Intelligent Windows Management

Common Criteria Security Target

For 1E Power and Patch Management Pack

30 September 2009

Document Version 1-0

Summary of Amendments

Version 1-0 30 Sept 2009

Final version, addressing evaluator comments.

0. Preface

0.1. Objectives of Document

This document presents the Common Criteria (CC) Security Target (ST) to express the security and evaluation requirements for the 1E Power and Patch Management product.

The product is designed and manufactured by 1E (http://www.1e.com/).

The Sponsor and Developer for the EAL2 evaluation is 1E.

0.2. Scope of Document

The scope of the Security Target within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a Security Target defines the IT security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements [CC1, Section C.1].

Security Functional Requirements (SFRs), as defined in [CC2], are the basis for the TOE IT security functional requirements expressed in this Security Target. These requirements describe the desired security behaviour expected of a TOE and are intended to meet the security objectives as stated in this Security Target. Security Functional Requirements express security requirements intended to counter threats in the assumed operating environment of the TOE, and cover any identified organisational security policies and assumptions.

0.3. Intended Readership

The target audience of this ST are consumers, developers and evaluators of the TOE, additional information can be found in [CC1, Section 6.2].

0.4. Related Documents

Common Criteria[1]

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2006-09-001, Version 3.1 Revision 1, September 2006.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2007-09-002, Version 3.1 Revision 2, September 2007.

[1] For details see http://www.commoncriteriaportal.org/

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2007-09-003, Version 3.1 Revision 2, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
CCMB-2007-09-004, Version 3.1, Revision 2, September 2007.

Developer documentation

[1] The NightWatchman Installation Guide, Version 5.6 document revision 3

[2] The 1E WakeUp Installation Guide, Version 5.6 document revision 5

[3] The NightWatchman Administrator's Guide, Version 5.6 document revision 4

[4] The 1E WakeUp Administrator's Guide, Version 5.6 document revision 2

0.5. Significant Assumptions

None.

0.6. Outstanding Issues

None.

0.7. Abbreviations

Acronym	Meaning
AFR	Agility Framework
ConfigMgr	Microsoft Config Manager
DCOM	Distributed Component Object Model
GPO	Group Policy Object
MAC Address	Media Access Control Address
NMC	NightWatchman Management Center
NWM	NightWatchman
SFR	Security Functional Requirement
SMS	Systems Management Server
SPD	Security Problem Definition

Acronym	Meaning
TSS	TOE Summary Specification
WCF	Windows Communications Foundation
WMI	Windows Management Instrumentation
WOL	Wake-On LAN

Glossary

Term	Meaning
Agent Services settings	Configuration of the WakeUp Agent, managed through the NMC and downloaded as part of the Health policy.
Computer Health Collections	Reports of Health check results.
Health Check	Specific diagnostic checks performed on the local machine by the 1E WakeUp Agent to highlight any local configuration and environment issues.
Health Policy	The set of rules to be applied to PCs in the enterprise network regarding diagnostic checks to be run on the PC and the download and application of fixes (patches/updates).
Magic Packet	A broadcast frame containing 6 bytes of 1's (i.e. FF FF FF FF FF FF) followed by sixteen repetitions of the target PC's MAC address.
Maintenance windows policies	Alarms/scheduled wakeups and shutdowns to ensure the workstation is available at certain times to receive maintenance updates from a 3rd party configuration management tool.
NMC	The 1E server components are collectively known as the NightWatchman Management Center, and include: • AgilityFramework server • 1E WakeUp server • NightWatchman Console
NWC Administrator	This refers to human users authorised to access the server and manage both the NightWatchman and WakeUp components of the Power and Patch Management product.
NWM User	This refers to the human users of the computer on which the client

Term	Meaning
	components (NightWatchman and WakeUp) of the Power and Patch Management product are installed.
PC	For the purposes of this ST, the term PC is used to cover any workstation, laptop or server on which the TOE client components are installed.
Policy Refresh	Message sent by WakeUp Server to a single machine to indicate that there is a new version of a policy to which they are subscribed.
Power Policy	The set of rules to be applied to PCs in the enterprise network regarding power scheme management (i.e. when the PC should standby or hibernate) and shutdown times, actions and exclusion lists.
Shutdown policies	Details of shutdown times and actions, configured through NMC.
Shutdown scripts	Scripts to be run (installed on individual workstations) during shutdown.
SID	Security Identifier assigned by Microsoft Windows upon creation of a user account
Sleepless client detection policies	Details of processes that are to be ignored during shutdown, which would otherwise keep the workstation alive.
Sleepless exclusion list	If the processes on this list are found to be running on a workstation during an attempted shutdown the shutdown is to be deferred.
Update Advertisement	Notifications from SMS/ConfigMgr that there is an update available
WakeUp policies	Details of wakeup times and lists of workstations to be woken, configured through NMC.
WakeUp Server settings	Configuration of the WakeUp server, managed through the NMC.

Table of Contents

Table of Figures

ST Introduction

In this section, the introduction to the ST is provided.

1.1 ST and TOE Reference Identification

TOE Reference:	Power and Patch Management Pack, including NightWatchman 5.6 and 1E WakeUp 5.6
ST Reference:	1ECC-SecurityTarget01
ST Version:	1-0
ST Date:	30 September 2009
Assurance Level:	EAL2
ST Author:	SiVenture

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

The Power & Patch Management Pack™ from 1E 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.

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[2], 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.

The key features of the 1E Power and Patch Management Pack are:

- Automatically powers down PCs according to a centrally controlled schedule to any state desired
- Protects unsaved user data prior to power down

[2] Microsoft System Center Configuration Manager is not included in the TOE.

- 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

1.2.2 TOE Type

The 1E Power and Patch Management Pack is a management tool enabling administrators to specify policies for power management and scheduling of maintenance updates for workstations across the corporate PC estate.

1.2.3 Required non-TOE hardware/software/firmware

NightWatchman Server

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

NightWatchman Console

- Microsoft.NET Framework 3.5 SP1

Workstation – running Windows XP or Vista

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

Additional Microsoft servers required in the environment:

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

- Microsoft Active Directory Server

1.3 TOE Description

1.3.1 Server Components

The server components are provided in the following installers:

1.3.1.1 NightWatchman® Management Center

The installer for the NightWatchman Management Center (NMC) includes a number of components:

- AgilityFramework Reporting Console
- AgilityFramework Web service
- AgilityFramework database schema for SQL Server
- NightWatchman Console
- NightWatchman service

1.3.1.2 "1E WakeUp" installer

The "1E WakeUp" installer includes the following components:

- 1E WakeUp for Microsoft Configuration Manager or Microsoft Systems Management Server
- 1E WakeUp for NightWatchman Management Center
- Intel AMT add-on for 1E WakeUp
- WakeUp console[3]

1.3.2 1E NightWatchman®

The NightWatchman agent powers down all unattended PCs automatically and remotely at the end of the day – saving significant amounts of energy and costs. During the day PCs are powered down after a set period of inactivity. NightWatchman also shuts down PCs following software updating and scheduled maintenance windows.

[3] Once 1E WakeUp is installed to be integrated with NMC, the NMC provides the management functions for WakeUp. These functions are integrated in the NightWatchman Console.

1.3.3 1E WakeUp™ Agent

1E WakeUp remotely powers up PCs that are asleep or shut down for successful deployment of software out of office hours. By allowing patches to be installed at any time, not just when the user next boots up their computer, 1E WakeUp closes the window of opportunity for security vulnerabilities.

1E WakeUP uses Magic Packet broadcast frames to wake-up workstations using Wake-on LAN (WOL) implemented on the workstation's motherboard.

1.3.4 Configuration

The NightWatchman Management Center components can either be installed on a single platform or across multiple platforms in accordance with the installation guidance [1]. The NMC can be integrated with one or more WakeUp Servers as follows.

1. Dedicated Agent mode – a machine on each remote subnet is identified as a 1E WakeUp Agent and the 1E WakeUp Server communicates only with this Agent. This mode means that the dedicated agent machine must remain on at all times in order to be able to process Server communications. For extra resilience, an alternate agent may also be specified if required.

2. Multi-Agent mode - If the network does not allow support for directed broadcasts and dedicated workstations are not required to be permanently on, 1E WakeUp can be used in Multi-Agent mode. The 1E WakeUp Agent should be installed on all workstations in the environment. This mode avoids the overhead of having to support a Dedicated Agent and is ideal if there are many remote subnets.

The WakeUp Server can use a machine on a remote subnet that is identified as the Dedicated WakeUp Agent (or Main Agent). In this instance the Server communicates only with the Main Agent, as shown in Figure 0-1 and the Main Agent broadcasts the Magic Packets on the subnet as directed by the WakeUp Server.

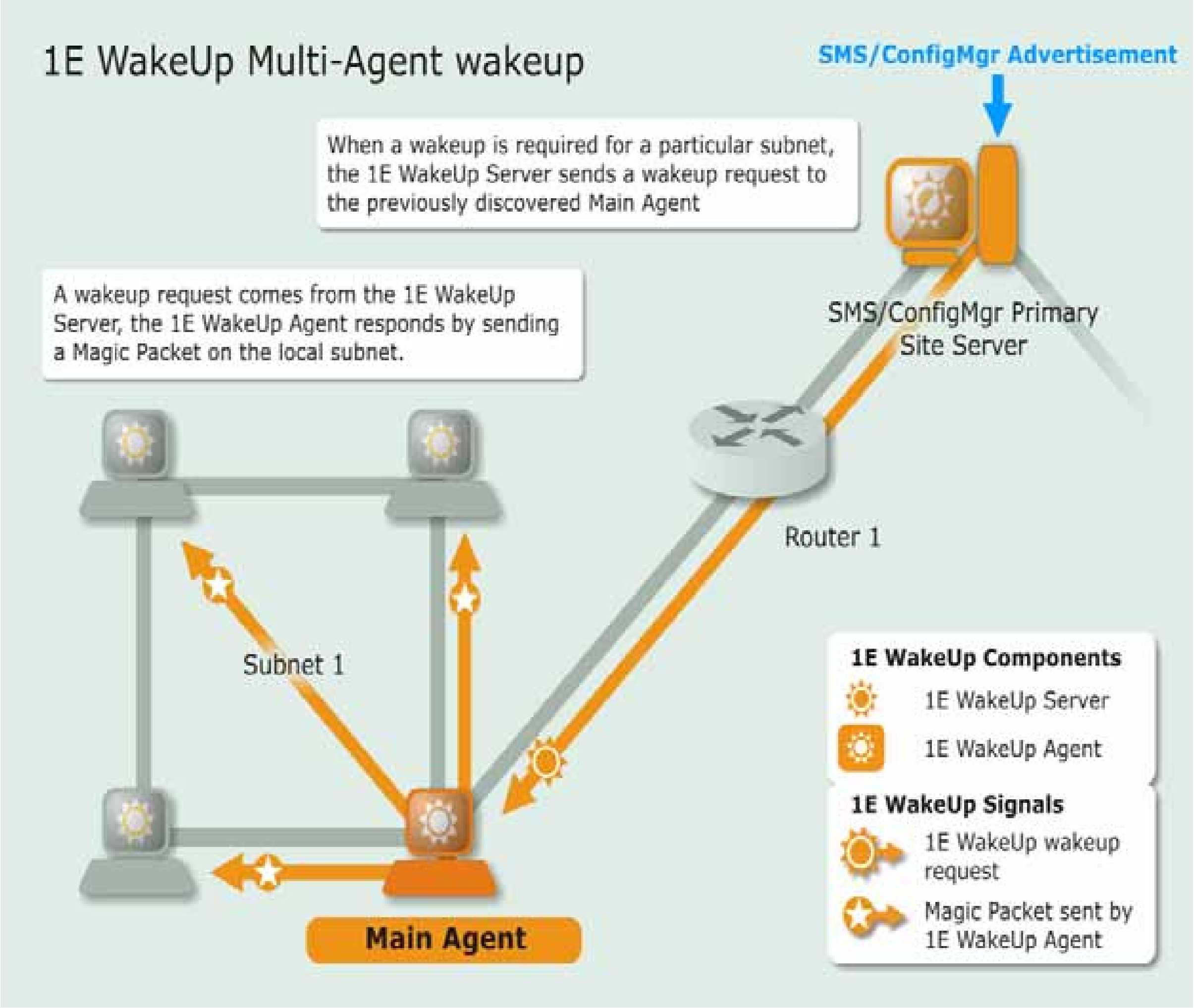
1E WakeUp Multi-Agent wakeup
SMS/ConfigMgr Advertisement
When a wakeup is required for a particular subnet, the 1E WakeUp Server sends a wakeup request to the previously discovered Main Agent
A wakeup request comes from the 1E WakeUp Server, the 1E WakeUp Agent responds by sending a Magic Packet on the local subnet.
SMS/ConfigMgr Primary Site Server
Router 1
Subnet 1
Main Agent
1E WakeUp Components
1E WakeUp Server
1E WakeUp Agent
1E WakeUp Signals
1E WakeUp wakeup request
Magic Packet sent by 1E WakeUp Agent

Figure 0-1 A network with dedicated 1E WakeUp Agents

In a configuration with multiple SMS/ConfigMgr Servers, a WakeUp Server should be installed onto each SMS/ConfigMgr Site server. In this scenario a list of sub-sites will be created from the SMS/ConfigMgr database. The only workstations that will be awakened by a WakeUp Server are those that are either local to the site or clients of non-primary sub-sites. The WakeUp Server will send the wake-up list to the local or distributed WakeUp Agents. The WakeUp Agent will then send out wakeup packets to all targeted systems, as shown in Figure 0-2.

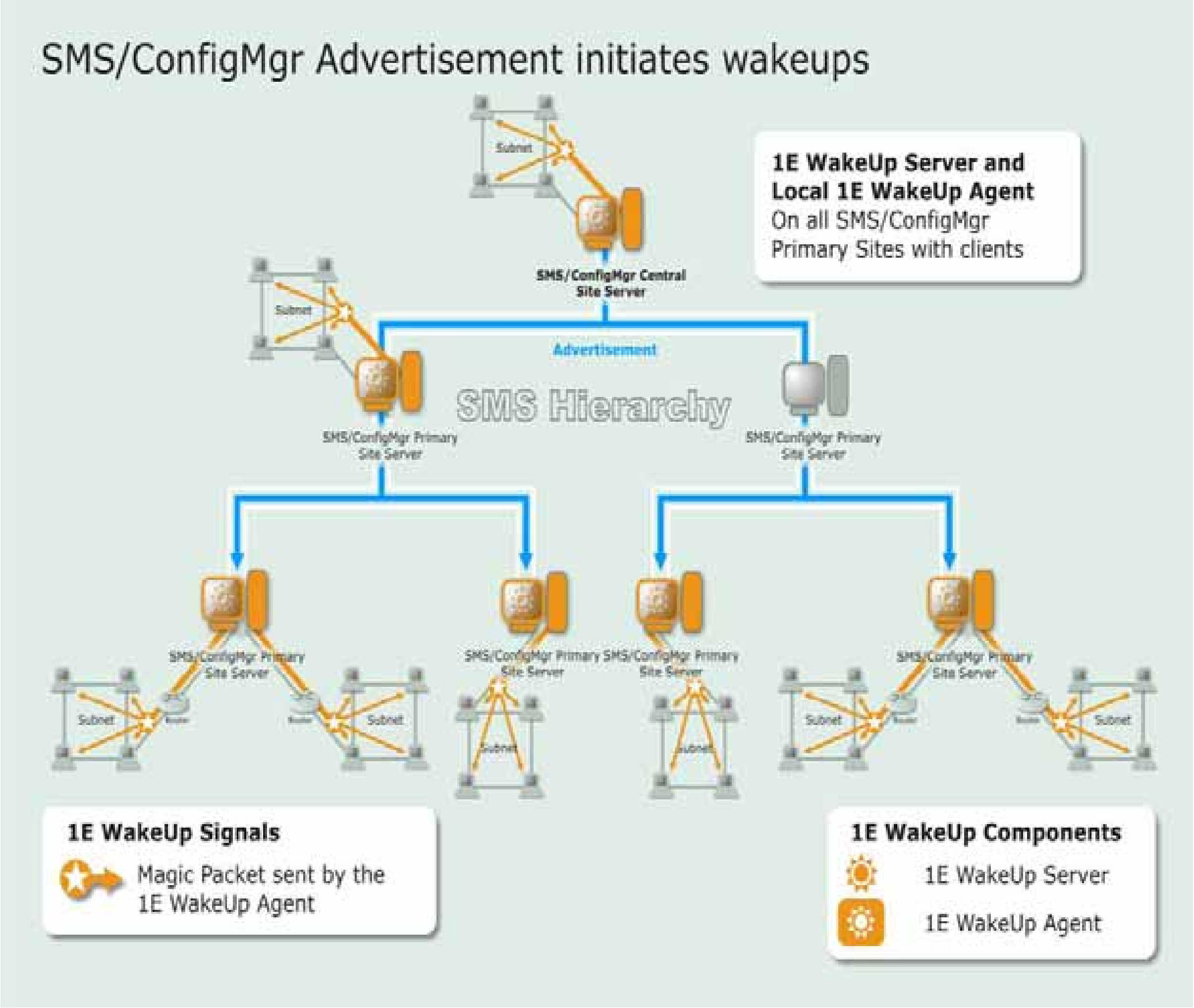
SMS/ConfigMgr Advertisement initiates wakeups
Subnet
1E WakeUp Server and Local 1E WakeUp Agent
On all SMS/ConfigMgr Primary Sites with clients
SMS/ConfigMgr Central Site Server
Advertisement
SMS Hierarchy
SMS/ConfigMgr Primary Site Server
SMS/ConfigMgr Primary Site Server
SMS/ConfigMgr Primary Site Server
SMS/ConfigMgr Primary Site Server
SMS/ConfigMgr Primary Site Server
SMS/ConfigMgr Primary Site Server
Router
Subnet
1E WakeUp Signals
Magic Packet sent by the 1E WakeUp Agent
1E WakeUp Components
1E WakeUp Server
1E WakeUp Agent

Figure 0-2 SMS/ConfigMgr Advertisement prompts 1E WakeUp to wake workstations

1.4 TOE Boundaries

1.4.1 Physical Boundary

The physical boundary of the TOE encompasses the platforms running the NightWatchman Management Centre including the NightWatchman Console application, 1E WakeUp including the WakeUp Console application, the NightWatchman agents and the WakeUp Agents.

1.4.2 Logical Boundary

The 1E Power and Patch Management Pack is comprised of the following items:

- 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

These provide the following key features:

- Power policy management and distribution
- Wake-up mechanism
- Controlled shutdown (including saving of user data)

1.4.3 Summary of items out of scope of the TOE

The items out of scope of the TOE are the following Microsoft components with which 1E Power and Patch Management Pack integrates:

- Microsoft Windows XP and Server
- Microsoft SQL Server
- Microsoft IIS
- Microsoft SMS
- Microsoft SMS/ConfigMgr

CC Conformance

As defined by the references [CC1], [CC2] and [CC3], this TOE conforms to the requirements of Common Criteria v3.1, Revision 1 for Part 1 and Revision 2 for Parts 2 and 3. The methodology applied for the evaluation is defined in [CEM].

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of EAL2.

This ST does not claim conformance to any PPs.

Security Problem Definition

1.5 Assets

The assets to be protected by the TOE are as follows:

- Currency and integrity of workstation configuration

  The currency and integrity of the workstation configuration increases the workstation's resilience against attack.

  "Currency" of the workstation configuration is defined for these purposes as the application of all advertised patches and updates for the workstation, and integrity of workstation configuration is defined for these purposes as one that reports no issues when the SMS/ConfigMgr health check defined by the Health Policy is run.

- Availability of workstation

  To maximise productivity the workstation should be powered on and ready to use at specified times of the day, reflecting the user's working pattern.

- Confidentiality of user data

  User data stored is stored on the workstation and access to this data is controlled through the workstation operating system (Windows) file sharing access control lists. Specifically, all data relating to and owned by a user should be stored under the path C:\Documents and Settings\<username>.

- Integrity of WakeUp and Health policies and workstation reporting statistics

  Policies are downloaded to the workstation in encrypted form and are decrypted and applied to the workstation registry under Local Machine. The workstation generates and stored reporting statistics from the execution of the policies on the workstation.

1.6 Users and Subjects

The following define the users and IT systems. The subjects are interpreted as those processes representing the defined users and external systems.

1.6.1 Human users

NWM User	The NWM user authenticates to the NWM workstation to access data and resources.
NWC Administrator	The NWC administrator manages the power and patch management policies for the workstations within the enterprise network.

1.6.2 IT Systems

SMS/ConfigMgr — The SMS/ConfigMgr performs health checks of workstations, provides updates and collections of fixes for workstations.

1.7 Threats

The following items detail threats in an enterprise network which the TOE is intended to address:

T.Ws_Unpatched **Exploit workstation weakness**

An attacker may exploit weaknesses in un-patched workstations.

T.Ext_Wake **Wake message from outside enterprise network**

An attacker may attempt to wake up a workstation from outside the enterprise network.

T.Ws_Svr_Spoof **Spoof server and client components and client data**

An attacker may attempt to replace server and client components and/or client data on a user's workstations.

T.Ws_Corrupt **User data corruption during power down**

There is user data loss and corruption due to non-graceful power down events.

The following threat is introduced because the TOE needs to report data and there is a danger that the wrong data could be provided:

T.Ws_Dataleak **Data leak from workstation**

User data is downloaded from the workstation in place of workstation reporting statistics.

1.8 Organizational Security Policies

OSP.Ws_Power **Workstation power policy**

All workstations should be powered off and put into low power modes when not in use, but are powered on in preparation for the standard working day and to perform maintenance, in accordance with the enterprise power policy.

1.9 Assumptions

1.9.1 Physical Assumptions

A.Svr_Physical **Physical protection of servers**

It is assumed that TOE servers are installed in a physically secure location that can only be accessed by authorised users.

1.9.2 Personnel Assumptions

None.

1.9.3 Connectivity Assumptions

A.Connectivity **Protect workstation/server connectivity**

Connectivity between the workstations and the NightWatchman servers will be protected from interception, eavesdropping and modification.

A.Fw_Block_Magic **Block magic packets from external network**

Magic packets originating from outside the enterprise network boundary will be blocked and will not be routed within the enterprise network.

A.Ws_Conn **Workstation connected to receive updates**

The workstation on which the TOE is installed is connected to the network to allow updates to be received.

1.9.4 IT Environment Assumptions

A.Ext_Manage **Maintain HW inventory**

A configuration management solution will be implemented to maintain a hardware inventory for all workstations and to provide a means for software distribution. This will define schedules for software update on individual workstations or collections.

A.User_Auth **Users authenticated by operating system**

All users will be authenticated by the underlying platform, which will pass the user ID to the TOE.

A.Ws_Access_Permissions **User access permissions reflect authorisation**

Users on the client workstations have access permissions appropriate to their level of authorisation.

Application Note: For example, a non-administrative user would have restricted user capability, only able to access their own folder under \Documents and Settings and unable to access files in \Program Files (controlled by Microsoft Windows). Also, a non-administrative user should not have access to facilities to edit the workstation registry, where workstation settings are stored, including power and health policies.

A.Reliable_Time **Reliable time source**

A time source provides reliable time input.

Security Objectives

1.10 Security Objectives for the TOE

O.Svr_Pwr_On **Scheduled workstation wakeup**

The TOE server will initiate a power-on event on a registered workstation in accordance with the defined power policy or on demand.

The TOE Objective O.Svr_Pwr_ON .helps to achieve the OSP OSP.Ws_Power by ensuring that the workstations can be powered on for scheduled maintenance activities, at the start of the working day and as required by the TOE users/administrators.

O.Ws_Pwr_Off **Scheduled workstation shutdown**

The TOE client will initiate a power-off event on a registered workstation in accordance with the defined power policy or on demand.

The TOE Objective O.Ws_Pwr_Off .helps to achieve OSP.Ws_Power by ensuring that the workstations can be powered off during a period of inactivity, when scheduled maintenance has been completed, at the end of the working day and as required by the TOE users/administrators.

O.Ws_Save_Data **Save user data on shutdown**

When powering-off a workstation the TOE client will ensure all defined user data is saved to prevent data loss.

The TOE Objective O.Ws_Save_Data helps to address the threat T.Ws_Corrupt by ensuring that the defined user data is saved prior to workstation power-off and this TOE Objective helps to achieve the OSP OSP.Ws_Power without resulting in user data loss when the workstation is powered off.

O.Ws_New_Pol **Update workstation policy**

The TOE client will check and download newer policies from the NMC database at period intervals, as specified by the client's active policy.

The TOE Objective O.Ws_New_Pol helps to achieve the OSP OSP.Ws_Power by ensuring the correct power policies are applied on the workstations. This objective also helps to address the threat T.Ws_Unpatched by ensuring the correct health policy is applied to the workstation so the TOE client on the workstation will know when to request the patch updates.

O.Ws_Extract **Workstation only provide reporting data**

The TOE client will only send reporting information to the server; no user data can be extracted from the workstation.

The TOE Objective O.Ws_Extract addresses the threat T.Ws_Dataleak by ensuring that only statistics relating to the power and health status of the machine are uploaded to the server and that no user data is uploaded from the workstation to the server.

O.Ws_Restore_Data **Restore user data on wakeup**

The TOE client will make available all user data that was saved on a workstation when the user next logs into that workstation.

The TOE Objective O.Ws_Restore_Data supports the OSP OSP.Ws_Power by ensuring the user is able to retrieve data that was saved during a power off event when the user was previously logged into the workstation.

O.Ws_Patch_Updates **Workstation prompt for software updates**

The TOE client will prompt the workstation to check for software updates from the SMS/ConfigMgr in accordance with the SMS/ConfigMgr policy.

The TOE Objective O.Ws_Patch_Updates addresses the threat T.Ws_Unpatched by ensuring the TOE client prompts the workstation to request the necessary patch information from the configuration management solution.

O.Ws_Valid_Fix **Verify integrity of fixes**

The TOE client will verify the integrity of all TOE software prior to execution and all TOE data upon receipt.

The TOE Objective O.Ws_Valid_Fix addresses the threat T.Ws_Svr_Spoof by ensuring the TOE client verifies the integrity of TOE workstation software before executing it and ensuring the TOE client verifies the integrity of all TOE policy updates received.

O.Policy_Integrity **Verify policy integrity**

The TOE client will provide the capability to verify the integrity of power and health policies received.

The TOE Objective O.Policy_Integrity helps to addresses the threat T.Ws_Unpatched by providing the capability to verify the integrity of received power and health policies ensuring the policy has not altered during transmission. This objective also supports the OSP OSP.Ws_Power by allowing the integrity of the policy applied at the workstation to be verified.

1.11 Security Objectives for the Environment

1.11.1 Security Objectives for the Technical Environment

The following technical objectives relate to the workstation components of the TOE:

OE.Auth_Users **Authenticate administrators and users**

The operational environment will provide the Microsoft Active Directory solution to identify and authenticate all users[4] on workstations and provide the user identity to the TOE.

The environment objective OE.Auth_Users meets the assumption A.User_Auth by ensuring Active Directory is used to authenticate all users and user identities will be provided to the TOE.

OE.Ws_Access **User workstation access control**

The operational environment will provide the Microsoft Windows XP/Vista access control mechanisms to restrict user access to data and program files on a workstation according to the user id.

The environment objective OE.Ws_Access meets the assumption A.Ws_Access_Permissions by ensuring users' access on the workstation will be restricted according to their user identity (as passed to the TOE from Active Directory) so provided the permissions are correctly set the user will only be able to access files in their own folder under \Documents and Settings and they will not be able to access the files in the \Program Files folder.

The following technical objectives relate to the server components of the TOE:

OE.Update_Tool **Software update tool**

The operational environment will provide the Microsoft SMS/ConfigMgr change and configuration management solution to support hardware inventory, software inventory and software distribution.

The environment objective OE.Update_Tool helps address the threat T.Ws_Unpatched and also meets the assumption A.Ext_Manage by maintaining details of the hardware and software status of each workstation and making software updates (including patches) available for download to the workstation.

The following technical objectives relate to connectivity between components of the TOE:

OE.Comms_Protection **Protection of server/workstation communication**

The operational environment shall provide protection for all communication between the workstations (including administration consoles) and the server portions of the TOE against eavesdropping, hijacking and replay.

The environment objective OE.Comm_Protection meets the assumption A.Connectivity by ensuring that all communication between the workstations and servers is protected.

OE.Boundary_Enforcement **Enforcement of network boundary**

[4] This is to include administrators as well as non-administrative users.

The operational environment shall ensure any Magic Packets originating from outside the enterprise network boundary are blocked by network router/firewall boundary devices and prevented from being routed within the enterprise network.

The environment objective OE.Boundary_Enforcement addresses the threat T.Ext_Wake and also meets the assumption A.Fw_Block_Magic by ensuring that all Magic Packets originating from outside the enterprise boundary are prevented from entering and being routed within the enterprise network.

OE.Ws_Network_Connection **Workstations connected to network for updates**

The operational environment shall ensure workstations on which the TOE is installed are connected to the network to allow the receipt of update advertisements and the download of updates to the workstation.

The environment objective OE.Ws_Network_Connection addresses the helps to address the threat T.Ws_Unpatched by ensure the workstation is available to receive updates and patches.

OE.Reliable_Time **Provision of reliable time**

The operational environment shall provide a reliable time source.

The environment objective OE.Reliable_Time meets the assumption A.Reliable_Time by ensuring a reliable time source is provided.

1.11.2 Security Objectives for the Procedural Environment

OE.Svr_Physical_Access **Control of physical access to servers**

The operational environment shall provide physical protection to the TOE servers to ensure only authorised users (administrators) are able to gain physical access the servers.

The environment objective OE.Svr_Physical_Access meets the assumption A.Svr_Physical by ensuring only administrators are able to gain physical access to the TOE servers.

1.12 Summary of SPD/Objectives Rationale

The following table provides a summary of the relationship between the security objectives and the security problem definition.

Superscript is used in the rationale where a threat/OSP/assumption maps to objectives for both TOE and environment to identify whether the rationale statement relates to TOE or environment objectives.

Threat/OSP/Assumption	Objectives	Rationale
T.Ws_UnPatched	O.Ws_New_Pol, O.WS_Patch_Updates, O.Policy_Integrity,	This threat is countered by the combination of TOE and

Threat/OSP/Assumption	Objectives	Rationale
	OE.Update_Tool	environment objectives to: • ensure the TOE client downloads any newer policy from the NMC database$^{\text{TOE}}$ and provide the capability to ensure the policy is received unaltered$^{\text{TOE}}$. • ensure the workstation requests all software updates when applicable$^{\text{TOE}}$ • ensure the software updates are made available on the (SMS/ConfigMgr Server)$^{\text{Environment}}$.
T.Ext_Wake	OE.Boundary_Enforcement	This threat is countered by the environment objective to ensure that no Magic Packets to wake workstations are permitted to enter the enterprise network boundary.
T.Ws-Svr_Spoof	O.Ws_Valid_Fix	This threat is countered by the TOE objective to ensure the TOE client verifies the authenticity of TOE workstation software before executing it and ensuring the TOE client verifies the integrity of all TOE policy updates received.
T.Ws_Corrupt	O.Ws_Save_Data	This threat is partially countered by the TOE objective to ensure that during power-off events all defined user data is saved prior to power-off. Corruption and the loss of user data during power-cuts remains.
T.Ws_Dataleak	O.Ws_Extract	This threat is countered by the TOE objective to ensure that

Threat/OSP/Assumption	Objectives	Rationale
		no user data will be uploaded from a workstation to the server when the workstation is sending report information.
OSP.Ws_Power	O.Svr_Pwr_On, O.Ws_Pwr_Off, O.Ws_Save_Data, O.Ws_New_Pol, O.Policy_Integrity	This OSP is addressed by the a combination of the TOE objectives to ensure that workstations are powered-on/off according to the policies (including taking all specified actions during power-off), in accordance with latest correct policies.
A.Svr_Physical	OE.Svr_Physical_Access	This assumption is achieved by the environment objective to ensure the TOE servers are located in a secure area which can only be accessed by administrators.
A.Connectivity	OE.Comms_Protection	This assumption is achieved by the environment objective to ensure all communication with the console is adequately protected.
A.Fw_Block_Magic	OE.Boundary_Enforcement	This assumption is achieved by the environment objective to ensure that all Magic Packets are blocked from entering the enterprise network.
A.Ws_Conn	OE.Ws_Network_Connection	This assumption is achieved by the environment objective to ensure that the workstation is physically connected to the network, together with the objective OE.ROUTE that ensures network packets can then be routed to the connection workstation.
A.Ext_Manage	OE.Update_Tool	This assumption is achieved by the environment objective

Threat/OSP/Assumption	Objectives	Rationale
		to ensure a configuration and change management solution is provide to support hardware & software inventory and software distribution.
A.User_Auth	OE.Auth_Users	This assumption is achieved by the environment objective to ensure Active Directory will identify and authenticate all users and will provide the user identity to the TOE.
A.Ws_Access_Permissions	OE.Ws_Access	This assumption is achieved by the environment objective to ensure the workstation operating system will provide access controls to restrict user access to TOE software (in \Program Files) and data (in \Documents and Settings).
A.Reliable_Time	OE.Reliable_Time	This assumption is achieved by the environment objective to ensure the TOE has a reliable time source.

Extended Security Requirements

This chapter defines components that are not drawn from [CC2] or [CC3].

1.13 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement and underlined text indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [*Italicised text within square brackets*] indicates the completion of a selection.

An identifier has been added as a suffix to each [CC2] component and element identifier (e.g. FMT_SMR.1/SVR, FMT_SMR.1.1/SVR) to indicate the related groups of requirements representing security functionality:

SVR:	server
WS:	workstation
POL:	policy
REP:	reporting
WU:	WakeUp

1.14 Extended Security Requirement

There are two security requirements defined for this TOE for which extended components are required as no applicable requirement is provided in [CC2] and [CC3].

1.14.1 Availability of TOE Client

A security requirement is necessary to express the capability of the TOE server to wake up the TOE client to ensure that the TOE client is available to receive any necessary updates and is available for use at the start of the working day. The component FPT_ICP.1 is an extension of the component FPT_ITA.1 Availability of exported data from the class Protection of the TSF, as it relates to the prevention of loss of availability of TSF components (i.e. the workstation running the TSF client).

FPT_ICP.1 Availability of inter-TSF capabilities

Hierarchical to:	No other components.
Dependencies:	No dependencies

FPT_ICP.1.1 The TSF shall ensure the availability of [assignment: list of TSF capabilities].

The major feature of the TOE server is to ensure that the workstation is available to receive advertised updates at the earliest opportunity (as described in Section 1.26).

FPT_ICP.1/WS Availability of inter-TSF capabilities

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ICP.1.1/WS The TSF shall ensure the availability of [**workstation to receive an update from the NMC**]. O.Svr_Pwr_On

1.14.2 Operation of the TSF (workstation related requirements)

A security requirement is necessary to express the 5 actions performed by the TOE that represent the major features of the TOE workstation components, namely saving defined user data during shutdown, restoring saved user data during start-up, entering the correct power mode and running the health policy. In a manner similar to the [CC2] self-test FPT_TST.1.1 element, these operations are to be performed during initial start-up, normal operation or at the request of the user. The FPT_TST.1 component, which specifies the testing of the critical functions of the TSF's operation, has been used as the basis to express the critical functions of the TSF's operation in FPT_TOP.1. In addition the requirements for detection of corrupted TSF executable code are taken from the [CC2] FPT_TST.1.2 and FPT_TST.1.3 elements, with the addition of a selection operation to identify which user roles will have the capability to verify the integrity of the TSF executable code and an assignment operation to list the applicable items of TSF executable code.

FPT_TOP.1 TSF Operations

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TOP.1.1 [Selection: *During initial start-up, Periodically during normal operation, At the request of the authorised user, At the conditions [assignment: conditions under which self test should occur]*] the TSF shall [assignment: *operation to be performed*].

FPT_TOP.1.2 The TSF shall provide [*assignment: the authorised identified roles*] the capability to verify the integrity of [*assignment: list of TSF executable code*].

There are 5 actions performed by the TOE that represent the major features of the TOE workstation components; namely checking for and saving all defined user data (e) as described in Section 1.20, providing a list of all saved user data to the user (only displaying data owned by that user) when the user next logs in (a) and upon request of the user during operation (d) as described in Section 1.21, perform frequent, periodic checks to ensure power policies are applied to the workstation as applicable (b) as described in Section 1.20 and perform frequent, periodic checks to ensure health policies are applied to the workstation as applicable (c) as described in Section 1.25.

FPT_TOP.1/WS TSF Operations

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TOP.1.1a/WS [[*During initial start-up*] the NWM client portion of the TSF shall [**determine whether any data was stored on the workstation for the NWM user during a power down operation since the user last logged on to the workstation**]; O.WS_Restore_Data

FPT_TOP.1.1b/WS [*Periodically during normal operation*] the NWM client portion of the TSF shall [**determine whether the workstation should go into a hibernate, low-power or shutdown state**]; O.Ws_Pwr_Off

FPT_TOP.1.1c/WS [*Periodically during normal operation*] the NWM client portion of the TSF shall [**run the health policy to determine the health of the workstation**]; O.Ws_Patch_Updates

FPT_TOP.1.1d/WS [*At the request of* [**the NWM user**]] the NWM client portion of the TSF shall [**check for and display the list of user files saved during a shutdown operation**]; O.Ws_Restore_Data

FPT_TOP.1.1e/WS [*At the conditions* [***power-off***] the NWM client portion of the TSF shall [**check for and save any unsaved data before a shutdown operation**]; O.Ws-Pwr_Off, O.Ws_Save_Data

The integrity of the fixes downloaded from the server is determined by verifying the digital signature of each fix downloaded to the workstation before it is applied (as described in 1.28).

FPT_TOP.1.2/WS The TSF shall provide [**all users**] the capability to verify the integrity of [fixes downloaded to the workstation]. O.Ws_Valid_Fix

IT Security Requirements

1.15 Conventions

The same conventions as those defined in section 1.13 are used to denote where the author intends an assignment or selection operation to be completed by the extended component.

1.16 Security Functional Requirements

1.16.1 FMT Management (Server related requirements)

There are two types of user of the TOE, namely –

1. Administrators accessing the NightWatchman and WakeUp servers through the NightWatchman Console (as described in 1.29)

2. Workstation users accessing the system tray icon (as described in 1.21).

FMT_SMR.1/SVR Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/SVR The TSF shall maintain the roles [NWC Administrator, NWM User].

FMT_SMR.1.2/SVR The TSF shall be able to associate users with roles according to the user identity provided by the domain controller. (OE.Auth_Users)

FMT _SMR.1 has a dependency on FIA_UID.1 to provide identification of users. The identification (and authentication) of users is provided by the (technical) operational environment, as reflected in OE.Auth_Users. Therefore, inclusion of this component is unnecessary, as the user identity is provided to the TOE as the Security Identifier assigned by Windows.

FMT_SMF.1/SVR Specification of Management Functions

The following specifies the administration features for both NightWatchman and 1E WakeUp during operation of the TOE (as described in 1.29). There are a number of features that are configured during the installation process, such as the mode in which the WakeUp Server and Agents are to be installed, in terms of dedicated agent mode, multi agent mode or standalone server mode. The features to be set during installation are described in [2].

Hierarchical to: No other components.

Dependencies: No dependencies

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

- **Scheduling shutdown events**
- **Defining the actions taken to log-off a user**

- **Creating or modifying any shutdown scripts needed in addition to the base set**
- **Setting the actions taken to power-off the machine**
- **Enabling sleepless client detection and advanced sleepless client detection, configuring the sleepless exclusion list**
- **Defining maintenance windows**
- **On-demand WakeUp of a workstation**
- **Scheduling WakeUp events**
- **Monitor Power Consumption and Health Reports**

]. O.Ws_Pwr_Off, O.Svr_Pwr_On, O.Ws_Patch-updates, O.Ws_Restore_Data

FMT_MTD.1/SVR Management of TSF data

Only administrators are able to access the data associated with the management functions specified in FMT_SMF.1/SVR above (as described in 1.29). Users are unable to access (query, modify, deleted, etc) TOE configuration data.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/SVR The TSF shall restrict the ability to [*change_default, query, modify, delete, clear,* ***[create]***] the [**shutdown policies, shutdown scripts, sleepless client detection policies and the sleepless exclusion list, maintenance windows policies, WakeUp policies, WakeUp Server settings, Agent Services settings, Computer Health Collections**] to [**NWC administrators**]. O.Ws_Pwr_Off, O.Svr_Pwr_On, O.Ws_Patch_Updates, O.Ws_Restore_Data

FMT_SMF.1/WS Specification of Management Functions

Local management functions, available to the workstation user, permit the user to defer shutdown instigated by application of a power management policy, to initiate shutdown of the workstation through the TOE to ensure unsaved, defined data is saved up before power-off and to view a list of all files saved during power-off (as described in 1.29).

Hierarchical to: No other components.

Dependencies: No dependencies

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

- **Defer shutdown for up to 24 hours** O.Ws_Pwr_Off
- **Initiate a local shutdown** O.Ws_Pwr_Off

- **View the list of files saved during shutdown** O.Ws_Restore_Data

].

1.16.2 FDP User data

When a workstation is restarted, access to data saved during scheduled shutdown is granted on the basis of the user's security identifier (SID). When a user logs in, only those documents with ownership of the user's SID[5] are detailed on the list of saved documents displayed to the user (as described in 1.21).

FDP_ACC.1/WS	**Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/WS The TSF shall enforce the [**userdata_save_policy**] on [**NWM User access to user saved data**]. O.Ws_Restore_Data

FDP_ACF.1/WS	**Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/WS The TSF shall enforce the [**userdata_save_policy**] to objects based on the following: [**workstation, id of the NWM user, id of the owner of the user saved data**]. O.Ws_Restore_Data

FDP_ACF.1.2/WS The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**access will only be permitted to data saved on the workstation during a scheduled shutdown of that workstation if the user id[6] of the NWM user matches the user id of the owner of the user saved data**]. O.Ws_Restore_Data

FDP_ACF.1.3/WS The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/WS The TSF shall explicitly deny access of subjects to objects based on the [**none**].

[5] The user id used is the Security Identifier assigned by Windows at creation of a user account.

[6] The user id used is the Security Identifier assigned by Windows at creation of a user account.

FDP_ACF.1 has a dependency on FMT_MSA.3 for specification of static attribute initialisation. The Part 2 component FMT_MSA.3 is unnecessary for this instantiation of FDP_ACF.1 as the security attribute in this instance is the SID which is inherited from the underlying operating system and is not controlled by the TOE.

1.16.3 FDP Information flow –WakeUp call

The TOE Server component is responsible for sending wake-up calls to the workstations using Magic Packets that contain the workstation's MAC address (as described in Section 1.26). The TOE Server is to send the wake-up call to the workstation at the time specified in the power management policy and when the administrator selects the option of the Wake-Up console to wake-up a single workstation or collection of workstations. If there is an alarm configured to wake a workstation and the workstation is in hibernate/standby mode the client will configure a BIOS event to wake the workstation, as described in Section 1.22.

FDP_IFC.1/WU Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/WU The TSF shall enforce the [**Wake_Up_policy**] on [**sending of wake-up messages to NWM registered workstations to power-on the workstation**]. O.Svr_Pwr_On

FDP_IFF.1/WU Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/WU The TSF shall enforce the [**Wake_Up_policy**] based on the following types of subject and information security attributes: [**a Magic packet containing the workstation MAC address will be issued on the subnet containing the workstation to be woken according to the scheduling in the policy associated with the workstation or at the instigation of the administrator**]. O.Svr_Pwr_On

FDP_IFF.1.2/WU The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**the NMC will according to the configuration specified in the NMC either[7] send a directed broadcast to the subnet containing the workstation to be woken or it will send an instruction to the WakeUp Agent on the subnet to broadcast a Magic Packet containing the workstation MAC address on the subnet on which the NWM workstation resides**]. O.Svr_Pwr_On

FDP_IFF.1.3/WU The TSF shall enforce ~~the~~ [**no additional rules**].

[7] Depending on the network topology and whether it supports directed subnet broadcasts.

FDP_IFF.1.4/WU The TSF shall explicitly authorise an information flow based on ~~the following rules~~: [**no additional rules**].

FDP_IFF.1.5/WU The TSF shall explicitly deny an information flow based on ~~the following rules~~: [**no additional rules**].

FDP_IFF.1 has a dependency on FMT_MSA.3 for specification of static attribute initialisation. The Part 2 component FMT_MSA.3 is unnecessary for this instantiation of FDP_IFF.1/WU as the security attributes in this instance are the power management policy settings, which are already considered in FMT_SMF.1.1/SVR.

1.16.4 FDP Information flow – Policy download

The workstation component is responsible for checking whether there are updated policies available for download. The workstation is 'registered' to a server (the workstation stores details of the server to which it is registered) and polls the server at defined intervals[8] reporting the name and version of the policy currently active on the workstation. The server checks whether there is an entry for the policy required by the workstation (to verify the workstation is 'subscribed' to the policy and is requesting the correct policy) and if there is a more recent version of the policy. If the server has a more up to date version of the policy than that reported by the workstation the server will send the policy to the workstation in response to the request. The server encrypts the policies ready for download by the workstation. When the workstation downloads a new policy it decrypts the received policy to verify that the integrity of the policy has been maintained during transfer from the server to the workstation (as described in Sections 1.19 and 1.24).

FDP_UIT.1/POL	**Data exchange integrity**

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path

FDP_UIT.1.1/POL The server TSF shall enforce the [**policy_deployment_policy**] to be able to [*transmit*] user data in a manner protected from [*modification*] errors. O.Policy_Integrity

FDP_UIT.1.2/POL The workstation TSF shall be able to determine on receipt of user data, whether [*modification*] has occurred. O. Policy_Integrity

FDP_ UIT.1 has a dependency on FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path for specification of the method used to protect the user data in transit. The method of protecting communications between client and server components is the subject of the environment objective OE.Comms_Protection. Therefore, the dependency on FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path is not necessary as the appropriate protection of the communication path will be provided in the environment of the TOE.

FDP_IFC.1/POL	**Subset information flow control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

[8] The polling interval is configured in the currently active workstation policy.

FDP_IFC.1.1/POL The TSF shall enforce the [**policy_deployment_policy**] on [**policies sent from NWM server to subscribing NWM workstations**]. O.Ws_New_Pol

FDP_IFF.1/POL Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/POL The TSF shall enforce the [**policy_deployment_policy**] based on the following types of subject and information security attributes: [**NWM workstation subscribing to power and patch management policies**]. O.Ws_New_Pol

FDP_IFF.1.2/POL The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**the NWM workstation subscribes to the policy**]. O.Ws_New_Pol

FDP_IFF.1.3/POL The TSF shall enforce the [**none**].

FDP_IFF.1.4/POL The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5/POL The TSF shall explicitly deny an information flow based on the following rules: [**none**].

FDP_IFF.1 has a dependency on FMT_MSA.3 for specification of static attribute initialisation. The Part 2 component FMT_MSA.3 is an unnecessary for this instantiation of FDP_IFF.1/POL as the security attribute in this instance is the subscription of the workstation to policies which is already considered in FMT_SMF.1.1/SVR.

FDP_IFC.1/REP Subset information flow control

At pre-defined intervals[9] the workstation reports health check results and energy consumption statistics to the (SMS/ConfigMgr) server (as described in Sections 1.23 and 1.27).

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/REP The workstation TSF shall enforce the [**Reporting_policy**] on [**health and energy consumption reports sent from NWM workstations to the NWM server**]. O.Ws_Extract

FDP_IFF.1/REP Simple security attributes

[9] In the case of health check reports, the intervals are defined during installation of the NWM client on the workstation. In the case of energy consumption reports, the intervals are specified in the NWM policy.

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/REP The workstation TSF shall enforce the [**Reporting_policy**] based on the following types of subject and information security attributes: [**NWM workstation will provide health check and energy consumption reports to the NWM server(s) with which it is registered**[10]]. O.Ws_Extract

FDP_IFF.1.2/REP The workstation TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**the NWM workstation is registered with the NWM server**]. O.Ws_Extract

FDP_IFF.1.3/REP The workstation TSF shall enforce the [**none**].

FDP_IFF.1.4/REP The workstation TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5/REP The workstation TSF shall explicitly deny an information flow based on the following rules: [**none**].

FDP_IFF.1 has a dependency on FMT_MSA.3 for specification of static attribute initialisation. The Part 2 component FMT_MSA.3 is unnecessary for this instantiation of FDP_IFF.1/REP as the security attribute in this instance is the registration of the NWM workstation with the NWM Server which is already considered in FMT_SMF.1.1/SVR.

1.17 Security Assurance Requirements

The Security Assurance Requirements for the TOE are those of EAL2, as defined in [CC3, 8.4].

1.18 Summary of Objectives/SFRs Rationale

The following table provides a summary of the relationship between the security objectives and the security functional requirements (including the extended component), as provided in the notes below each objective in section 0 above.

Objective	SFR	Rationale that objective is met by SFR(s)
O.Svr_Pwr_On	FPT_ICP.1/WS FDP_IFC.1/WU & FDP_IFF.1/WU	This objective is met through a combination of the availability (extended) requirement to check if according to the policy the workstation should be powered on, information flow requirements that

[10] The WakeUp Agent running on the workstation has been identified during agent discovery.

Objective	SFR	Rationale that objective is met by SFR(s)
	FMT_SMF.1/SVR FMT_MTD.1/SVR	Magic Packets are broadcast on the subnet(s) to which the workstation(s) are connected and the management requirements to configure the WakeUp policies and issue the WakeUp frames (Magic Packets). If the SMS/ConfigMgr server is integrated then 1E WakeUp needs to be installed on all SMS/ConfigMgr Primary Site Servers with clients and on the central site. The 1E WakeUp scans the SMS/ConfigMgr database for mandatory advertisements. It will then use system inventory information to send out wake-up frames (Magic Packets) in time for the advertisement schedule. 1E WakeUp also contains extensions to the SMS/ConfigMgr Administrator console. These extensions permit the explicit waking up of single workstations or whole collections. (FPT_ICP.1/WS, FDP_IFC.1/WU & FDP_IFF.1/WU) The NightWatchman Console and 1E WakeUp extensions to the SMS/ConfigMgr Administrator console permit the explicit waking up of single workstations or whole collections on the demand of the administrator (FMT_SMF.1_SVR and FMT_MTD.1/SVR).
O.Ws_Pwr_Off	FPT_TOP.1.1b/WS & FPT_TOP.1.1e/WS FMT_SMF.1/SVR FMT_MTD.1/SVR FMT_SMF.1/WS items 1&2	This objective is met by a combination of the TSF operation requirement to check whether the workstation should be shutdown in accordance with a defined policy, save any unsaved data and the management requirements to configure the policies and user management actions that can be taken during power-off. If SMS/ConfigMgr server is configured, this will issue a shutdown command to the workstation in accordance with the policy and save any unsaved data (FPT_TOP.1.1e/WS). Alternatively this could be specified through GPO, in which

Objective	SFR	Rationale that objective is met by SFR(s)
		case the workstation will shut itself down. The administrator configures the schedule for shutdown events, actions to be taken (including saving of unsaved user data on the workstation), scripts to be run, exclusion lists, etc at the NightWatchman console (FMT_SMF.1/SVR, FMT_MTD.1/SVR). In accordance with the power-off policy, the user can defer the power-off for a period of time up to 24 hours and can initiate power-off of the workstation on which they are authenticated using the NightWatchman system tray icon, which will ensure that any unsaved data is saved (FPT_TOP.1.1e/WS and FMT_SMF.1/WS items 1&2) and that the saved data is made available to the NWM user at the next login.
O.Ws_Save_Data	FPT_TOP.1.1b/WS FPT_TOP.1.1e/WS FMT_SMF.1/SVR FMT_MTD.1/SVR	This objective is met by a combination of the TSF operation requirement to determine whether the workstation should be shutdown in accordance with a defined policy (FPT_TOP.1.1b/WS) and the management requirements to configure the policies. The administrator configures the actions to be taken at power-off of a workstation, including saving of unsaved user data on the workstation (FMT_SMF.1/SVR and FMT_MTD.1/SVR). When the workstation is powered-off it applies the actions specified in the policy and, if applicable, will save unsaved user data on the workstation in the user's home directory (FPT_TOP.1.1e/Ws).
O.Ws_New_Pol	FDP_IFC.1/POL FDP_IFF.1/POL	This objective is met by the information flow requirements (FDP_IFC.1/POL & FDP_IFF.1/POL) to send the configured policies to the workstation when the workstation next requests a policy update (within a 150 hr cycle).

Objective	SFR	Rationale that objective is met by SFR(s)
O.Ws_Extract	FDP_IFC.1/REP FDP_IFF.1/REP EAL2 (ADV_ARC.1 & AVA_VAN.2)	This objective is met by a combination of the information flow policies to report the results of a workstation health check and power consumption (FDP_IFC.1/REP, FDP_IFF.1/REP), and the assurance requirements (ADV_ARC.1 and AVA_VAN.2 in EAL2) that determine that when sending health check results to the server (SMS/ConfigMgr) no other data will be sent from the workstation (e.g. user data).
O.Ws_Restore_Data	FPT_TOP.1.1a/WS & FPT_TOP.1.1d/WS FDP_ACC.1/WS & FDP_ACF.1/WS FMT_SMF.1/WS item 3	This objective is met through a combination of TSF operation requirements, the NWM user management requirement and an access control requirement. The TSF operation requirements determine if any data was saved for the user when the workstation was shutdown and displays a list of the files saved to the user when requested by the user (FPT_TOP.1.1a/WS & FPT_TOP.1.1d/WS). The access control requirements for saving user data ensure that the user is able to (only) access saved data associated with their account (FDP_ACC.1/WS & FDP_ACF.1/WS). The NWM user management requirement ensures that the saved data identified by the previous requirements is then presented to the user so that the user can manage its long term storage (FMT_SMF.1/WS item 3).
O.Ws_Patch_Updates	FPT_TOP.1.1c/WS FMT_SMF.1/SVR FMT_MTD.1/SVR	This objective is met by a combination of the TSF operation requirement where Policy Refresh prompts the systems that have just been awoken to immediately check SMS/ConfigMgr for the presence of new advertisements and the management requirements to configure the health check policies for the workstation. If SMS/ConfigMgr server is configured this can issue advertisements of new patches to target workstations, which will then check

Objective	SFR	Rationale that objective is met by SFR(s)
		for new patches to download (FPT_TOP.1.1c/WS). Policy Refresh prompts the systems that have just been awoken to immediately check SMS/ConfigMgr for the presence of new advertisements. This can drastically reduce the time taken for patch implementation, allowing more patches to take place in a given time period; particularly useful when patching large numbers of systems overnight. Workstations which are already on will check for a policy update immediately without regard to the normal polling cycle (FPT_TOP.1.1c/WS). The administrator configures the workstation health check policies through the WakeUp console (FMT_SMF.1/SVR and FMT_MTD.1/SVR). The policy determines what actions the workstation is to take to fix issues (e.g. restart of remote registry service, creation of Admin$ share, repair of WMI repository, restart Windows Update service, run disk cleanup utility).
O.Ws_Valid_Fix	FPT_TOP.1.2/WS	This objective is met by the requirements for the client to verify the integrity fixes downloaded to the workstation (FPT_TOP.1.2).
O.Policy_Integrity	FDP_UIT.1/POL	This objective is met by the requirement for the client to decrypt the received policy to enable the client to determine that integrity has been maintained during transmission and to ensure no modifications are made.
OE.Auth_Users	*(FMT_SMR.1/SVR)*	*The TSF indirectly supports this objective by taking the user identities provided by Active Directory and using them to associate users with administrator roles. If the user is not associated with an administrator role they are by default a TOE user.*

TOE Summary Specification

The following sections describe how the TOE provides the security functional requirements described in section 1.16 above.

1.19 Power Policy Download

The NWM Agent will periodically (between 1 minute and 43,200 minutes, as configured by the NWC administrator) make a request to the NWM Server to see there is a more recent (higher) version of the policy than that applied on the client. In the request to the NWM Server, the NWM Agent will include the name and version of the policy currently applied. If the NWM Server reports a higher version of the policy is available, the NWM Agent will make a request to the NWM Server to download the policy. The NWM Server provides the (encrypted) policy, which the NWM Agent decrypts and applies to its registry.

This maps to the following SFRs:

- FDP_IFC.1/POL
- FDP_IFF.1/POL
- FDP_UIT.1/POL

1.20 Scheduled Shutdown

The NWM Agent constantly polls to check if the configured shutdown time has been reached. When the shutdown time arrives the NWM Agent runs the shutdown scripts, which includes any scripts to save user data in the applications still running, deferring shutdown if any excluded processes are running, overriding any processes that keep the client awake (sleepless client processes), contacting the ConfigMgr Agent to see if there are any scheduled events which require deferment of shutdown and prompting the user of impending shutdown event to allow the user to defer shutdown.

If control of shutdown has been passed from the WakeUp Agent (see Scheduled WakeUp), the NWM Agent will wait for a non-configurable period of time to allow any updates to begin, and then it will attempt the shutdown process, determining whether an update is in progress and checking with ConfigMgr Agent to determine whether there are any scheduled events.

This maps to the following SFRs:

- FMT_SMF.1/WS
- FPT_TOP.1.1b/WS
- FPT_TOP.1.1e/WS

1.21 Saved User Data

When the NWM user logs in to the workstation the NWM Client will display a list of all data saved when the workstation was last shutdown with or without the user first logging out. The NWM user can also obtain the list of files by selecting the NWM icon from the systray. Other options on the systray icon allow the user to shutdown the workstation.

This maps to the following SFRs:

- FPT_TOP.1.1a/WS
- FPT_TOP.1.1d/WS
- FDP_ACC.1/WS
- FDP_ACF.1/WS

1.22 NWM Wake From Hibernate

If an NWM alarm is configured to wake the NWM Agent workstation, a BIOS event will wake the workstation at the specified time if (and only if) the workstation is in standby/hibernate mode.

This maps to the following SFRs:

- FPT_ICP.1.1

1.23 NWM Reporting

On the basis of reaching elapsed time or message limit[11], the NWM Agent will report Power Data to the NWM Server. Other messages reported by the NWM Agent to the NWM Server are hardware inventory (reported every 30days or following a change), maintenance (after each maintenance activity) and sleepless client detection.

This maps to the following SFRs:

- FDP_IFC.1/REP
- FDP_IFF.1/REP

[11] The elapsed time and message limit can be set by the administrator during installation; the default elapsed time is 14400 seconds and the default message limit is 25 messages.

1.24 Health Policy Download

The WakeUp Agent will periodically (from a minimum of 2 hours, as configured by the NWC administrator) make a request to the WakeUp Server to see there is a more recent (higher) version of the policy[12] than that applied on the WakeUp Agent. The WakeUp Agent will send in the request to the WakeUp Server the version of the policy currently applied. If the WakeUp Server reports a higher version of the policy is available, the WakeUp Agent will make a request to the WakeUp Server to download the policy. The WakeUp Server provides the (encrypted) policy, which the client stores on the workstation and decrypts in memory.

This maps to the following SFRs:

- FDP_IFC.1/POL
- FDP_IFF.1/POL
- FDP_UIT.1/POL

1.25 Health Policy Run

At periodic intervals (configured by the NWC administrator) the WakeUp Agent will run the health policy to perform checks on the workstation, e.g. to check if specified services are running. If issues are reported from the health check and a fix is specified the WakeUp Agent will perform the defined fixes, e.g. restart stopped services. The WakeUp Agent will send back a report of the health check results, see Section 1.27, WakeUp Reporting.

This maps to the following SFRs:

- FPT_TOP.1.1c/WS

1.26 Scheduled WakeUp

The Scheduler on the WakeUp Server will identify a list of all workstations to be woken at a configured time (or from the SMS/ConfigMgr[13]). The WakeUp Server will send a message to the applicable Primary Agent(s)[14], which will send a wakeup packet (Magic Packet) to all appropriate agents on it's subnet. The Primary Agent will report (see Section 1.27, WakeUp Reporting) what workstations were woken and which failed. Once the workstation is awake,

[12] There is a single global Health Policy applied to all WakeUp clients performing health checks.

[13] If configured with SMS/ConfigMgr, the WakeUp Server constantly polls the SMS/ConfigMgr for WakeUp events (configured in the plugin for the SMS/ConfigMgr user interface).

[14] In Dedicated configuration this will be a specified machine that is always running or in Multi-Agent configuration this will be send to the reported "last agent standing" on the subnet.

the WakeUp Agent on the workstation passes control to the NWM Agent on the workstation to control the shutdown of the workstation.

If configured with SMS/ConfigMgr, the WakeUp Server can also send a message to the WakeUp Agent to tell the ConfigMgr Agent to check for updates. The WakeUp Server is prompted to send this message by the SMS/ConfigMgr.

This maps to the following SFRs:

- FPT_ICP.1.1/WS
- FDP_IFC.1/WU
- FDP_IFF.1/WU

1.27 WakeUp Reporting

On the basis of reaching elapsed time or message limit[15], the WakeUp Client will report Health Data to the WakeUp Server. Other messages reported by the WakeUp Client to the WakeUp Server are hardware inventory (reported every 30days or following a change) and WakeUp statistics (including timestamp, advert name, subnet and number of clients awake, woken, failed).

This maps to the following SFRs:

- FDP_IFC.1/REP
- FDP_IFF.1/REP

1.28 Force Update

To force a download of an update, the details for the update are sent to WakeUp Server (e.g. from ConfigMgr, or another 3rd party update tool) and WakeUp Server sends the update to the WakeUp Agent on the workstation, which will verify the update has been signed by the WakeUp Server and will pass the update to the update agent (e.g. ConfigMgr Agent) to be applied.

This maps to the following SFRs:

- FPT_TOP.1.2/WS

[15] The elapsed time and message limit can be set by the administrator during installation; the default elapsed time is 14400 seconds and the default message limit is 25 messages.

1.29 Console

The NWM Console (also known as the NMC) is used to manage the NWM components[16], including the following:

- To configure Power policy, including power scheme, sleepless client and excluded processes
- To configure Health policy, including new health policy fixes.

This maps to the following SFRs:

- FMT_SMR.1/SVR
- FMT_SMF.1.1/SVR
- FMT_MTD.1/SVR

1.30 Summary of TSS Mapping to SFRs

The following table summarises the mapping between the TOE Summary Specification and the SFRs.

Security Functional Requirement	TOE Summary Specification
FPT_ICP.1.1/WS	1.22,1.26
FPT_TOP.1.1a/WS	1.21
FPT_TOP.1.1b/WS	1.20
FPT_TOP.1.1c/WS	1.25
FPT_TOP.1.1d/WS	1.21
FPT_TOP.1.1e/WS	1.20
FPT_TOP.1.2/WS	1.28
FMT_SMR.1/SVR	1.29
FMT_SMF.1/SVR	1.29
FMT_MTD.1.1/SVR	1.29
FMT_SMF.1/WS	1.20
FDP_ACC.1/WS	1.21

[16] With the exception of scripts to be applied during shutdown which must be loaded at each applicable workstation.

Security Functional Requirement	TOE Summary Specification
FDP_ACF.1/WS	1.21
FDP_IFC.1/WU	1.26
FDP_IFF.1/WU	1.26
FDP_UIT.1/POL	1.19,1.24
FDP_IFC.1/POL	1.19, 1.24
FDP_IFF.1/POL	1.19, 1.24
FDP_IFC.1/REP	1.23,1.27
FDP_IFF.1/REP	1.23,1.27

End of Document