SENTINEL TECHNICAL DESCRIPTION

1. *Lamda SENTINEL™ Features and Capabilities*

Lamda SENTINEL™ by **Lamda System Engineering Ltd** is a software tool that controls access to I/O devices resident on computers, such as CDs or floppy drives and removable devices such as USB sticks, SD cards (digital cameras), etc.

Lamda SENTINEL™ was designed to protect computers connecting to the enterprise network where the organization security policy is determined by the security authority. Administrators of this tool are often security personnel and their point of view as well as ease of use was intensely considered in the design of the human interface of Lamda SENTINEL™.

The security approach implemented by this tool is somewhat different from other tools like an Antivirus, Antispam and Firewalls. These tools are welcomed by end users that understand the need for protecting their computer from Malware. A tool that restricts end user's relative freedom in using the devices or ports of his computer is perceived as a nuisance and is prone to removal attempts. This aspect was a major design goal in the development of the Lamda SENTINEL™ product and caused the implementation of several Anti-Tampering mechanisms.

Lamda SENTINEL™ software includes the following elements:

- Lamda SENTINEL™ Management – central administration element.
- Lamda SENTINEL™ Agents - clients installed on the network computers.

The Lamda SENTINEL™ management element includes a server application, a database schema and a management console. The server communicates with the agents, receiving on-the-fly events and sending basic settings and security policies. Settings, events and policy data are stored in the database.

The Lamda SENTINEL™ management console is a GUI application that communicates with the server. Through this interface, the administrator can configure system settings and set policy for security objects. An online monitor screen displays in real time the agents' status and last reported events.

Lamda SENTINEL™ agents are small footprint clients installed on each of the network desktops and laptops. The agent is the application that enforces the security policy for each device type or specific device as defined by the administrator.

By default, Lamda SENTINEL™ defines a "White" policy. Any device is allowed for use, unless a different policy is defined by the administrator. The security policy that can be defined for a specific device (or class of devices), includes a real time report to the server, a user displayed popup message and one of the following actions at the violating station:

- Locking of keyboard
- Read-only access
- Disable access
- Logoff user
- Shutdown computer.

Different policy settings can be configured for situations where the computer is connected to or disconnected from the network. These policies can be set differently for each device class or specific device, to form the policy that is assigned to a specific user, group or computer. For a logged in user on a certain computer, conflicting policies may exist. The precedence order (from higher to lower) is: Computer, User, Group of Computers and Group of Users. If the individual user is a member of several groups the most restrictive rule policy prevails.

The device class list includes most of the common devices included in a computer configuration, as well as the most common external devices, plugged in through connection points such as a USB, FireWire etc. The specific device list is a global list that includes any device the corporation intends to treat as an exception to the security policy rule. For example, if USB memory sticks are "banned" (denied access), a specific USB memory stick chosen by the corporation for a specific user, may have allowed access.

Specific device credentials are "imported" by querying an agent on the list of devices connected to the computer. From this list, the administrator can choose to add to the global list any device that is intended to be assigned an exception policy. Any device included in the global list can be included with the set of a specific user.

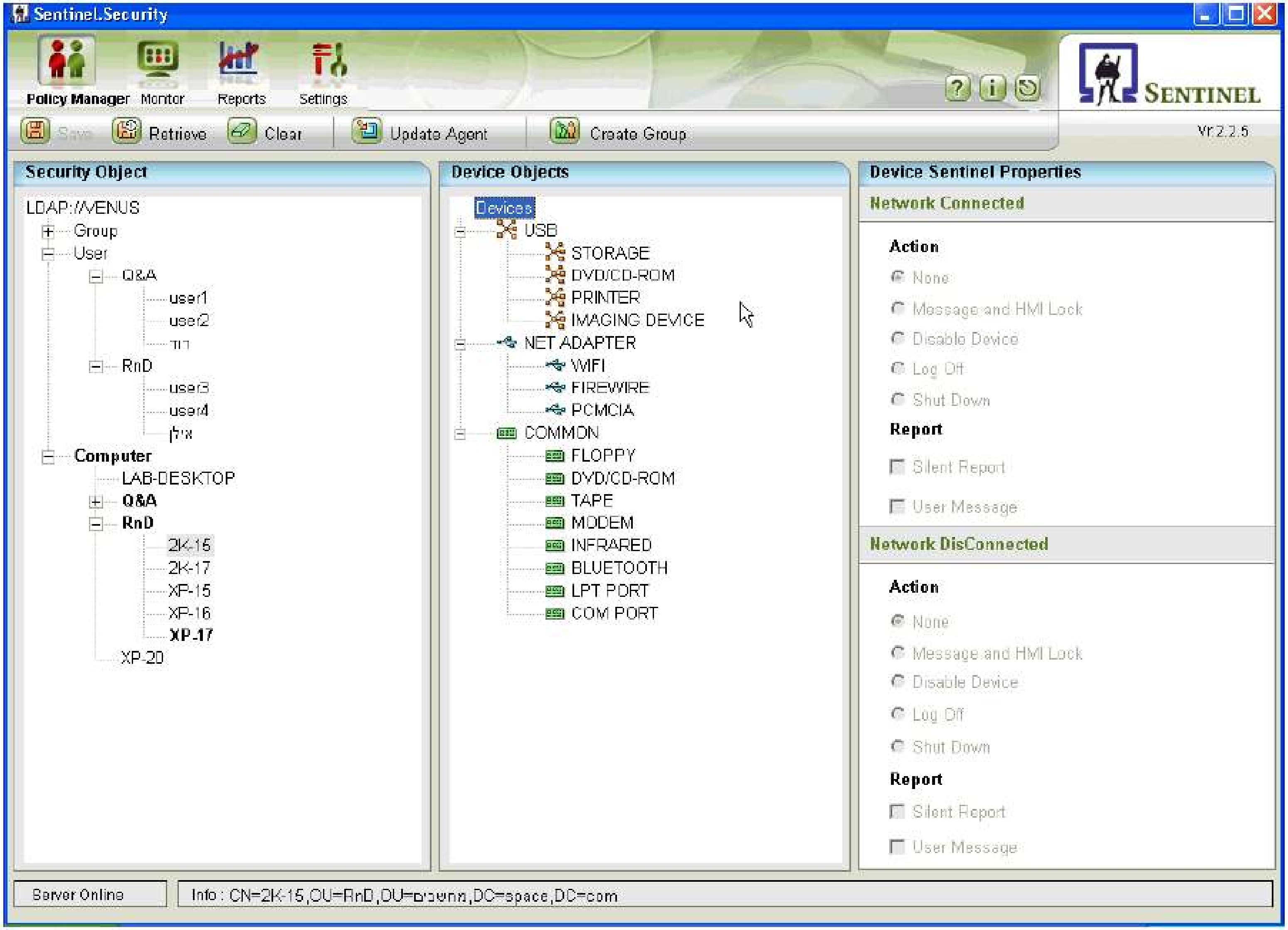
The lists of users, groups and computers are retrieved from the Active Directory of the domain. A "Default Policy" can be configured by the administrator to be the effective policy for users (or computers) not managed in the Active Directory.

When a device is connected, the agent sends an event message to the server. This log includes details of the device, user and computer properties and the time of occurrence. Locally, the agent logs this event into the OS event log. If the event occurred at a time the computer was disconnected from the network, the event is stored and at reconnection dispatched to the server.

In the server, the event details are stored in the database table and also sent to the connecting consoles for the update of the online monitor. Event reports can be created by querying the database. A console report screen enables the creation of reports from some predefined templates.

Lamda SENTINEL™ is a field-proven product with excellent feed-back from clients that already use it as a fully commercial product or as a successful pilot. The following table represents several differences between Lamda SENTINEL™ and its direct competitors:

#	Characteristics	SENTINEL	Others
1	Real time monitoring	yes	Y / N
2	Supported devices	All	Limited
3	Hierarchy levels (Groups, Users, Computers)	3 levels	Limited
4	Immunity	Very robust	Low-medium
5	Compatible with Personal Firewalls (SP2)	Yes	Limited
6	Smooth assimilation with enterprise network	Easy	
7	Local Administrator definition at endpoints	No Need	
8	Reaction Type	7 x 2	≤ 4
9	Friendly user interface	Yes	Medium
10	Data Base Interface	Several	
11	Work in Safe mode	Yes	
12	Improved specific device list	Yes	Y / N
13	Read only option	Yes	Y / N



Vr 2.2.5

Security Object

LDAP://VENUS
- Group
- User
  - Q&A
    - user1
    - user2
    - דוד
  - RnD
    - user3
    - user4
    - אילן
- **Computer**
  - LAB-DESKTOP
  - **Q&A**
  - **RnD**
    - 2K-15
    - 2K-17
    - XP-15
    - XP-16
    - **XP-17**
  - XP-20

Device Objects

Devices
- USB
  - STORAGE
  - DVD/CD-ROM
  - PRINTER
  - IMAGING DEVICE
- NET ADAPTER
  - WIFI
  - FIREWIRE
  - PCMCIA
- COMMON
  - FLOPPY
  - DVD/CD-ROM
  - TAPE
  - MODEM
  - INFRARED
  - BLUETOOTH
  - LPT PORT
  - COM PORT

Device Sentinel Properties

Network Connected

Action

● None

○ Message and HMI Lock

○ Disable Device

○ Log Off

○ Shut Down

Report

☐ Silent Report

☐ User Message

Network DisConnected

Action

● None

○ Message and HMI Lock

○ Disable Device

○ Log Off

○ Shut Down

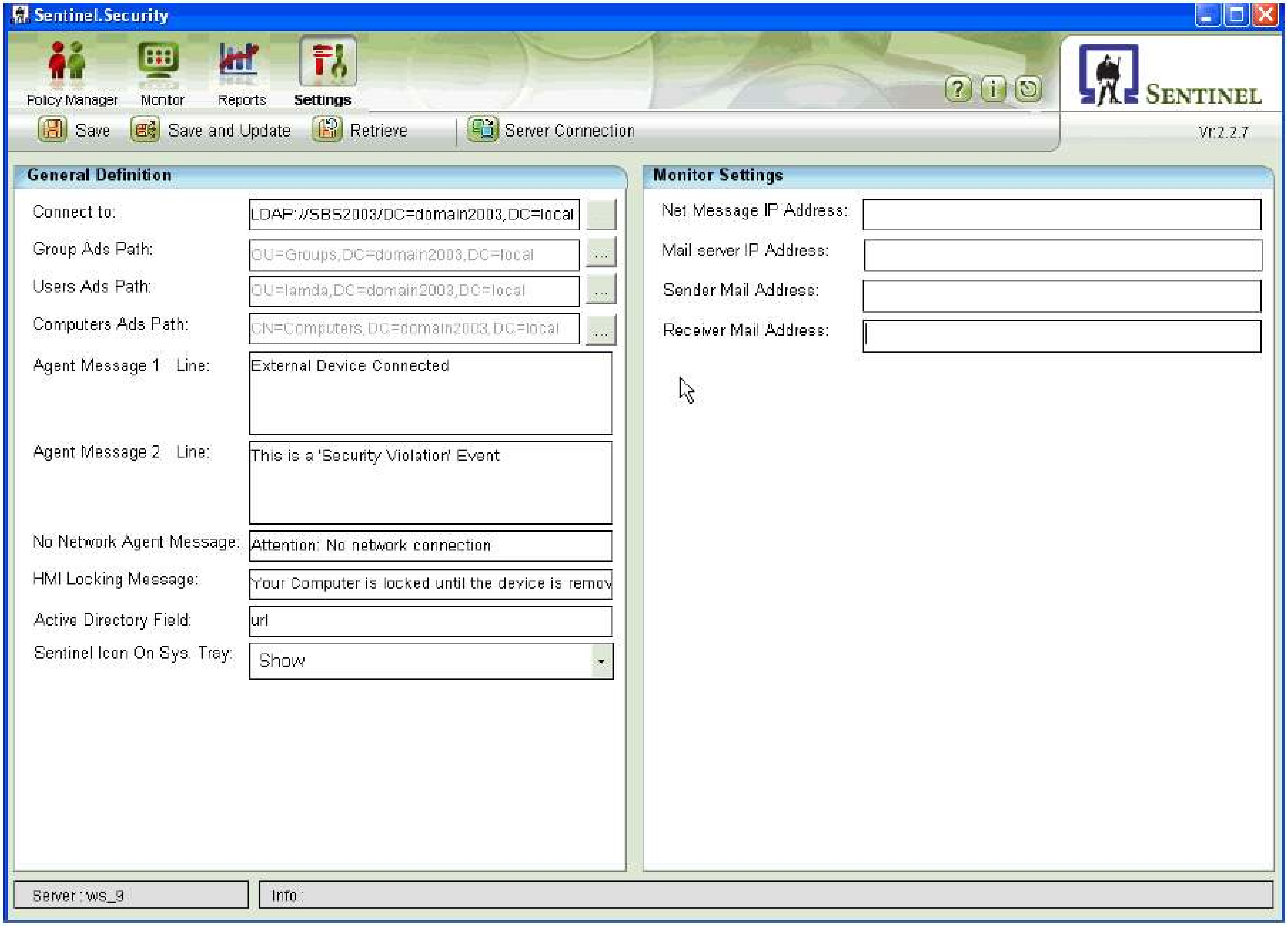
Report

☐ Silent Report

☐ User Message

Server Online

Info : CN=2K-15,OU=RnD,OU=מחשבים,DC=space,DC=com



General Definition

Connect to: LDAP://SB52003/DC=domain2003,DC=local

Group Ads Path: OU=Groups,DC=domain2003,DC=local

Users Ads Path: OU=lamda,DC=domain2003,DC=local

Computers Ads Path: CN=Computers,DC=domain2003,DC=local

Agent Message 1 Line: External Device Connected

Agent Message 2 Line: This is a 'Security Violation' Event

No Network Agent Message: Attention: No network connection

HMI Locking Message: Your Computer is locked until the device is remov

Active Directory Field: url

Sentinel Icon On Sys. Tray: Show

Monitor Settings

Net Message IP Address:

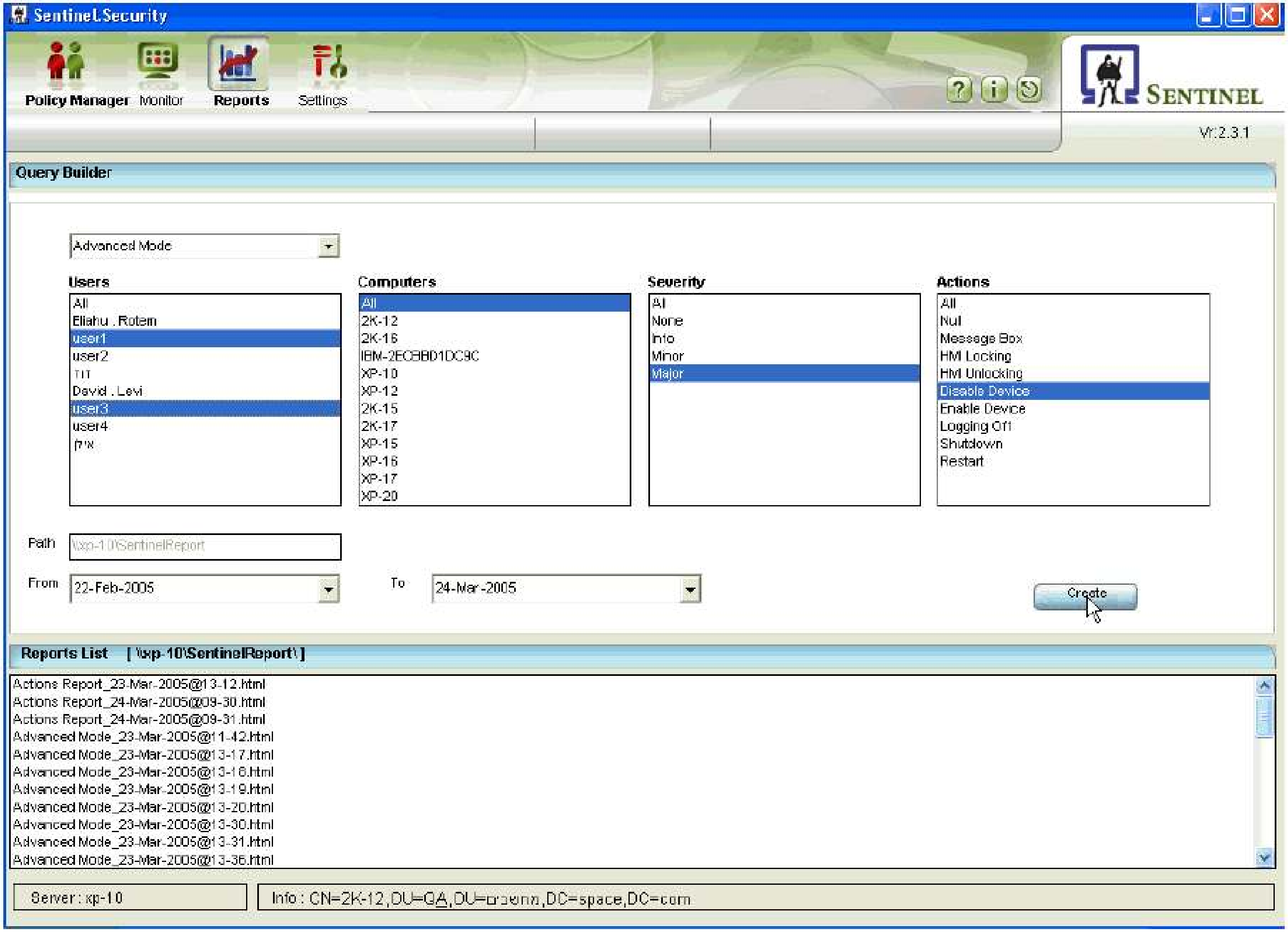
Mail server IP Address:

Sender Mail Address:

Receiver Mail Address:

Server : ws_9

Info :



Query Builder

Advanced Mode

Users
All
Eliahu . Rotem
user1
user2
דוד
David . Levi
user3
user4
איק

Computers
All
2K-12
2K-16
IBM-2ECBBD1DC9C
XP-10
XP-12
2K-15
2K-17
XP-15
XP-16
XP-17
XP-20

Severity
All
None
Info
Minor
Major

Actions
All
Nul
Message Box
HM Locking
HM Unlocking
Disable Device
Enable Device
Logging Off
Shutdown
Restart

Path: \\xp-10\SentinelReport

From: 22-Feb-2005

To: 24-Mar-2005

Reports List [\\xp-10\SentinelReport\ ]

Actions Report_23-Mar-2005@13-12.html
Actions Report_24-Mar-2005@09-30.html
Actions Report_24-Mar-2005@09-31.html
Advanced Mode_23-Mar-2005@11-42.html
Advanced Mode_23-Mar-2005@13-17.html
Advanced Mode_23-Mar-2005@13-18.html
Advanced Mode_23-Mar-2005@13-19.html
Advanced Mode_23-Mar-2005@13-20.html
Advanced Mode_23-Mar-2005@13-30.html
Advanced Mode_23-Mar-2005@13-31.html
Advanced Mode_23-Mar-2005@13-36.html

Server : xp-10

Info : CN=2K-12,OU=QA,OU=מחשבים,DC=space,DC=com

2. Detailed Description Table

2.1. Overview

Subject	Reply
Steps required to install Sentinel.	Installation of Lamda SENTINEL™ is performed using the following steps: 1. Creation of a database schema on a server running SQL Server (optional for usage of this specific db). A System DSN to the created database (optional creation of Access db) is needed for the next step. 2. Installation of Lamda SENTINEL™ Server on designated station/server. 3. Installation of Lamda SENTINEL™ Console on the administrator station. Setup of parameters. 4. Installation of Lamda SENTINEL™ agents on network computers (installation via an installation tool is recommended).
Industry certifications attained by the product	Lamda Systems Engineering, the mother company is ISO9001/2000 certified and the companies have adopted strict and standard internal regulations.
Is there a client side GUI? If so, is it possible to run the client without the GUI? a) If there is a client side GUI, is it easily brandable? b) Localization capabilities if applicable? If the agent can be run without the GUI, is there a way to manage the agent? If so, what is it?	The client side does not require a GUI. Agents are managed remotely via server controls only. The end user is blocked from changing the setup the administrator has configured.

2.2. Platform Support

Platform	Version	Supported
Windows NT 4.0 Workstation	None	-
Windows 2000 Professional	No SP, SP1-SP4	√
Windows 2000 Server Family	SP4	√
Windows 2003 Server Family	Enterprise	√
Windows XP Home	SP2	√
Windows XP Pro	No SP, SP1, SP2	√
Windows XP Tablet PC Edition		Not tested
Windows Media Center Edition 2005		√
Windows Vista		√

2.3. Alternative Hardware Access Points Supported

Technology	Supported
USB 1.1	√
USB 2.0	√
Firewire (IEEE 1394)	√
PCMCIA	√
Serial	√
Parallel	√
WiFi	√
Bluetooth	√
IrDA	√
Keyboard (PS/2)	√
Mouse (PS/2)	√
CD/DVD –R/RW	√
Hot-Swap device port (on notebook systems)	√
Floppy	√
S-ATA	√

2.4. Protective Schemes

Subject	Reply
Support for defining access, based on wireless encryption?	Wireless access control is available at adapter level.
Authorization to a device based on recognition and matching of a device class?	The supported classes are: Floppy, CD/DVD, Removable Storage, Tape, Imaging device, Printer, Modem, Windows CE device, Palm OS device, Other USB connected classes (i.e. eToken, Cryptographic) , PCMCIA adapters, Network adapter, Ports, IEEE 1394 controller.
Authorization to a device based on recognition and matching of a device product ID?	Via the specific device policy.
Authorization to a device based on recognition and matching of a unique device ID?	The user can choose whether a specific device is identified based on product ID or unique device ID.
Can the agent be instructed via policy to allow a normally barred device (based on class, product, and/or unique device ID) to exclude and allow a specific unique device ID access? Please explain how.	Yes, a policy for a device usually includes the policy set for the device class. The administrator can add any specific device (based on product and/or unique ID) to the policy set. The client always checks and enforces the policy for the specific device before the class policy.
WiFi Protection: Can authorization be set by SSID, WiFi Channel, access point MAC address?	WiFi protection is implemented at the adapter level.
Can each of the protections on each agent be turned on and off independently of each other?	Yes.
Is the agent capable of protecting itself from user or external, non-authorized tampering techniques? If so, explain how this is achieved.	Yes, the agent has a built-in immunity against tampering. The processes have system privileges and persistent data is hidden in a private registry. Agents react only to messages received from the server they

Subject	Reply
	are signed in to. Uninstall action is permitted under the restriction that the administrator allowed it at the management console. The agent guards files security permissions.
Does an authorized administrator have a way to override the security restrictions set on the agent without access to the management console? If so, please explain how.	No, for reasons of immunity, we have banned such a possibility.

2.5. Management

Subject	Reply
Is there a remote management element?	Yes, the management contains a console (GUI) element that can be installed on any computer with access to the network. The console is connected to the server application that controls all installed agents in the network.
Is the security policy enforced by an agent based on user logged in, system ID, etc.?	The policy is based on the logged on user and the station ID. The client retrieves from the server the policy for the user and station objects along with the policy for the groups for which these objects are members. The actual enforced policy follows the following order of precedence: 1. Computer 2. User 3. Group of Computers 4. Group of Users.
Is there a management console to create and instruct the agents of the security policy in effect?	All policies are stored by the server in the database. The policy is created in the management console and sent to the server to store and update the agents.
Does a security policy get pushed down by the management console or is it pulled by the agents?	The security policy is pulled by the agent at system startup, login and whenever a connection to the network is renewed. In the management console an "Update Agents" action allows the administrator to manually signal to agents to reread their policy.
Does the management console require a dedicated system?	The management server can run on any station on the network. In small networks the management server does not require a dedicated system. The management console (GUI) can be installed on any station on the network. Multiple consoles can coexist.

Subject	Reply
What would be the typical system requirements for a management console managing 1000 agents? 10,000 agents? 100,000 agents?	Up to 10,000 agents: Intel Pentium 4 2 GHz computer with 512 MB RAM can run the server and database applications on the same system. Above 10,000 agents: it is recommended that database and server applications run on separate computers. Networks of 100,000: agents should be managed by several servers.
Is there any fault tolerance and/or fail-over capabilities built into the management console?	The Lamda SENTINEL™ agent saves the allocated policy in a persistent storage, allowing for states where no server responses are available. In these cases the local policy is enforced. Server unavailability causes restrictions on policy changes only. The rest of the system functions as designed. When desired, redundancy of the server application can be achieved by a fail-over cluster configuration.
Does the management console require a dedicated database for operation? If not, please explain how policy and agent data is stored.	Yes, the server uses a dedicated database for operation.
If a database is required, what database platforms are supported?	The supported databases are: SQL Server 2000, MSDE, .Jet (Access) and MySQL.
Does the management console require a dedicated database schema, instance, or etc.?	The management requires a dedicated schema.
Does the creation and assignment of the security policy support Active Directory accounts?	Yes
Does the creation and assignment of security policy support LDAP Directory (normal and/or Secure LDAP) accounts? What authentication types are supported?	LDAP directory accounts are supported via a normal connection. Secure connections can be added with minor modifications.
Upon action, does the agent provide an explanation to the end user of the blocked action?	Yes, if the administrator chooses that option in the policy. The displayed message (to the end user) includes an

Subject	Reply
a) Is this a generic message built into the agent? (i.e. “You’ve attempted to access a restricted device”) b) If not, does it contain any specifics as to which AHAP and device was involved? (i.e. “You’ve attempted to access a Belkin Flash device attached to your USB port”) c) Can the administrator customize the end user messages? d) Can the administrators create multiple messages, depending on user, machine, domain, etc. of where the event occurred?	administrator customized text and the details of the involved device. Example: An external device connection was detected! Device: "M-Sys DiskOnKey USB device" The message customization is system wide.
Can the agent settings be set via command line execution? a) Can a security policy be set via the command line? Does the client support XML policy? If so, what’s the spec?	The agent can receive settings only through its server communication in order to prevent tampering.
Describe remote management capabilities Is there a remote management SDK?	The remote capabilities of the agent include the following: 1. Operational parameter settings such as: a. License details b. Keep Alive frequency, c. User displayed texts d. Local logging flag e. Icon display 2. Suspend/Resume command 3. Uninstall enabling/disabling 4. Controlling Server address 5. Policy updated indication 6. User initiated Keep Alive message

2.6. *Installation*

Subject	Reply
Installer size?	Agent - 350 KB Server - 500 KB Console - 1 MB
Installer type?	MSI package
Is silent install possible?	Yes, for the client side.
If installed by one user, would it work for other users on the same machine?	Yes, installation is per machine regardless of the user that installed it.
Is it possible to change permissions on the fly (e.g. go from USB is read-only to USB is read/write)?	Yes.
Is it possible to ask the user for permission at real-time (e.g. detect USB auto execution, put it on hold, ask the user, kill or allow based on user's response)?	The user is not allowed to affect the policy assigned by the administrator in any way.
Can agents be installed remotely? How?	Yes, using any installation tool that can deploy MSI packages.
Can agents be installed using SMS and GPO?	Yes.
Can agents be installed silently (without user intervention)?	Yes.
What applications are required to be turned off for agent installation, if any?	None
List any known conflicts between your agent application and any other known application?	None
Does the agent installation require administrative-level access to the endpoint system?	Identical to other installed software.

Subject	Reply
What is the size of the current agent installation package?	350 KB
What user documentation is provided with your product?	Installation and user manual.
In what format is the documentation?	Word and PDF.
Is the agent application localized? If so, list all languages it has been localized in. Also list future plans for localization and estimated release dates for each.	User messages displayed by the agent are customized at the management console in any locale the administrator chooses to setup Windows. The agent does not include a GUI therefore no localization is required.
Is the management console localized? If so, list all languages it has been localized in. Also list future plans for localization and estimated release dates for each.	At this time we support English only at the management console.

2.7. *Logging, Reporting and Performance*

Subject	Reply
Does the agent log each protected event? a) Are allowed access events logged on the agent? b) Are blocked access events logged on the agent? c) Are administrative (override) access events logged on the agent? (if applicable) d) Are policy-change events logged on the agent? What is the expected log size for average use?	The agent sends, in real time, a log message to the server concerning access to any monitored device. In addition, the agent logs blocked access events locally in the system event log. Policy change events are sent to the server (acknowledge) but are not logged locally. Assuming 3 event occurrences per day the local log entries size are 1 KB/day
What format does the agent use to store logged events?	Locally, Windows Event Log.is used. Proprietary format (binary) is sent to the server.
How often are agent event logs uploaded to the management console?	Lamda SENTINEL™ system uses a real time events reporting scheme, therefore no periodic uploading of log files exist.
If the agent has no connectivity to the management console, how are event logs treated? a) Can limits be set on the size of agent logs? What log file controls are built into the agent?	Events are stored locally by the agent until reconnection occurs and then the events are transmitted to the server. Event log entries are independently locally entered as well.
Can limits be set on the size of management console logs?	At present, no limits are set on management logs.
What log file controls are built into the management console?	At present, no log file controls are built into the console.
Please list ALL the fields included in an event log.	The fields of an event log are: ▪ Computer name ▪ Domain name ▪ User name ▪ IP address

Subject	Reply
	▪ Agent version ▪ Occurrence time (date, time, time zone) ▪ Arrival time (date, time, time zone) ▪ Severity code ▪ Device ID ▪ Device description ▪ Message ID ▪ Policy
What are the minimal system requirements for proper agent operation? What are the optimal system requirements for proper agent operation?	The agent usage of system resources is negligible therefore any computer accommodating the Windows 2000 operating system requirements is suitable for the agent operation.
What are the average CPU, memory, and other system resource loads added by an active agent enforcing the security policy on an endpoint?	Peak of 2% CPU time for 2 seconds at event occurrence. Average of 3 MB of memory use.
What Reports are provided, please provide examples?	Reports of events are created by queries to the database. Provided templates include query by user name, computer name, policy action or severity. An advanced mode enables an AND query of these fields. The user can create specific queries and save them for later use.
How are endpoints identified in Reports?	Endpoints are identified by the computer name.