticated before being allowed access to Atmos resources. Atmos identifies and authenticates administrative users logging in at the System management GUI. Identification and authentication are provided by Atmos' internal LDAP directory service which is used for user authentication.

Access to the System management GUI with the SysAdmin role is through a web browser with a user name and password with local authentication set as the 'Auth Type'. Likewise access to the System management GUI as a TenantAdmin and Subtenant Admin is through a web browser with a user name and password with a specification of the 'Tenant' and optionally 'Subtenant'.

7.1.3.2 Web-services Users

Web-services users are defined by the tenant administrator when they create web-services users. The web-services users are stored in an either in an internal file or in an external LDAP server. For the purposes of the evaluated configuration they will be stored internally. The authentication is done by Atmos by

comparing the user id (UID), shared secret, and subtenant ID. If there is a match the Web-services request is allowed. The shared secret is stored either in an internal file or an external LDAP server.

7.1.3.3 Web services applications

All web-service applications must authenticate to their assigned node with a UID and shared secret.

TOE Security Functional Requirements Satisfied: FIA_UAU.5, FIA_UID.2, FIA_ATD.1.

7.1.4 Security Management

Security management specifies how Atmos manages several aspects of the TSF: security attributes, TSF data, and functions. Atmos provides authorized administrators with the System management GUI to easily manage the security functions of Atmos such as the management of TSF data and management of security attributes.

Atmos implements role-based access control for administrative tasks. The following Roles as pre-configured in Atmos:

- SecurityAdmin
- SysAdmin
- TenantAdmin
- SubTenantAdmin

7.1.4.1 SecurityAdmin

The SecurityAdmin is a built-in super-user responsible for initial installation and creating SysAdmins. During the installation process, the SecurityAdmin does the following:

- Resets the default SecurityAdmin password
- Creates a SysAdmin role, which is then used to complete the installation

This is the only SysAdmin until and unless others are added.

The system supports only one SecurityAdmin.

7.1.4.2 SysAdmin

The SysAdmin role is responsible for overall management of an Atmos system, including management of segments, tenants, RMGs, and nodes; changing faulty disks; and adding new hardware. Specified users may be assigned the SysAdmin role. The SysAdmin role is maintained in the Atmos system management database and role based authorization is handled by the Atmos system management.

Multiple users may be assigned the SysAdmin role.

7.1.4.3 TenantAdmin

The TenantAdmin role is responsible for managing subtenants, and policies for the tenant to which they are assigned. The SysAdmin assigns specific users the TenantAdmin role within a given tenant. Policies are assigned by the TenantAdmin to a specific subtenant. TenantAdmins are unaware of system resources other than those assigned to their tenant. A TenantAdmin also can do anything that a SubtenantAdmin can do. A TenantAdmin registers applications (which involves generating and adding new UID/Shared Secret pair) and adds policies for the corresponding applications. A given tenant can have multiple TenantAdmins, but a given TenantAdmin can be a TenantAdmin for only one tenant.

7.1.4.4 SubtenantAdmin

Subtenants are logical partitions of tenants that group together selected policies and data access. Each subtenant has a unique set of users and sees a unique set of data. A given object can be seen by only one subtenant. When the SysAdmin creates a tenant, the system automatically creates one corresponding subtenant (which has a name identical to the tenant). SysAdmins can choose to create additional subtenants within each tenant. SubtenantAdmins create users for a subtenant.

A SubtenantAdmin can only create a UIDs for its subtenant and re-order the way storage policies are applied.

TSF data is the data used by Atmos for security functionality purposes. For example, user roles and passwords are considered to be TSF data. The allowed operations on TSF data and the authorized roles required to execute them are listed in Table 16.

The Atmos server uses restrictive default values for its security attributes. The allowed operations on security attributes are described in Table 15.

Table 15 – Management of Security Attributes

Operation	Security Attribute	Role
Query, add, delete	Administrative user	SysAdmin, TenantAdmin
Create, change	password	SysAdmin, TenantAdmin, and SubtenantAdmin
Query, assign, delete	role	SysAdmin, TenantAdmin
Query, modify, set	ACL	Owner of the object
Query, create UID and assign to Subtenant, delete	UID	TenantAdmin, SubtenantAdmin

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified.

The Atmos servers will maintain a secure state when there is a failure of one Atmos server when the TOE is set up in a multi-server configuration

TOE Security Functional Requirements Satisfied: FPT_FLS.1.

7.1.6 Resource Utilization

Atmos allows for data to be replicated across multiple nodes in a mulit-node configuration. The data storage service provides for multiple storage options.

During the RMG configuration step of the installation process, an authorized administrator is prompted to define the storage service attributes. The storage service attributes define how the Atmos data is placed and transformed. By default Atmos provides for 'optimal' data placement which provides for round robin storage services. Atmos rotates requests equally among all available storage disks. In the event a storage disk fails, data availability is still provided by Atmos.

The authentication service comprises multiple authentication servers (one master and several read-only slaves). If the master authentication server temporarily is unavailable (for example, because it is down or there is a network disconnection), a failover process is triggered. While failover is in progress, administrative users can be authenticated against only those authentication servers which are up. During the failover window, while the master authentication server is unavailable, write operations (adding and deleting system-management users) will fail until the new master authentication server is up and running. If an administrator has been authenticated and is connected during an Atmos Server failure they will still have a valid token and will be able to fully manage the system. If the administrator user is trying to connect during the failover they will not be able to connect and therefore cannot perform any operations (write or otherwise). I/O[27] is not impacted by an Atmos Server failure. End users will continue to be able to access their data while the failover is in progress.

When Atmos is installed, there are two MDS instances running on two different nodes in the same RMG, in a master-slave mode. The master MDS replicates its data to the slave MDS. If this RMG goes offline (e.g., due to a power or network outage), all objects owned by this MDS pair are unavailable to the user. The MDS remote replica feature enables an authorized SysAdmin to configure a secondary RMG location to replicate metadata. Then, if the primary RMG becomes unavailable, Atmos can read from the secondary RMG. In the evaluated configuration, a second RMG will be configured in order to provide continuous availability to MDS.

TOE Security Functional Requirements Satisfied: FRU_FLT.1.

[27] I/O = Input / Output

8 Rationale

8.1 Conformance Claims Rationale

This Security Target is considered to be Part 2 and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1 and 8.2.2 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 - Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ACCOUNT The security relevant actions of users may go undetected which could lead to a misconfiguration of the TOE or loss of data being unaccounted for.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must record audit records for use of the TOE functions.	O.AUDIT counters this threat by ensuring that all relevant TOE security actions are recorded.
T.ACCESS An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.	O.ACCESS The TOE will allow authorized TOE users to access only authorized TOE functions and data.	O.ACCESS counters this threat by ensuring the TOE will allow authorized TOE users to access only authorized TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.
	O.AUDIT The TOE must record audit records for use of the TOE functions.	O.AUDIT counters this threat by ensuring that all relevant TOE security actions are recorded.
T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE to access and use security functions and/or other functionality provided by the TOE.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges	O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.

Threats	Objectives	Rationale
	and only those TOE users, may exercise such control.	
	O.AUTHEN The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHEN counters this threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
T.TOEFAIL The failure of a TOE server may result in a failure to meet the TSF.	O.SAFEFAIL The TOE must protect the TSF in the event of failure of a single TOE server in a redundant pair configuration.	O.SAFEFAIL mitigates this threat by protecting the TSF in the event of a failure of a single TOE server in a redundant pair configuration.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 17 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware with the recommended third party software.	OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with the Product Documentation.	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with the Product Documentation.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE must be competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
A.PROTECT The components of the TOE critical to security policy	OE.PROTECT Those responsible for the TOE must ensure that the physical	Those responsible for the TOE must ensure that the physical environment must be suitable for

Assumptions	Objectives	Rationale
enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.	environment must be suitable for supporting a computing device in a secure setting.	supporting a computing device in a secure setting.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	The TOE environment must provide reliable timestamps to the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no Extended TOE Security Functional Requirements.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended TOE Security Assurance Requirements.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 - Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring administrators with the ability to manage security attributes for the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE defining the access control policy as restrictive by default.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only

Objective	Requirements Addressing the Objective	Rationale
		authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ACCESS The TOE will allow authorized TOE users to access only authorized TOE functions and data.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing an access control policy on users and administrators.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by defining the attributes that are used to enforce the access control policy.
O.AUDIT The TOE must record audit records for use of the TOE functions.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
O.AUTHEN The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing an access control policy on users and administrators.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by defining the attributes that are used to enforce the access control policy.
	FIA_ATD.1 User attribute definition	The requirement meets this objective by defining the attributes of users.
	FIA_UAU.2 User authentication before any	FIA_UAU.2 supports this objective by requiring users to

Objective	Requirements Addressing the Objective	Rationale
	action	authenticate before allowing them to perform any actions on the TOE.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that each administrator is authenticated before gaining access to TOE functions.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that each administrator is identified before gaining access to TOE functions.
O.SAFEFAIL The TOE must protect the TSF in the event of failure of a single TOE server in a redundant pair configuration.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by providing that the TOE will preserve a secure state through specified failure events.
	FRU_FLT.1 Degraded fault tolerance	The requirement meets the objective by providing for a specific level of functionality given a specified failure mode.

8.5.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2. EAL2+ was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. EMC Atmos v2.0.1 is targeted to be installed in an environment with good physical access security (OE.PROTECT) and competent administrators (OE.MANAGE, A.MANAGE), where EAL 2 should provide adequate assurance. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users. This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 19 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 19 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time

SFR ID	Dependencies	Dependency Met	Rationale
			stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FAU_GEN.1	✓	
FAU_SAR.1	No dependencies	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.2	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UID.2	No dependencies	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	No dependencies	✓	
FRU_FLT.1	FPT_FLS.1	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 20 - Acronyms

Acronym	Definition
ACL	Access Control List
AD	Active Directory
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
COS	Cloud Optimized Storage
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GID	Group Identification
GUI	Graphical User Interface
IFS	Installable File System
I/O	Input / Output
IS	Installation Segments
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MDS	Metadata Service
MES	Micro Edition Suite
MP3	MPEG-1 Audio Layer 3
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
REST	Representational State Transfer
RHEL	Red Hat Enterprise Linux
RMG	Resource Management Groups
SAR	Security Assurance Requirement

Acronym	Definition
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
U	Unit
UID	User Identification

9.2 Terminology

Table 21 - Terms

Term	Definition
cloud	The concept of an intentionally abstracted storage or computing network which, although technically complicated and highly distributed, appears to end-users to be simple and centralized ("on the Internet" or "on the corporate network").
managed device	A managed device is the hardware that the Atmos Server relies upon.
master node	The *master node* is installed in each installation segment. When a new RMG is added to the system, it has one installation segment, hence one master node. If more installation segments are added to that RMG later, there are more master nodes: an RMG with N installation segments has N master nodes. The very first master node in an Atmos system is the initial master node.
MDS	Metadata Service. This is where the metadata is stored.
metadata	One of two components of an object, along with user data. Metadata is divided into: • System metadata—Examples are filename, file size, modification date, timestamps, and access-control lists. • User metadata — This comprises arbitrary key/value pairs. Examples of user metadata is artist name (e.g., for MP3 data) and customer type.
node	A physical server containing a collection of Atmos services
petabyte	A quadrillion bytes (10^15 bytes or 2^50 bytes), 1,000 terabytes.

Term	Definition
rPath Linux v2	The rPath Linux v2 OS provides a platform for software vendors to create and maintain software appliances. A major feature of rPath is Conary, a software package management and configuration program that allows rollbacks, incremental ("changeset") updates, and distributed downloading..
RMG	A collection of installation segments that share a single domain. In almost all cases, this is equivalent to a subnet on the "public," customer network. You can create multiple RMGs on the same subnet, as long as each RMG has a unique address. RMGs are responsible for monitoring and discovering nodes within the subnet.
Sub-tenant	A logical subset of a tenant that group together selected policies, data access (i.e., file-system or Web-service namespaces), and reporting capabilities. When the SysAdmin creates a tenant, the system automatically creates one corresponding subtenant (which is identical to the tenant). SysAdmins can choose to create additional subtenants within each tenant.
tenant	A conceptual subset of the storage resources within an Atmos system. Associated with a tenant are specific storage resources, security control, storage policies, and access to the data stored on that tenant's resources. Each tenant has a name that is unique system-wide.
TSF data	Security relevant data managed by the TOE. This is data for the operation of the TOE upon which the enforcement of the SFR relies.
user data	One of two components of an object, along with metadata. This is data for the user that does not affect the operation of the TSF.

9.3 Documentation References

Table 22 – Documentation References

Term	Definition
Admin Guide	EMC Atmos v2.0 Administrator's Guide
Programmer's Guide	EMC Atmos v2.0 Programmer's Guide
Security Config	EMC Atmos v2.0 Security Configuration Guide
License Agreements	EMC Atmos v2.0 Non-EMC Software License Agreements
Installation Guide	EMC Atmos v2.0.1 Physical Hardware Installation Procedures
Release Notes	EMC Atmos v2.0.1 Release Notes

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com