Wyse Technology Inc.
Wyse Device Manager™
Enterprise Edition
Version 4.7.2
Security Target

Version 1.8

April 18, 2011

Wyse Technology Inc.
3471 N. First Street
San Jose, CA 95134

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Wyse Technology Inc.
3471 N. First Street
San Jose, CA 95134
http://wyse.com/

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Wyse Device Manager™ Enterprise Edition Version 4.7.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
1.0	January 30, 2010 – Initial release
1.1	May 17, 2010 – Addressed EFS-T022-EOR-001-1.0 from stratsec
1.2	June 17, 2010 – Updates for FSP consistency
1.3	July 8, 2010 – Clarified Remote Repository functionality, deleted IP Ranges
1.4	December 7, 2010 – Only HTTP is used for Repositories in the evaluated configuration
1.5	March 16, 2011 – TFTP/PXE not used
1.6	April 10, 2011 – Added HAgent versions
1.7	April 14, 2011 – Limited the HAgent variants included in the TOE
1.8	April 18, 2011 – Addressed EFS-T022-EOR009-1.0

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

CC ..... **Common Criteria**
CM ..... **Configuration Management**
CPU ..... **Central Processing Unit**
DBMS ..... **DataBase Management System**
DDC ..... **Default Device Configuration**
DHCP ..... **Dynamic Host Configuration Protocol**
EAL ..... **Evaluation Assurance Level**
FIPS ..... **Federal Information Processing Standard**
FTP ..... **File Transfer Procotol**
GUI ..... **Graphical User Interface**
HTTP ..... **HyperText Transfer Protocol**
HW ..... **HardWare**
IIS ..... **Internet Information Services**
IP ..... **Internet Protocol**
IT ..... **Information Technology**
LAN ..... **Local Area Network**
MDAC ..... **Microsoft Data Access Components**
MMC ..... **Microsoft Management Console**
OS ..... **Operating System**
RAM ..... **Random Access Memory**
ST ..... **Security Target**
TCP ..... **Transmission Control Protocol**
TFTP ..... **Trivial File Transfer Procotol**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
UDP ..... **User Datagram Protocol**
WAN ..... **Wide Area Network**
WDM ..... **Wyse Device Manager**
WES ..... **Windows Embedded Standard**
WTOS ..... **Wyse Thin Operating System**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Wyse Device Manager™ (WDM) Enterprise Edition Version 4.7.2. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*and all international interpretations through April 30, 2010. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Wyse Technology Inc. Wyse Device Manager™ Enterprise Edition Version 4.7.2 Security Target, Version 1.8, dated April 18, 2011.

1.2 TOE Reference

Wyse Device Manager© Enterprise Edition Version 4.7.2 Build 374 with Hot Fixes HF04072025609 and HF04072036209 and Web Agent (HAgent) versions 5.1.1.31 (WES and XPe) and 4.0.4.2 (Wyse Thin OS)

Note that the Web Agent (referred to as HAgent) is versioned independently for the supported client operating systems.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

1.4 Keywords

Thin client, remote management, software repositories, remote software repositories, policy management, asset management

1.5 TOE Overview

1.5.1 Usage and Major Security Features

Wyse Device Manager (WDM) is an enterprise solution for managing network intelligent devices. It enables IT administrators to organize, upgrade, control, and support thousands of WES, Windows CE, Linux, Wyse Thin OS, or XPe devices across any LAN, WAN, or wireless network. Note that Windows CE and Linux devices are not included in this evaluation.

WDM uses industry standard communication protocols and a component-based architecture to efficiently manage the network devices. It provides a GUI management interface built to operate as a standard snap-in to the Microsoft Management Console (MMC) and capable of managing all of the network devices.

WDM manages software images and configurations for download to thin clients. WDM also maintains a list of network devices and their properties. The images and configurations are available to thin clients based on configuration parameters specified by WDM administrators and the properties of the clients.

WDM supports multiple users with user-based role and permissions, enabling different users to be authorized for different functions. WDM integrates with Active Directory or locally defined users in Windows.

WDM keeps a log of activities performed by users. The log may be queried to generate a report of activities and events. The report may be filtered for a specific user.

WDM features include:

- Device Discovery - You can easily configure WDM (setting up different subnets) to discover devices on the network. Once configured, you can then use WDM to easily find and automatically add the devices to the system. Once they are added to the system, the devices are available for future management.
- Device Management - WDM allows you to view the status of your devices at any point in time. WDM can also be configured to automatically provide you with up-to-date status information on all of your devices.
- Remote Control of Devices - You can shutdown, reboot, or wake-up devices from the remote console without having to visit the end-user desktop.
- Device Organization - WDM is a robust management tool that allows you to organize your devices according to groups that makes the most sense to your organization, regardless of the physical or network location of devices.
- Device Update Scheduling - WDM configurations allow you to schedule software deployment and updates to devices (preventing down-time). You can schedule device updates immediately, at a pre-determined time, or when a device next boots.
- Device Configuration Deployment - You can create different configurations that can be deployed to a device independent of an image.
- Device Configuration Capture - You can easily capture device configurations to prepare for deployment.
- Default Device Configuration - The Default Device Configuration functionality allows you to configure default software and device configurations for a group of devices. This functionality ensures that the device conforms to your configurations from a software and device configuration perspective. If there is any deviation from default configurations, WDM will revert the device back to your specified configurations. This feature automates the recovery of failed devices, the re-purposing of existing devices, and the addition of new devices within an existing infrastructure.
- Distributed Architecture - This feature allows you to place the WDM components on one or more computers located on your network.
- Repository Creation and Administration - WDM allows you to easily build and administer a repository of software, images, and configuration updates for distribution.
- Secure Communication Between a WDM Server, Repository, and a Device - Provides secure communications between client and web server by encrypting traffic to and from the client and server and by issuing certificates. Certificates must be signed by an authority which certifies that the certificate holder is the entity it claims to be. Organizations may choose to be their own certificate authority for internal web server access. Because the cryptographic functionality of the TOE is not yet FIPS 140-2 validated, this functionality is not evaluated.

- Distributed Administration - Provides you with granular control of administrator rights based on user groups or individual users. This functionality is not evaluated.
- Device Shadowing - WDM also provides your help desk with a shadowing capability to diagnose issues within end-user environments from a remote location. This functionality of WDM is not evaluated.

1.5.2 TOE type

Network and Network related Devices and Systems

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE consists of two software components: WDM Enterprise Edition, executing on a Windows Server platform; and Web Agent, executing on thin clients.

WDM executes on a Windows platform dedicated to the WDM function. The minimum hardware and software requirements for this platform are described in the following table.

Table 1 - WDM Platform Hardware and Software Requirements

Item	Requirements
Operating System	Microsoft 2003 Standard or Enterprise Server with R2 SP2
CPU	1GHz Intel or AMD X86
RAM	512 MB
Available Disk Space	500 MB
DBMS	Microsoft SQL Server 2005 (Server or Express Edition) or Microsoft SQL Server Desktop Engine 2005 (MSDE 2005) or Microsoft SQL Server 2008 (Server or Express Edition)
Other Software	Microsoft Data Access Components (MDAC) version 2.8 or above Microsoft Management Console 3.0 Microsoft Internet Information Services (IIS) version 5.0 or above, with WebDAV installed Microsoft Internet Explorer 5.5 or above DHCP Server

Credential validation for WDM GUI users is performed by Windows locally or via Active Directory. Authorized WDM users must be configured within WDM in order to define their role and permissions. The Windows username used to login to the WDM platform is also used as the WDM GUI username.

For large or geographically distributed networks, Remote Repositories may be installed on additional Windows platforms, using the database and repository functionality of WDM to provide faster downloads to the clients. Since the Distributed Architecture functionality of the TOE is not included in the evaluation, Remote Repositories do not include the user interface component of the TOE. The minimum hardware and software requirements for Remote Repositories are the same as for the complete WDM functionality.

The Web Agent is downloaded from WDM to managed clients by defining it as a mandatory application for all the devices. The minimum hardware requirements for any clients that will execute the Web Agent are determined by the operating system executing on the clients. Web Agent is supported for the following operating systems:

- Wyse Thin Operating System (WTOS)
- Windows CE (not included in the evaluation)
- Linux (not included in the evaluation)
- Windows Embedded Standard (WES)
- Windows XP Embedded

WDM includes encryption functionality, but it is not yet FIPS 140-2 validated. Therefore, protection of the communication between WDM and any Remote Repositories, between WDM and the clients, and between WDM and users of the GUI management interface is the responsibility of the operational environment.

1.6 TOE Description

The TOE consists of software executing on dedicated servers (WDM and Remote Repositories) and thin clients (Web Agent).

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

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

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

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

1.6.1 Physical Boundary

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

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

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

The physical boundary includes the following guidance documentation:

1. *Installation Guide Wyse Device Manager™ Release 4.7.2*
2. *Administrators Guide Wyse Device Manager™ Release 4.7.2*
3. *Common Criteria Installation Supplement Wyse Device Manager™ Release 4.7.2*

1.6.2 Logical Boundary

The TOE provides the following security functionality:

1. User Role and Permission Binding – Access to the TOE 's WDM GUI is restricted to Windows users that have been configured for access in the WDM database. When the GUI is invoked, the username is learned from Windows and checked against the authorized GUI users. If the user is authorized, the configured role and permissions are bound to the session. Windows users that are not authorized to use the WDM GUI are not able to access any TOE functions or data.
2. Management – Management of the TOE functions and data is provided by the TOE's WDM GUI. Functions provided by the GUI may be restricted to specific users through configuration of the roles and permissions.
3. Audit – Logs are maintained of configuration actions performed via the WDM GUI as well as security-relevant events. The logs may be reviewed via the GUI.
4. Download – The TOE shall maintain properties for Packages and Devices so that download filename requests from Devices may be responded to with the names of Package files that are appropriate for the Device to download.

1.6.3 TOE Data

The following table describes the TOE data.

Table 2 - TOE Data Descriptions

TOE Data	Description
Audit Log	A log of audit records.
Configurations	Packages containing configuration values to be downloaded to a device. Configurations are tracked for specific operating system types to ensure an appropriate choice is made for each device.
Default Device Configurations (DDC)	Configured default software and device configurations for a group of devices. Each DDC includes: • The applicable client operating system, media size, and OS image • The applicable packages • The reconciliation schedule with the devices • The group the DDC applies to
Device Views	Views of devices defined for configured group types/instances to filter the displayed devices. Device views may be configured as public or private (only available to the user that created them).

TOE Data	Description
Devices	A set of managed clients learned dynamically or manually added by a user. The properties collected for each device include: • General Info (e.g. OS and HW vendor) • Hardware Info (e.g. CPU and RAM) • Network Info (e.g. IP address) • Application Info (e.g. installed apps) • Deployed Package (e.g. package name) • Custom Info (e.g. info configured by WDM GUI users) • Disk Details (if any)
Group Types	A hierarchical definition of device properties used to organize the devices for display. Group Types may be predefined (e.g. Operating Systems) or configured by a user. Devices may belong to multiple group types since they are organized by different device properties. Devices are assigned to groups automatically (based on predefined or configured criteria) or manually.
Images	Packages containing some or all of the BIOS, CMOS, OS and data partition information to be downloaded to a device. Images are tracked for specific operating system types and media sizes to ensure an appropriate choice is made for each device.
Other Packages	Packages containing applications or script commands to be downloaded to a device. They are tracked for specific operating system types (or ALL) to ensure an appropriate choice is made for each device.
Packages	Refers to images, configurations or applications that may be downloaded to devices. All package types may be marked Active or Inactive to specify if they are available for download.
Preferences for Device Manager	Specifies WDM settings related to device management, including: • Web Agent check-in frequency • Whether DDCs are enabled • DDC reconciliation schedule
Preferences for DHCP/TFTP	Specifies WDM settings related to DHCP and TFTP, including: • Whether the servers for the protocols are started • What WDM-related options are supported
Preferences for Logging	Specifies WDM settings related to logging, including: • The minimum level to store in the log • Whether configuration changes to preferences are saved in the log • The maximum number of records in the log • The number of entries in the log to delete when it exceeds the configured maximum number of records • The frequency at which warning messages are displayed to GUI Users when the audit log size is exceeded • What event types should be stored in the log
Preferences for Scheduling	Specifies WDM settings related to DHCP and TFTP, including: • Whether repository synchronization is automatic • Scheduling options for device updates
Preferences for Services	Specifies WDM settings related to services provided, including: • Whether log entries related to services are generated • Whether to use FTP, HTTP or both for repository updates • Network ports to use for services

TOE Data	Description
Remote Repositories	A set of configured repositories, including the following information: • Name • Location (e.g. IP address) • Protocols used for synchronization • Credentials for authentication
Reports	Configured reports displaying the specified information in the GUI when a report is selected.
Scheduled Updates	Configured repository synchronizations or updates for devices. Device updates include: • The packages to be distributed • The set of devices to receive the update • The schedule for the update • The Remote Repository to download from (optional)
Subnets	A set of subnets used by WDM to discover devices via UDP traffic. Subnets ay also specify: • The repository to download packages from • Default groups to assign discovered devices to
User Accounts	A configured list of Windows userids authorized to use the WDM GUI. Each entry also specifies the role and permissions for that user.

1.7 Evaluated Configuration

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

The following configuration parameter settings in WDM must be used:

1. In Service Preferences, “Enable Legacy Agent Service” must not be set since legacy agents are not included in the evaluated configuration.
2. In Service Preferences, “Enable WDM Service Logs” must be set.
3. In Logging Preferences, “Write Preferences changes to system log” must be selected and all the event types must be selected.
4. In Scheduling Preferences, “Enable WDM Service Logs” must be set.
5. In Logging Preferences, all the logging levels are configured for Warnings.
6. HTTP is used for communication with repositories; FTP is not enabled.
7. Merlin is used as the imaging option; WISard is not used since it is dependent on the repositories supporting FTP.
8. In DHCP/TFTP Preferences, TFTP is not enabled. Since PXE operations depend on TFTP, PXE is not supported. All clients must use HTTP to interact with the WDM server.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 3, dated July 2009

Common Criteria conformance: Part 2 conformant and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 - Assumptions

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

3.3 Threats

The threats identified in the following table are addressed by the TOE and/or the Operational Environment.

Table 4 - Threats

Threat	Description
T.AUDIT_ COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNIDENT_ACTIONS	A user may perform unintended actions that compromise the security of the TOE data or resources.

3.4 Organisational Security Policies

The organizational security policies identified in the following table are addressed by the TOE and/or the Operational Environment.

Table 5 - Organizational Security Policies

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

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 6 - Security Objectives for the TOE

O.Type	Security Objective
O.AUDIT_GEN	The TOE will provide the capability to detect and create records of security-relevant events.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information from unauthorized access.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information in a human readable form.
O.DOWNLOAD	The TOE will maintain package and device information and associate appropriate packages with devices for downloads.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the WDM component of the TOE, and restrict these functions and facilities from unauthorized use.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 7 - Security Objectives of the Operational Environment

OE.Type	Operational Environment Security Objective
OE.COMM	The Operational Environment will protect management information between the TOE and remote users from disclosure.
OE.ENVIRON	The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
OE.IandA	The Operational Environment will successfully identify and authenticate users of the WDM system prior to allowing them access to the WDM GUI.
OE.INSTALL	The Administrator will install and configure the TOE according to the administrator guidance.
OE.NETWORK	The Administrator will install and configure a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. The administrator will ensure that this network functions properly.
OE.NOEVILADMIN	Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.
OE.TIME_STAMP	The Operational Environment will provide reliable time stamps for accountability purposes.

5. Extended Components Definition

5.1 Extended Security Functional Components

None

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events specified in the table below*.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional details specified in the table below*.

Table 8 - FAU_GEN.1 Detail

SFR	Event	Audit Record	Additional Details
FAU_GEN.1	The TOE has been started	Rapport Standard Services initialized and ready	None
FMT_MTD.1	Preferences updated	Preferences: *Name* changed from *old_value* to *new_value*	*Name* specifies which preference parameter was changed, *old_value* specifies the previous value, and *new_value* specifies the new value

SFR	Event	Audit Record	Additional Details
	Device manually added	Device Manager – Device manually added	None
	Package created	Package Wizard – Package *Name* registered	*Name* identifies the name configured for the package
	Package modified (status change)	Configuration Manager – Package status changed to *Status*	*Status* is Active or Inactive
	Configuration updated	Configuration Manager – *Type Name Operation*	*Type* specifies Group Type, Subnet, View definition, User, or Software Repository; *Name* identifies the name configured for the object, and *Operation* specifies Created, Updated, or Deleted
	Scheduled Update completed	Script success to *MACAddress*	*MACAddress* is the MAC address of the Device that received the update. The audit record also includes the Device name, IP address, and Package name sent to the Device.

Application Note: The audit function is executing whenever the TOE is executing according to the evaluated configuration. Therefore there is no audit event corresponding to shutdown of the audit functions.

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *GUI Users with the "Create and Review Reports" permission* with the capability to read *all audit information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply *filtering* of audit data based on *the userid of the GUI User that caused a record to be generated and/or the time a record was generated*.

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

6.1.1.7 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall *display a warning message to GUI Users and permit authorized GUI Users to archive records from the audit log* if the audit trail exceeds *the configured maximum number of records for the audit log*.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. *Administrators and Users:*
    a. *userid*
    b. *role (Administrator or User)*
    c. *permissions from the following list:*
        i. *Archive Log*
        ii. *Create and View Reports*
        iii. *Create/Modify Device Groups*
        iv. *Create/Modify Device Info*
        v. *Create/Modify Subnets*
        vi. *Create/Modify Updates*
        vii. *Create/Modify Views*
        viii. *Delete Devices*
        ix. *Delete Package*
        x. *Distribute Packages*
        xi. *Manually Add Devices*
        xii. *Modify Package*
        xiii. *Register Package*
2. *Devices:*
    a. *IP Address*
    b. *Role (Device).*

6.1.2.2 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

1. *Administrators and Users:*

a. *userid*

b. *role*

c. *permissions*

2. *Devices:*

a. *IP Address*

b. *role.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1. *The userid is associated with an Administrator or User session from the authenticated Windows username when the GUI is invoked.*
2. *The role and permissions are associated with an Administrator or User session from the corresponding user account when the GUI is invoked. If no corresponding user account exists no role or permissions are bound to the session.*
3. *The IP Address is associated with a Device from the source IP address when an incoming IP datagram is received.*
4. *The Device role is automatically associated with all Devices upon receipt of an IP datagram.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *the security attributes do not change during a session.*

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to modify, *create and download* the *data specified in the following table* to *Devices as specified in the following table.*

Table 9 - FMT_MTD.1 Detail for Devices

TSF Data	Access
Audit Log	None
Configurations	Download
Default Device Configurations (DDC)	None
Device Views	None
Devices	Create for its own IP Address if the IP Address is within a defined Subnet; Modify for its own IP Address only
Group Types	None
Images	Download
Other Packages	Download
Packages	Download
Preferences for Device Manager	None
Preferences for DHCP/TFTP	None
Preferences for Logging	None
Preferences for Scheduling	None

TSF Data	Access
Preferences for Services	None
Remote Repositories	None
Reports	None
Scheduled Updates	None
Subnets	None
User Accounts	None

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, *distribute, and create* the *data specified in the following table* to *Administrators and Users with the permissions specified in the following table*.

Table 10 - FMT_MTD.1 Detail

TSF Data	Permission	Access
Audit Log	"Create and View Reports"	Query
	"Archive Log"	Delete (records from the log)
Configurations	Any defined User or Administrator	Query
	"Register Package"	Create
	"Modify Package"	Modify
	"Delete Package"	Delete
	"Distribute Packages"	Distribute
Default Device Configurations (DDC)	Any defined User or Administrator	Query
	Administrator	Create, Modify, Delete
Device Views	Any defined User or Administrator	Query
	"Create/Modify Views"	Create, Modify, Delete
Devices	Any defined User or Administrator	Query
	"Create/Modify Device Info"	Modify
	"Manually Add Devices"	Create
	"Delete Devices"	Delete
Group Types	Any defined User or Administrator	Query
	"Create/Modify Device Groups"	Create, Modify, Delete
Images	Any defined User or Administrator	Query
	"Register Package"	Create
	"Modify Package"	Modify
	"Delete Package"	Delete
	"Distribute Packages"	Distribute
Other Packages	Any defined User or Administrator	Query
	"Register Package"	Create
	"Modify Package"	Modify
	"Delete Package"	Delete
	"Distribute Packages"	Distribute
Packages	Any defined User or Administrator	Query

TSF Data	Permission	Access
	"Register Package"	Create
	"Modify Package"	Modify
	"Delete Package"	Delete
	"Distribute Packages"	Distribute
Preferences for Device Manager	Administrator	Query, Modify
Preferences for DHCP/TFTP	Administrator	Query, Modify
Preferences for Logging	Administrator	Query, Modify
Preferences for Scheduling	Administrator	Query, Modify
Preferences for Services	Administrator	Query, Modify
Remote Repositories	Any defined User or Administrator	Query
	Administrator	Create, Modify, Delete
Reports	"Create and View Reports"	Query, Create, Modify, Delete
Scheduled Updates	Any defined User or Administrator	Query
	"Create/Modify Updates"	Create, Modify, Delete
Subnets	Any defined User or Administrator	Query
	"Create/Modify Subnets"	Create, Modify, Delete
User Accounts	Any defined User or Administrator	Query
	Administrator	Create, Modify, Delete (except their own account)

6.1.3.2 FMT_SMF.1 Specification of Management Functions

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

1. *Manage Devices*
2. *Manage Packages*
3. *Manage Preferences*
4. *Manage User Accounts*

6.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Administrator, User and Device*.

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

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the following table.

Table 11 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design

Assurance Class	Component ID	Component Title
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 12 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied in the operational environment (OE.TIME_STAMP)
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the operational environment (OE.IandA)
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.1	No other components.	FAU_GEN.1	Satisfied
FAU_STG.3	No other components.	FAU_STG.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by the operational environment (OE.IandA) for GUI Users; the role is implied for Devices.

7. TOE Summary Specification

7.1 FAU_GEN.1

The TOE generates audit records for the events specified in the table included with FAU_GEN.1. The audit records are stored in the audit log, a circular file of a configured size. All records include a time stamp (supplied by the operating system), event identifier (type of event), and the userid for actions associated with a management action. Different event identifiers are used to indicate the success or failure of events. Audit records generated on Remote Repositories are pulled to the Master Repository during synchronizations.

7.2 FAU_GEN.2

All records include the userid for records associated with an Administrator or User action.

7.3 FAU_SAR 1

Administrators and Users with the "Create and View Reports" permission may view the audit records using the TOE's report capability supplied by the WDM GUI. Once a report is created, the current audit records satisfying each report's criteria may be viewed by selecting that report from the list of defined log reports.

7.4 FAU_SAR 2

Devices and Users that do not have the "Create and View Reports" permission are not provided a mechanism to view the audit records.

7.5 FAU_SAR 3

When Administrators and Users with the "Create and View Reports" permission create a log report, they may specify filters for the time range and/or userid to be included in the report.

7.6 FAU_STG.1

The audit records are stored in the audit log. The TOE does not provide any mechanism for users to modify audit records. Administrators and Users with the "Archive Log" permission may delete (archive) records from the audit log when the audit record count exceeds the configured maximum size. No other mechanism to delete audit records is provided.

7.7 FAU_STG.3

The first time the audit record count in the audit log exceeds the configured maximum size, a warning message is displayed to the Administrators or User. If the Administrators or User has the "Archive Log" permission and clicks OK, a pop-up window is displayed permitting the user to archive all records; the oldest "n" records, where "n" is the configured number specified via Logging Preferences; or all the records in a specified time range. If the Administrators or User selects Cancel, a timer is started and the warning message is again displayed after the amount of time configured via the Logging Preferences.

7.8 FIA_ATD.1

For each defined Administrator and User account, a user name, role and permissions are configured by Administrators. Administrators have all permissions. Administrators may not modify or delete their own accounts.

For each defined Device, the IP Address associated with the device is maintained. The IP Address may be dynamically learned by the TOE from the source IP address in received IP datagrams for previously unknown devices, or configured by an Administrator or User with either the “Manually Add Devices” or “Create/Modify Device Info” permissions.

7.9 FIA_USB.1

When the WDM GUI is invoked by a Windows user, the Windows userid is bound to the user session. The userid is used to search the defined User Accounts in WDM for a match. If one is found, the configured role and permissions for the account are bound to the session. If no match is found, no role or permissions are bound to the session and the user is not granted access to any TSF data or functions.

When an IP datagram is received from a Device, the source IP address from the received IP datagram is bound to the session for processing of the datagram.

7.10 FMT_MTD.1

The table included with FMT_MTD.1 specifies the TSF data that may be accessed by users as well as the operations that may be performed.

For Administrators and Users, these operations are performed via the WDM GUI provided by the TOE. For Devices, the operations are performed by sending network packets to the WDM system. Configuration and status updates identified on Remote Repositories are pulled to the Master Repository during synchronizations.

7.11 FMT_SMF.1

The TOE provides users with the functionality to manage the following:

1. Devices
2. Packages
3. Preferences
4. User Accounts

These functions are primarily managed by Administrators and Users via the WDM GUI provided by the TOE. The ability to create and modify Devices is provided to the Devices for their own Device only; this functionality is invoked when the Devices send network packets to the WDM system.

7.12 FMT_SMR.1

The TOE supports the following roles: Administrators, Users and Devices. Administrators and Users interact with the TOE via the WDM GUI executing on the main WDM server, while Devices interact via network packets sent to the WDM system. Administrators and Users are further categorized by the role and permissions assigned to their user account in WDM, based on the userid they supplied when logging in to the Windows operating system hosting the WDM system. Devices are automatically associated with their role upon receipt of network packets by WDM.

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 13 - Threats and Assumptions to Security Objectives Mapping

	O.AUDIT_GEN	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.DOWNLOAD	O.MANAGE	OE.COMM	OE.ENVIRON	OE.landA	OE.INSTALL	OE.NETWORK	OE.NOEVILADMIN	OE.TIME_STAMP
A.ENVIRON							X					
A.INSTALL									X			
A.MGMT						X						
A.NETWORK										X		
A.NOEVILADMIN											X	
P.ACCESS					X	X		X				
P.PACKAGE				X								
T.AUDIT_ COMPROMISE		X										
T.MASQUERADE					X	X		X				
T.UNIDENT_ACTIONS	X		X									X

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 14 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.AUDIT_COMPROMISE	**O.AUDIT_PROTECT** mitigates this threat by controlling access to the audit trail.

T.TYPE	Security Objectives Rationale
T.MASQUERADE	**O.MANAGE** mitigates this threat by controlling the logical access to the WDM component of the TOE and its resources based on roles/permissions. **OE.IandA** mitigates this threat by requiring the operational environment to authenticate user credentials so that authorized users may be validated. **OE.COMM** mitigates this threat by protecting information (including user credentials) from disclosure when it is transferred across a network.
T.UNIDENT_ACTIONS	**O.AUDIT_REVIEW** helps to mitigate this threat by providing GUI users with a mechanism to review audit events that could indicate a security compromise of the TOE resulting from unintended user actions. **O.AUDIT_GEN** helps to mitigate this threat by recording actions for later review. **OE.TIME_STAMP** helps to mitigate this threat by ensuring that audit records have correct timestamps.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 15 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ENVIRON	**OE.ENVIRON** addresses this assumption by restating it as an objective for the administrator to satisfy.
A.INSTALL	**OE.INSTALL** addresses this assumption by restating it as an objective for the administrator to satisfy.
A.MGMT	**OE.COMM** addresses this assumption by protecting information from disclosure when it is transferred between the systems.
A.NETWORK	**OE.NETWORK** addresses this assumption by restating it as an objective for the administrator to satisfy.
A.NOEVILADMIN	**OE.NOEVILADMIN** addresses this assumption by restating it as an objective for the administrator to satisfy.

8.1.3 Rationale Showing OSPs to Security Objectives

The following table describes the rationale for the organizational security policies to security objectives mapping.

Table 16 - OSPs to Security Objectives Rationale

P.TYPE	Security Objective Rationale
P.ACCESS	**O.MANAGE** addresses this OSP by controlling the logical access to the WDM component of the TOE and its resources based on roles/permissions. **OE.IandA** addresses this OSP by requiring the operational environment to authenticate user credentials so that authorized users may be validated. **OE.COMM** addresses this OSP by protecting information (including user credentials) from disclosure when it is transferred across a network.
P.PACKAGE	**O.DOWNLOAD** addresses this OSP by requiring the TOE to provide appropriate packages to devices based upon device properties and package attributes.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.AUDIT_GEN	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.DOWNLOAD	O.MANAGE
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1			X		
FAU_SAR.2		X			
FAU_SAR.3			X		
FAU_STG.1		X			
FAU_STG.3		X			
FIA_ATD.1					X
FIA_USB.1					X
FMT_MTD.1				X	X
FMT_SMF.1					X
FMT_SMR.1					X

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDIT_GEN	**FAU_GEN.1** defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. **FAU_GEN.2** requires the TOE to include information about the user who causes an event to be generated.
O.AUDIT_PROTECTION	**FAU_SAR.2** restricts the ability to access the audit trail to the authorized administrators, thus preventing the disclosure of the audit data to any other user. **FAU_STG.1** requires the TOE to prevent unauthorized modification or deletion of the audit records. **FAU_STG.3** defines the actions of the TOE in the event of potential storage exhaustion.

Security Objective	SFR and Rationale
O.AUDIT_REVIEW	**FAU_SAR.1** provides authorized administrators with the capability to read the audit data contained in the audit trail. This requirement also mandates the audit information be presented in such a way that the administrator can examine an audit record and have the appropriate information presented together to facilitate the analysis of the audit review. **FAU_SAR.3** provides authorized administrators with the capability to filter the audit data to enable more effective review of the audit events.
O.DOWNLOAD	**FMT_MTD.1** defines the privileges granted to Devices and GUI users to manage Devices and packages so that appropriate downloads may be associated with the Devices.
O.MANAGE	**FIA_ATD.1** defines the attributes of users that must be configured by administrators or learned dynamically for Devices. **FIA_USB.1** requires the TOE to bind the role to each management session upon invocation of the WDM GUI or receipt of IP datagrams from Devices, which enables enforcement of role-based management capabilities. **FMT_MTD.1** requires that the ability to manipulate TOE content is restricted to authorized administrators and identifies the role required for specific actions. **FMT_SMF.1** defines the specific security management functions to be supported. **FMT_SMR.1** defines the specific security roles to be supported.

8.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.