LANDesk® Management Suite 8, V8.6.1

Security Target

Version 1.0

October 24, 2006

Prepared for

LANDesk Software, Ltd

Prepared by:

CygnaCom

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: LANDesk® Management Suite 8, Version 8.6.1

The following updates must be applied to the client systems:

- LD-861-Mimi-Rollup-February-2006 (contains 15 fixes), and
- LD-861-SP1 that update installs LANDesk Software 8.6.1 Service Pack.

ST Title: LANDesk® Management Suite 8, V8.6.1 Security Target

ST Version: Version 1.0

ST Authors: CygnaCom Solutions, Inc.

ST Date: October 24, 2006

Assurance Level: EAL2

Strength of Function: SOF Basic

Registration: <To be filled in upon registration>

Keywords: Identification, Authentication, Access Control, Security Management, Vulnerability Scanner, LANDesk® Management Suite

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for LANDesk® Management Suite 8, version 8.6.1.

LANDesk® Management Suite 8 (LDMS) is a remote desktop management solution which enables network administrators to view, configure, and manage the devices on a network. It includes a full range of remote administration tools that can manage complex, heterogeneous computing environments by supporting multiple OS platforms, directories, databases and hardware platforms. It provides an integrated systems and a security management solution that can be used to distribute software packages, monitor software usage, deploy OS images and migrate profiles, remote control devices, and complete many other management tasks.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria for Information Technology Security Evaluation Version 2.3, (CC v2.3), August 2005.

1.4 Document Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. All of the components are taken directly from Part 2 of the CC except the ones noted with “(exp)” in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in CC Part 1 and Part 2, and this ST identifies them as the following:

- Assignment: allows the specification of an identified parameter. In this ST the assignments are specified in italicized text (e.g. *assignment*).
- Iteration: allows a component to be used more than once with varying operations. Iterations are identified with a lower case letter following the typical CC requirement naming for each new iteration (e.g. FMT_MOF.1a).
- Refinement: allows the addition of details or the narrowing of requirements. In this ST, refinements are specified in italicized, bold, underlined text for additional text (e.g. ***additional text***), and strikethrough for deletion text (e.g. ~~deletion text~~).
- Selection: allows the specification of one or more elements from a list. Selections are specified in bold text in this ST (e.g. **selection**).

Explicitly Stated Requirements will be noted with a "(exp)" added to the component name in this ST.

1.5 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to the secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9 provides acronyms, definitions and references.

2 TOE Description

LANDesk Management Suite enables administrators to automate desktop management tasks and proactively control, and update desktops, servers and mobile devices. It consists of tools that can be used to view, configure, and manage the devices in a complex, heterogeneous computing environment (Windows NT, Windows 2000/2003, NetWare, Macintosh, Linux, and UNIX networks).

All of the following tasks can be done through the LANDesk Management Suite main console:

- Maintains security and keeps up with patches and updates
- Efficiently installs and maintains software on the desktop
- Provides Asset Management by inventorying devices on the network
- Migrates users and their profiles to new operating systems.

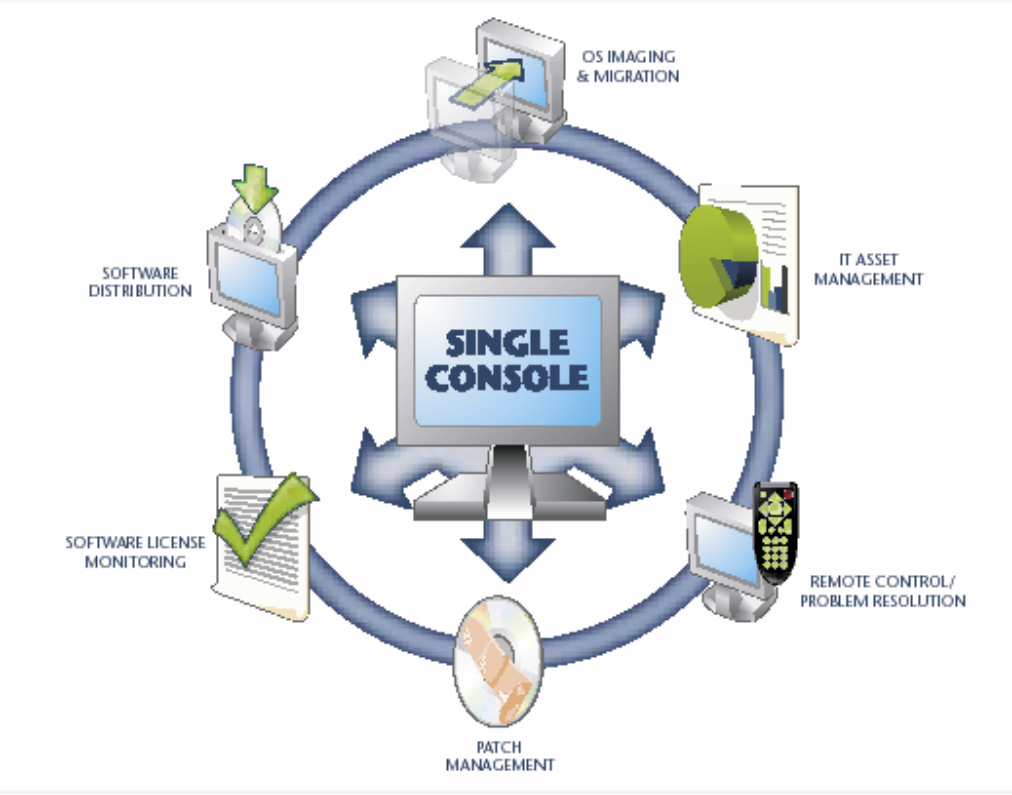

Figure 2-1: LANDesk Management Suite console tasks

2.1 Product Type

LANDesk® Management Suite 8 (LDMS) is a remote desktop management solution which enables network administrators to view, configure, and manage the devices on a network. It includes a full range of remote administration tools that can manage complex, heterogeneous computing environments by supporting multiple OS platforms, directories, databases and hardware platforms. It provides an integrated systems and a security management solution that can be used to distribute software packages, monitor software usage, deploy OS images and migrate profiles, remote control devices, and complete many other management tasks.

2.1.1 LANDesk Management Suite Components

The most important concept that a LDMS users need to understand before installing and deploying the software is the Management Suite management domain. Each management domain consists of a core server and the devices that core server manages. Each core server can manage multiple devices. The number of the devices that can be managed is depending on the server speed[1].

2.1.2 List of Management Suite tools[2]

The following tools with the support of the IT environment provide all the TOE security functions described in this ST:

- **Reports**: Manages predefined LDMS service and asset reports, and lets the users create their own custom asset reports.
- **Unmanaged device discovery**: Finds new devices on the network that have not been scanned and inputs them into the core database.
- **Users**: Controls Management Suite user access to tools and devices based on user rights and scope.
- **Client setup**: Configures devices with LANDesk agents in order to make them fully manageable.
- **Scheduled tasks**: Schedules device agent configuration, software package distribution, OS deployment and profile migration, and other management tasks.

The following tools are also part of the TOE; however none of these tools provide any of the TOE security functions included in this ST:

- **Manage scripts**: Manages OS deployment and profile migration scripts, distribution scripts, file transfer scripts, and other custom scripts.
- **Application policy management**: Manages sets of applications on groups of devices.
- **Software license monitoring**: Implements software asset management and license compliance policies.
- **Custom data forms**: Collects custom information from users and adds it to the core database.
- **Directory manager**: Queries LDAP directories for devices.
- **PXE boot menu**: Configures the boot menu that appears on PXE devices when they first boot.

---

[1] Each core server can manage up to 10,000 devices.

[2] Note that not all of tools provide functions that are security related; as a result they are not reflected in section 5 or 6 of this ST.

2.2 TOE Physical Boundary and Scope of the Evaluation

2.2.1 Physical Boundary

The TOE includes the two main components of the LANDesk Management Suite: the server and the client (Figure 2-2 TOE Boundary).

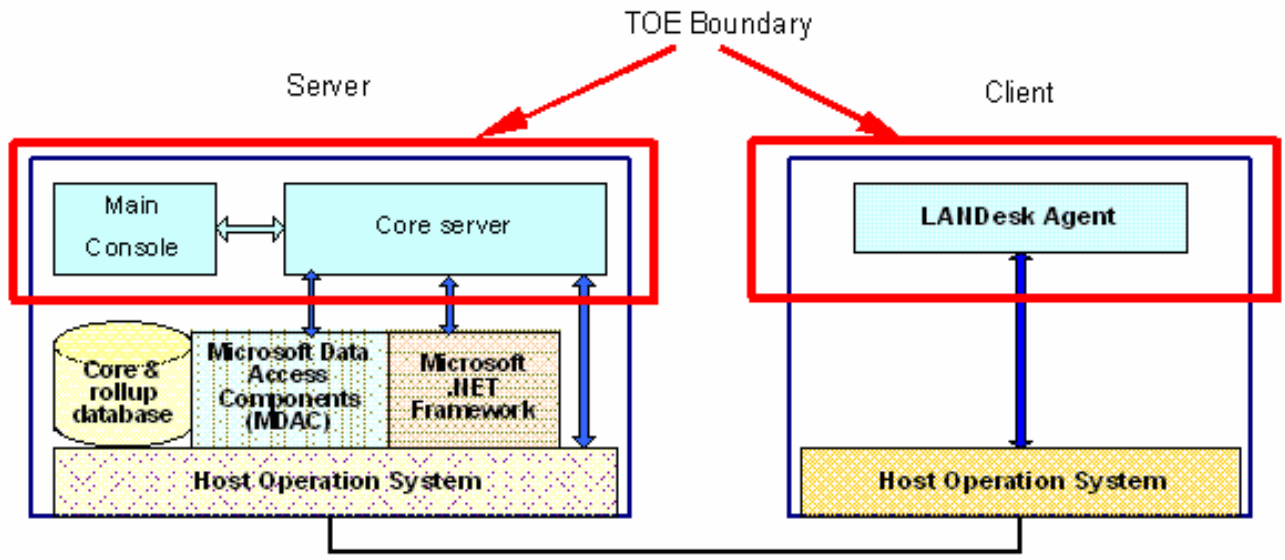

Figure 2-2 TOE Boundary

2.2.1.1 LANDesk Core Server

The server component consists of:

- Core server - all the key files and services for Management Suite are on the core server,
- Main Console[3] - the main LANDesk Management Suite interface,
- Core database - LANDesk Management Suite requires one database for each core server (not included within the TOE)
- Core rollup database - a database that is optimized for querying. Core rollup databases summarize data from multiple core servers. Only the Web console can access the core rollup database (not included within the TOE).

Hardware and the third party software are not considered part of the TOE.

The server should be dedicated to hosting LANDesk Management Suite with the minimum of Intel Pentium III processor (Pentium 4 is recommended), 512 MB of main memory, 900 MB of free hard disk, 100 Mbps NIC, CDROM drive, mouse, keyboard, and monitor.

[3] A subset of the features available in the main console of the LANDesk Management Suite can be available through a web console. However the Security and Patch Manager functionality is not accessible via that web console, therefore the web console is not included within the TOE boundary and it is not been part of this evaluation.

It requires Windows 2000 Server or Advanced Server with SP 4, or Windows Server 2003 Standard or Enterprise Edition as the Operating System using the Microsoft NT File System (NTFS).

An account with administrator rights is required for the installation. The core server must be installed as a standalone server and cannot be a domain controller, active directory controller, or backup domain controller. A static IP address and an active internet connection are needed.

The default installation of LANDesk Management Suite uses Microsoft MSDE database on the core server. However the database schema also supports other database management systems (DBMS) such as Microsoft SQL Server 2000, Oracle8i, and Oracle9i. The LDMS requires interaction with the DBMS, and Microsoft Data Access Components (MDAC) version 2.8 or newer is needed in all database servers to provide database connectivity on Windows platforms. Microsoft .NET Framework (V1.1 or newer) – a component of the Windows OS that is used to build and run Windows-based applications – and Microsoft Internet Explorer (V.6.x or newer) are also required to be installed in the core server.

2.2.1.2 LANDesk Client

The LANDesk client component is a small software program (sometimes referred to as ”agent”) that runs on each LDMS device. This software program allows the LANDesk server to communicate directly with those devices that it will be managing. The device can be any desktop computers, servers, or laptops in the network that have LANDesk agent installed.

The client can run in any of the standard LANDesk Management Suite devices including Windows 98 SE, Windows NT (4.0 SP6a and higher), Windows 2000 SP4 / 2003 / XP SP2, Mac OS X 10.2.x and 10.3.x, Red Hat Linux, version 9 (scanning from the console), SUSE Linux (scanning from the console), and Sun Solaris (scanning from the console).

LANDesk client does not require any specific minimum hardware to run. The minimum hardware specifications of the devices are determined by the OS and other applications that might be installed running in those computers. A 100 Mbps NIC, an IP address, and an active internet connection are needed for all the devices.

2.2.2 Evaluated Configuration

The complete TOE consists of at least two physical machines. The first machine will be the server and have installed the core server, console, and database. The other machine will have installed the LANDesk client (agent).

The evaluated configuration is illustrated in the following diagram (Figure 2-3) consists of 3 machines. As it is shown in this diagram, the LDMS server will be installed in Windows 2003 Server. The LDMS agent[4] can run in all of the OS-s mentioned in section 2.2.1.2, however for this evaluation it will be used only in MS Windows platforms[5].

---

[4] The following updates have been applied to the client systems before testing the TOE:

- LD-861-Mimi-Rollup-February-2006 (contains 15 fixes), and
- LD-861-SP1 that update installs LANDesk Software 8.6.1 Service Pack.

[5] LANDesk core server can be considered as a device, and installing the LDMS agent on it allows scanning and managing the core server as well.

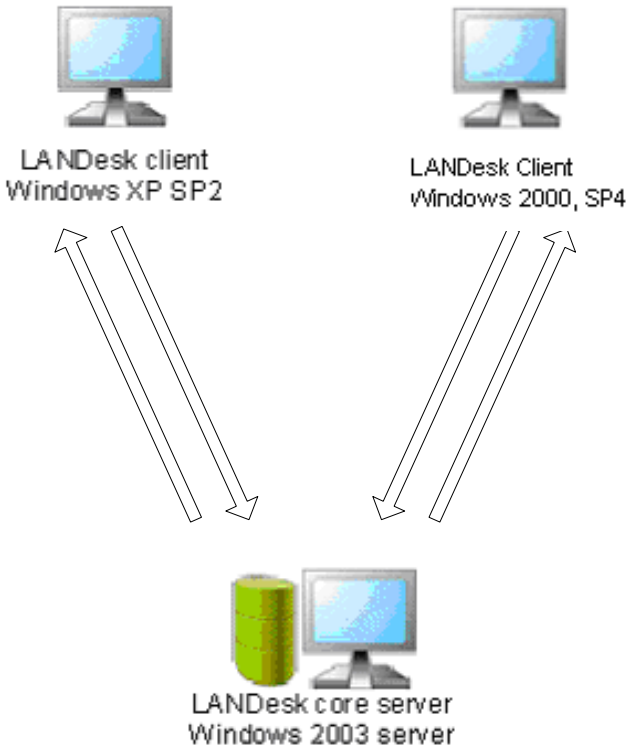

Figure 2-3 TOE evaluated configuration

2.3 TOE Logical Boundary

The logical boundary is defined by the external interfaces at which the Security Functions are implemented. The LDMS security functions are:

- **Scan managed devices** - LANDesk Management Suite Patch Manager tool provides the ability to scan managed devices for known vulnerabilities.
- **LANDesk report generation** - LANDesk Management Suite includes a reporting tool that can be used to generate a wide variety of specialized reports that provide critical information about the managed devices on a network. Security and Patch Manager can be used to update the most common types of security and patch content (such as vulnerabilities) from LANDesk Security services, download the required patches, and configure and run security scans on the LANDesk managed devices.
  LDMS reporting tool allows LANDesk users to create their own custom definition reports, however this feature is not considered part of the TSF, and therefore custom reports are not included in this evaluation.
- **Security Management** – LANDesk Management Suite provides security management function for the report generation, and of security attributes using role base administration. The TOE provides the ability to control what devices a user can manage and which tools they can access and utilize with those devices.
- **Identification and Authentication** - The LDMS Role-base administration uses user ID, user rights, and group membership to control the access to all the tools and devices.

LANDesk users first must identify and authenticate themselves through the OS, and then LANDesk console requires each user to be successfully identified and authenticated before using the LDMS.

2.4 IT Environment

The LANDesk Management Suite relies upon the underlying operating system (OS) and hardware platform to provide protection and execution of the TOE software, disk storage, and reliable timestamps and identification and authentication. In addition, LANDesk Management Suite relies upon the underlying operating system (OS) and hardware platform to protect the core server from other interference or tampering.

Communication between the TSF itself and a remote trusted IT product for the download of vulnerability updates is done via https. Each vulnerability definition carries an MD-5 hash to ensure data security. Data transmitted between separate parts of the TOE for trusted operations is protected from disclosure and modification. Trusted operations use SSL with X509 authentication via a certificate key pair stored on the core.

By default, inventory data transmitted from agents to the core server is compressed but is not encrypted. To configure the inventory service to communicate to the core server via SSL, the administrator must use the LANDesk Configure Services utility after installation. Steps for configuring inventory data encryption are located in LANDesk® Management Suite 8, V8.6.1 Installation, generation and startup document.

LANDesk Management Suite relies on a third party database server to store its data in.

The underlying operating system (OS) together with physical computers and network interfaces, and the third party relational database are not included within this TOE.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

Intended Usage Assumptions:	
A.INSTALL	It is assumed that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
Personnel Assumptions:	
A.ADMIN	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges.
A.USER	Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.
Physical Assumptions:	
A.LOCATE	It is assumed that the TOE processing resources, devices managed by the TOE and the connections are located within controlled access facilities which will prevent unauthorized physical access.
Connectivity Assumptions:	
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

The TOE must counter the following threats to security:

Table 3-2 Threats

T.ACCESS	An authorized user of the TOE may attempt to access TOE information or resources without having permission from the person who is responsible for the information or resources.
T.IMPERSON	An attacker (whether an outsider or insider) may attempt to gain access to the TOE security functions and data by impersonating an authorized user of the TOE.

T.EXPLOIT	An attacker may attempt to gain unauthorized access to the resources of the client system(s) managed by the TOE, by exploiting vulnerabilities on a client system(s).

3.3 Organizational Security Policies

There are not organizational security policies for this TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4-1 Security Objectives for TOE

O.AUTHORIZATION	The TSF must ensure that only authorized users can gain access to the TOE data and its resources.
O.ACCESS	The TOE must provide a controlled interface that limits access to the tools and devices to only authorized administrators.
O.SCAN	The TSF must be able to configure and run security scans on the TOE managed devices. In addition, data collected by the TOE must be organized in useful report formats.
O.MANAGE	The TSF must allow authorized administrators to effectively manage the TOE and its security functions.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for IT Environment

OE.TIME	The IT environment must provide reliable timestamps for the TOE.
OE.AUTHENTICATE	The IT environment must provide a mechanism to validate LANDesk user authentication.
OE.PROTECT	The IT Environment must provide mechanisms to protect TSF executables, and executing TSF processes from untrusted processes on the host. It also must protect the TSF data when it is transmitted between separate parts of the TOE.
OE.COMMUNICATION	The IT Environment must provide mechanism to secure the communication channel between the TSF and a remote trusted IT product.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Environment

OE.ADMIN	Any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
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 IT

	security.
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.USER	Those responsible for the TOE must ensure that only authorized users will have access to the information managed by the TOE.
OE.PEER	Those responsible for the TOE must ensure that any other systems with which the TOE communicates are under the same management control and operate under the same security policy constraints.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies upon are described. These requirements consist of functional components from Part 2 of the CC as well as explicitly stated components derived from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations.

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1 Functional Components.

Table 5-1 Functional Components

Item	Component	Component Name	CC or Explicated
1	FAU_ LRG.1 (exp)	LANDesk report generation	Explicated
2	FAU_LRR.1 (exp)	LANDesk reports review	Explicated
3	FAU_LRR.2 (exp)	LANDesk restricted reports review	Explicated
4	FAU_LRR.3 (exp)	LANDesk selectable reports review	Explicated
5	FIA_ATD.1	User attribute definition	CC Part 2
6	FIA_LAU.2 (exp)	LANDesk user authentication before any action	Explicated
7	FIA_UID.2	User identification before any action	CC Part 2
8	FMT_MTD.1a, b, c, d	Management of TSF data	CC Part 2
9	FMT_SMR.1	Security roles	CC Part 2
10	FMT_SMF.1	Specification of Management Functions	CC Part 2

5.1.1 FAU_LRG.1 (exp) LANDesk report generation

FAU_LRG.1.1 The TSF shall be able to scan managed devices for the following types of security risks:

a) Vulnerabilities, and

b) LANDesk updates.

FAU_ LRG.1.2 The TSF shall be able to generate security and patch manager reports for each type of the security risks.

5.1.2 FAU_LRR.1 (exp) LANDesk reports review

FAU_LRR.1.1 The TSF shall provide the LANDesk user that is a member of the LANDesk reports group] with the capability to read all the information from the security and patch manager reports.

FAU_LRR.1.2 The TSF shall provide the security and patch manager reports in a manner suitable for the user to interpret the information.

5.1.3 FAU_LRR.2 (exp) LANDesk restricted reports review

FAU_LRR.2.1 The TSF shall prohibit all users read access to the security and patch manager reports, except those users that have been granted explicit read-access.

5.1.4 FAU_LRR.3 (exp) LANDesk selectable reports review

FAU_LRR.3.1 The TSF shall provide the ability to perform sorting of the LANDesk reports based on criteria as listed in following (Table 5-2 Criteria for sorting the LANDesk security and patch manager reports):

Table 5-2 Criteria for sorting the LANDesk security and patch manager reports

LANDesk security and patch manager reports:	Criteria for sorting the reports:
Vulnerabilities reports	• Detected vulnerabilities • Detected vulnerabilities by computer • Detected vulnerabilities by detection date • Detected vulnerabilities by location • Devices not scanned for vulnerabilities • Devices that could not be remediated • Devices that were never vulnerable • Remediated vulnerabilities • Remediated vulnerabilities by computer • Remediated vulnerabilities by date • Remediated vulnerabilities by location • Vulnerability threat overview.
LANDesk updates reports	• Applied LANDesk updates • Applied LANDesk updates by computer • Applied LANDesk updates by date • Applied LANDesk updates by location • Devices not scanned for LANDesk updates • Devices that could not be updated • Required LANDesk updates • Required LANDesk updates by computer • Required LANDesk updates by detection date • Required LANDesk updates by location.

5.1.5 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*user ID, user rights, group membership*].

5.1.6 FIA_LAU.2 (exp) LANDesk user authentication before any action

FIA_LAU.2.1 The TSF, with the support of the IT environment, shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.7 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.8 FMT_MTD.1a Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[***full access***]] the [*Management Suite Tools*] to [*user with the LANDesk Management Suite administrator right*].

5.1.9 FMT_MTD.1b Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[***create, run, view, publish, import and export***]] the [*Reports*] to [*user with the Reports right*].

5.1.10 FMT_MTD.1c Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[***download, and update***]] the [*most common types of security and patch content*] to [*user with the Security and Patch Manager right*].

5.1.11 FMT_MTD.1d Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[***configure and run***]] the [*security scan on the LANDesk managed devices*] to [*user with the Security and Patch Manager right*].

5.1.12 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*user with one or more of the following rights:*

- *LANDesk Management Suite administrator,*
- *Reports,*
- *Security and Patch Manager].*

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

5.1.13 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- *LANDesk report generation*
- *Management of security attributes*].

5.2 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-3 EAL2 Assurance Components below.

Table 5-3 EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

5.3 Security requirements for the IT Environment

LANDesk Management Suite 8 requires that the operating system platform provide reliable time stamps.

Table 5-4 Functional Components for the IT environment

No.	Component	Component Name
1	FPT_STM.1	Reliable time stamps
2	FIA_OAU.2 (exp)	OS user authentication before any action
3	FPT_SEP_ENV.1 (exp)	TSF domain separation
4	FTP_ITC.1	Inter-TSF trusted channel
5	FPT_ITT.1	Basic internal TSF data transfer protection

5.3.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The ***IT environment*** ~~TSF~~ shall be able to provide reliable time stamps for ***the TSF and*** its own use.

5.3.2 FIA_OAU.2 (exp) OS user authentication before any action

FIA_OAU.2.1 The operating system shall validate user authentication data provided by the TSF.

5.3.3 FPT_SEP_ENV.1 (exp) TSF domain separation

FPT_SEP_ENV.1.1 The IT Environment shall provide access control and process separation that protect TSF executables, TSF data, and executing TSF processes from untrusted processes on the host.

5.3.4 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The ***IT Environment*** ~~TSF~~ shall provide a communication channel between ***the TSF*** ~~itself~~ and a remote 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 ***IT Environment*** ~~TSF~~ shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The ***IT Environment*** ~~TSF~~ shall initiate communication via the trusted channel for [*the download of vulnerability updates*].

5.3.5 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The ***IT Environment*** ~~TSF~~ shall protect TSF data from [**disclosure**, and **modification**] when it is transmitted between separate parts of the TOE.

5.4 Strength of Function

The overall strength of function requirements claim for all of these IT security functions is SOF-Basic. FIA_SOS.1 is not included as a TSFR; however specific SOF can be mapped to FIA_LAU.2 (exp) as SOF-Basic.

6 TOE Summary Specification

6.1 IT Security Functions

Section 6.1 describes the specific security functions that meet the criteria of the security class features that are described in section 2.4. The following sections describe the IT Security Functions of the LANDesk Management Suite 8. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. .

Table 6-1 Security Functional Requirements mapped to Security Functions

Security Class	Item	SFRs	Sub-functions	Security Functions
Security audit	1	FAU_ LRG.1 (exp)	SR-1	LANDesk scanning and report generation
	2	FAU_LRR.1 (exp)	SR-2	
	3	FAU_LRR.2 (exp)	SR-3	
	4	FAU_LRR.3 (exp)	SR-4	
Identification and authentication	5	FIA_ATD.1	IA-1	Identification and authentication
	6	FIA_LAU.2 (exp)	IA-2	
	7	FIA_UID.2	IA-3	
Security management	8	FMT_MTD.1a, b, c, d	SM-1	Security management
	9	FMT_SMR.1	SM-2	
	10	FMT_SMF.1	SM-3	

6.1.1 LANDesk Report Generation Function

SR-1 LDMS provides the ability to scan managed devices for the following types of security risks:

a) Vulnerabilities, and

b) LANDesk updates

The following describes how the security scanner works for each content type:

When scanning for...	Security and Patch Manager...
Windows vulnerabilities	Uses vulnerability definitions published by LANDesk (based on official security bulletins) to check for known operating system and/or application vulnerabilities.
Macintosh vulnerabilities	Uses vulnerability definitions published by LANDesk (based on official security bulletins) to check for known vulnerabilities.
Linux/UNIX vulnerabilities	Uses vulnerability definitions published by LANDesk (based on official security bulletins) to check for known vulnerabilities.
LANDesk software updates	Uses software update definitions published by LANDesk to check for LANDesk software versions.

LANDesk Management Suite includes a reporting tool that can be used to generate a wide variety of specialized reports that provide critical information about the managed devices on a network. LANDesk is able to generate security and patch manager reports for the following categories:

a) Vulnerabilities reports

b) LANDesk updates reports

SR-2 The report tool's publishing feature provides a quick and easy way to save the report data in a secure location, and to make the report available to LANDesk users.

Only a user that is a member of the LANDesk reports group (this is a group created on the core server along with a default reports user at LDMS install) has rights to view the published reports. LDMS install creates a webshare on the core and only gives the LANDesk reports group rights to view this share. This is outside of the LANDesk management group. So a user does not need management suite rights at all to view the reports

LANDesk user with the administrator or reports rights has the capability to read all the information from the security and patch manager reports.

To protect the report data, published reports can only be accessed with valid authentication credentials to a secure share on the core server.

Within the LDMS product, (using the LDMS console):

- Only administrators can view the contents of all of the report groups.
- Users with the Reports right can also see and run reports, as well as publish reports, but only on the devices included in their scope.

The security and patch manager reports are in a manner suitable for the user to interpret the information. Published reports can be saved in files in any of the following formats:

- HTML,
- PDF,
- XLS,
- DOC, and
- RTF.

SR-3 The LANDesk Management group does not provide read access to the security and patch manager reports, except to those users that have been granted explicit read-access.

- Only administrators can view the contents of all of the report groups.

Users with the Reports right can also see and run reports, as well as publish reports, but only on the devices included in their scope.

SR-4 Reports are organized in groups. The LANDesk console provides the ability to sort different security and patch manager reports based on specific criteria. The following provide the lists of the all security and patch manager reports, grouped in the following categories:

a) Vulnerabilities reports:

- **Detected vulnerabilities:** Lists all industry or vendor defined vulnerabilities that were detected by the latest vulnerability scan for all scanned devices.
- **Detected vulnerabilities by computer:** Lists all vulnerabilities detected by the latest vulnerability scan, organized by scanned device name.

- **Detected vulnerabilities by detection date:** Lists all vulnerabilities detected by the latest vulnerability scan, organized by the date they were detected.
- **Detected vulnerabilities by location:** Lists all vulnerabilities detected by the latest vulnerability scan, organized by the location of the scanned device.
- **Devices not scanned for vulnerabilities:** Lists the devices in your scope that were not scanned specifically for industry or vendor defined vulnerabilities as part of the latest vulnerability scan job.
- **Devices that could not be remediated:** Lists all scanned devices whose detected vulnerabilities could not be remediated as part of the latest repair job.
- **Devices that were never vulnerable:** Lists the devices in your scope that were scanned by the latest vulnerability scan and did not report any vulnerabilities.
- **Remediated vulnerabilities:** Lists all vulnerabilities that were successfully remediated by the latest repair job.
- **Remediated vulnerabilities by computer:** Lists all vulnerabilities that were successfully remediated by the latest repair job, organized by device.
- **Remediated vulnerabilities by date:** Lists all vulnerabilities that were successfully remediated by the latest repair job, organized by date.
- **Remediated vulnerabilities by location:** Lists all vulnerabilities that were successfully remediated by the latest repair job, organized by the location of the repaired device.
- **Vulnerability threat overview**

b) LANDesk updates reports

- **Applied LANDesk updates:** Lists all LANDesk product updates that were installed on devices as part of the latest patch job.
- **Applied LANDesk updates by computer:** Lists all LANDesk product updates that were installed by the latest patch job, organized by device.
- **Applied LANDesk updates by date:** Lists all LANDesk product updates that were installed as part of the latest patch job, organized by date.
- **Applied LANDesk updates by location:** Lists all LANDesk product updates that were installed as part of the latest patch job, organized by the location of the device.
- **Devices not scanned for LANDesk updates:** Lists the devices in your scope that were not scanned specifically for LANDesk updates as part of the latest vulnerability scan job.
- **Devices that could not be updated:** Lists all scanned devices whose detected LANDesk update could not be installed.
- **Required LANDesk updates:** Lists all LANDesk updates (LANDesk products

whose version is obsolete and requires an updated version be installed) detected by the latest vulnerability scan for all scanned devices.

- **Required LANDesk updates by computer:** Lists all LANDesk updates detected by the latest vulnerability scan, organized by device.
- **Required LANDesk updates by detection date:** Lists all LANDesk updates detected by the latest vulnerability scan, organized by date.
- **Required LANDesk updates by location:** Lists all LANDesk updates detected by the latest vulnerability scan, organized by the location of the scanned device.

6.1.2 Identification and authentication

IA-1 LANDesk console uses user ID, user rights, and group membership to control the access to all the tools and devices. Role-based administration enhances LANDesk Management Suite's network security by providing a Users tool that allows the administrators (users with the LANDesk Administrator right) to manage devices, console views, and specific features and tools. It allows those administrators to control what devices a Management Suite user can manage and which tools they can access and utilize with those devices.

IA-2 **IA-3** LANDesk console requires each user to be successfully identified and authenticated before allowing any other actions on behalf of that user. LANDesk users first must identify and authenticate themselves through the OS, and then LANDesk console requires each user to be successfully identified and authenticated before using the LDMS.

Although these two I&A mechanisms are independent steps, they use the same credentials (UID and passwords) which are managed by the OS and every LANDesk user must be member of LANDesk Management Suite or LANDesk Reports groups in Windows. These two groups are created during the LDMS installation.

6.1.3 Security management

SM-1 The LDMS Role-based administration provides the ability to control what devices a Management Suite user can manage and which tools they can access and utilize with those devices.

- LANDesk restricts the ability to fully access all Management Suite Tools to the user with the LANDesk Management Suite administrator right.
- LANDesk restricts the ability to create, run, view, publish, import and export reports to users with the Reports right.
- LANDesk restricts the ability to download, and update the most common types of security and patch content to users with the Security and Patch Manager right.
- LANDesk restricts the ability to configure and run the security scan on the LANDesk managed devices to users with the Security and Patch Manager right.

SM-2 The LDMS uses Role-based administration provides the capability to define roles by assigning special administrative roles based on their rights and scopes to those users that are member of LANDesk Management Suite user group in Windows OS. Rights determine the Management Suite tools and features a user can see and utilize and scopes

determine the range of devices a user can see and manage.

The LDMS maintains the roles defined for a user with one or more of the following rights:

- LANDesk Administrator,
- Reports,
- Security and patch manager.

The LDMS associates users with roles identified by their rights. The devices a LANDesk user can view and manage in the network view, and the management tools he can use, are determined by their access rights and device scope assigned by the Management Suite administrator as the following:

- *User with LANDesk Management Suite administrator right* has full access to the Management Suite tools (administrators with full rights can perform any management tasks).
- *User with Reports right* can view reports that have been run; and publish reports in order to make them available to users with access credentials.
- *User with Security and Patch Manager right* can use the Security and Patch Manager tool to download and update security and patch content (vulnerabilities) from LANDesk Security services; and can configure and run security scans on the LANDesk managed devices.

SM-3 Using role-based administration, the LDMS provides the capability to perform the following security management functions:

- LANDesk report generation
- Management of security attributes.

6.1.4 SOF Claims

IA-2 is realized by probabilistic mechanisms. The TOE makes sure that user has been authenticated by the OS before allowing access. As a result the authentication process is shared with the OS.

6.2 Assurance Measures

The LANDesk Management Suite 8 satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-2 Assurance Measures

Item	Security Assurance Requirement	How Satisfied
1	ACM_CAP.2	LANDesk Management Suite 8, 8.6.1 Configuration management and delivery procedures.
2	ADO_DEL.1	LANDesk Management Suite 8, 8.6.1 Configuration management and delivery procedures. LANDesk Management Suite 8, 8.6 Installation and Deployment Guide

Item	Security Assurance Requirement	How Satisfied
3	ADO_IGS.1	LANDesk® Management Suite 8 Installation and Deployment Guide
4	ADV_FSP.1	LANDesk Management Suite 8, 8.6.1 Functional Specification (FSP)
5	ADV_HLD.1	LANDesk Management Suite 8, 8.6.1 High-level Design (HLD)
6	ADV_RCR.1	LANDesk Management Suite 8, 8.6.1 Representative Correspondence (RCR)
7	AGD_ADM.1	LANDesk® Management Suite 8 User's Guide
8	AGD_USR.1	LANDesk® Management Suite 8 User's Guide
9	ATE_COV.1	Test Case Identification version 2.6.xls
10	ATE_FUN.1	Test Case Identification version 2.6.xls
11	ATE_IND.2	TOE for Testing
12	AVA_SOF.1	LANDesk Management Suite 8, 8.6.1 Strength of Function Analysis
13	AVA_VLA.1	LANDesk Management Suite 8, V8.6.1 Vulnerability Analysis

7 PP Claims

The LANDesk Management Suite 8 Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

This section provides evidence demonstrating coverage of the TOE security environment by the IT security objective. The security objectives were derived exclusively from statements of threats and assumptions (there are no OSP in this ST). The following table demonstrates that the mapping between the assumptions and threats to the security objectives is completed and the rationales in the following sections provide evidence of coverage for each statement of TOE security environment.

Table 8-1 Mapping of Security Environment to Security Objectives, shows that:

- Each threat and assumption is addressed by at least one security objective, and
- Each security objective addresses at least one threat or assumption.

Table 8-1 Mapping of Security Environment to Security Objectives

Security Objectives / Security Environment	O.AUTHORIZATION	O.ACCESS	O.SCAN	O.MANAGE	OE.TIME	OE.ADMIN	OE.INSTALL	OE.PHYSICAL	OE.USER	OE.PEER	OE.AUTHENTICATE	OE.PROTECT	OE.COMMUNICATION
T.ACCESS	X	X		X							X	X	X
T.IMPERSON	X			X							X		
T.EXPLOIT	X	X	X	X	X						X		
A.INSTALL						X	X						
A.ADMIN						X			X				
A.USER									X				
A.LOCATE								X					
A.PEER										X			

8.1.1 Threats

T.ACCESS: An authorized user of the TOE may attempt to access TOE information or resources without having permission from the person who is responsible for the information or resources.

Coverage Rational:

O.AUTHORIZATION and **OE.AUTHENTICATE** ensure that only authorized users gain access to the TOE data and its resources. **O.ACCESS** partially addresses this threat by requiring the TOE to provide a controlled interface that will limit access to the tools and devices to users with authorization and appropriate privileges Only administrators will be able manage the TOE and its security functions(**O.MANAGE**).

OE.PROTECT and **OE.COMMUNICATION** partially address this threat by requiring the IT Environment to protect the TSF data when it is transmitted between separate

parts of the TOE, and secure the communication channel between the TSF and a remote trusted IT product.

T.IMPERSON: An attacker (whether an outsider or insider) may attempt to gain access to the TOE security functions and data by impersonating an authorized user of the TOE.

Coverage Rational:

O.AUTHORIZATION provides that only authorized users gain access to the TOE data and its resources, and the IT environment will validate LANDesk user authentication (**OE.AUTHENTICATE).**

O.MANAGE provides that TOE administrators will manage the TOE and its security functions in an effective way.

T.EXPLOIT: An attacker may attempt to gain unauthorized access to the resources of the client system(s) managed by the TOE, by exploiting vulnerabilities on a client system(s).

Coverage Rational:

O.SCAN provides that the TOE will be able to configure and run security scans on the TOE managed devices and generates reports. Timestamp is included within the reports information (**OE.TIME**).

O.ACCESS provides that TOE provides a controlled interface that limits access to the tools and devices to users with authorization and appropriate privileges (i.e. downloading updates from LANDesk service).

O.MANAGE provides that administrators will effectively manage the TOE and its security functions, and must ensure that only authorized users are able to access such functionality (**O.AUTHORIZATION, OE.AUTHENTICATE**).

8.1.2 Assumptions

A.INSTALL: It is assumed that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

Coverage Rational:

OE.INSTALL provides that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. Administrator is the responsible person to install the TOE and he is trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE (**OE.ADMIN**).

A.ADMIN: It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can trusted not to deliberately abuse their privileges.

Coverage Rational:

OE.ADMIN provides that administrators of the TOE are trusted, and will have access to the TOE information to manage it effectively (**OE.USER**)

A.USER: Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.

Coverage Rational:

> **OE.USER** provides that the TOE will allow only authorized users to have access to the information managed by the TOE.

A.LOCATE: It is assumed that the TOE processing resources, devices managed by the TOE and the connections are located within controlled access facilities which will prevent unauthorized physical access.

Coverage Rational:

> **OE.PHYSICAL** requires that those parts of the TOE critical to security policy are protected from any physical attack.

A.PEER: Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

Coverage Rational:

> **OE.PEER** provides that any other systems with which the TOE communicates are under the same management control and operate under the same security policy constraints.

8.2 Security Requirements Rationale

This section provides evidence demonstrating that the security objectives for the TOE and the TOE IT environment are satisfied by the security requirements. The mapping show that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Functional Requirements

Table 8-2 Mapping of Security Functional Requirements to Security Objectives

TOE security Objectives / Security Functional Requirements	O.AUTHORIZATION	O.ACCESS	O.SCAN	O.MANAGE	OE.TIME	OE.AUTHENTICATE	OE.PROTECT	OE.COMMUNICATION
FAU_ LRG.1 (exp)			X					
FAU_LRR.1 (exp)			X					
FAU_LRR.2 (exp)			X					
FAU_LRR.3 (exp)			X					
FIA_ATD.1	X	X						

TOE security Objectives / Security Functional Requirements	O.AUTHORIZATION	O.ACCESS	O.SCAN	O.MANAGE	OE.TIME	OE.AUTHENTICATE	OE.PROTECT	OE.COMMUNICATION
FIA_LAU.2 (exp)	X							
FIA_UID.2	X							
FMT_MTD.1(a, b, c, d)		X		X				
FMT_SMR.1		X		X				
FMT_SMF.1				X				
FPT_STM.1					X			
FIA_OAU.2 (exp)	X					X		
FPT_SEP_ENV.1 (exp)							X	
FTP_ITC.1								X
FPT_ITT.1							X	

O.AUTHORIZATION: The TSF must ensure that only authorized users can gain access to the TOE data and its resources.

Coverage Rational:

> [**FIA_LAU.2 (exp)**] and **[FIA_UID.2**] implement the objective by requiring authorized users to successfully identify and authenticate themselves before giving access to the TOE data and functions. The OS will validate user authentication data provided by the TSF **[FIA_OAU.2 (exp)].**
>
> [**FIA_ATD.1**] Implements the objective by requiring the TOE to maintain user ID, user rights, and user group membership attributes for the access rights to the TOE.

O.ACCESS: The TOE must provide a controlled interface that limits access to the tools and devices to only authorized administrators.

Coverage Rational:

> [**FIA_ATD.1**] Implements the objective by requiring the TOE to use user ID, user rights, and user group membership attributes to provide access to the tools and devices. [**FMT_MTD.1 (a, b, c, d)**] implements the objective by allowing users with a certain role to manage values of TSF data. The users are assigned to a role within the [**FMT_SMR.1**] component.

O.SCAN: The TSF must be able to configure and run security scans on the TOE managed devices. In addition, data collected by the TOE must be organized in useful report formats.

Coverage Rational:

[**FAU_ LRG.1 (exp)**] defines the scan function of the TOE on managed devices for the different types of security risks. It also provides what types of the security and patch manager reports that the TOE generates, and the criteria used for sorting these reports [**FAU_LRR.3 (exp)**].

[**FAU_LRR.2 (exp)**] implements the objective by requiring that there are no other users except those that have been identified as the authorized users in [**FAU_LRR.1 (exp)**] that can read the information within the security and patch manager reports.

O.MANAGE: The TSF must allow authorized administrators to effectively manage the TOE and its security functions.

Coverage Rational:

[**FMT_MTD.1 (a b, c, d)**] implies the objective by allowing only authorized users with the roles identified in [**FMT_SMR.1**] to manage TSF data. [**FMT_SMF.1**] partially implements the objective by providing specific management functions provided by the TSF.

OE.TIME: The IT environment must provide reliable timestamps for the TOE.

Coverage Rational:

[**FPT_STM.1**] implements reliable timestamps for the TSF.

OE.AUTHENTICATE The IT environment must provide a mechanism to validate LANDesk user authentication.

[**FIA_OAU.2 (exp)**] implements the objective by requiring the operating system to validate user authentication data provided by the TSF during the LANDesk user identification and authentication process.

OE.PROTECT The IT Environment must provide mechanisms to protect TSF executables, and executing TSF processes from untrusted processes on the host. It also must protect the TSF data when it is transmitted between separate parts of the TOE.

[FPT_SEP_ENV.1 (exp)] implements the objective by requiring the IT Environment to provide access control and process separation that will protect TSF executables, TSF data, and executing TSF processes from untrusted processes on the host.

[**FPT_ITT.1**] requires the IT Environment to protect TSF data from disclosure, and modification when it is transmitted between separate parts of the TOE.

OE.COMMUNICATION The IT Environment must provide mechanism to secure the communication channel between the TSF and a remote trusted IT product.

[FTP_ITC.1] requires that the IT Environment provide a trusted communication channel between the TOE and another trusted IT product for the download of vulnerability updates.

8.2.2 Security Functional Requirements Dependencies

Table 8-3 shows the dependencies between the functional requirements. All dependencies are satisfied.

Table 8-3 Functional Requirements Dependencies Satisfied

Item	Component	Component Name	Dependencies	
			SFR	Included
TOE Security Functional Requirements				
1	FAU_ LRG.1 (exp)	LANDesk report generation	FPT_STM.1	Yes (No.11, IT Environment)
2	FAU_LRR.1 (exp)	LANDesk reports review	FAU_LRG.1	Yes (No. 1)
3	FAU_LRR.2 (exp)	LANDesk restricted reports review	FAU_LRR.1	Yes (No. 2)
4	FAU_LRR.3 (exp)	LANDesk selectable reports review	FAU_LRR.1	Yes (No. 2)
5	FIA_ATD.1	User attribute definition	None	-
6	FIA_LAU.2 (exp)	LANDesk user authentication before any action	FIA_UID.1	Yes (No. 7 is hierarchical to FIA_UID.1)
7	FIA_UID.2	User identification before any action	None	-
8	FMT_MTD.1a,b,c,d	Management of TSF data	FMT_SMF.1	Yes (No. 10)
			FMT_SMR.1	Yes (No. 9)
9	FMT_SMR.1	Security roles	FIA_UID.1	Yes (No. 7 is hierarchical to FIA_UID.1)
10	FMT_SMF.1	Specification of Management Functions	None	-
Security Requirements for the IT Environment				
11	FPT_STM.1	Reliable time stamps	None	
12	FIA_OAU.2 (exp)	OS user authentication before any action	FIA_UID.1	Yes (No. 7 is hierarchical to FIA_UID.1)
13	FPT_SEP_ENV.1 (exp)	TSF domain separation	None	
14	FTP_ITC.1	Inter-TSF trusted channel	None	
15	FPT_ITT.1	Basic internal TSF data transfer protection	None	-

8.2.3 Explicitly Stated Requirements

FAU_ LRG.1 (exp) LANDesk report generation, FAU_LRR.1 (exp) LANDesk reports review, FAU_LRR.2 (exp) LANDesk restricted reports review, and FAU_LRR.3 (exp) LANDesk selectable reports review are very similar to the respective CC components (FAU_GEN.1). However the CC

components are written for the audit records rather than for audit reports, and therefore they have been explicitly stated in this ST.

FIA_LAU.2 (exp) LANDesk user authentication before any action and FIA_OAU.2 OS user authentication before any action are very similar to the FIA_UAU, whereas FPT_SEP_ENV.1 (exp) TSF domain separation, is based on the FPT_SEP.1 TSF domain separation; however these have been explicitly stated in this ST because the TOE needs OS support to perform the user authentication and protect the TSF data. These had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection.

According to CCIMB RI#19, which states the following: “Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE“. Since the authentication mechanism spans both the TOE requirement (FIA_LAU.2) and IT Environment (FIA_OAU.2), they must be explicitly stated following the same guidance as stated above.

8.2.4 Strength of Function

Strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

8.2.5 EAL Justification

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance. The TOE is assumed to be used in an environment with low level threat of malicious attacks.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-4 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-4 Mapping of Functional Requirements to TOE Summary Specification

Security Functions	SFRs	Rationale

Security Functions	SFRs	Rationale
LANDesk report generation	FAU_LRG.1 (exp) FAU_LRR.1 (exp) FAU_LRR.2 (exp) FAU_LRR.3 (exp)	LDMS provides the ability to scan managed devices for the different types of security risks, and generate security and patch manager reports [**FAU_ LRG.1 (exp)**].These reports are available to LANDesk users with appropriate right(s), and are formatted in suitable manner for the user to interpret the information [**FAU_LRR.1 (exp)**]. The LANDesk console provides the ability to sort different security and patch manager reports based on specific criteria [**FAU_ LRR.3 (exp)**]. The LANDesk Management group does not provide read access to the security and patch manager reports, except those users that have been granted explicit read-access [**FAU_ LRR.2 (exp)**].
Identification and authentication	FIA_ATD.1 FIA_LAU.2 (exp) FIA_UID.2	The LANDesk console uses user ID, user rights, and group membership to control the access to all the tools and devices [**FIA_ATD.1**]. It requires each user to be successfully identified [**FIA_UID.2**] and authenticated [**FIA_LAU.2 (exp)**] before allowing any other actions on behalf of that user.
Security management	FMT_MTD.1a,b,c,d FMT_SMR.1 FMT_SMF.1	The LDMS provides the capability to perform the following security management functions: • LANDesk report generation • Management of security attributes [**FMT_SMF.1**]. The LDMS provides the capability to define roles by assign special administrative roles based on their rights and scopes [**FMT_SMR.1**]: • Users with LANDesk Management Suite administrators right have full access all Tools • Users with the Reports right can create, run, view, publish, import and export reports • Users with the Security and Patch Manager right can download, and update the common types of security and patch content, and can configure and run the security scan on the LANDesk managed devices

Security Functions	SFRs	Rationale
		[**FMT_MTD.1**].

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-5.

Table 8-5 Assurance Measures Rationale

Item	Security Assurance Requirement	LANDesk Document(s)	Rationale
1	ACM_CAP.2	LANDesk Management Suite 8, 8.6.1 Configuration management and delivery procedures.	Configuration management (CM) helps to ensure that the integrity of the TOE is preserved, by requiring discipline and control in the processes of refinement and modification of the TOE and other related information. CM prevents unauthorized modifications, additions, or deletions to the TOE, thus providing assurance that the TOE and documentation used for evaluation are the ones prepared for distribution. CM document includes: • Proof that the CM system is being used. • Provides configuration Item List(s) the TOE is comprised of • List of the source code files and version numbers • List of design documents with version numbers • Test documents with version numbers • User and administrator documentation with version numbers
2	ADO_DEL.1	LANDesk Management Suite 8, 8.6.1 Configuration management and delivery procedures. LANDesk Management Suite 8, 8.6 Installation and	Delivery covers the procedures used to maintain security during transfer of the TOE to the user. Applicable across all phases of delivery from packaging, storage, distribution. Such procedures and measures are the basis for ensuring that the security protection offered by the TOE is not compromised during transfer.

Item	Security Assurance Requirement	LANDesk Document(s)	Rationale
		Deployment Guide	
3	ADO_IGS.1	LANDesk® Management Suite 8 Installation and Deployment Guide	Provides detailed instructions for installation of the product by the distributor (vendor).
4	ADV_FSP.1	LANDesk Management Suite 8, 8.6.1 Functional Specification (FSP)	Describes the TSF interfaces and TOE functionality
5	ADV_HLD.1	LANDesk Management Suite 8, 8.6.1 High-level Design (HLD)	Describes the TOE subsystems and their associated security functionality
6	ADV_RCR.1	LANDesk Management Suite 8, 8.6.1 Representative Correspondence (RCR)	Provides the following two dimensional mappings: • TSS and functional specification; • Functional specification and high-level design.
7	AGD_ADM.1	LANDesk® Management Suite 8 User's Guide	Describes how to administer the TOE securely.
8	AGD_USR.1	LANDesk® Management Suite 8 User's Guide	Describes the secure use of the TOE.
9	ATE_COV.1	Test Case Identification version 2.6.xls	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1	Test Case Identification version 2.6.xls	Test documentation includes: • Test plans, • Test procedures • Expected results, and • Actual results.
11	ATE_IND.2	TOE for Testing	N/A
12	AVA_SOF.1	LANDesk Management Suite 8, 8.6.1 Strength of	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.

Item	Security Assurance Requirement	LANDesk Document(s)	Rationale
		Function Analysis	
13	AVA_VLA.1	LANDesk Management Suite 8, V8.6.1 Vulnerability Analysis	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 Appendix

Table 9-1 Acronyms

CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
LDMS	LANDesk® Management Suite
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFR	TOE Security Functional Requirement
TSP	TOE Security Policy

Table 9-2 References

CCITSE	Common Criteria for Information Technology Security Evaluation Version 2.3, (CC v2.3), August 2005.