122-B

CERTIFICATION REPORT No. CRP252

1E POWER AND PATCH MANAGEMENT PACK INCLUDING WAKEUP AND NIGHTWATCHMAN Version 5.6

running on multiple platforms

Issue 1.0

December 2009

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor:	1E
Developer:	1E
Product and Version:	1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6
Platform:	NightWatchman Server - Microsoft Windows Server 2003/2008 or Microsoft SQL Server 2005 SP2/2008 or Microsoft .NET Framework 2.0 SP1 or Microsoft IIS 6.0 NightWatchman Console – Microsoft .NET Framework 3.5 SP1 Workstation – Microsoft Windows Vista (Business, Enterprise, Enterprise x64 and Ultimate) or Microsoft Windows XP SP2 Additional Microsoft servers required in the environment - Microsoft SMS 2003 or Configuration Manager 2007 (SMS/ConfigMgr), or Microsoft Active Directory Server
Description:	The product forces unused computers to be powered down centrally, safely and remotely to an automated schedule to save power.
CC Version	3.1
CC Part 2:	extended
CC Part 3:	conformant
EAL:	EAL2
PP Conformance:	None
CLEF:	SiVenture
CC Certificate:	CRP252
Date Certified:	18 December 2009

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

CERTIFICATION STATEMENT **2**

TABLE OF CONTENTS **4**

I. EXECUTIVE SUMMARY **5**

Introduction 5
Evaluated Product and TOE Scope 5
Security Claims 5
Evaluation Conduct 6
Conclusions and Recommendations 6
Disclaimers 6

II. TOE SECURITY GUIDANCE **8**

Introduction 8
Delivery 8
Installation and Guidance Documentation 8

III. EVALUATED CONFIGURATION **10**

TOE Identification 10
TOE Documentation 10
TOE Scope 10
TOE Configuration 10
Environmental Requirements 11
Test Configuration 12

IV. PRODUCT ARCHITECTURE **14**

Introduction 14
Product Description and Architecture 14
TOE Design Subsystems 15
TOE Dependencies 16
TOE Interfaces 16

V. TOE TESTING **17**

TOE Testing 17
Vulnerability Analysis 17
Platform Issues 17

VI. REFERENCES **19**

VII. ABBREVIATIONS **21**

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of 1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6, running on multiple platforms, to the Sponsor, 1E, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL2** on 29 October 2009:

- 1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6 running on multiple platforms

4. The Developer was 1E. The 1E Power & Patch Management Pack comprises two leading applications: NightWatchman and 1E WakeUp. The solution enables unused computers to be powered down centrally, safely and remotely – to an automated schedule. Before powering down a PC, it saves any open documents so users don't lose any work.

5. The pack provides the power to manage software patches and updates across the enterprise network in a less intrusive, more effective manner. It can wake up PCs out of office hours, install the latest updates through Microsoft System Center Configuration Manager 2007 or SMS 2003, and then shut them down 'en masse' moments later. Staff can remain productive and work without interruption on secure, well-protected PCs, without the risk and potential cost of a virus attack.

6. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

7. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 1.3 of [ST].

Security Claims

8. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which these Objectives meet and the Security Functional Requirements (SFRs) and Security Functions that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products. For explicitly stated SFRs see Section 6.2 of [ST].

9. The TOE security policies are detailed in [ST]. The OSPs that must be met are specified in [ST] Section 1.8.

10. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

11. The CESG Certification Body monitored the evaluation which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in October 2009, were reported in the Evaluation Technical Report [ETR].

Conclusions and Recommendations

12. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

13. Prospective consumers of 1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6, running on multiple platforms, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

14. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

15. In addition, the Evaluators' comments and recommendations are as follows:

- TOE consumers should adhere closely to the administrative guidance in order to maintain security.

Disclaimers

16. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

17. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

18. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate,

should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

19. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

20. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

21. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

22. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised during delivery.

23. Software packages are uploaded as zip files with the name of the file indicating the product and version in the format of *ProductName.vMajor.Minor.Maintenance.Build.zip.* This contains the actual product installer (digitally signed and time stamped with a 1E key issued by VeriSign), product documentation files and release notes. This uniquely defines the software purchased by the customer. The versions that have been evaluated are:

- NightWatchman Management Center v5.6.10.35
- 1E WakeUp v5.6.200.10
- NightWatchman (agent) v5.6.10.11
- 1E WakeUp Agent v5.6.200.10.

24. All software is delivered and made available for all latest versions via the 1E web site which is hosted by a third party (CrystalTech). Customers can download the software via the site where they are prompted to use a web login, so that 1E can record who downloaded what. Customers are sent details with a link to the site and the licence key by email.

25. Documentation for a release is provided both within the delivered package release and as a separate PDF file. Each document is versioned using the Major.Minor attributes and a revision number (as this update process is not part of the software build process).

Installation and Guidance Documentation

26. The Installation and Secure Configuration documentation is as follows:

- The NightWatchman Installation Guide [NWIG];
- The NightWatchman Management Center Installation Guide [NWMCIG];
- The 1E WakeUp Installation Guide [WUIG].

27. The three installations need to be performed to install the TOE. The order of installation is unimportant. All these guides should be followed precisely to ensure secure installation, particularly the notes regarding the evaluated product.

28. The User Guide and Administration Guide documentation is as follows:

- The NightWatchman User's Guide [NWUG]
- The NightWatchman Administrator's Guide [NWAG]
- The 1E WakeUp Administrator's Guide [WUAG].

29. These guidance documents contain all the required information for the administrator(s) to maintain security of the TOE.

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is 1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6, running on multiple platforms, which consists of:

- NightWatchman Management Center v5.6.10.35
- 1E WakeUp v5.6.200.10
- 1E NightWatchman (agent) v5.6.10.11
- 1E WakeUp Agent v5.6.200.10

TOE Documentation

31. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

32. The TOE Scope is defined in the Security Target [ST] Sections 1.4.1 and 1.4.2. Functionality that is outside the TOE Scope is defined in [ST] Section 1.4.3.

TOE Configuration

33. The evaluated configuration of the TOE is defined in [ST] Section 1.3.4.

34. The TOE will run on multiple platforms as follows:

a) NightWatchman Server:

- Microsoft Windows Server 2003/2008
- Microsoft SQL Server 2005 SP2/2008
- Microsoft .NET Framework 2.0 SP1
- Microsoft IIS 6.0

b) NightWatchman Console:

- Microsoft .NET Framework 3.5 SP1

c) Workstation – running Windows XP or Vista:

- Microsoft Windows Vista (Business, Enterprise, Enterprise x64 and Ultimate)

- Microsoft Windows XP SP2

d) Additional Microsoft servers required in the environment:

- Microsoft SMS 2003 or Configuration Manager 2007 (SMS/ConfigMgr)
- Microsoft Active Directory Server

35. It is important to note that the product will operate with workstations that run Windows 2000 SP4 but this was not part of the evaluated configuration of the TOE, so potential customers should be aware of this.

Environmental Requirements

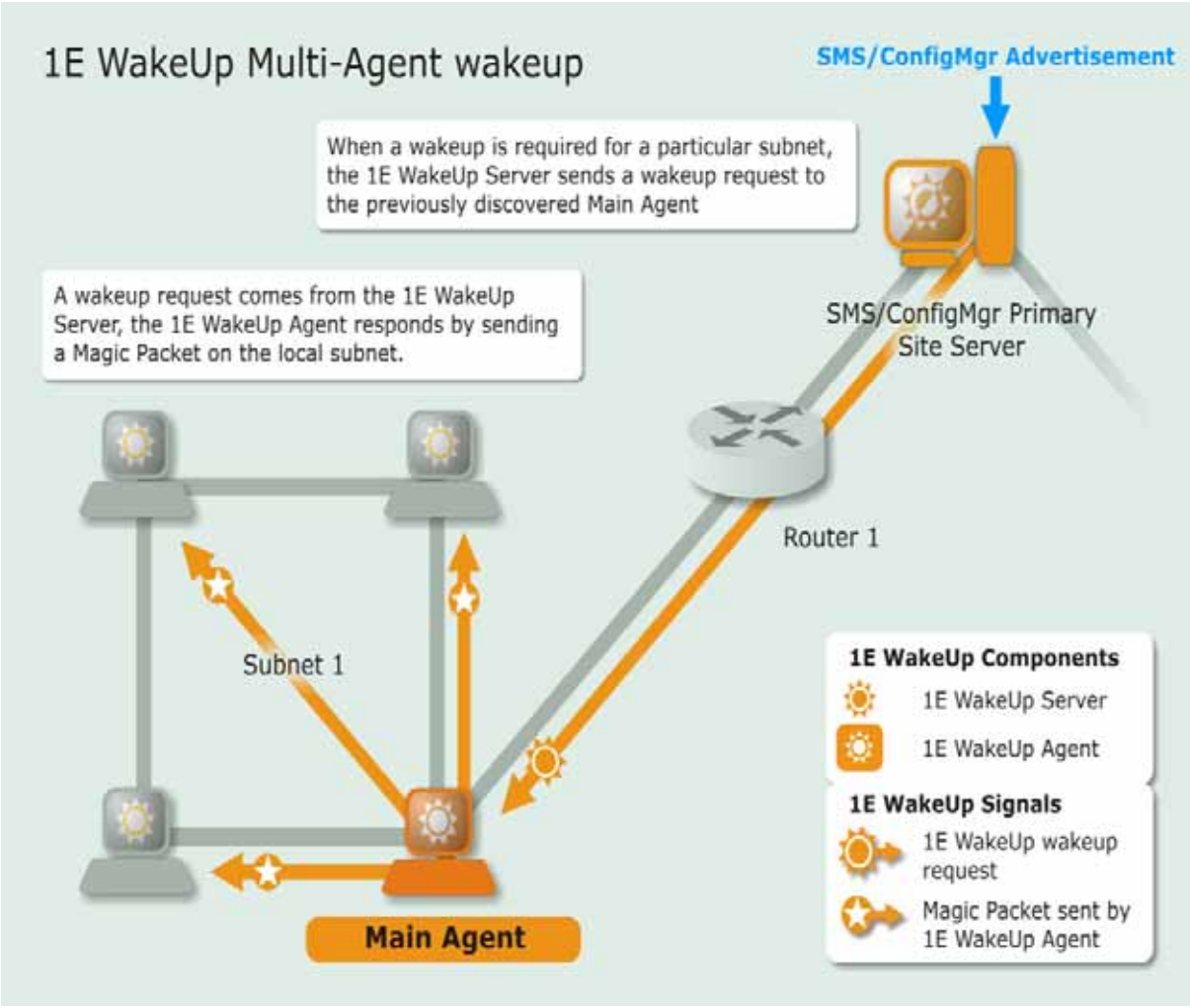
36. The environmental assumptions for the TOE are stated in [ST] Section 3.5.4.

37. The TOE was evaluated running on the platforms given in the previous section.

38. The environmental IT configuration is as follows:

- Hardware as described in the previous section.
- Environmental assumptions as provided in Section 3.5.4 of [ST].

An example environmental IT configuration is provided in the diagram below.



Test Configuration

39. The Developers tested their software on all combinations of the following hardware:

a) NightWatchman Server:

- Microsoft Windows Server 2003/2008
- Microsoft SQL Server 2005 SP2/2008
- Microsoft .NET Framework 2.0 SP1
- Microsoft IIS 6.0

b) NightWatchman Console:

- Microsoft .NET Framework 3.5 SP1

c) Workstation – running Windows XP or Vista:

- Microsoft Windows Vista (Business, Enterprise, Enterprise x64 and Ultimate)
- Microsoft Windows XP SP2

d) Additional Microsoft servers required in the environment:

- Microsoft SMS 2003 or Configuration Manager 2007 (SMS/ConfigMgr)
- Microsoft Active Directory Server

40. The Evaluators performed the majority of their testing on the following configuration although some tests were run on other combinations:

a) NightWatchman Server:

- Microsoft Windows Server 2003/2008

b) NightWatchman Console:

- Microsoft .NET Framework 3.5 SP1

c) Workstation:

- Microsoft Windows XP SP2

d) Additional Microsoft servers required in the environment:

- Configuration Manager 2007 (SMS/ConfigMgr)

IV. PRODUCT ARCHITECTURE

Introduction

41. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

42. The key features of 1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6, running on multiple platforms, are as follows:

- Automatically powers down PCs according to a centrally controlled schedule to any state desired;
- Protects unsaved user data prior to power down;
- Works with or without existing systems management infrastructures;
- Provides organization and location based reporting on current and future potential savings;
- Integration with ConfigMgr and SMS 2003;
- Minimizes network impact by using ConfigMgr/SMS site hierarchy to stagger distribution;
- Reports on ConfigMgr/SMS clients and deployment success;
- Co-operates with Windows power management & adds enhancements to ensure PCs successfully enter low power states during idle periods for greater savings;
- Ability to set daily maintenance windows to allow scheduled maintenance;
- PCs with health problems are automatically grouped into ConfigMgr/SMS collections.

Product Description and Architecture

43. An overview of the TOE is provided in Section 1.3 of [ST]. This section describes example architectures for the TOE in its environment.

44. The TSF alone does not protect itself because it depends on the underlying Microsoft Windows (server and workstation) operating systems to provide some of the protection. Therefore, the developer has applied self-protection to the services provided by the TSF through its TSFI, and not to services provided by underlying IT entities that it uses.

45. The GUI provided to the administrators limits the input that an administrator can submit. With the exception of names (e.g. when creating a new policy the administrator enters a name to identify the policy), most input provided by the administrator is entered through selection of values provided in drop-down boxes, toggling switches on / off and selecting submission

/confirmation / cancel buttons. Physical access to the server components is limited to administrators.

46. As in the case of the graphic user interface provided to the NWM administrator, the GUI provided to the user also limits the input that a user can submit. A user can only provide input through the selection of predefined values through the selection of values provided in drop-down boxes, toggling switches on / off and selecting submission / confirmation / cancel buttons.

47. The design of the TOE requiring the Client to pull down new / updated power and health policies, rather than the server pushing them, provides further protection against replay attacks. The agents on the Client workstation are configured to only connect to specified servers to receive new policies. This prevents attackers attempting to connect to workstations to manipulate the settings of the TOE agents installed on the workstation. To prevent random wake-up broadcasts being issued to Clients within an enterprise, the assumption A.Fw_Block_Magic specified in the [ST] details that Magic packets originating from outside the enterprise network boundary will be blocked and will not be routed within the enterprise network. Protection of remote connections to the server (e.g. to run the Console application on the server) are controlled by the underlying Windows Server operating system. Attempts to connect directly to TOE server components using WCF are subject to Active Directory authentication and access is granted / denied on the basis of the permissions associated with the Active Directory user. (By default this connection uses TCP.)

48. As the servers are physically protected and any attempt to establish a remote session with a server will be subject to authentication, system calls between server components are considered to be protected by the TOE's environment. As noted above, the TOE is intended to be used in a non-hostile environment and hence someone with access to a workstation would not attempt to perform malicious actions against the TOE. Therefore, someone using the workstation locally would be expected not to attempt to use system calls to insecurely manipulate the TOE.

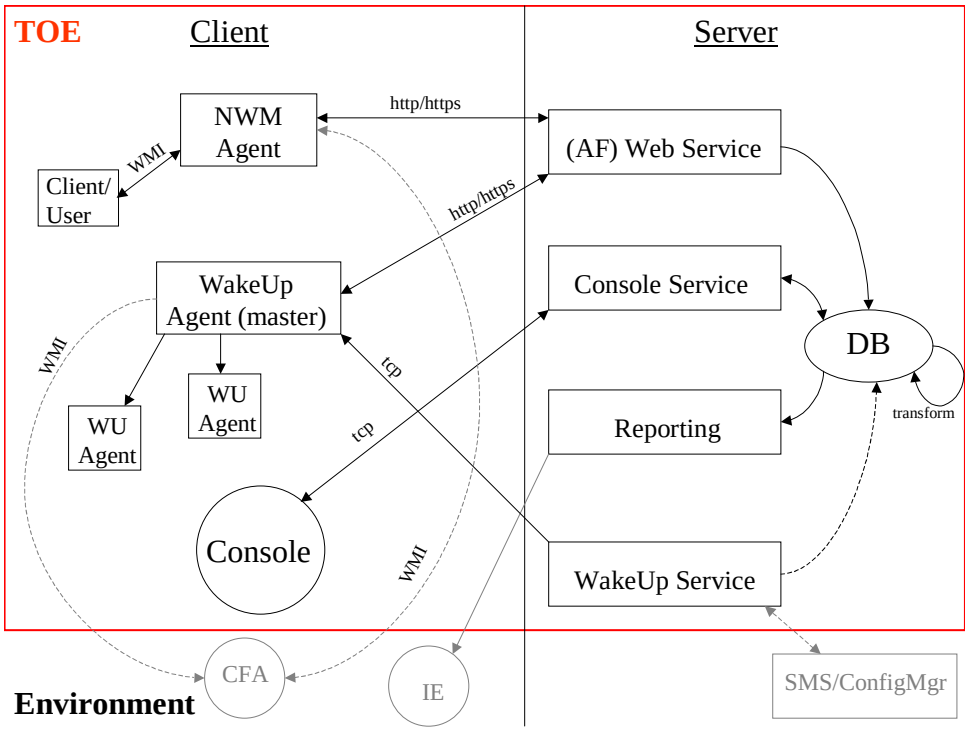
TOE Design Subsystems

49. The TOE subsystems, and their security features/functionality, are as follows:

- Web Service (NWM Server)
- Console Service (NWM Server)
- Reporting (NWM Server)
- WakeUp Service (WakeUp Server)
- NWM Agent (NWM Client)
- Client/User Interface (NWM Client)
- WakeUp Agent (WakeUp Client)

- Console Admin (NWM Server).

The interactions between the subsystems can be seen diagrammatically below.



TOE Dependencies

50. The TOE dependency is as follows:

- The underlying operating system.

TOE Interfaces

51. The external TOE Security Functions Interface (TSFI) is described as follows:

- Client;
- Console;
- Network.

V. TOE TESTING

TOE Testing

52. The Developer's tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

53. The Developer's tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

54. The developer carried out their testing on all combinations of hardware as described in Chapter III ('Test Configuration') of this report.

55. The Evaluators repeated approximately 20% of the developer tests on a single hardware combination.

56. The Evaluators devised and ran a total of 32 independent functional tests, different from those performed by the Developer. No anomalies were found.

57. The Evaluators also devised and ran a total of 10 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

58. The Evaluators performed the majority of their testing on the hardware combination described in Chapter III, although some tests were repeated on other hardware combinations.

59. The Evaluators finished running their penetration tests on 25 September 2009.

Vulnerability Analysis

60. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. Particular attention was taken to information relating to magic packets, SMS/ConfigMgr servers and the other hardware on which the software runs.

Platform Issues

61. The following platform issues should be considered:

- The TOE has been evaluated on the platforms described in Chapter III.

- Although the software will run on Windows 2000 workstations, this was not in scope of the evaluation and therefore the evaluation results are not valid for this platform.

VI. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2006-09-001, Version 3.1 R1, September 2006.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Requirements, Common Criteria Maintenance Board, CCMB-2007-09-002, Version 3.1 R2, September 2007.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Requirements, Common Criteria Maintenance Board, CCMB-2007-09-003, Version 3.1 R2, September 2007.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2007-09-004, Version 3.1 R2, September 2007.

[ETR] Evaluation Technical Report, SiVenture CLEF, LFV/T004/ETR, Issue 1.1, 3 December 2009

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee of Agreement Group, Senior Officials Group – Information Systems Security, Version 2.0, April 1999.

[NWAG] The NightWatchman Administrator's Guide, 1E, Version 5.6, Revision 4, 2009.

[NWIG] The NightWatchman Installation Guide, 1E, Version 5.6, Revision 3, 2009.

[NWMCIG] The NightWatchman Management Center Installation Guide,
1E,
Version 5.6, Revision 4, 2009.

[NWUG] The NightWatchman User's Guide,
1E,
Version 5.6, Revision 1, 2009.

[ST] Security Target,
1E,
1ECC-SecurityTarget01, Issue 1.0, 30 September 2009.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.5, October 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.2, October 2008.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.1, October 2008.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.3, October 2008.

[WUAG] The 1E WakeUp Administrator's Guide,
1E,
Version 5.6, Revision 2, 2009.

[WUIG] The 1E WakeUp Installation Guide,
1E,
Version 5.6, Revision 5, 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

Term	Meaning
AFR	Agility Framework
CFA	ConfigMgr Agent
ConfigMgr	Microsoft Configuration Manager
DCOM	Distributed Component Object Model
GPO	Group Policy Object
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MAC Address	Media Access Control Address
NMC	NightWatchman Management Centre
NWM	NightWatchman
RTL	Register Transfer Language
SID	Security Identifier
SMS	Systems Management Server
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WCF	Windows Communications Foundation
WMI	Windows Management Instrumentation
WOL	Wake-On LAN