National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

LANDesk® Management Suite 8, V.8.6.1

Report Number: CCEVS-VR-06-0034
Dated: October 18, 2006
Version: Version 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the LANDesk® Management Suite 8, Version 8.6.1, and a product of LANDesk Software, Ltd, Salt Lake City, UT.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

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.

The Target of Evaluation (TOE) includes the two main components of the LANDesk Management Suite: the server and the client (agent). The LANDesk client components or agents are deployed on each monitored LDMS device throughout the network. All user operations and security management functions are performed via the Main Console of the server component.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

- Identification and Authentication
- Scan managed devices
- LANDesk report generation (excluding customized reports)
- Security management

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

- Hardware platforms and Operating Systems;
- Third party core and rollup relational databases;
- Web browsers;
- Web servers;
- data encryption mechanism; and
- Network hardware and software (e.g., firewalls and routers)

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during October 2006. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all

written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for LDMS Platform is contained within the document Security Target for LANDesk® Management Suite 8, V8.6.1 [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	LANDesk Management Suite 8 Version 8.6.1
Evaluated Software:	LANDesk Management Suite 8 Version 8.6.1 with patches: LD-861-Mini-Rollup-February-2006 and LD-861-SP1
Developer:	LANDesk Software, Ltd, Salt Lake City, UT.
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Team:	Sunil Trivedi (The MITRE Corporation)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. A description of the principle security policies is as follows:

- **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.

- **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.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Report Generation	
FAU_ LRG.1 (exp)	LANDesk report generation
FAU_LRR.1 (exp)	LANDesk reports review
FAU_LRR.2 (exp)	LANDesk restricted reports review
FAU_LRR.3 (exp)	LANDesk selectable reports review
Class FIA: Identification & Authentication	
FIA_ATD.1	User attribute definition
FIA_LAU.2 (exp)	LANDesk user authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MTD.1a, b, c, d	Management of TSF data
FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions

IT Environment Security Functional Requirements

Class FPT: Protection of TSF	
FPT_STM.1	Reliable time stamps
FPT_SEP_ENV.1 (exp)	TSF domain separation
Class FIA: Identification & Authentication	
FIA_OAU.2 (exp)	OS user authentication before any action
Class FPT: Protection of the TSF	
FTP_ITC.1	Inter-TSF trusted channel
FPT_ITT.1	Basic internal TSF data transfer protection

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- It is assumed that TOE components are stored in a secure physical location to prevent unauthorized physical modification.
- Only trusted, knowledgeable, and authorized administrators will be able to manage, configure, operate, and access TOE, database and the underlying operating system according to the TOE documentation.
- No untrusted users will access the TOE or no untrusted software or data will reside on the TOE.
- TOE depends on the underlying operating system for a reliable time stamps.
- It is assumed that users will protect their authentication data.
- It is assumed that there is the capability to hash and store user passwords.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).

2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or "vulnerabilities" to objectives not claimed in the ST.
4. LDMS depends on IT environment to provide
    a. access control and process separations that protect LANDesk Management Suite executables, and LANDesk Management Suite data from untrusted processes on the host.
    b. assured client identification
    c. trusted communication channel between the TSF and a remote trusted IT product.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The LDMS Platform consists of the Core Server and main Console. In addition LANDesk Management Suite requires one database for each core server and a rollup database optimized for querying (databases are not included within the TOE). The TOE Components include the LDMS Core Server, main Console and LANDesk client (agent) that runs on each LDMS managed device.

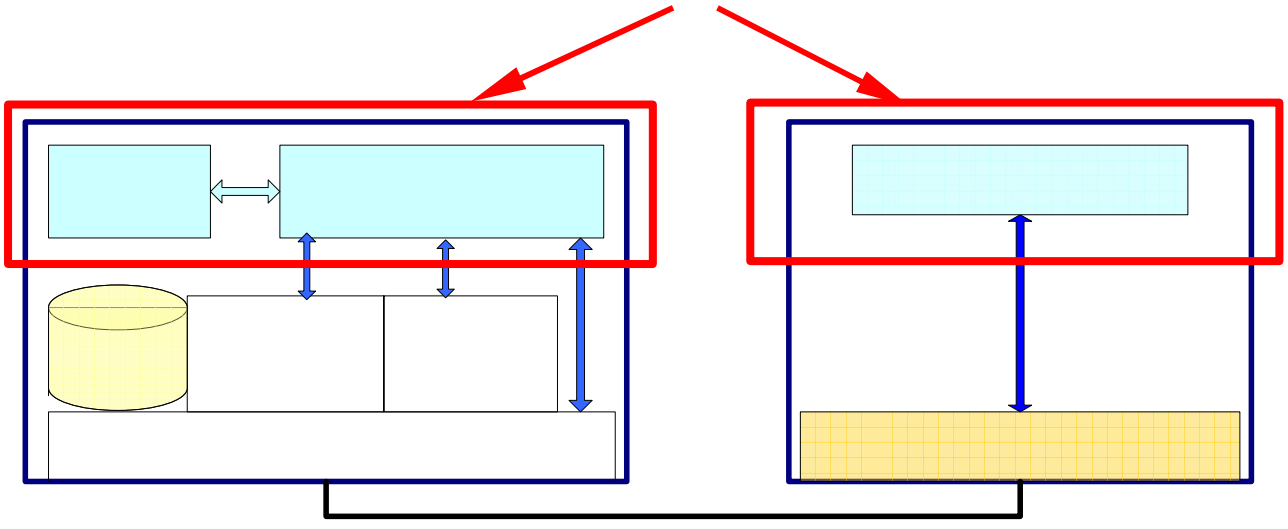

Figure 1. TOE Physical Boundary.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- LANDesk Management Suite 8 Version 8.6.1 Security Target Version 1.0, dated October 17, 2006.
- LANDesk® Management Suite 8.6 Installation and Deployment Guide.
- LANDesk® Management Suite 8.6 User's Guide
- LANDesk® Management Suite 8, V8.6.1, Configuration management and delivery procedures, Revision 0.7, dated October 17, 2006
- LANDesk® Management Suite 8.6.1 Common Criteria Installation and Configuration Supplement, Revision 0.5, dated October 17, 2006.

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Security audit (Scanning and Report generation), Identification and Authentication, and Security Management.

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. In general, only those user interface functions that were directly related to SFRs were explicitly verified.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

The installation of the TOE was done in accordance with the product's Installation and Deployment guide on two Microsoft's Windows 2000 server and one Windows XP machine. The test configuration included:

- Server 1: Core Server on Windows 2000 Server SP4
- Client 1: LANDesk Client on Windows XP SP2
- Client 2: LANDesk Client on Windows 2000 Professional SP4

The latest security-critical patches for Windows 2000 Server and Professional SP4 were installed prior to the evaluation testing activities. The Windows XP SP2 client machine was updated with the latest security-critical patches except for the Malicious Software Removal Tool (KB890830). This update was installed as a part of the initial test prior to the rest of the evaluation testing activities. The LANDesk client update function was tested using the LD-ICF-CONFIG update, which configures Window's Internet Connection Firewall functionality.

The evaluation team reran most of the developer tests and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluator tests successfully demonstrated deploying agents on two machines, a Windows 2000 server and a Windows XP. This was followed up by successfully downloading 8.6.1 software updates (3 patches) and Microsoft Windows vulnerabilities

(12 definitions). Other aspects of patch management were not demonstrated such as on multiple OS platforms (UNIX, Linux, MAC), directories, and databases. Microsoft MSDE database was used for demonstrating all tests.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The LANDesk SOF analysis assumes passwords length to be a minimum of 8 with at least one special character, at least one numeric character, and at least one uppercase and one lowercase character. It further assumes that common dictionary words are not used and that passwords expire in 30 days.

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.

7.4 Vulnerability Analysis

The developer searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of LDMS Platform were found. The following public domain sources were used to identify and search for relevant vulnerabilities:

- http://cve.mitre.org/cve
- http;//www.google.com

Known vulnerabilities in the IT environment could also be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will installed the latest security critical patches to the operating system and database software. Under unusual circumstances a patch to TOE may also be required to address compatibility issues with a specific operating system or

database patch. The customer is advised to check the LANDesk support web site for any restrictions on specific patches to components of the IT environment.

The assumed level of expertise of an attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter, are listed in section 3.2 of the ST.

8. Evaluated Configuration

The evaluated version of the LDMS Platform is version 8.6.1, internally identified as build 8.6.100.62 with the following two client patches installed:

1. LD-861-Mini-Rollup-February-2006
2. LD-861-SP1

LANDesk provides delivery of this product's components through the LANDesk web site or via CD. It requires authentication information (user name and password) prior to allowing access to the file containing the TOE. Authentication data is provided to customers via email. The authentication data is good for one-time file transfer of the TOE.

The customers must download the above patches to bring the delivered software to the evaluated configuration and verify the version number and installed patches according to CC Installation and Configuration Supplement-V0.2.doc.

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

As with any evaluation, this evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).

Be sure to note the assumptions and clarifications of scope in section 4 of this report. Additionally:

1. Note that this tool is designed to view, configure, and manage the devices on a network (multiple Windows domains) using a full range of remote administration tools. According to the ST claims, it can manage complex, heterogeneous computing environments by supporting multiple OS platforms, directories, databases and hardware platforms. However, the test configuration included only a windows 2000 LDMS server and two local clients (Windows 2000 and XP workstations) on a standalone network, a workgroup, without a domain controller.
2. According to ST, each LANDesk client device needs a 100 Mbps NIC, IP address, and an active internet connection. Based on this, ST claim of automating desktop management tasks for mobile devices is questionable due to 100 Mbps NIC requirements. The evidences supporting TOE behavior in the DHCP and in the mobile environments were not presented.
3. The firewall feature that was introduced in Window XP SP2 prevents push-based installation of the LANDesk client software. The vendor's administrator guide describes a procedure as a work around for this problem that involves changing the firewall's default configuration to enable the "File and Printer Sharing" exception. The LD-ICF-CONFIG update should be installed by end-users that want to reduce the security risks associated with unnecessary exceptions to the firewall policy. This update enables narrowly defined firewall policy exceptions that are specifically required for LANDesk server to remotely access the LANDesk client. After the LD-ICF-CONFIG update is installed the "File and Printer Sharing" exception is not required and may be disabled. The LD-ICF-CONFIG update is

automatically installed when the LANDesk client is installed using the pull-based procedure.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the LANDesk Management Suite 8 V8.6.1.

11. Security Target

The Security Target for LANDesk Management Suite 8 V8.6.1 is contained within the document Security Target for LANDesk Management Suite 8 V8.6.1, Version 1.0 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LDMS	LANDesk® Management Suite
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

4. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://niap.nist.gov/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- LANDesk® Software (http://www.landesk.com/).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Security Target for LANDesk Management Suite 8 V8.6.1, Version 1.0, October 17, 2006.