Adapting Endpoint Security to “Mobilized” Consumerization of Corporate IT

Designed for
Microsoft®
Windows® XP
Windows® 2000
Windows NT®

Contents

Introduction

Consumer electronics and applications are proliferating in corporate IT environments, significantly increasing the threat of lost and stolen data. Personal devices such as Smartphones and Mobile Internet Devices (MIDs) are now commonly brought to work and used for business purposes.

This *consumerization of corporate IT* is predicted to accelerate in coming years[1] as *Digital Natives*[2] - those raised playing computer games - penetrate corporate ranks. This generation not only has a great fascination with ultra-modern electronic gadgets, they also have a natural ability to operate them. This fact along with continued progress in microelectronics, telecommunications, and consumer product offerings will make it virtually impossible for IT departments to stop the spread of consumer habits and tools in the workplace.

In preparation, significant attention must be paid to the definition and enforcement of IT security policies related to personal devices and corresponding changes in security threat profiles. To meet the challenge, the industry should have an effective solution for every aspect of endpoint security.

Consumerization Goes Mobile

Today’s personal mobile devices (smartphones and PDAs) have been a boon to employee productivity. Though the number of mobile business applications is limited today – mostly email, IM and, less frequently, Presence Awareness – smartphones are already actively used in mid-sized and large organizations.

[1] “On the Edge: Exploring Next-Generation Digital Disruptions”, Computer Sciences Corporation, May 6, 2002 (http://www.csc.com/newsandevents/news/1750.shtml)
[2] "On the Horizon", NCB University Press, Vol. 9 No. 5, October 2001, Marc Prensky (http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf)

According to a recent report from Osterman Research[3], about 15% of the corporate workforce in North America used employer-supplied mobile devices in 2007. And a survey from TechTarget[4] forecasts that this figure will exceed 25% in 2008.

If we take a "hardware" look at IT consumerization, it is clear that several decisive trends will make tomorrow's personal mobile devices a vitally important component of the corporate IT environment.

- Firstly, the 2008 International CES has confirmed the full validity of Moore's Law[5] once again with Intel introducing 16 new processors based on 45 nm technology.

- Secondly, the world is entering the age of ubiquitous mobile broadband connectivity with today's global proliferation of Wi-Fi, the fast growing commercial deployment of 3G/HSPA networks with more than 150 operators in 72 countries[6], and the "injection" of Mobile WiMAX by Intel's Montevina with its promise to enable wireless mobility for 750 million people by 2010[7].

- Thirdly, Intel's invasion of the mobile SoC (System-on-a-Chip) market with Moorestown will force mobile OS vendors to standardize and consolidate the industry, thus igniting explosive growth in enterprise-class mobile applications. With the new generation of SoC platforms, "the world is going ultra mobile" whatever mobile OS it will be running - Windows XPe, Ubuntu, Mac OS X, Android, Windows Mobile, or all of them.

Consumerized Mobile Threat

Undoubtedly, the consumerization of corporate IT will soon "mobilize" the entire corporate workforce, with everyone using either company-supplied or individually-owned mobile devices. The Yankee Group is proposing a Zen-like co-operative IT management model for the consumerized enterprise[8] as optimal for maximizing employee productivity.

But from the IT security perspective, the task "of rogue employee management" in a *consumobilized* enterprise will become a real *art* – especially as co-operative behavior and self-discipline will be expected from disgruntled, malicious, negligent, or forgetful employees. Because the very same technology achievements and social trends that drive the progress of consumerization will cause a sharp increase in information security risks for the enterprise related primarily to the development of "production quality" mobile malware, and – to an even larger extent - to the ***growth of corporate data leakage from and through employees' mobile devices***.

Mobile Malware "Roadmap"

The typical size of a mobile device removable flash memory (4-8GB) is already sufficient for storing and running a standard Operating System (OS). The expected significant increase in

[3] "Mobile Messaging Market Trends, 2007-2010", Osterman Research, Inc., October 2007 (http://www.ostermanresearch.com/or_mm07es.pdf)

[4] "Mobile phone beats out smartphone as device of choice", Copyright: 2007 TechTarget (http://searchmobilecomputing.techtarget.com/originalContent/0,,sid40_gci1278692,00.html)

[5] CES 2008: Intel Debuts 16 New Processors Based on 45nm Silicon Technology http://blog.wired.com/gadgets/2008/01/ces-2008-intel.html

[6] Official HSPA web-site (http://hspa.gsmworld.com/networks/)

[7] http://www.wimax-vision.com/newt/l/wimaxvision/article_view.html?artid=20017463390

[8] As Yankee Group has named this kind of management :-) in their report "Zen and the Art of Rogue Employee Management", August 6, 2007 (http://www.yankeegroup.com/pressReleaseDetail.do?actionType=getDetailPressRelease&oldId=24)

MID's computing power together with a tenfold drop in their power consumption (as promised in Intel's Moorestown platform) has already triggered the chain reaction of mobile OS and application industry growth.

This high-speed process will make the development of "commercial" mobile malware really profitable. From its current stage of proof-of-concept prototypes, this cybercrime industry segment will soon move to the delivery of "production-quality" malware, thus increasing the probability of attacks to mobile devices and their infection at least up to the level of modern PCs connected to the Internet.

How soon could it happen? It depends on how quick and dedicated the mobile OS vendors will be in their drive to control this huge emerging market. It is unlikely though that we will see any impact immediately because the "target market" for commercial malware needs to mature enough to justify investments in their "product" development. Realistically, we could expect something significant in this area closer to the end of 2009.

Mobile Data Leakage Threat: Immediate and Fast Growing

On the other hand, the threat of rapidly growing corporate data leakage through personal mobile devices is unavoidable and immediate.

Unavoidable – because certain features of human nature are not going to change: we cannot inoculate against accidental errors, occasional negligence, and the rare incidence of malicious intent. Moreover, mobile devices will continue to be lost and stolen in the future as they are today.

Immediate – because nothing new is required for exercising the threat, it is happening right now; technology advancements will just multiply its severity and impact.

So what is the scale of this threat today, when we are just entering the early stages of IT consumerization? The situation with regard to mobile device security is already deeply concerning.

- In-Stat[9] has estimated that over 8 million mobile phones went missing in the U.S. in 2007. And for smartphone users, the ones with the most access to sensitive information, the probability of loosing a device was 40% higher.

- The latest "2007 CSI Computer Crime and Security Survey"[10] revealed, that last year about **7%** of total financial losses incurred by US corporations from IT security incidents were related to the loss of proprietary or confidential data from mobile device theft.

- According to U.K. Home Office statistics[11], **2%** of individual mobile phone owners had experienced theft annually.

Projecting these figures onto the latest mobile device market growth predictions[12] from Tim Bajarin, President of Creative Strategies, one can calculate an alarming forecast: In 2008, 5

[9] In-Stat research "Mobile Security 2007: End Users Are Losing It" (#IN0703622MBM) (http://www.instat.com/abstract.asp?id=229&SKU=IN0703622MBM);
"Mobile Security Still a Misunderstood Issue", Hardware Zone, 27 April 2007 (http://hardwarezone.co.th/news/view.php?id=7153&cid=5)

[10] "2007 CSI Computer Crime and Security Survey", September 13, 2007, Computer Security Institute (http://www.gocsi.com/forms/csi_survey.jhtml)

[11] "Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey" (http://uk.sitestat.com/homeoffice/homeoffice/s?rds.hosb1007pdf&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf%5D)

million smartphones will be lost or stolen with the number increasing to 14 million in 2010. The percentage of total financial losses related to these losses will represent some 14% in 2008 and 21% in 2010 of all types of attacks on corporate IT resources.

Mobile Leak Mechanics

Basically, every instance of data leakage through a mobile device is a two-step process:

- *Firstly*, uncontrolled data transfer from a corporate server/host-based resource to the device;

- *Secondly*, further unauthorized transfer of these data from the device to the outside.

To mitigate this two-step leakage workflow, existing Data Leakage Prevention (DLP) solutions for mobile devices include two layers of defense:

1. DLP components residing at servers, PCs or dedicated network appliances that prevent data leakage from the corporate resources to the mobile devices by intercepting and filtering data in all communications channels used by the devices.

2. Device-resident Infosecurity components designed to prevent data from uncontrollably leaking from the mobile devices.

On-Device DLP Components

By analyzing the functions of existing security components running on mobile devices, it appears that today there is only one effective mechanism that directly prevents data leakage from mobile devices - it is *device-resident* encryption. Typically implemented as “whole device encryption” or “file/volume encryption”, this solution blocks access to encrypted files and other objects stored in the memory of stolen or lost devices, as well as their removable memory cards.

Although security vendors tout *remote data wiping* as an additional mechanism for preventing data leakage from missing mobile devices, practically speaking, it is not, because every sensible cyber thief will immediately turn a stolen phone off and remove its memory card for analysis on a “failproof” device.

All other device-resident security components – FW, VPN, Device/Port Control, Anti-Virus/Anti-Malware, IDS, Application Control, NAC, User/Device Authentication – are not designed for *informational* data filtering and cannot be used to decide whether outbound traffic contains any leak to block.

As to Anti-Spam device components[13], they work in the opposite direction, preventing the downloading of unsolicited data to the device.

Mobile Encryption≠ Panacea

Although cryptographic solutions like “whole device encryption” could completely eliminate data leakage from stolen or lost mobile devices, they are not a mobile DLP panacea.

[12] Creative Strategies (http://www.creativestrategies.com/downloads.php); “Tech Predictions for 2008”, PC Magazine, 28.12.2007 (http://www.pcmag.com/article2/0,2704,2241562,00.asp)

[13] For instance, SMS Spam Filtering in Trend Micro Mobile Security 5.

The reason is that any running application uses data in RAM in plain, non-encrypted form, and nothing prevents users from deliberately or accidentally sending plain data to an external destination from within an opened network application like email, a web-browser, or instant messaging (IM).

For instance, a negligent employee could forward a previously received email with order delivery instructions to a subcontractor without noticing that the attachment to the email contains client's personal data prohibited to be revealed to 3rd parties.

Moreover, in the consumerized corporate future, due to employees' privacy concerns, the percentage of personal mobile devices protected by employer-supplied encryption solutions will likely be much less than today. According to Deloitte & Touche and Ponemon Institute, today only 55% of North American businesses use encryption to protect their data at rest[14].

Without underestimating the value of encryption for preventing data leakage from missing mobile devices, it should be accepted though that once the data get to the device there is, and always will be, a high risk of it being uncontrollably leaked to the outside.

This is why, for the foreseeable future, a critically important layer of corporate defense against mobile data leaks is intelligent *control over data delivery channels to mobile devices*.

Blocking Leaks to Mobile Devices

Mobile devices can basically import data through three channel types: network applications, removable memory cards, and local connections to PCs.

Today, there are plenty of products and solutions on the market for preventing data leakage to mobile devices through network applications like email, web-browsing, file transfer, web-mail, instant messaging, etc.

Being implemented as server-side components or dedicated network appliances that use well-developed Data/File Type Filtering, as well as Content-Based Filtering technologies, these solutions have proven to be highly effective for fighting data leaks and ensuring their users' compliance with applicable security-related state and industry standards.

The same types of data filtering technologies have already been integrated in several Endpoint Device/Port Control products available today, so the data uploaded from PCs to removable memory cards are intercepted and filtered to reliably block detected leaks.

Gone with the Sync: the Urgent Priority to Address

Important is that existing DLP solutions are designed as channel-specific, and those for network applications and removable storage are based on underlying techniques of protocol parsing for the most popular network applications, and intercepting file system calls from some office applications.

However, local data synchronizations between mobile devices and PCs are implemented as very specific applications that do not use network application protocols, and do not interact with office applications. Technically speaking, this means that no existing File Type Detection or Content-Based Filtering solution can control data flow through local connections from PCs to mobile devices.

[14] "Enterprise@Risk: 2007 Privacy & Data Protection Survey", Deloitte & Touche LLP and Ponemon Institute LLC (http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf)

In this situation, the only available method of eliminating data leakage through local sync is to completely block mobile device connections to the PC at its interface or port level. Regretfully, this is not always possible because most existing Device/Port Control products cannot even detect the presence of a mobile device if it is connected to the PC through a non-USB port (e.g. Bluetooth or COM).

From the corporate standpoint, it means that any company concerned with uncontrolled data leakage though mobile devices should prohibit their employees from synchronizing data between corporate PCs and mobile devices. This is obviously unacceptable even today because it would completely block the use of mobile devices in the business.

The problem is that if local syncs are allowed – as is the case in most organizations today – then every click on a “Sync” button means that highly-valued corporate data may be transferred to a personal mobile device without any way of controlling or tracing the action.

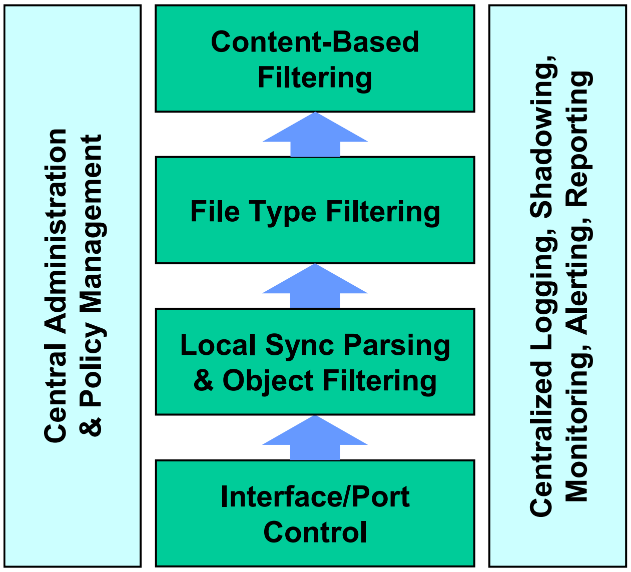
Weakly protected local sync communications have already become a serious security issue for many organizations. In the future, as consumerization progresses this issue could grow into a major security problem and business risk.

This is why the ***development of a comprehensive DLP solution for local sync connections should be an urgent priority for the infosecurity industry to address***.

Local Sync DLP Architecture

The Local Sync Data Leakage Prevention architecture should be built as a stack of *integrated* security mechanisms including *bottom-up* Endpoint Device/Port Control, Local Sync Application Parsing and Object Filtering, File Type Filtering, and Content-Based Filtering technologies.

In addition to these functional components, a central policy-based management console integrated with a major systems management platform, as well as centralized logging, reporting and evidence enablement components should be in place to complete the solution.


Central Administration & Policy Management
Content-Based Filtering
File Type Filtering
Local Sync Parsing & Object Filtering
Interface/Port Control
Centralized Logging, Shadowing, Monitoring, Alerting, Reporting

In this architecture, every layer controls those parameters of a local connection it is designed to deal with by blocking or filtering prohibited elements out, and detecting and marking the types of objects to be controlled by a higher-layer architecture component to which the classified data flow is then passed for further processing.

For instance, the Device/Port Control component is responsible for detecting and controlling the presence of a locally connected mobile device, the type of connection interface or port type (e.g. USB, Bluetooth, IrDA, COM), device type (e.g. Windows Mobile, Palm, Symbian, etc.), if possible – device model and its unique ID.

The output is then passed to the Local Sync Parsing component, which parses the sync traffic, detects its objects (e.g. files, pictures, calendars, emails, tasks, notes, etc.), filters out those prohibited, and passes allowed ones up to the File Type Filter.

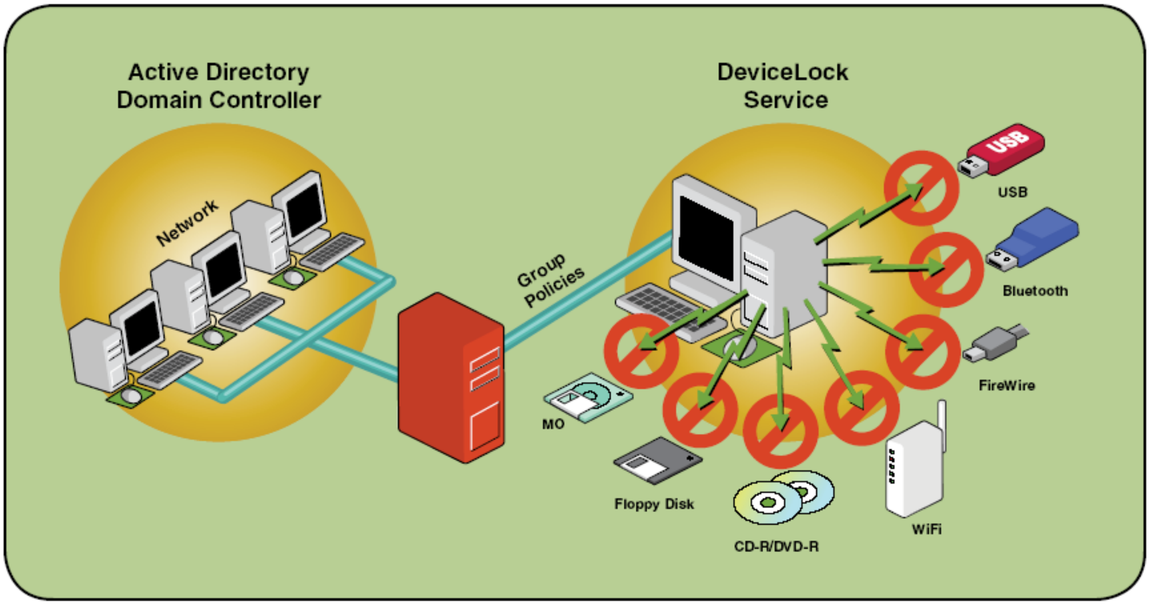
The File Type Filtering component checks the input flow, detects if any files are in, deletes those not allowed, and delivers the rest to the Content-Based Filtering component, which performs an *informational* data control to detect and block the pieces of human-understandable data failing to comply with the corporate security policy.

The Local Sync Parsing & Filtering component is the key to the entire solution because it implements the specificity of the data leakage channel, and it facilitates underlaying and building over other functional layers of the DLP stack.

With Local Sync Parsing in place, the rest of the required enforcement components of the architecture can be stepwise integrated in the stack by adjusting the existing ones – already available on the market, although in implementations designed not for local sync.

DeviceLock – Foundation of the Local Sync DLP Platform

By utilizing an internally developed patent-pending technology, DeviceLock, Inc. has implemented the fundamental components of the complete local sync DLP architecture in its DeviceLock® software product that enforces mechanisms of mobile device connection control in combination with local sync data type detection and filtering.



Today, DeviceLock is the only product on the market that controls local sync connections for Windows Mobile® 5, Windows Mobile® 6, and Palm® OS based mobile devices by filtering Microsoft ActiveSync®, Windows Mobile Device Center (WDMC), and HotSync protocols with granularity down to protocol objects and types.

With DeviceLock, security administrators can centrally and dynamically define which types of data specified users or user groups are allowed to synchronize between corporate PCs and their

Windows Mobile or Palm OS personal devices. These data types include files, pictures, calendars, emails, tasks, notes, and other ActiveSync, WDMC and HotSync protocol objects.

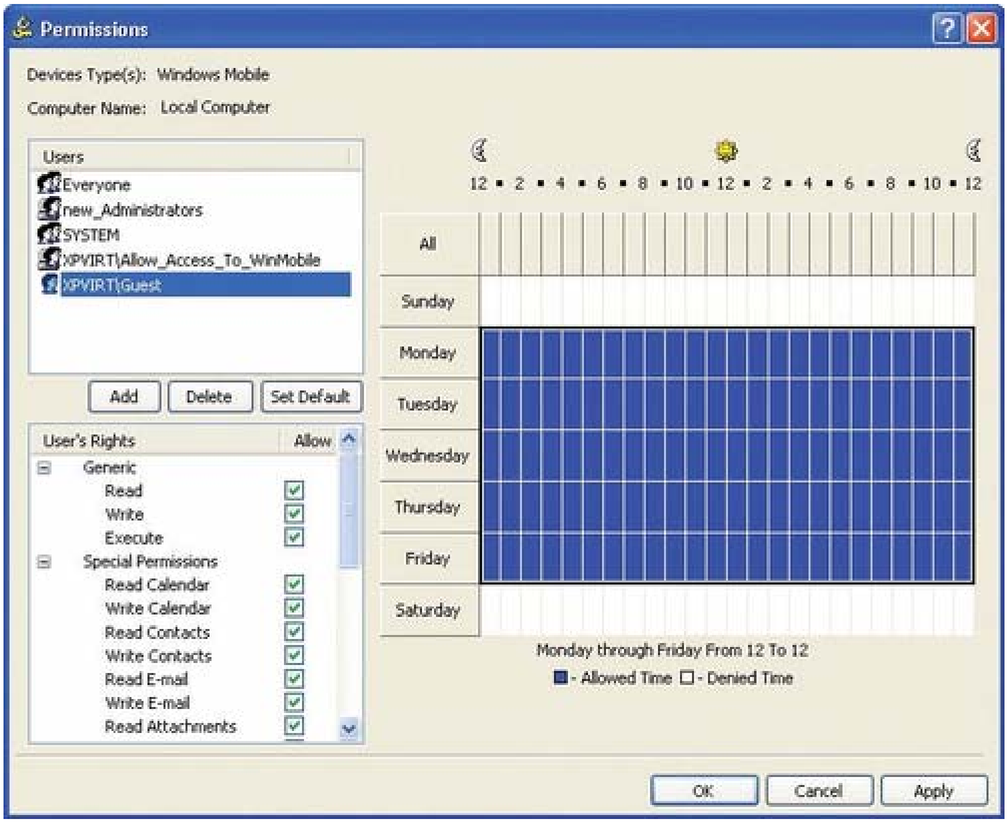
For example, corporate executives can be allowed to synchronize all types of objects with their mobile devices, while other employees can only import emails, tasks and calendar events to their devices. In addition, time-based filtering policy is supported, which may be useful to additionally restrict local sync exchanges, for instance, during weekends.

DeviceLock detects the presence of any Windows Mobile or Palm OS device regardless of which local port or interface it is connected to – USB, COM, IrDA, or Bluetooth. Moreover, the mobile device connections through any USB port can be blocked or allowed on the basis of device model and even for a unique device.

In addition, a Remote Code Execution Control feature enables the administrator to centrally block or allow the installation and execution of applications on corporate mobile devices.

Flexible local sync filtering policy management for all DeviceLock agents deployed on protected PCs across the corporate network, as well as all agents' life-cycle administration tasks are performed centrally either from a dedicated DeviceLock Enterprise Server management platform, or – if customers use Microsoft Active Directory® – through a special Group Policy object called DeviceLock Group Policy Manager (DL GPM) developed by DeviceLock, Inc. as an MMC snap-in for full native integration into the Microsoft Active Directory management platform.

The key advantages of DeviceLock GPM are that customers need not spend additional resources installing and operating a separate server platform to manage DeviceLock products, and – what is equally valuable – DeviceLock solution scalability depends completely on the scale of the Microsoft Active Directory installation in the organization, thus automatically corresponding to customer needs.



Permissions

Devices Type(s): Windows Mobile

Computer Name: Local Computer

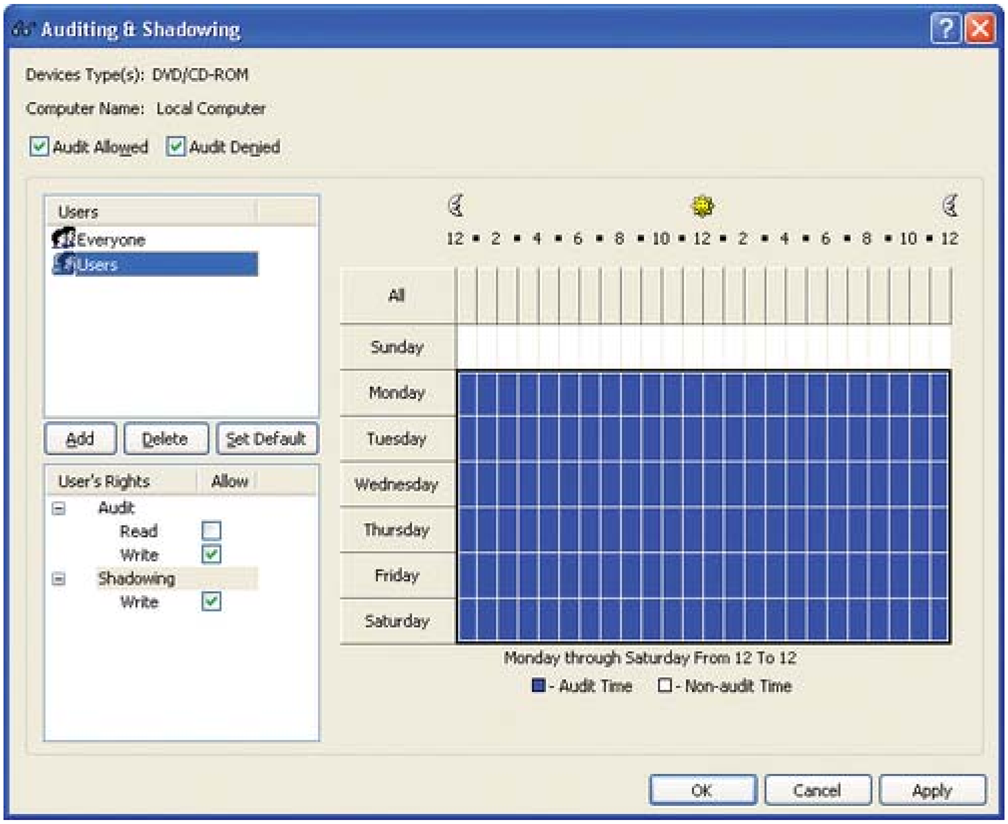
Users
- Everyone
- new_Administrators
- SYSTEM
- XPVIRT\Allow_Access_To_WinMobile
- XPVIRT\Guest

User's Rights	Allow
⊟ Generic	
Read	☑
Write	☑
Execute	☑
⊟ Special Permissions	
Read Calendar	☑
Write Calendar	☑
Read Contacts	☑
Write Contacts	☑
Read E-mail	☑
Write E-mail	☑
Read Attachments	☑

Monday through Friday From 12 To 12

■ - Allowed Time □ - Denied Time

On top of all this, detailed centralized logging and shadowing of files and other data copied between PCs and Windows Mobile devices are also supported. All locally gathered log and shadow data are automatically collected and stored in DeviceLock Enterprise Server's central database. Audit log generation and data shadowing policies are easy to define centrally from either DeviceLock Group Policy Manager, or DeviceLock Enterprise Server consoles.



Devices Type(s): DVD/CD-ROM

Computer Name: Local Computer

☑ Audit Allowed ☑ Audit Denied

User's Rights	Allow
Audit	
Read	□
Write	☑
Shadowing	
Write	☑

Monday through Saturday From 12 To 12

■ - Audit Time □ - Non-audit Time

To ease the tasks of log auditing and security incident investigations including evidence provisioning, DeviceLock Enterprise Manager is equipped with an embedded Log Viewer and Shadow Log Viewer, as well as report generation tools.

By using DeviceLock, corporations of all types and sizes can centrally, flexibly and economically control local sync communications between employees' mobile devices and their PCs thus increasing corporate workforce productivity "on the road" and at the same time reducing information security risks resulting from otherwise uncontrolled transfers of sensitive corporate information to inherently less secure personal mobile devices.

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 2 million computers in more than 50 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany

TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy

TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK

TEL (toll-free): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA

TEL (toll-free): +1-866-668-5625
FAX: +1-646-349-2996

sales@devicelock.com

support@devicelock.com

www.devicelock.com