SECURITY TARGET

FOR

CENTRIFY SUITE VERSION 2013.2

Document No. 1769-000-D0007

Version: v0.89, 12 September 2013

Prepared for:

Centrify Corporation

785 N. Mary Avenue, Suite 200

Sunnyvale, California

USA, 94085

Prepared by:

Electronic Warfare Associates-Canada, Ltd.

1223 Michael St.

Suite 200
Ottawa, Ontario, Canada
K1J 7T2

TABLE OF CONTENTS

1 ST INTRODUCTION 6
1.1 DOCUMENT ORGANIZATION 6
1.2 SECURITY TARGET REFERENCE 6
1.3 TARGET OF EVALUATION REFERENCE 7
1.4 TOE OVERVIEW 8
1.4.1 Centrify DirectControl 8
1.4.2 Administrative Roles 9
1.4.3 DirectControl Security Features 9
1.4.4 DirectControl Role Assignments 11
1.4.5 Zone Technology 12
1.4.6 Identification and Authentication for Users and Groups 13
1.5 TOE DESCRIPTION 13
1.5.1 Physical Scope 13
1.5.2 DirectControl UNIX Components included in the TOE 13
1.5.3 DirectControl Windows Components included in the TOE 14
1.5.4 DirectControl TOE and External Interfaces 15
1.5.5 TOE Environment Software 15
1.5.5.1 TOE Guidance Documentation 16
1.5.6 Logical Scope 16

2 CONFORMANCE CLAIMS 18
2.1 COMMON CRITERIA CONFORMANCE CLAIM 18
2.2 PROTECTION PROFILE CONFORMANCE CLAIM 18

3 SECURITY PROBLEM DEFINITION 19
3.1 THREATS, POLICIES AND ASSUMPTIONS 19
3.1.1 Threats 19
3.1.2 Organizational Security Policies 19
3.1.3 Assumptions 19

4 SECURITY OBJECTIVES 21

4.1 SECURITY OBJECTIVES FOR THE TOE 21
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 21
4.3 SECURITY OBJECTIVES RATIONALE 23
4.3.1 Security Objectives Rationale Related to Threats 24
4.3.2 Security Objectives Rationale Related to Organizational Security Policies 26
4.3.3 Security Objectives Rationale Related to Assumptions 27

5 EXTENDED COMPONENTS DEFINITION 29
5.1 FTA_IDM_EXT.1 29

6 SECURITY REQUIREMENTS 30
6.1 CONVENTIONS 30
6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 30
6.2.1 Security Audit (FAU) 31
6.2.1.1 FAU_GEN.1 Audit data generation 31
6.2.2 Cryptographic Support (FCS) 32
6.2.2.1 FCS_CKM.1 Cryptographic key generation 32
6.2.2.2 FCS_CKM.4 Cryptographic key Destruction 32
6.2.2.3 FCS_COP.1 Cryptographic operation 32
6.2.3 Identification and Authentication (FIA) 33
6.2.3.1 FIA_AFL.1 Authentication failure handling 33
6.2.3.2 FIA_ATD.1 User attribute definition (UNIX User) 33
6.2.3.3 FIA_UAU.1 Timing of authentication 34
6.2.3.4 FIA_UID.1 Timing of identification 34
6.2.4 Security Management (FMT) 34
6.2.4.1 FMT_MOF.1 Management of security functions behaviour 34
6.2.4.2 FMT_SMF.1(1) Specification of Management Functions (DirectManage Access Manager) 35
6.2.4.3 FMT_SMF.1(2) Specification of Management Functions (Centrify DirectControl UNIX Agent) 35
6.2.4.4 FMT_SMR.1 Security roles 35
6.2.4.5 FTA_IDM_EXT.1 Identity Management 35
6.2.4.6 FTP_ITC.1 Inter-TSF trusted channel 35
6.3 SECURITY REQUIREMENTS RATIONALE 36
6.3.1 Security Functional Requirements Rationale Related to Security Objectives 36
6.4 DEPENDENCY RATIONALE 38

6.5 TOE SECURITY ASSURANCE REQUIREMENTS 39

7 TOE SUMMARY SPECIFICATION 41

7.1 TOE SECURITY FUNCTIONS 41

7.1.1 Security Audit 41

7.1.2 Cryptographic Support 42

7.1.3 Identification and Authentication 42

7.1.4 Security Management 42

7.1.5 TOE Access 43

7.1.6 Trusted Channel 44

8 ACRONYMS 45

LIST OF FIGURES

Figure 1 - DirectControl TOE and External Interfaces 15
Figure 2 - FTA_IDM_EXT Component Levelling 29

LIST OF TABLES

Table 1 - Logical Scope of the TOE 17
Table 2 - Mapping Between Objectives, Threats, Organizational Security Policies, and Assumptions 23
Table 3 – Summary of Security Functional Requirements.....31
Table 4 – Auditable Events.....32
Table 5 – Cryptographic Operation.....33
Table 6 – Security Functions Behaviour 34
Table 7 - Mapping of SFRs to Security Objectives 36
Table 8 - Security Functional Requirements Rationale.....38
Table 9 - Functional Requirement Dependencies 39
Table 10 - EAL 2 Assurance Requirements 40
Table 11 – Mapping of Security Functions to Security Functional Requirements.....41

1 ST INTRODUCTION

1.1 DOCUMENT ORGANIZATION

Section 1**, ST Introduction**, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2**, Conformance Claims**, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, **Security Problem Definition**, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4**, Security Objectives**, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7**, TOE Summary Specification**, describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.

Section 8**, Acronyms**, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

This document, version v0.89, dated 12 September 2013, is the Security Target for the Centrify Suite 2013.2. Centrify Suite is an integrated family of Active Directory-based auditing, access control and identity management solutions that secure an enterprise's cross-platform environment and strengthen its regulatory compliance initiatives.

Only a subset of the Centrify Suite functions is included in the security target. This subset is referred as the ***feature set.***

The feature set installs partly on Windows and partly on UNIX platforms. The Windows components of the feature set, referred to as the ***Centrify Administrator Consoles*** are a set of GUI based management tools used to assign UNIX identity attributes to Active Directory users and groups, define and apply role-based access control (RBAC) rights and roles. The UNIX components of the feature set, referred to as ***Centrify DirectControl*** implement the authentication and identity mapping functions necessary for Active Directory users and groups to behave like UNIX users and groups on UNIX platforms. Centrify DirectControl enforces the

RBAC roles managed by the Centrify Administrator Consoles and the Windows group policies that are managed outside the Security Target.

The Centrify Administrator Consoles include the following:

- ***DirectManage Access Manager Console*** – GUI based program for managing Centrify's Active Directory objects
- ***ADUC Property page extensions Snap-in*** - Centrify's extension to the Microsoft Management Console (MMC) Active Directory Users and Computers (ADUC) utility also referred to in this document as the "***DirectManage ADUC Snap-in*** or simply ***ADUC Snap-In***". The ADUC Snap-in manages the UNIX identity attributes assigned to Active Directory users and groups.

Centrify DirectControl includes the following:

- ***DirectControl UNIX agent*** – The Centrify UNIX daemon also referred to in this document as "***adclient***".
- ***DirectControl UNIX tools*** – A subset of the Centrify Suite UNIX command line utilities.
- ***DirectControl UNIX libraries*** – The Centrify supporting libraries for logon, cryptography and trusted channel functions.
- ***DirectControl UNIX files*** –Centrify DirectControl managed files for the purposes of
  - Static Configuration
  - Active Directory object caching
  - Role-based Access Control (RBAC) object caching
  - Auditing

Centrify Suite runs on over 200 different UNIX-based operating systems. This evaluation is to be performed on three different platforms as detailed below.

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation for this Security Target is the Centrify Suite 2013.2 feature set and is a software only TOE. The feature set includes:

Name	Version	Build
DirectManage Access Manager Console	5.1.1	831
DirectManage ADUC Snap-in	5.1.1	831
Centrify DirectControl (RedHat)	5.1.1	831
Centrify DirectControl (Mac)	5.1.1	831

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.

1.4.1 Centrify DirectControl

Centrify DirectControl provides Active Directory-based authentication, access control, single sign-on and group policy support for UNIX, Linux and Macintosh platforms.

Through the DirectControl UNIX Agent, UNIX, Linux, and Mac OS X servers and workstations can become part of an Active Directory domain and act as Active Directory domain members. Once part of a domain, you can secure those systems using the same authentication, access control, and group policy services you deploy for Windows computers. Additional modules work with the DirectControl UNIX Agent to provide services such as single sign-on for Web applications and SAP, and Samba integration. Centrify Suite 2013 also provides a set of management utilities that include an administrator console called DirectManage Access Manager, extensions for Active Directory Users and Computers, out-of-the-box reporting, and account migration tools. With Centrify DirectControl, organizations with diverse IT environments can leverage their investment in Active Directory to:

- Move to a central directory with a single point of administration for user accounts and security policy.
- Use Centrify DirectControl Zones to provide secure, granular access control and delegated administration.
- Extend Web single sign-on to internal end-users and external business partners and customers.
- Simplify compliance with regulatory requirements.
- Deploy quickly without intrusive changes to the existing infrastructure.
- Control TOE user operations with Role Based Access Control (RBAC).

By extending Active Directory to manage Linux, UNIX, and Mac OS X computers, Centrify DirectControl provides administrators with a comprehensive identity and access management solution while reducing administrative complexity and overhead.

By consolidating user accounts in Active Directory, organizations can improve IT efficiency and move toward a more secure, connected infrastructure for their heterogeneous environment. Using DirectControl enables an organization to:

- Strengthen security by consolidating user accounts into Active Directory, making it easy for IT managers to disable the accounts of departing employees, and locate and eliminate security risks posed by orphan accounts.
- Reduce infrastructure costs by eliminating redundant identity stores, including legacy directories, unsecured NIS servers, dedicated application databases and locally managed /etc/passwd files.

- Streamline operations by standardizing on a single set of Active Directory-based tools to simplify administrative training and in-house processes for account provisioning, maintenance, and other tasks.
- Establish consistent password policies across a heterogeneous environment by enforcing Active Directory's rules for password complexity and expiration for all users regardless of where they log in.
- Improve productivity and satisfaction for end-users, who now have only one password to remember, and make fewer Help Desk calls to reset passwords or update their account information.
- Enforce consistent security and configuration policies across UNIX, Linux, and Mac OS X servers and workstations by adding Centrify DirectControl group policy templates for computer- and user-based configuration settings to Windows Group Policy Objects.
- Improves compliance by limiting the access rights of privileged users, consistently applying security policy across platforms and providing the detailed and specific reports on access controls that auditors demand.
- Control access to sensitive systems and applications by using Centrify zones, rights and role assignments, and delegated administration to grant role-based access to network resources.

1.4.2 Administrative Roles

Three distinct security roles are defined for the TOE: The Windows Administrator, the UNIX Administrator and the UNIX User.

The Windows Administrator uses the DirectManage Access Manager and other Windows-based utilities (such as the Windows Group Policy Editor) to configure all of the data used by the TOE and stored in Active Directory. This Windows Administrator can be any Windows user who has been granted appropriate permissions to manage Active Directory objects. The account can be, but is not necessarily, the default Administrator account for the domain or the local computer.

The UNIX Administrator uses TOE programs and UNIX-based utilities to connect to Active Directory and manage the operation of the UNIX TOE components and all TOE-related data.

The UNIX User is allowed to log on and access TOE resources, and perform allowed operations based on the permissions granted by the TOE administrators.

1.4.3 DirectControl Security Features

Authentication

After a computer joins an Active Directory domain, when an Active Directory user needs to be authenticated, the TOE passes the user's account name and password credentials to Active Directory to authenticate the user's identity. This pass-through authentication takes place in the following scenarios:

Console Logon

Users log on to UNIX computers locally from a login prompt or login window using their Active Directory domain credentials.

Smart Card

Users may logon to UNIX computers using several different types of supported smart cards including Common Access Card (CAC) and Personal Identify Verification (PIV) smart cards. Note that smart card hardware and drivers are outside of the TOE, and no specific card is claimed in the evaluation. However Smart cards are legitimate sources of credentials, just as a local user performing a console logon.

Offline Logon

In the Common Criteria configuration, the TOE supports local caching of authentication credentials. By caching authentication credentials, the TOE allows users to log on to computers even if they are disconnected from network or if an Active Directory domain controller is not available.

User UNIX Identity Assignment and Configuration

A UNIX profile for an Active Directory user determines how the user is identified on UNIX computers managed by the TOE. Windows administrators use the DirectManage Access Manager to configure the UNIX profile data. The UNIX profile data resides in Active Directory within DirectControl zones structures. The TOE applies the UNIX profile from TOE configured data on the Active Directory user's behalf whenever the user's identity is being established.

User UNIX Group Membership Assignment and Configuration

As part of their UNIX profile in Active Directory, users are assigned a default primary group, either automatically as a private group or configured by the Windows administrator using the TOE. In addition the user's primary group, the user's UNIX profile can include Active Directory group membership for groups that are assigned UNIX attributes using the TOE.

Windows administrators use the DirectManage Access Manager to configure UNIX profile data for Active Directory groups.

User Auditing Functions

The TOE generates audit events for Active Directory user operations. The audit log file name, location, modules audited, and level of detail are all configurable.

Group Security Policy Configuration and Enforcement

DirectControl provides several sets of group policies that administrators can use to control the configuration and operation of UNIX, Linux, and Mac OS X computers. DirectControl also makes available group policies that control settings for users logging on to UNIX, Linux, and Mac OS X computers. By using Active Directory group policy, administrators can centrally enforce security and configuration policies across the enterprise. These policies are available as extensions to the standard Windows group policy interfaces.

Group security policy settings are applied to UNIX computers and users at startup, user logon, and at regular intervals. In addition, an administrator can update policies immediately by running the adgpupdate command line program. An administrator can configure group security policies to control a TOE user's access to resources.

Role-Based Access Control (RBAC) Security Configuration and Enforcement

Windows administrators use the DirectManage Access Manager to centrally manage the operations users can perform on DirectControl-managed computers, including the ability to log on to a computer (logon role), through the assignment of pre-defined or user-defined rights and roles. A right represents a specific operation that the user is allowed to perform. Rights are combined into roles that reflect the needs of a specific job function, such as database or web site administration, or the ability to perform a particular task, such as log in. Roles are then assigned to individual Active Directory users or groups. To access a computer, a user must have an identity in the form of a complete UNIX profile and an assignment to at least one role that is valid in the zone to which the computer is joined.

Beyond simple access control, administrators can control the operations that a TOE user can perform using the TOE's role-based access control mechanism. For instance, an administrator can control whether a user can establish a logon shell by assigning a logon role or be authenticated without logon access by assigning a listed role. Administrators can also use roles to grant a user elevated privileges to perform specific tasks, or to strictly limit his access to a defined subset of commands in a customized restricted environment shell.

Please note that the Role-Based Access Control feature is available only on Red Hat. On Mac, only the system UNIX Login role applies: i.e. every user still needs to be assigned this role in order to login to Mac machines.

Offline Authentication

Once an Active Directory user logs on to a UNIX computer successfully, the authentication credentials are cached by the TOE. These credentials can then be used to authenticate the user in subsequent logon attempts if the user is disconnected from the network or an Active Directory domain controller is not available. Any Role-Based Access Control configuration still applies to the user in offline mode.

FIPS compliant cryptography

The TOE provides a group policy that requires all cryptographic functions to use FIPS 140-2 Level compliant cryptographic algorithms.

1.4.4 DirectControl Role Assignments

DirectControl's built-in authorization facility centrally manages and enforces RBAC-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems. By controlling how users access systems and what they can do on those computers, DirectControl role assignments enable organizations to lock down sensitive systems and eliminate uncontrolled use of root accounts and passwords.

As mentioned before, a role definition is comprised of rights. A right represents a specific operation that the user is allowed to perform. Rights are classified as follows:

- **System rights**, specifically UNIX rights, specify whether and how a user can login to a computer (with and/or without password) and determine whether a user logs into a normal shell or a restricted shell.

- **Audit rights** specify whether auditing is requested, required, or neither, in order for a user to login.
- **PAM access rights** identify the specific UNIX PAM-enabled applications a user can access. In addition to the predefined PAM rights such as login-all and SSH, users can create new ones.
- **Commands** identify specific commands a user can run and what user account should be used to invoke the commands. There are no pre-defined commands.
- **SSH rights** identify the specific SSH services (e.g. SCP, SFTP) available to a user with PAM SSH access rights assigned.

Rights are combined into roles that reflect the needs of a specific job function or the ability to perform a specific task. Centrify DirectControl pre-defines some commonly used roles, such as the UNIX Login role that grants all UNIX system login rights and access to all PAM applications; and Listed role which makes the user visible in a zone but does not assign any UNIX system rights or PAM access rights. It is also possible to create new roles. Administrators then assign roles to individual Active Directory users or Active Directory groups. When multiple roles are assigned to a user or group, the rights from these roles accumulate. During role assignment, the administrator can also define the specific days and times the role takes effect.

Centrify DirectControl also provides another type of role called Computer role, which is a set of role assignments (a set of users with a set of roles) linked to a group of computers.

Please note that the DirectControl UNIX Agent on Mac supports only the UNIX Login role.

1.4.5 Zone Technology

DirectControl's unique zone technology provides an enterprise-class solution for assigning UNIX identity attributes and configuring granular access control for both users and administrators across a heterogeneous environment.

Administrators can create logical groupings of UNIX, Linux, or Mac computers within Active Directory as Centrify zones. Each zone can have a unique set of users, a unique set of administrators, and a unique set of role definitions and access rights. IT managers can use DirectControl zones to manage UNIX, Linux and Mac computers using Active Directory while preserving existing security boundaries and privileges. Zones can be flat in structure (known as classic zones), or are arranged in a hierarchical structure of parent and child zones (referred to as hierarchical zones) that allows for the inheritance of data from the top to the bottom of the zone tree. For this evaluation, only hierarchical zones were considered.

With Active Directory, only users that are members of a domain can access computers and resources that are also members of the domain. With zones, administrators can create more granular sets of users and computers that can have their own members and access privileges. By using zones, organizations can secure users and resources into any logical grouping that meets their organizational needs, thus allowing them to restrict access to certain groups of systems to a very specific subset of the Active Directory domain user community. These capabilities allow organizations to meet the regulatory demands of Sarbanes-Oxley, Payment Card Industry (PCI)

standards, and other government and industry regulations that require verifiable controls over access to systems with critical organizational information.

1.4.6 Identification and Authentication for Users and Groups

DirectControl enables you to automatically or manually assign UNIX identity attributes to Active Directory users and groups. The collection of these identity attributes for a user or a group is defined as the user or group profile. For example, the UNIX attributes that define a user profile for identification and authentication are:

- Login name
- User identifier (UID)
- Primary group identifier (GID)
- User password
- Home directory
- Default shell

DirectControl hierarchical zones allow user and group profiles to be partially or completely defined in any parent or any child zone. Profile attributes can then be inherited down the zone hierarchy and used as defined or individually overridden in any zone or on any specific computer. Profiles can also use variables that are inherited and resolved at run-time with appropriate platform-specific values on individual computers.

Only users and groups with completely defined profiles are valid. The profile attributes are stored in Active Directory and are defined and managed with Active Directory Users and Computers (ADUC), the DirectManage Access Manager, custom scripts, or programs developed internally for managing users and groups.

Broad Platform Support

Centrify DirectControl is compatible with many different versions and builds of UNIX, Linux, and Mac OS X operating environments. The complete and most up-to-date list of supported operating systems and vendors is available on the Centrify Support portal of the Centrify web site.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

Deploying Centrify DirectControl consists of installing the Centrify DirectControl UNIX Agent on each managed system and the DirectManage Access Manager Console on at least one Windows computer.

1.5.2 DirectControl UNIX Components included in the TOE

Centrify DirectControl UNIX Agent or Daemon

The Centrify DirectControl UNIX Agent, adclient, is installed on each UNIX, Linux, and Mac OS X computer to be included in the Active Directory environment. This agent

handles all of the direct communication with Active Directory. It contacts Active Directory with requests for authentication, authorization, or policy updates, and passes valid credentials or other requested information along to the programs or applications that need the information.

1.5.3 DirectControl Windows Components included in the TOE

DirectManage Access Manager

DirectManage Access Manager provides a central location for managing UNIX users, groups, and computers and performing administrative tasks, such as importing accounts, running reports, and analyzing account information.

Using Access Manager console, Windows administrators can view and configure zones, including user, group, and computer properties, role assignments, and permissions for performing administrative tasks. With DirectManage Access Manager, administrators can see who has access to which systems and control what users in different roles can do on those computers. DirectManage Access Manager also enables administrators to manage permissions, auditing, and reporting.

In a typical configuration, the Access Manager console is installed on at least one computer that can access domains in Active Directory. DirectManage Access Manager enables an organization to automatically update the Active Directory forest without changing the Active Directory schema installed.

DirectMange Active Directory Users and Computers (ADUC) Plug-in

DirectControl provides property extensions that allow administrators to use Active Directory Users and Computers to store and manage UNIX-specific attributes. These attributes may also be managed through DirectManage Access Manager.

1.5.4 DirectControl TOE and External Interfaces

Figure 1 shows the physical scope and the physical boundary of the TOE and illustrates the TOE deployment configuration.

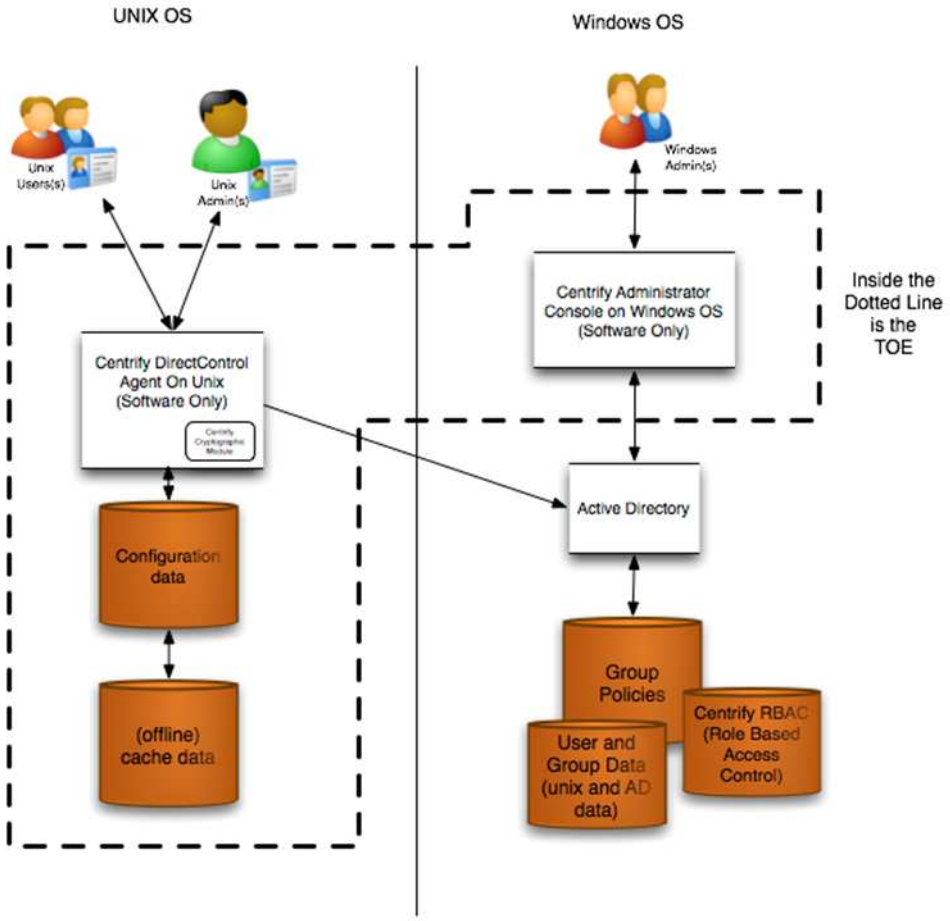

Figure 1 - DirectControl TOE and External Interfaces

1.5.5 TOE Environment Software

The Centrify DirectControl UNIX Agent must be installed on each UNIX, Linux, and Mac OS X computer that will join an Active Directory domain. Therefore, Centrify DirectControl requires an organization to have at least one functioning and correctly configured Microsoft Active Directory domain and domain controller. Centrify DirectControl also must be able to locate and connect to at least one Active Directory domain controller and DNS server. Therefore, an organization must have DNS name servers that are configured to allow the UNIX, Linux, or Mac OS X computer to communicate with domain controllers. To accomplish this, the DNS name servers must be configured with the service locator (SRV) records necessary for domain controller discovery.

DirectManage Access Manager can be installed on any Microsoft Windows computer with access to the domain. To set properties using Active Directory Users and Computers, Centrify DirectControl property extensions for ADUC must be installed on a Windows computer that has Active Directory Users and Computers installed.

The TOE will be evaluated on the following operating systems:

- UNIX: RedHat Linux Enterprise5.6
- Mac: Mac OS 10.6.5 and Mac 10.7
- Windows 2008 Server R2 SP1

DirectManage Access Manager also requires the .NET Framework, version 2.0 or later, to be installed. The Centrify DirectControl setup program installs .NET if it is not found on the target computer.

1.5.5.1 TOE Guidance Documentation

The following guidance documentation is an integral part of the TOE:

- Centrify Suite 2013 Operational User Guidance and Preparative Procedures Supplement for Common Criteria
- Centrify Suite 2013 Administrator's Guide for Linux and UNIX
- Centrify Suite 2013 Configuration and Tuning Reference Guide
- Centrify Suite 2013 Planning and Deployment Guide
- Centrify Suite 2013 Administrator's Guide For Mac OS X
- Centrify Suite 2013 Group Policy Guide

1.5.6 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. The following breakdown also provides the description of the security features of the TOE, and loosely follows the security functional classes described in Section 6. Table 1 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated by the TOE for security related events. The TOE also provides a capability to generate events based on user-configured log levels.
Cryptographic Support	Cryptographic functionality is provided to protect the communications links between the TOE and the Active Directory server, and between the TOE and its remote administrators and users.
Identification and Authentication	Users must identify and authenticate prior to TOE access.
Security Management	The TOE provides management functions that allow the administrators to manage the functions provided by the TOE.

Functional Classes	Description
TOE Access	The TOE provides secure single sign on to UNIX resources based on identity information held in the Windows environment.
Trusted Path/Channels	The TOE provides a secure channel between itself and the Active Directory server.

Table 1 - Logical Scope of the TOE

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, CCMB-2006-09-001 September 2012 Revision 4.

The Target of Evaluation (TOE) for this ST, the Centrify DirectControl feature set in Centrify Suite Version 2013.2, is conformant with CC Part 2.

The TOE for this ST is conformant to the CC Part 3 assurance requirements for EAL 2, augmented with ALC_FLR.1 Basic flaw remediation.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS, POLICIES AND ASSUMPTIONS

3.1.1 Threats

The threats discussed below are addressed by the TOE. Potential threat agents are users of the TOE, system users such as Administrators, and persons who are not authorized to access the TOE or its Operational Environment.

T.ACCESS	An unauthorized user obtains access to resources or security attributes before authentication via an access request to the TOE.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.PRIVILEGE	A non-administrative user may gain privileged access to the TOE and exploit system privileges to gain elevated access to TOE security functions and data.
T.BYPASS	A user may bypass the TOE's security policy resulting in unauthorized access to data.
T.ATTACK	Unauthorized users may initiate attacks on the system resulting in an undetected compromise of IT assets.

3.1.2 Organizational Security Policies

The TOE must address the organizational security policies described below.

P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall be managed only by authorized users.

3.1.3 Assumptions

The following specific conditions are assumed to exist in the TOE operational environment.

A.LOCATE	The TOE will be located within controlled access facilities or will otherwise be secured in a manner which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned

	to manage the TOE.
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.ACCESS	The TOE is configured such that only an approved system user may obtain access.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). The mapping of security objectives to assumptions, threats and organizational security policies along with the rationale for this mapping is found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE and its environment.

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.PROTECT	The TOE must protect its functions and data from unauthorized access and modifications.
O.SECURE	The TOE must ensure the security of all TOE system data.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed and operated in accordance with the operational documentation of the TOE.
OE.TIME	The IT environment will provide the TOE with reliable timestamps.

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE.

	T.ACCESS	T.UNAUTH	T.PRIVILEGE	T.BYPASS	T.ATTACK	P.ACCOUNT	P.INTEGRITY	P.MANAGE	A.LOCATE	A.MANAGE	A.INSTALL	A.NOEVIL	A.ACCESS	A.TIMESTAMP
O.ACCESS	X							X						
O.AUDIT		X			X	X	X							
O.IDENTAUTH	X	X	X			X		X						
O.ADMIN	X	X	X		X			X						
O.PROTECT			X	X			X							
O.SECURE			X	X										
OE.PERSON										X		X		
OE.PHYSICAL									X					
OE.INSTALL											X		X	
OE.TIME														X

Table 2 - Mapping Between Objectives, Threats, Organizational Security Policies, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

Threat: T.PRIVILEGE	A non-administrative user may gain privileged access to the TOE and exploit system privileges to gain elevated access to TOE security functions and data.	
Objectives:	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.PROTECT	The TOE must protect its functions and data from unauthorized access and modifications.
	O.SECURE	The TOE must ensure the security of all TOE system data.
Rationale:	O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized users. O.PROTECT mitigates this threat by ensuring that system and audit data are not accessible and protects data from modification. O.SECURE mitigates the threat by ensuring that system data is protected.	
Threat: T.BYPASS	A user may bypass the TOE's security policy resulting in unauthorized access to data.	
Objectives:	O.PROTECT	The TOE must protect its functions and data from unauthorized access and modifications.
	O.SECURE	The TOE must ensure the security of all system data.
Rationale:	O.PROTECT mitigates this threat by protecting TOE functions from being accessed by unauthorized users. O.SECURE ensures policy cannot be bypassed to access system data.	
Threat: T.ACCESS	An unauthorized user obtains access to resources or security attributes before authentication via an access request to the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.

	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
Rationale:	O.ACCESS directly counters this threat by preventing unauthorized users from accessing TOE functions, and ensuring that authorized users only access those functions and data to which they have been granted access. O.IDENTAUTH mitigates this threat by providing the means to securely identify the user attempting to access an IT asset. O.ADMIN mitigates this threat by ensuring only authorized administrators have access to the management functions of the TOE.	
Threat: T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE. The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded. The objective O.IDENTAUTH ensures that users are identified and authenticated prior to gaining access to TOE security data.	
Threat: T.ATTACK	Unauthorized users may initiate attacks on the system resulting in an undetected compromise of IT assets.	

Objective:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
Rationale:	O.AUDIT and O.ADMIN mitigate this threat by ensuring the TOE has the means of recording and investigating security relevant events which could be indicative of an attack aimed at defeating the TOE security features.	

4.3.2 Security Objectives Rationale Related to Organizational Security Policies

Policy: P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.IDENTAUTH supports this policy by ensuring that the TOE has a clear identity for any user granted access to TOE functionality. O.AUDIT ensures that the use of the TOE is recorded. This may be used to provide evidence of a user's actions.	
Policy: P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.	
Objectives:	O.PROTECT	The TOE must protect its functions and data from unauthorized access and modifications.
	O.AUDIT	The TOE must record audit records for use of the TOE functions, and use of the resources protected by the TOE.
Rationale:	O.PROTECT supports this policy by preventing unauthorized access which could allow the integrity of the system or audit data to be compromised. O.AUDIT further protects the security of the audit and system data by ensuring that attempts to modify data collected and produced by the TOE are recorded.	

Policy: P.MANAGE	The TOE shall be managed only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
Rationale:	O.ACCESS supports this policy by restricting authorized users to the functions and data to which they have been granted access. O.IDENTAUTH ensures that only credentialed users have access to the TOE. O.ADMIN ensures that access to the security functions of the TOE are restricted to authorized users.	

4.3.3 Security Objectives Rationale Related to Assumptions

Assumption: A.LOCATE	The TOE will be located within controlled access facilities or will otherwise be secured in a manner which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	
Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that trained individuals are in place to manage the TOE.	
Assumption:	The TOE is configured such that only an approved system user may	

A.ACCESS	obtain access.	
Objectives:	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed and operated in accordance with the operational documentation of the TOE.
Rationale:	OE.INSTALL supports this assumption by ensuring that the TOE is installed, configured and operated properly.	
Assumption: A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
Rationale:	OE.PERSON supports this assumption by ensuring that the individuals managing the TOE have been specifically chosen to be careful, attentive and non-hostile.	
Assumption: A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.	
Objectives:	OE.TIME	The IT environment will provide the TOE with reliable timestamps.
Rationale:	OE.TIME supports this assumption by ensuring the necessary reliable timestamps.	
Assumption: A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.	
Objectives:	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed and operated in accordance with the operational documentation of the TOE.
Rationale:	OE.INSTALL ensures that the TOE hardware and OS supports the TOE functions.	

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFR) used in this ST.

5.1 FTA_IDM_EXT.1

This extended requirement is explicitly created because the CC does not provide a means to specify Identity Management capabilities as implemented in the feature set. A new family, Identity Management is explicitly created as part of the FTA TOE Access class. The Identity Management family was modelled after FTA_TSE TOE Session Establishment. Component levelling is shown in Figure 2.

Figure 2 - FTA_IDM_EXT Component Levelling

Management: FTA_IDM_EXT.1

The following actions could be considered for the management functions in FMT:

- The management of adding UNIX roles to Active Directory objects.

Audit: FTA_IDM_EXT.1

The following actions should be auditable:

- Minimal: login using a UNIX role established by the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_IDM_EXT.1.1 The TSF shall establish a session on a [assignment: *protected resource*] based on [assignment: *identified credentials*].

FTA_IDM_EXT.1.2 The TSF shall enforce [assignment: *policy*] on [assignment: *TOE users accessing a protected resource*].

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item]. To improve readability selections of [none] are generally not shown.
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are generally not shown.
- Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (UNIX Administrator)' and 'FDP_ACC.1(2) Subset access control (UNIX User)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC summarized in Table 3 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication (FIA)	FIA_AFL.1	Authentication Failure Handling
	FIA_UAU.1	Timing of authentication
	FIA_ATD.1	User attribute definition (UNIX User)
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of Security Functions Behaviour

Class	Identifier	Name
	FMT_SMF.1(1)	Specification of Management Functions (Centrify DirectManage Access Manager)
	FMT_SMF.1(2)	Specification of Management Functions (Centrify DirectControl UNIX Agent)
	FMT_SMR.1	Security roles
TOE Access (FTA)	FTA_IDM_EXT.1	Identity Management
Trusted channel (FTP)	FTP_ITC.1	Inter-TSF trusted channel (Centrify DirectControl UNIX Agent)

Table 3 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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 on UNIX platforms;
b) All auditable events for the [not specified] level of audit; and
c) [*All auditable events listed in Table 4*].

FAU_GEN.1.2 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 ST, [*information specified in Table 4 Auditable Events.*]

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of audit	
FIA_UAU.1	Use of the authentication mechanism	Claimed identity of the user
FIA_UID.1	Use of the identification mechanism	Claimed identity of the user

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1	Management of Security Functions	
FMT_SMF.1	Use of any of the management functions	
FMT_SMR.1	Modifications to an access profile or user.	The identity of the Administrator performing the function
FTA_IDM_EXT.1	Login using a UNIX role established by the TOE.	The identity of the user logging in.
FTP_ITC.1	Trusted Channel	All attempts include the identities of the initiating security principal and the target server. Failures additionally include the error reason.

Table 4 – Auditable Events

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*algorithms listed in Table 5*] and specified cryptographic key sizes [*listed in Table 5*] that meet the following: [*standards listed in Table 5*].

6.2.2.2 FCS_CKM.4 Cryptographic key Destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*cryptographic key zeroization method*] that meets the following: [*FIPS PUB 140-2 Key Management Security Level 1*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key generation

FCS_CKM.1 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations specified in Table 5*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms specified in Table 5*] and cryptographic key sizes [*cryptographic key sizes specified in Table 5*] that meet the following: [*standards listed in Table 5*].

Application Note: The CMVP number for the Centrify Cryptographic Module is 1604.

Operation	Algorithm	Key Size or Digest Length	Standard	CAVP Certificate Numbers
Encryption and Decryption	Triple-DES	112, 168	FIPS 46-3	1018, 1208
	AES	128, 192, 256	FIPS 197	1554, 1861
Message authentication coding	HMAC	128	FIPS 198	904, 1108
Hashing	SHS	N/A	FIPS 180-3	1375, 1637
Random Number Generation	DRBG	256	FIPS 197	69, 149

Table 5 – Cryptographic Operation

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_AFL.1.1 **In offline mode,** the TSF shall detect when [*an administrator configurable positive integer within[1-999,999]*] consecutive unsuccessful authentication attempts occur related to [*login attempts*].

FIA_AFL.1.2 When the defined number of unsuccessful consecutive authentication attempts has been [met], the TSF shall [*lock the user account*].

6.2.3.2 FIA_ATD.1 User attribute definition (UNIX User)

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users [*user passwords*].

6.2.3.3 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.4 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*no actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [enable] the functions [*listed in Table 6*] to [*the authorized roles listed in Table 6*].

Function	Authorized User
managing zones, users, groups and computers, managing rights and roles of users, groups and computers, delegating administrative operations	Windows Administrators
refresh local object cache files, reload security attributes from the local configuration file	UNIX Administrators

Table 6 – Security Functions Behaviour

6.2.4.2 FMT_SMF.1(1) Specification of Management Functions (DirectManage Access Manager)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1 (1).1 The TSF shall be capable of performing the following management functions [*query, modify, and delete object attributes; delegate management functions*].

6.2.4.3 FMT_SMF.1(2) Specification of Management Functions (Centrify DirectControl UNIX Agent)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1(2).1 The TSF shall be capable of performing the following management functions:[*join and leave Active Directory domains, flush cached data, reload Centrify DirectControl UNIX Agent configuration, retrieve up-to-date group policies, query security attributes*].

6.2.4.4 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*UNIX User*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.4.5 FTA_IDM_EXT.1 Identity Management

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_IDM_EXT.1.1 The TSF shall establish a session on a [*UNIX resource*] based on [*credentials held in Active Directory*].

FTA_IDM_EXT.1.2 The TSF shall enforce [*group policy and role-based access control*] on [*Active Directory users logging into a UNIX resource*].

6.2.4.6 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*Reading and Writing Active Directory Security objects and attributes*].

6.3 SECURITY REQUIREMENTS RATIONALE

The following table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.AUDIT	O.IDENTAUTH	O.ADMIN	O.PROTECT	O.SECURE
FAU_GEN.1		X				
FCS_CKM.1						X
FCS_CKM.4						X
FCS_COP.1						X
FIA_ATD.1				X		
FIA_AFL.1			X			
FIA_UAU.1	X		X			
FIA_UID.1	X		X			
FMT_MOF.1			X	X	X	
FMT_SMF.1(1)				X		
FMT_SMF.1(2)				X		
FMT_SMR.1			X			
FTA_IDM_EXT.1	X		X		X	X
FTP_ITC.1					X	X

Table 7 - Mapping of SFRs to Security Objectives

6.3.1 Security Functional Requirements Rationale Related to Security Objectives

Table 8 shows the Security Functional Requirements Rationale related to Security Objectives.

Objective: O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
	FTA_IDM_EXT.1	Identity Management
Rationale:	FIA_UAU.1 and FIA_UID.1 support this objective by ensuring that users are identified and authenticated prior to access. FTA_IDM_EXT.1 controls access to the TOE by providing secure identity management.	
Objective:	The TOE must record audit records for use of the TOE functions, and	

O.AUDIT	use of the resources protected by the TOE.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
Rationale:	FAU_GEN.1 supports the creation of audit records.	
Objective: O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
	FTA_IDM_EXT.1	Identity Management
	FDP_AFL.1	Authentication failure handling
	FMT_MOF.1	Management of functions in TSF
	FMT_SMR.1	Security roles
Rationale:	FIA_UID.1 and FIA_UAU.1 support the identification and authentication of users, respectively. FTA_IDM_EXT.1 controls access to the TOE by providing secure identity management to the UNIX user role described in FMT_SMR.1. FDP_AFL.1 restricts the number of authentication attempts. FMT_MOF.1 provides management functionality and restricts that functionality to users in prescribed roles.	
Objective: O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FMT_MOF.1	Management of security functions behaviour
	FMT_SMF.1	Specification of management functions
Rationale:	FIA_ATD.1 allows UNIX users to change their own passwords. FMT_MOF.1 provides management functionality and restricts those security functions to authorized users of the TOE. FMT_SMF.1 ensures that management functions exist to support the management of the TOE.	
Objective: O.PROTECT	The TOE must protect its functions and data from unauthorized access and modifications.	

Security Functional Requirements:	FMT_MOF.1	Management of security functions behaviour
	FTA_IDM_EXT.1	Identity Management
	FTP_ITC.1	Inter-TSF trusted channel
Rationale:	FTP_ITC.1 protects the audit data from unauthorized modification or deletion. FTA_IDM_EXT.1 restricts access to authorized users. FMT_MOF.1 restricts the security functions to authorized users of the TOE.	
Objective: O.SECURE	The TOE must ensure the security of all TOE system data.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FTA_IDM_EXT.1	Identity Management
	FTP_ITC.1	Inter-TSF trusted channel
Rationale:	FTP_ITC.1 supports the security of object and attributes by ensuring that it is protected from unauthorized viewing, modification and deletion. FTA_IDM_EXT.1 restricts access to authorized users. FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 provide for the cryptography required to support secure communications of data.	

Table 8 - Security Functional Requirements Rationale

6.4 DEPENDENCY RATIONALE

Table 9 - Functional Requirement Dependencies identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependencies	Dependency Satisfied?
FAU_GEN.1	FPT_STM.1	Yes, by the IT environment
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Yes
FCS_CKM.4	FCS_CKM.1	Yes
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	None	Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	Yes

SFR	Dependencies	Dependency Satisfied?
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_SMF.1(1)	None	Yes
FMT_SMF.1(2)	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FTA_IDM_EXT.1	None	Yes
FPT_ITC.1	None	Yes

Table 9 - Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Basic Flaw Remediation (ALC_FLR.1). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.1 augmentation since there are a number of areas where current Centrify practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in the Table 10 - EAL 2 Assurance Requirements.

Assurance Class	Assurance Components	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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.1	Basic flaw remediation
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition

Assurance Class	Assurance Components	
	Identifier	**Name**
	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
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 10 - EAL 2 Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 TOE SECURITY FUNCTIONS

Each of the security requirements and the associated descriptions correspond to the security functions. 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.

TOE Security Function	SFR ID	Description
Security Audit (FAU)	FAU_GEN.1	Audit data generation
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication (FIA)	FIA_AFL.1	Authentication Failure Handling
	FIA_UAU.1	Timing of authentication
	FIA_ATD.1	User attribute definition (UNIX User)
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_SMF.1(1)	Specification of Management Functions (DirectManage Access Manager)
	FMT_SMF.1(2)	Specification of Management Functions (Centrify DirectControl UNIX Agent)
	FMT_SMR.1	Security roles
TOE Access (FTA)	FTA_IDM_EXT.1	Identity Management
Trusted channel (FTP)	FTP_ITC.1	Inter-TSF trusted channel (Centrify DirectControl UNIX Agent)

Table 11 – Mapping of Security Functions to Security Functional Requirements

7.1.1 Security Audit

The TOE generates audit records for Security Relevant events. The table of the audit events generated by the TOE is provided in Table 4 - Auditable Events.

Centrify DirectControl logs errors, warnings and informational messages. It is possible to activate Centrify DirectControl-specific logging and record that information in a Centrify

DirectControl log file. The TOE provides a capability to generate events based on user-configured log levels.

The user identity for users that utilize Centrify DirectControl UNIX Agent for authentication is provided by the TOE.

TOE Security Functional Requirements addressed: FAU_GEN.1.

7.1.2 Cryptographic Support

The Centrify DirectControl UNIX Agent uses a FIPS 140-2 validated cryptographic module for cryptographic functions. The cryptographic operations, algorithms implemented by the Centrify module, key size and Cryptographic Standards are specified in the corresponding FIPS 140-2 security policy document listed in Table 5 - Cryptographic Operation. FIPS-140-2 compliance is maintained on the operating systems identified in section 1.5.5 for which the binary executable remains unchanged.

All of the cryptographic functions implemented by the TOE are implemented in software. The TOE does not provide hardware-accelerated cryptographic functions.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4 and FCS_COP.1.

7.1.3 Identification and Authentication

Users must be identified and authenticated before being given access to the TOE.

The TOE applies access control policies to UNIX users in both connected and offline mode.

The TOE and the environment (operating system) utilize password-based authentication.

Authentication Failure Handling – In offline mode, the TOE enforces the User Account lockout policy based on a configurable user's maximum number of consecutive failed attempts to enter a user password correctly before the TOE locks the account.

User attribute definition – UNIX Users can change their own passwords.

Timing of authentication – Users are not allowed to perform any actions prior to authentication.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_ATD.1 FIA_UAU.1 and FIA_UID.1.

7.1.4 Security Management

The TOE security-related objects, attributes and files are managed by Windows administrators on Windows, and by the UNIX administrator on UNIX.

The Windows Administrator has access to functions through the DirectManage Access Manager to facilitate managing zones, users, groups and computers, managing rights and roles, and defining group policy to be applied to users and machines. DirectManage Access Manager is a Microsoft Management Console (MMC) snap-in. It provides access to a full spectrum of management activities that are specific to DirectControl. The Windows Administrator uses the Access Manager console to create, modify and delete all Windows – stored data used by the TOE. This data includes:

- Centrify Zones – an Active Directory-based hierarchical store for UNIX Identity attributes and Centrify RBAC security data.
    - UNIX Identity attributes include such things as UNIX Names, UIDs, GIDs and user home directory paths that allow AD users and groups to operate as UNIX users and groups. A UNIX user's identity and group membership is used by the UNIX operating system to determine the user's access to resources on UNIX machines.
    - Centrify RBAC (role based access control) data is used by the UNIX TOE components to enforce a user's logon rights and what services/commands can be used.

All of the security function behavior of the Windows Administrator can be delegated to sub-administrators.

In the Centrify DirectControl UNIX Agent, only the UNIX Administrator is allowed to manage the TOE security configuration settings and to invoke utilities involved in the management of UNIX components of the TOE. The UNIX Administrator uses both standard UNIX system tools as well as DirectControl UNIX Agent tools to do so. The DirectControl UNIX Agent tools perform tasks such as joining and leaving Active Directory domains, and forcing the refresh of UNIX-side cached data. It should be noted that while the TOE stores its security data in storage facilities provided by the Microsoft Active Directory server, for performance as well as offline usage, DirectControl UNIX Agent also keeps a local cache of UNIX user and group identity attributes, Centrify RBAC configuration data and Group Policies. The UNIX Administrator is responsible for managing UNIX-side TOE data, including configuration settings, auditing data, as well as the local cached data described above.

The UNIX Administrator can delegate administrative tasks as well but typically does not.

The UNIX user is a user within Active Directory who has been assigned one or more UNIX identities by the TOE. By using the DirectControl UNIX Agent tools, the UNIX user may change his own password as well as query and view non-restricted information.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1.

7.1.5 TOE Access

Centrify DirectControl provides Active Directory-based authentication, access control, single sign-on and group policy support for UNIX, Linux and Macintosh platforms.

Users are able to access configured UNIX (including Macintosh) resources based on credentials and policies as defined by the Windows Administrator and contained in Active Directory. Once the Windows Administrator assigns a user to a Centrify zone, defines a UNIX profile as well as assigns the pre-defined UNIX Login role to him, this user is able to login to any computers in this zone. In addition, for users accessing Red Hat machines, the Windows Administrator can also define new roles to grant a user elevated privileges to perform specific tasks, or to strictly limit his access to a specific time of day or week, or to a defined subset of commands in a customized restricted environment shell.

TOE Security Functional Requirements addressed: FTA_IDM_EXT.1.

7.1.6 Trusted Channel

The TOE utilizes cryptographic functions for authentication to establish a secure channel between the Centrify DirectControl UNIX Agent and the Active Directory server. The trusted channel is implemented with Kerberos 5 using AES and SHA1.

The Centrify DirectControl UNIX Agent only implements client functionality and does not accept connection requests from outside sources.

TOE Security Functional Requirements addressed: FTP_ITC.1.

8 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ANSI	**American National Standards Institute**
CAVP	**Cryptographic Algorithm Validation Program**
CC	**Common Criteria**
CLI	**Command Line Interface**
CMVP	**Cryptographic Module Validation Program**
DES	**Data Encryption Standard**
EAL	**Evaluation Assurance Level**
FIPS	**Federal Information Processing Standards**
FTP	**File Transfer Protocol**
GUI	**Graphical User Interface**
IT	**Information Technology**
PP	**Protection Profile**
SFP	**Security Function Policy**
SFR	**Security Functional Requirement**
SHA	**Secure Hash Algorithm**
ST	**Security Target**
RBAC	**Role Based Access Control**
TOE	**Target of Evaluation**
TSF	**TOE Security Functionality**