Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2011/76

18 Jul 2011

Version 1.0

Amendment Record

Version	Date	Description
1.0	18/07/2011	Public release.

Executive Summary

1 Wyse Device Manager Enterprise Edition Version 4.7.2 is a product that is designed to provide an enterprise solution for managing network intelligent devices. It enables IT administrators to organise, upgrade, control, and support Windows Embedded Standard (WES), Wyse Thin OS, or Windows XPe devices across any LAN, WAN, or wireless network. Wyse Device Manager Enterprise Edition Version 4.7.2 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Wyse Technology Inc.'s Wyse Device Manager Enterprise Edition Version 4.7.2, to the Common Criteria (CC) Evaluation Assurance Level EAL 2. The report concludes that the product has met the target assurance level of EAL 2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed in May 2011.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Ensure that non-required services (e.g. TFTP and FTP) are disabled within the TOE;

c) Operate the TOE according to the administrator guidance document (Ref [3]); and

d) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at (Ref [1]) and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE, Wyse Device Manager Enterprise Edition Version 4.7.2, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 2; and

b) Provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Wyse Device Manager Enterprise Edition Version 4.7.2
Software Version	Wyse Device Manager Enterprise Edition Version 4.7.2 Build 374 with Hot Fixes HF04072025609 and HF04072036209 Web Agent (HAgent) versions 5.1.1.31 (WES and XPe) and 4.0.4.2 (Wyse Thin OS)
Security Target	Wyse Technology Inc. Wyse Device Manager Enterprise Edition Version 4.7.2 Security Target, Version 1.8, dated April 18 2011
Evaluation Level	EAL 2
Evaluation Technical Report	EFS-T022-ETR
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009, with interpretations as of 28 April 2010
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 3, July 2009, with interpretations as of 28 April 2010
Conformance	Common Criteria Part 2 conformant Common Criteria Part 3 conformant
Product Developer	Wyse Technology Inc. 3471 N. First Street San Jose, CA 95134 United States
Evaluation Facility	stratsec Suite 1, 50 Geils Court Deakin, ACT 2600 Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Wyse Device Manager Enterprise Edition Version 4.7.2 developed by Wyse Technology Inc. Its primary role is to provide an enterprise solution for managing network intelligent devices. It enables IT administrators to organise, upgrade, control, and support WES, Wyse Thin OS, or XPe devices across any LAN, WAN, or wireless network.

12 Wyse Device Manager (WDM) acts as a device manager for managed clients. It maintains a list of the managed devices and their properties. It also serves as a download repository for the managed clients. The client properties, together with parameters specified by the WDM GUI users, are used to determine appropriate packages for download to each client. Packages may include images, configuration parameters, or applications.

13 Remote Repositories provide a subset of the WDM functionality (the user interface is not included). They maintain a copy of the packages and other configuration information maintained on WDM to facilitate more efficient downloads to distributed clients. The clients communicate with WDM (on the main server or a Remote Repository) to determine what packages to download, and WDM directs the clients to perform the download as configured by the WDM users.

14 Web Agent is an application downloaded to managed clients. It provides information about the clients to WDM and executes operations directed by WDM (e.g. downloaded an updated version of a package).

15 The TOE consists of one instance of the full WDM functionality, zero or more instances of Remote Repositories, and one or more instances of the web agent executing on clients. Remote Repositories are optional and the number installed is dependent on the scope and distribution of the managed clients.

2.3 Security Policy

The Security Target (Ref [1]) contains no explicit security policy statements.

2.4 TOE Architecture

16 The TOE consists of the following major architectural components:

a) WDM Server.

b) WDM Repository (optional).

c) Web Agent (HAgent).

17 The developer's architectural design identifies the following components of the TOE:

a) The **WDM** component consists of software executing on a dedicated Windows Server 2003 platform. The hardware, operating system, DBMS, DHCP Server and web server (IIS) are not included in the TOE boundary.

b) A **Remote Repository** consists of a subset of the WDM software executing on a dedicated Windows Server 2003 platform. The user interface component of the TOE is not installed on Remote Repositories. The hardware, operating system, DBMS, DHCP Server and web server (IIS) are not included in the TOE boundary.

c) The **Web Agent** component is an application executing on a thin client. The hardware and operating system are not included in the TOE boundary.

2.5 Clarification of Scope

18 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

19 The TOE provides the following evaluated security functionality as described in Table 2.

Table 2: Evaluated Functionality

Security Function	Description
Security Audit	Logs are maintained of configuration actions performed via the WDM GUI as well as security-relevant events. The logs may be reviewed via the GUI.
Identification and Authentication	Access to the TOE's WDM GUI is restricted to Windows users that have been configured for access in the WDM database. When the GUI is invoked, Windows learns the username and it is checked against the authorised GUI users. If the user is authorised, the configured role and permissions are bound to the session. Windows users that are not authorised to use the WDM GUI are not able to access any TOE functions or data.
Security Management	Management of the TOE functions and data is provided by the TOE

2.5.2 Non-evaluated Functionality and Services

20 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

21 The functions and services that have not been included as part of the evaluation are provided below:

a) **Secure Communication Between a WDM Server, Repository, and a Device.** Provides secure communications between client and web server by encrypting traffic to and from the client and server and by issuing certificates. Cryptographic functionality of the TOE is not evaluated.

b) **Device Shadowing.** WDM also provides an organisations help desk with a shadowing capability to diagnose issues within end-user environments from a remote location. This functionality of WDM is not evaluated.

2.6 Usage

2.6.1 Evaluated Configuration

22 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

23 The evaluated configuration is based on a default installation of the TOE detailed below with additional configurations.

24 Wyse Device Manager with all supported features (including the master repository) is installed on a single Windows server dedicated to the WDM function. Any number of Remote Repositories (with a subset of the WDM functionality) may be installed on additional Windows servers, depending on the size and distribution of the managed devices.

25 The following configuration parameter settings in WDM **must** be used:

a) In *Service Preferences*, “Enable Legacy Agent Service” **must not** be set since legacy agents are not included in the evaluated configuration.

b) In *Service Preferences*, “Enable WDM Service Logs” **must** be set.

c) In *Logging Preferences*, “Write Preferences changes to system log” **must** be selected and all the event types must be selected.

d) In *Scheduling Preferences*, “Enable WDM Service Logs” **must** be set.

e) In *Logging Preferences*, all the logging levels are configured for Warnings.

f) HTTP is used for communication with repositories; FTP is **not enabled**.

g) Merlin is used as the imaging option; WISard is **not used** since it is dependent on the repositories supporting FTP.

h) In *DHCP/TFTP Preferences*, TFTP is **not enabled**. Since PXE operations depend on TFTP, PXE is not supported. All clients **must** use HTTP to interact with the WDM server.

2.6.2 Delivery procedures

26 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

27 New customers are registered with the Wyse Support web site by Wyse personnel when their first order is placed. The registration includes a primary Point of Contact (POC) email address to send information to. Once registration is complete, a welcome email is sent to the POC (with a “From” address of “Wyse Workflow”.

28 Customers download the TOE software and guidance documentation via the Wyse Support web site. The URL for the web site is communicated to users in the welcome email. After logging in to the web site, users navigate to the download page. Additional information about the files required to download and install the evaluated version of the TOE is provided in the *Common Criteria Installation Supplement Wyse Device Manager™ Release 4.7.2* that is also available on the web site. Users are directed to download the following:

a) **WDM 4.7.2** – ZIP file containing the base WDM version 4.7.2 installation files along with the standard user documentation for the release.

b) **Hotfix HF04072025609** – ZIP file containing the installation files and release notes for the hot fix.

c) **Hotfix HF04072036209** – ZIP file containing the installation files and release notes for the hot fix.

29 The HAgents (Web Agents) are included with the distribution of WDM 4.7.2 and are downloaded to the thin clients by the administrators if the appropriate version is not already executing on the thin clients.

30 The licence key required to permanently activate the software is sent to the POC via email from licensing@wyse.com.

2.6.3 Determining the Evaluated Configuration

31 User verification of the TOE is performed at the product level. The version may be verified in the following ways:

a) The file downloaded to install the full product includes the version in the file name;

b) The installation scripts display the product version; and

c) The product version of the operational product may be displayed from the user interface.

32 Application of hot fixes to a product version may be verified via the Installation Details display in the Report Manager section of the user interface.

33 Users should also check that the additional configuration parameters have been set, as outlined in Section 2.6.1 Evaluated Configuration

2.6.4 Documentation

34 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to download with the TOE:

a) Installation Guide Wyse Device Manager™ Release 4.7.2 (Ref [3]).

b) Administrators Guide Wyse Device Manager™ Release 4.7.2 (Ref [4]).

c) Common Criteria Installation Supplement Wyse Device Manager™ Release 4.7.2 (Ref [5]).

d) Wyse Device Manager™ Integration Add-Ons (Ref [6]).

2.6.5 Secure Usage

35 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions, as detailed in Table 3, must hold in order to ensure the security objectives of the TOE are met.

Table 3: Assumptions

Assumption	Description
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
A.MGMT	The network interconnecting the TOE and IT systems used to manage the TOE will protect data transmitted over the network from disclosure.
A.NETWORK	There will be a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. This network functions properly.
A.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and ongoing.

36 In addition, the organisational security policies detailed in Table 4 must be in place:

Table 4: Organisational Security Policies

OSP	Description
P.ACCESS	The TOE shall support multiple administrator roles and limit the management functionality accessible to administrators according to their role.
P.PACKAGE	The TOE shall manage multiple packages for download to devices.

Chapter 3 - Evaluation

3.1 Overview

37 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

38 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [7], [8] and [9]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [10]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [11], [12], [12] and [14]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [15]) were also upheld.

3.3 Functional Testing

39 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

40 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. The evaluators performed these tests to determine if the TOE is resistant to attacks performed by an attacker possessing a Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit.

b) Specialist technical expertise required.

c) Knowledge of the TOE design and operation.

d) Window of opportunity.

e) IT hardware/software or other equipment required for exploitation.

41 This vulnerability analysis also included a search through public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables.

Chapter 4 - Certification

4.1 Overview

42 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

43 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [16]), the Australasian Certification Authority certifies the evaluation of Wyse Device Manager Enterprise Edition Version 4.7.2 performed by the Australasian Information Security Evaluation Facility, stratsec.

44 stratsec has found that Wyse Device Manager Enterprise Edition Version 4.7.2 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 2.

45 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

46 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

47 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

48 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

49 This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

4.4 Recommendations

50 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

51 The Australasian Certification Authority (ACA) recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Ensure that non-required services (e.g. TFTP and FTP) are disabled within the TOE;

c) Operate the TOE according to the administrator guidance document (Ref [3]); and

d) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

Annex A - References and Abbreviations

A.1 References

[1] Wyse Device Manager Enterprise Edition Version 4.7.2 Security Target, ST Version 1.8, April 2011, Wyse Technology Inc.

[2] Australian Government Information Security Manual (ISM), November 2010, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Installation Guide Wyse Device Manager™ Release 4.7.2.

[4] Administrators Guide Wyse Device Manager™ Release 4.7.2.

[5] Common Criteria Installation Supplement Wyse Device Manager™ Release 4.7.2.

[6] Wyse Device Manager™ Integration Add-Ons.

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-001.

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-002.

[9] Common Criteria for Information Technology Security Evaluation Part 1: Security assurance components July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.

[10] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 3 July 2009, CCMB-2009-07-004.

[11] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[13] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[14] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[15] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[16] Evaluation Technical Report for Wyse Device Manager (WDM) EFS-T022-ETR, 30 May 2011.

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DHCP	Dynamic Host Configuration Protocol
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
HTTP	Hypertext Transfer Protocol
OS	Operating System
OSP	Organisational Security
POC	Point Of Contact
PP	Protection Profile
PXE	Preboot eXecution Environment
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WDM	Wyse Device Manager
WES	Windows Embedded Standard
WISard	Wyse Imaging System
WTOS	Wyse Thin Operating System
XPe	(Windows) XP embedded