Marshal EndPoint Security

From

Best Practice Document
Hints and Tips

Privacy Control:	None		
Version:	1.8	**Status:**	Full
Volume:	1.8	**Restrictions:**	Unrestricted
Author:	Marshal Ltd.	**Date:**	02/06/2007
Privacy Control:	None		

Responsibility for ensuring the currency of any paper copy of this document rests with the user.

This copy was printed on 5 June, 2007

0 Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide useful information on the setting up and using of the Marshal EndPoint Security™ product.

1.2 Scope

This document covers version 4.6 of the Marshal EndPoint Security™ product.

1.3 Structure

Standard.

1.4 Terms and Abbreviations

Device Class	The term used within Marshal EndPoint Security™ to indicate a collection of related devices. For example, the Plug and Play Device Class, MP3 players such as the iPod, external removable memory sticks and internal multi-format card readers.
USB	Universal Serial Bus – this is a common wired connection standard to allow the rapid transfer of data to and from devices that support this standard.
Firewire	A common wired connection standard to allow the rapid transfer of data to and from devices that support this standard.
Other Disk Based Plug and Play	Plug and Play refers to automatic detection and configuration of devices by the operating system In the context of EndPoint Security™ we manage Disk Based Devices that are Plug and Play compatible.
WiFi	Communication medium for electronic devices using radio technology in place of wired connections
Bluetooth	Common standard short-range wireless connectivity for electronic devices
Infra-Red	Short range serial communication medium utilising Infra-Red light

1.5 References

2 Hints and Tips

2.1 Attached Storage on Palm-based Devices

Blocking Palm OS-based devices does not prevent a memory device mounted on the Palm device from being accessed.

Access must be denied to both the Palm and Other Plug And Play Storage Device Classes in the EndPoint Security™ policy. The former will prevent the ability to Hotsync with Palm devices whilst the latter will block any attached storage such as Secure Digital, Sony Memory Stick or Compact Flash cards.

Further, in EndPoint Security™ it is also necessary to disable the WiFi, Bluetooth and Infra-Red capabilities of a computer to prevent access by Palm OS devices over these connection methods.

Therefore, in summary, to completely block a Palm OS-based device one must deny access to the following Device Classes:

- Palm
- Infra-Red
- WiFi
- Bluetooth

2.2 Correct Handling of USB Memory Devices

If the user inserts a USB memory device, or external hard disk connected by either a USB or Firewire interface, after the Diskette Drives, USB Flash Disks, Digital Media Players, Digital Cameras, Bluetooth or Infra-Red Device Classes have been blocked, then the attached device will not appear in the list of mounted volumes, however it will have been mounted - but is just not visible to that particular user

2.3 Prevention of Bypassing Security

Because the EndPoint Security™ security policy is applied after Windows™ switches into Protected Mode it is possible to bypass the deployed security policy by booting from an external device before Windows™ loads up. For example, from an external memory device, floppy diskette or CD-ROM.

To prevent this loophole from being exploited, Administrators should ensure that the boot order in the BIOS specifies the hard disk as the first bootable device. The BIOS should be password protected so that this setting cannot be changed easily.

2.4 Issues with Removable Plug-and-play Storage Devices

If a device class has been locked and a user removes an attached USB or Firewire device in the same Device Class, all other devices in the same device class are no longer visible.

A reboot will be required before devices in the locked class are visible again.

2.5 Virtual PC Users

When specifying access policies for users or groups on your network it is important to remember to set the appropriate rights for groups or users using virtual PC's as these will have to be correctly set in order to block access to physical devices from within the virtual PC session.

2.6 Avoid System Vulnerabilities

In order to prevent access to writable CDROMS devices with Roxio Easy CD Creator, Administrators should ensure that their Windows™ 2000 installations have the latest service patch applied. Currently this is SP4 for Windows™ 2000.

2.7 Remote Access to Locked Devices

When accessing a mounted device remotely over the network, the user accessing the device will gain the rights of the person currently logged into the target PC at that time. If this access is not to be permitted then System Administrators should ensure that they appropriately restrict both local and remote access to devices on their network.

2.8 Blocking Access to Externally Mounted Memory on PDA's

Some PDA's, such as the Tungsten T5 PDA, can mount externally inserted memory sticks (SD cards) or a portion of their internal RAM. Normally, these are blocked through the Other Disk Based Plug & Play Storage Class settings but in the case of devices such as the Tungsten T5, the memory will have to be blocked through the Palm OS Devices class.

Administrators should confirm to their satisfaction that the relevant classes are set correctly for the device range expected to be used on their network.

Additional complications arise with later devices because the memory can be mounted by alternate means. Therefore memory sticks on some Palm OS devices are locked using the Other Disk Based Plug and Play Device Class, while some others are locked using the Palm Device Class; and in the latter case, as one can mount them both through the File Transfer and other third party direct USB-mount software, one must remember to lock both device classes.

Further, it is possible to mount inserted memory sticks via an FTP connection over Bluetooth with Palm OS-based devices. Therefore the Bluetooth Device Class will also need to be appropriately locked down.

2.9 Active Directory and DNS Configuration Considerations

You must configure DNS correctly to ensure that Active Directory will function properly. EndPoint Security™ makes extensive use of Active Directory, consequently, malfunctioning of the DNS will significantly affect the operation of Active Directory with EndPoint Security™.

For a more in-depth treatment of DNS configuration for Active Directory, see the following Microsoft Knowledge Base article:

237675 Setting Up the Domain Name System for Active Directory

Review the following configuration items to ensure that DNS is healthy and that the Active Directory DNS entries will be registered correctly:

- DNS IP configuration
- Active Directory DNS registration
- Dynamic zone updates
- DNS forwarders

2.10 Alternate Domain Browsing – Trusted Relationships

To select users and groups in a different domain and to deploy computers via the Control Center's Active Directory browser, you need to have established a trusted relationship between the domain you are logged in to and the target domain.

2.11 Minimum Requirements for Client Machines with NT Operating System

The minimum specification for EndPoint Security™ client machines running NT is Service Pack 6a together with IE4 at a minimum. Certain operating system files that are required for EndPoint Security™ are not present if a lesser specification is installed. Read-only access is not supported under Windows™ NT.

2.12 Mounting NTFS Partitions

If a user already has an existing USB drive that they have mounted as an NTFS folder rather than a drive letter, then applying EndPoint Security™ will not block the device. It only affects the specific device, not any similar device they may attach at a later date. Devices are uniquely identifiable and Windows™ remembers how it mounted each unique device.

Once EndPoint Security™ is present, the user cannot mount any more devices as folders. Administrators may have to unblock the USB class for that user on that machine to permit the new folder to be mounted and then re-apply the policy.

2.13 Deny Access for Authorised User on Kodak Digital Camera

EndPoint Security™ can incorrectly block access to a Kodak EasyShare CX7530 digital camera for an authorised user. If an un-authorized user has tried to access the device and been denied access, then an authorised user logs in later whilst the device is turned off, turning the device on will not permit access. The authorised user will need to re-log in again with the device turned on to gain access.

2.14 Policy Updates after Re-installation

After re-installing EndPoint Security™, clients will automatically pick up a new policy if the policy on the server has been updated.

It is possible that the clients may not automatically pick up the policy if the default has not been changed.

Administrators should ensure that the policy is re-setup after a re-installation to ensure that the clients collect the new policy.

However, in this situation the Policy Update and Client status wizard will not know what clients have been deployed, therefore for this reason the clients should be re-deployed after re-installation of the product.

2.15 Effect of Changing the Target Share on a client PC

Care should be taken not to disable or rename the share (c$ by default) previously used in deployment to target computers. This is because EndPoint Security™ remembers the share previously used and will subsequently attempt to re-use that share for future deployments and policy updates. If it becomes necessary to change the default share, the EndPoint Security™ clients will need to be removed, the share changed and then the clients re-deployed.

2.16 No EndPoint Security ™ Enforcement Pop-Ups

On Windows™ 2000 machines a reboot is required before policy enforcement pop-ups are visible. A reboot notification will only be displayed if the EndPoint Security™ administrator has not disabled it from the Control Center – Client Settings dialog.

2.17 Scanners are Sometimes Blocked

In some instances scanner hardware may identify itself as a member of the Digital Cameras Device Class. The solution to this is to create a new class for the scanner in question, using the Policy Customizer tool contained within the current release of EndPoint Security™.

2.18 Get I/O Error when Reading Encrypted USB Sticks

If a user tries to access an encrypted USB stick without the correct password, the user will get an I/O error dialog. This is because Windows™ returns this error when accessing media that cannot be read.

2.19 Unable to open EndPoint Security ™ Control Center

The message 'Another instance of the Control Center is running' may display if the user has insufficient privileges to open Control Center. The Control Center may only be opened by those users with local or domain administrator right.

2.20 An Error Occurs when Performing an Encrypted Format on a Memory Stick.

The minimum size supported for USB Devices is 64MB due to the fact that EndPoint Security™ uses a FAT32 file system.

2.21 Encryption

Administrators are advised to ensure that any data stored on an encrypted device is backed-up elsewhere in case the private or global key used is lost. To ensure the security of encrypted data, if the encrypted device is used on a PC not running the client with encryption support, the user will be prompted to format the device before they can use it.

2.22 Additional Information on Client Deployment using the MSI Installer

The following setting must be added to POLICY.XML before the </ClientSettings> element to enable the client to register with the EndPoint Security™ Control Center when installing using the MSI package;

```
<EnableRegMsg val="1" />
```

Additionally, the EndPoint Security™ Control Center must be running in order for registration to occur.

2.23 Difference in Policy Management Introduced in 4.0

Prior to 4.0 when setting a closed policy, EndPoint Security™ would show Builtin/Administrators and Full control. This group has now been removed and the default closed policy will now also deny access to local administrators.

2.24 "Microsoft VC++ Run Time Library Error" Message

If you experience this error message when trying to access the EndPoint Security™ Control Center, then apply the following Microsoft patch to your system to update the MDAC components.
http://www.microsoft.com/downloads/details.aspx?FamilyId=39472EE8-C14A-47B4-BFCC-87988E062D91&displaylang=en

2.25 User is Prompted for Password on Silent MSI Uninstall.

The EndPoint Security™ MSI installer supports all the commonly used switches including silent uninstall. If an admin invokes a silent uninstall and an uninstall password has been set in the control center the user will be prompted for the password. To avoid this, the EndPoint Security™ administrator should remove the password in the EndPoint Security™ control center.

2.26 U-Storage Security Software causes EndPoint Security ™ to Recognise USB Storage Device as Other Plug and Play Storage.

After using the U-Storage software, the USB storage device may have multiple partitions or hidden security depending on the software options chosen.

Therefore, to manage this device set an access policy for 'U3 & Other Multi-Drive USB Devices.

2.27 Access Restriction Does not Prevent Smartphone from being Accessed via Windows™ Explorer.

This can happen when the device had already been used in the user session in which the client agent was deployed. A logoff event or system restart is required before the device is totally blocked. In the meantime access is still restricted via using the bundled Smartphone software.

2.28 Temporary Access Period

If temporary access is granted for less than 30 minutes then access is allowed for 30 minutes. Likewise if temporary access is granted for a period exceeding 5 days access will only be allowed for 5 days.

2.29 No Audit logging for Inbuilt Floppy Disk Drives

Inbuilt floppy disk drives are legacy devices and as such no insertion is logged in the EndPoint Security™ Audit Log. However for USB based Floppy Drives audit logging is performed.

2.30 File Auditing under Windows NT ™

File Auditing is not available under Windows™ NT. Windows™ NT does not provide Support for the Windows™ Driver Model available in more recent Windows™ operating systems.

2.31 Backing up the Global Key for a Re-Instalation

Care should be taken that the Global Key is backed up to a folder, other than the default path presented. The default path is the EndPoint Security™ install folder; this folder is deleted when EndPoint Security™ is uninstalled.

2.32 File Access Summary Screen is not Automatically Updated

The Audit Log Devices and File Access Summary screens are not refreshed automatically, refresh is manual via the 'Refresh' button at the top of the screen.

2.33 Securing Access to SmartPhones

Smartphones use multiple communication technologies. In order to secure access to these particular types of device, the EndPoint Security™ administrator should block all the technologies these devices use. For Example you may need to block, Smartphone, WiFI, Bluetooth and Infra-Red.

2.34 Policy Update and Client Status Show '??' as the Client Version Number.

This may happen if the client computer is rebuilt or fails in some manner. Redeploying the client will solve this problem

2.35 U3 Devices and Audit Logging.

Access denied to U3 devices will show two access attempts per single access action. This occurs because the U3 device mounts itself as two distinct drives. If access is permitted, only one access is logged as only a single mounted drive will be accessed.

2.36 Unable to Deploy to the Server PC on a Standalone System.

This may occur on an XP server that is not plugged in to a network, such that ipconfig shows no available network adaptors, the Control Centre is unable to connect to the local computer when deploying a client. This situation is rectified by installing the standard Microsoft Loopback Adaptor. Details of how to do this can be found at the following URL. **http://support.microsoft.com/kb/839013**

2.37 Policy Customizer Custom Classes and USB Flash Disks

If a custom class contains specific definitions of USB Flash disk(s), they will appear in the “Detected By EndPoint Security” window as assigned to that custom class, while the custom class is above the pre-defined "USB Flash disks" class in Policy Customizer’s hierarchy. If the custom class is moved below the pre-defined “USB Flash Disks” then the Policy Class changes to "USB Flash Disks"

This behavior is specific to USB Flash Disks and does not affect any other device which may be detected by EndPoint Security.