



US 20090265754A1

(19) **United States**

(12) **Patent Application Publication**
HINDS

(10) **Pub. No.: US 2009/0265754 A1**

(43) **Pub. Date: Oct. 22, 2009**

(54) **POLICY ENFORCEMENT IN MOBILE DEVICES**

Publication Classification

(51) **Int. Cl.**
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **726/1**

(57) **ABSTRACT**

(75) **Inventor:** **Donald W. HINDS**, Alpharetta, GA
(US)

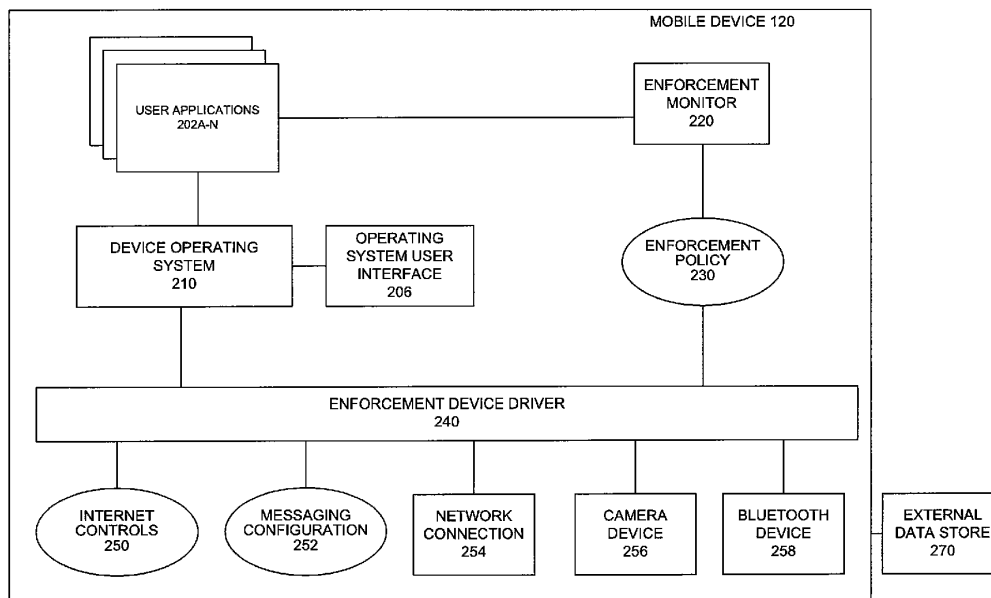
Correspondence Address:
Sterne, Kessler, Goldstein & Fox P.L.L.C.
1100 New York Avenue, N.W.
Washington, DC 20005 (US)

(73) **Assignee:** **Sybase, Inc.**

(21) **Appl. No.:** **12/105,003**

(22) **Filed:** **Apr. 17, 2008**

Systems, methods and computer program products for enabling enforcement of an administrative policy on one or more mobile devices are described herein. In an embodiment, an administrator uses a policy server to create and provide an enforcement policy to a mobile device. An enforcement policy may include information on mobile device resources which may be controlled by an administrator. An enforcement policy also includes information on how mobile device features will be set, configured or disabled. An enforcement device driver and an enforcement monitor on a mobile device use the enforcement policy to control access to resources associated with the mobile device regardless of whether the mobile device is "online" and connected to a network or "offline" and disconnected from a network.



100

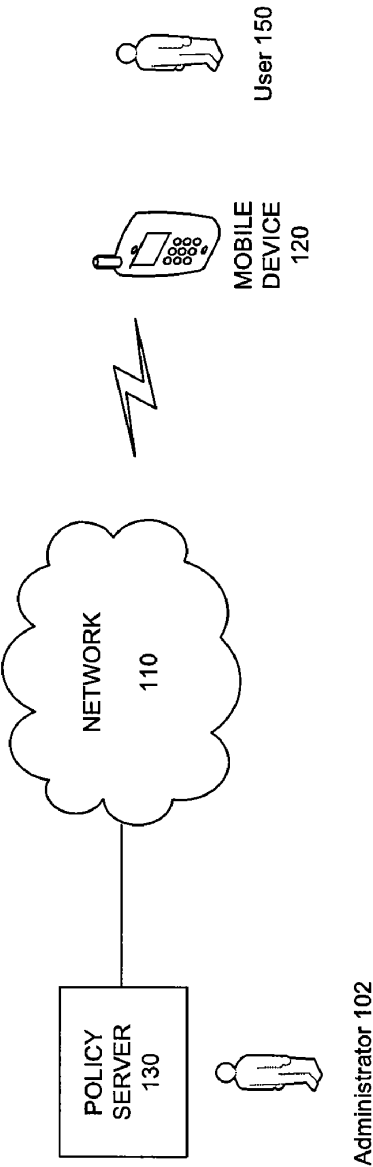


FIG. 1

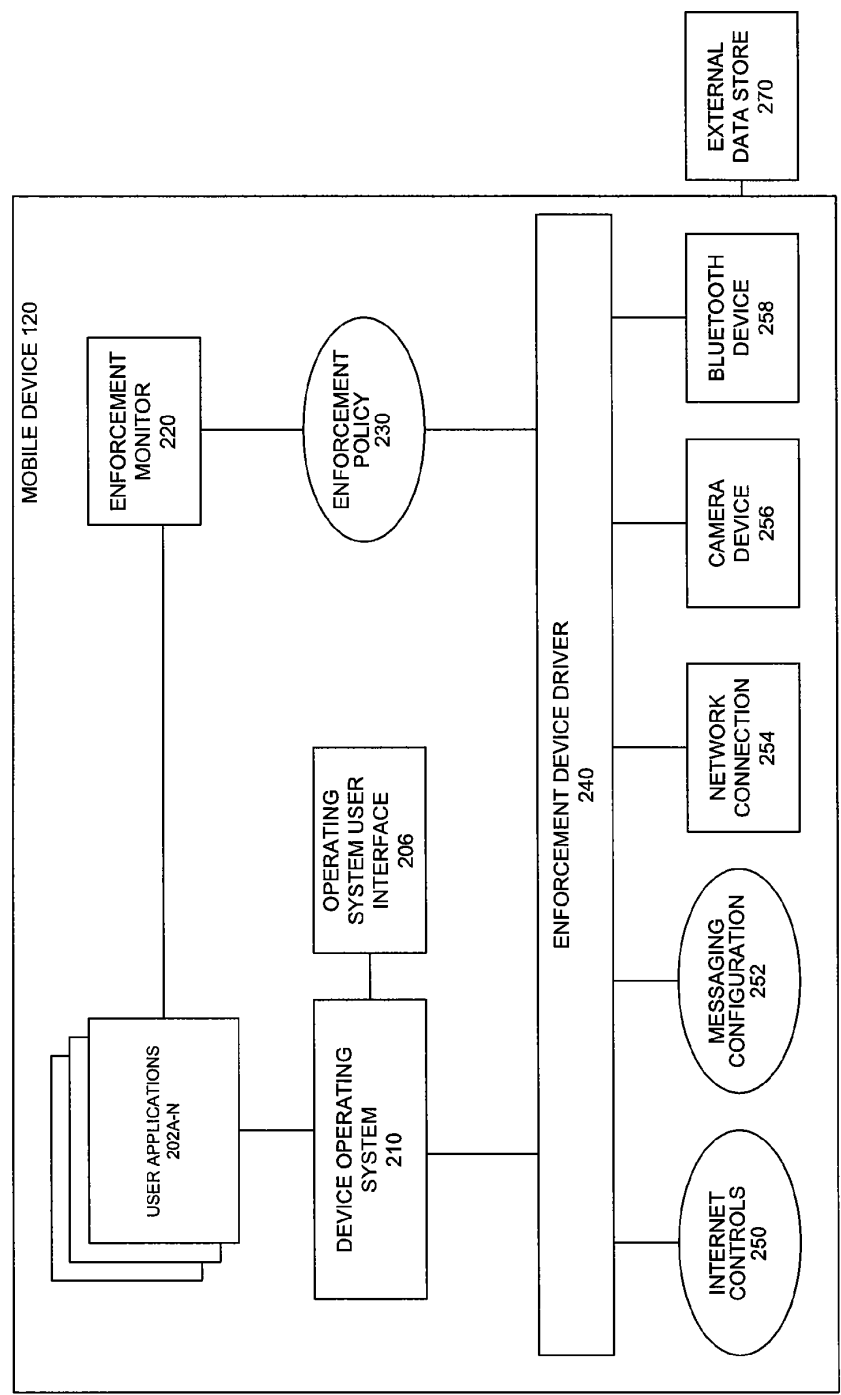
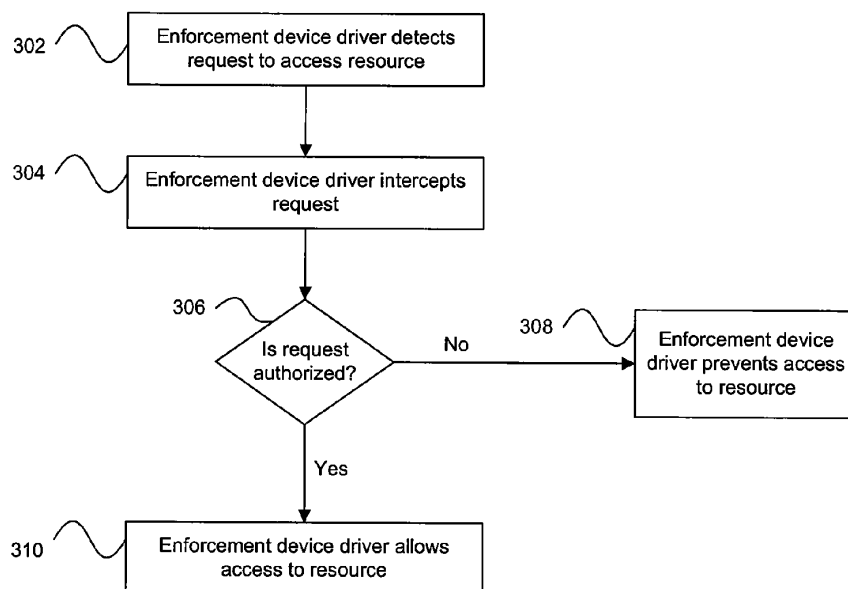
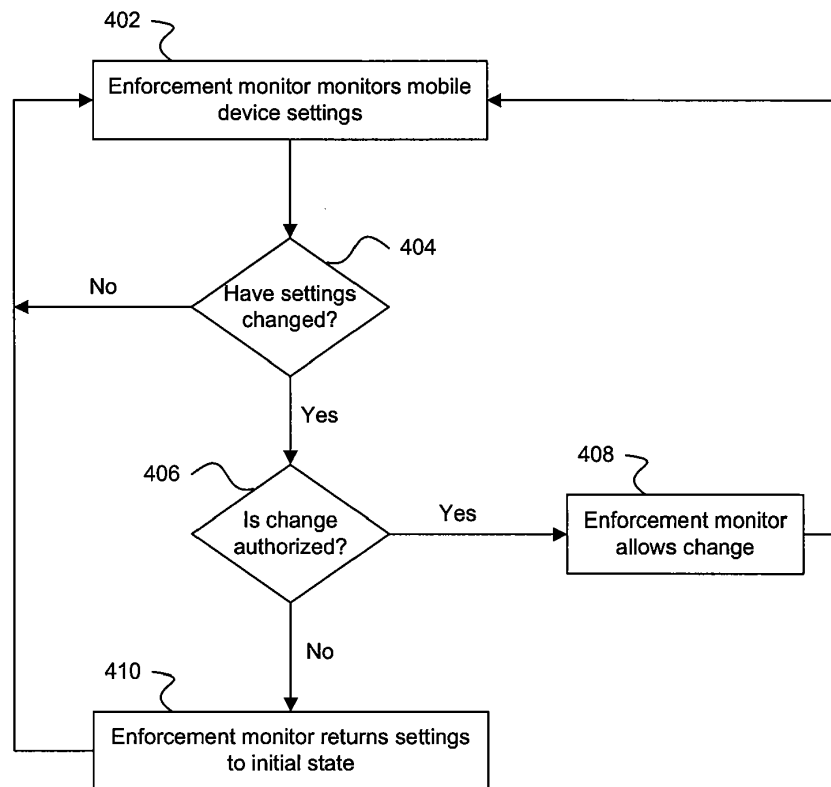


FIG. 2

300**FIG. 3**

400**FIG. 4**

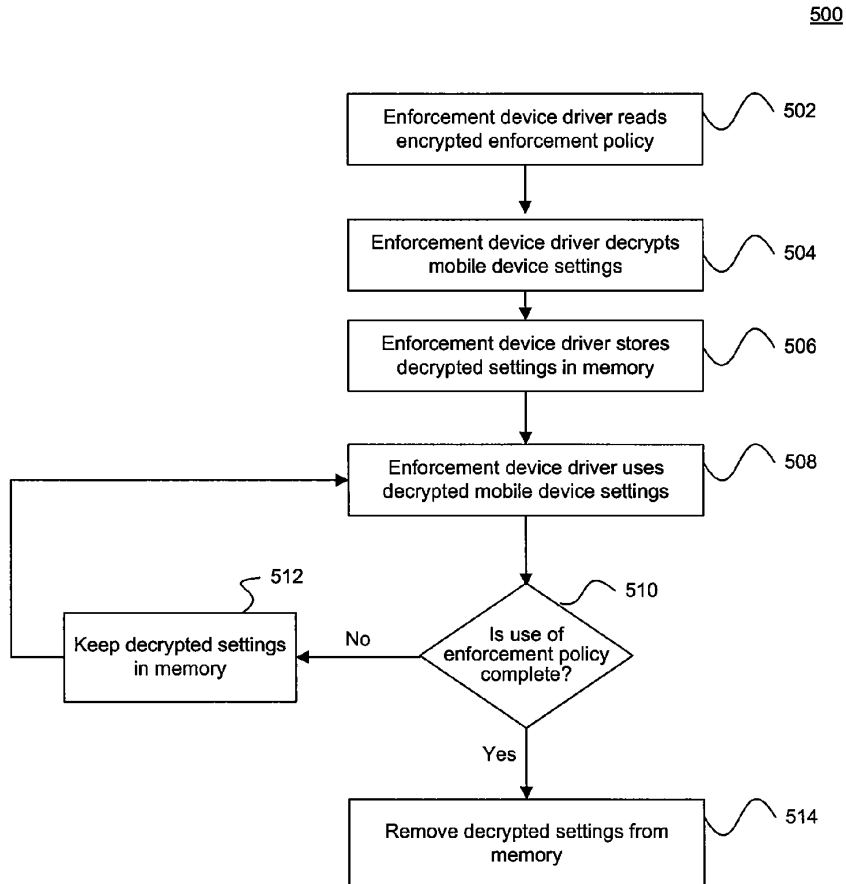


FIG. 5

600

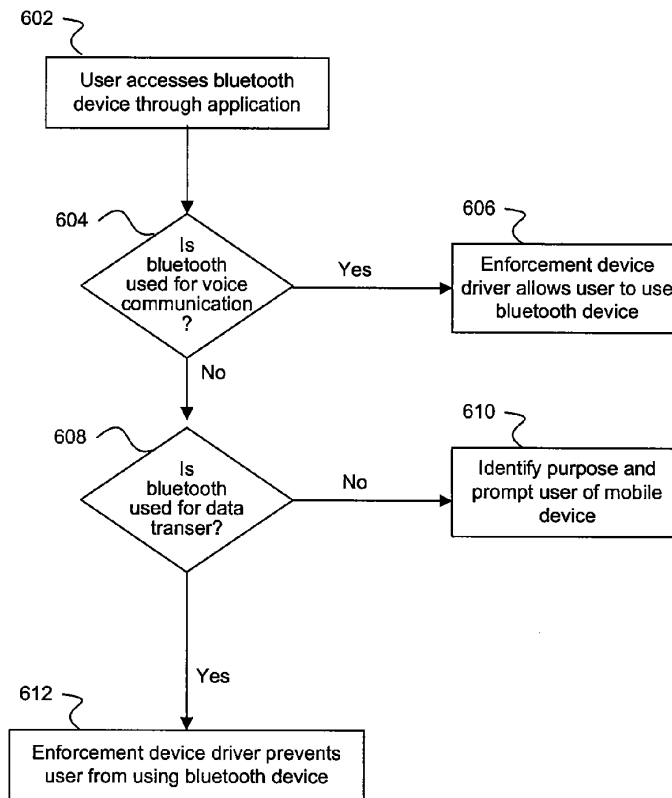
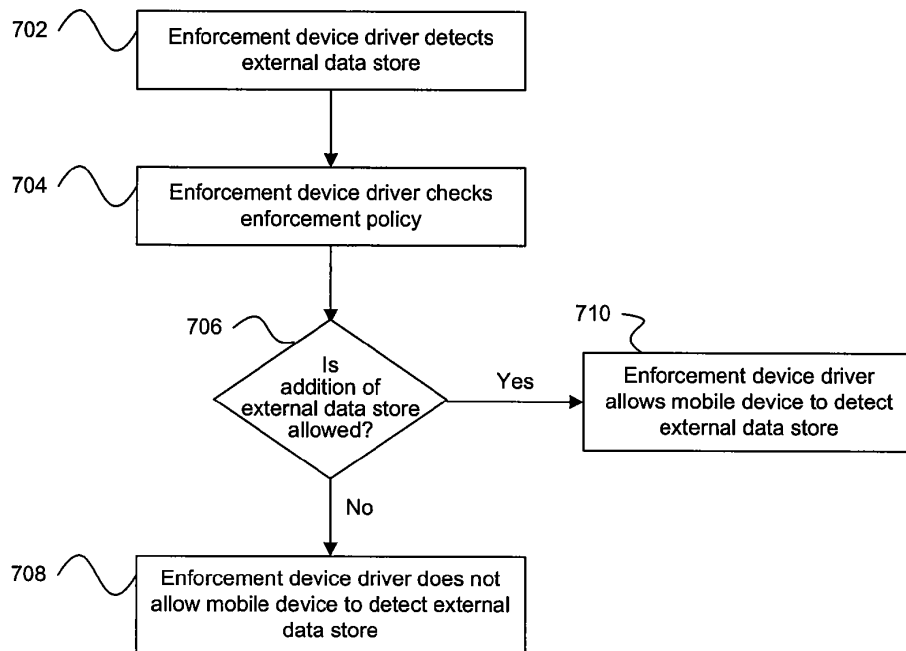


FIG. 6

700**FIG. 7**

802

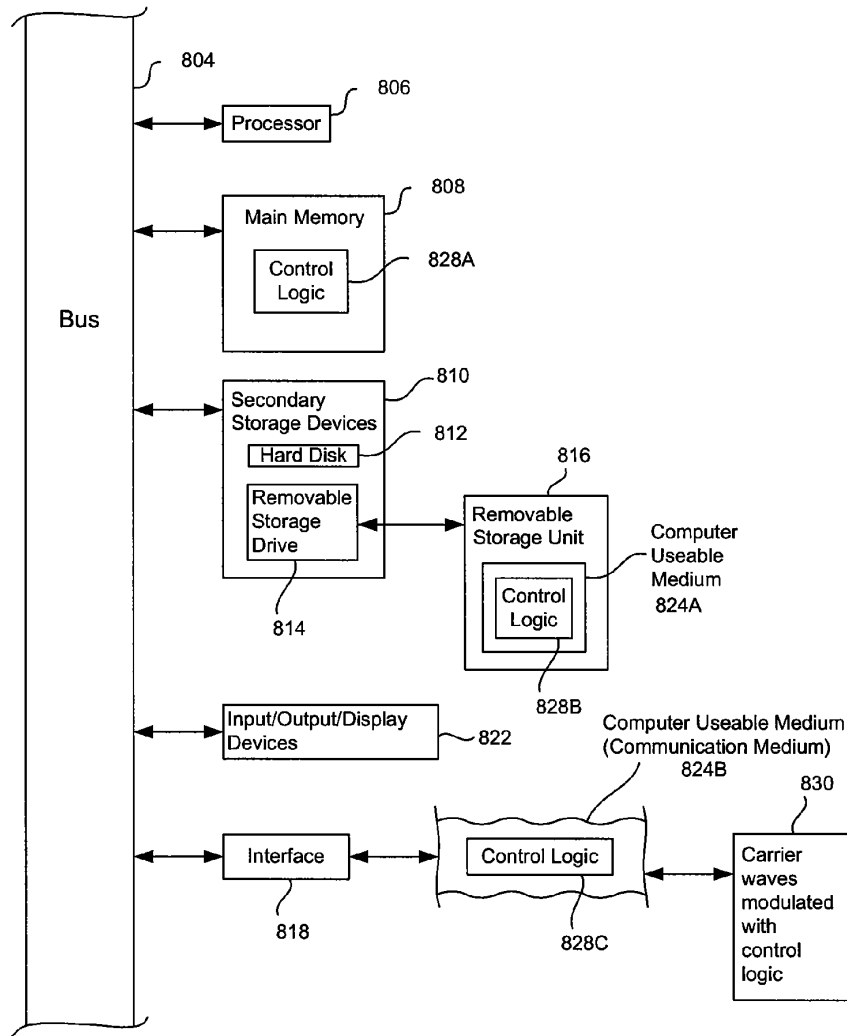


FIG. 8

POLICY ENFORCEMENT IN MOBILE DEVICES

BACKGROUND

[0001] 1. Field of the Invention

[0002] The present invention relates generally to mobile technology, and more particularly to the enforcement of an administrative policy on a mobile device.

[0003] 2. Related Art

[0004] A variety of mobile devices (such as personal data assistants, or PDAs, handheld computers, cellular phones, pagers, etc.) exist. Such mobile devices include ones based on the Palm operating environment and the Windows CE operating environment.

[0005] Mobile devices are being increasingly used across organizations where several employees are provided with mobile devices which enable them to communicate with their respective organizations or access sources of information.

[0006] Each user of a mobile device may have a different purpose of use or a different pattern of use relative to other users. For example, one user may need only email access while another user may need both Internet and email access. Furthermore, it may be the policy of an organization, for example, to allow employees Internet access but block them from accessing certain web sites on the Internet. Other policies may also include selective access to organizational resources or blocking users from using certain applications on their mobile devices (such as camera, Bluetooth, etc.) It may also be necessary to prevent users from modifying policies set by an administrator of a network even when a mobile device is offline or disconnected from the network.

[0007] Therefore, what is needed is a system, method and computer program product that enables enforcement of an administrative policy deployed by an administrator on a mobile device.

BRIEF SUMMARY

[0008] Briefly stated, the invention includes system, method, computer program product embodiments and combinations and sub-combinations thereof for enabling enforcement of an administrative policy on one or more mobile devices. In an embodiment, an administrator uses a policy server to create and provide an enforcement policy to a mobile device. The enforcement policy may include information on mobile device resources which may be controlled by an administrator and resources to which a user may or may not have access. The enforcement policy may also include information on how mobile device features may be set, configured or disabled.

[0009] An enforcement device driver and an enforcement monitor in a mobile device use the enforcement policy to control access to resources associated with the mobile device regardless of whether the mobile device is "online" and connected to a network or "offline" and disconnected from a network.

[0010] In this way, an administrator may control mobile device resources available to a user.

[0011] Further embodiments, features, and advantages of the invention, as well as the structure and operation of the

various embodiments of the invention are described in detail below with reference to accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The accompanying drawings, which are incorporated herein and form part of the specification, illustrate embodiments of the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the relevant art(s) to make and use the invention.

[0013] FIG. 1 is an architecture diagram of a system to enable deployment of an enforcement policy, according to an embodiment of the invention.

[0014] FIG. 2 is an architecture diagram of a mobile device, according to an embodiment of the invention.

[0015] FIG. 3 is a flowchart illustrating processing of a request to access mobile device resources, according to an embodiment of the invention.

[0016] FIG. 4 is a flowchart illustrating operation of an enforcement monitor, according to an embodiment of the invention.

[0017] FIG. 5 is a flowchart illustrating decryption and encryption of mobile device settings, according to an embodiment of the invention.

[0018] FIG. 6 is a flowchart illustrating exemplary processing of a request to access a Bluetooth device according to an embodiment of the invention.

[0019] FIG. 7 is a flowchart illustrating detection of an external data store based on an enforcement policy, according to an embodiment of the invention.

[0020] FIG. 8 illustrates an example computer useful for implementing components of the invention.

[0021] The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. Generally, the drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

DETAILED DESCRIPTION

[0022] The present invention relates to systems, methods and computer program products for enabling enforcement of an administrative policy on a single or a fleet of mobile devices. In an embodiment, an administrator uses a policy server to create an enforcement policy. An enforcement policy may include information on mobile device resources which may be controlled by an administrator and resources to which a user may or may not have access. An enforcement policy also includes information on how mobile device features may be set, configured or disabled.

[0023] An enforcement device driver and an enforcement monitor in a mobile device use the enforcement policy to control access to resources associated with the mobile device regardless of whether the mobile device is "online" and connected to a network or "offline" and disconnected from a network.

[0024] While the present invention is described herein with reference to illustrative embodiments for particular applications, it should be understood that the invention is not limited thereto. Those skilled in the art with access to the teachings provided herein will recognize additional modifications,

applications, and embodiments within the scope thereof and additional fields in which the invention would be of significant utility.

System

[0025] FIG. 1 illustrates a general system architecture for enabling deployment of an enforcement policy on one or more mobile devices, according to an embodiment of the invention. (While the following is described in terms of mobile devices, the invention is not limited to this embodiment. The invention is applicable to any system having generally the structure of FIG. 1, or that would benefit from the functions as described herein.)

[0026] Network 110 can be any type of network or combination of networks such as, but not limited to, a local area network, wide area network or the Internet. Network 110 may be a form of a wired network or a wireless network, or a combination thereof. Network 110 may allow policy server 130 and mobile device 120 to communicate with each other.

[0027] Mobile device 120 can include, but is not limited to, a device having a processor (or state machine) and memory for executing and storing instructions. Mobile device 120 includes, but is not limited to, PDAs, cell phones, game devices, music devices, portable multimedia devices etc. (While a single mobile device 120 is shown in FIG. 1, in practice the invention operates with any number of mobile devices.) Such a mobile device may include software, firmware, and hardware or some combination thereof. The software may include one or more applications and an operating system. The hardware can include, but is not limited to, a processor, memory and user interface display. An optional input device, such as a mouse, stylus or any other pointing device, may be used. An exemplary architecture of mobile device 120 according to an embodiment of the invention is described below in further detail.

[0028] Policy server 130 allows administrator 102 to create an enforcement policy according to an embodiment of the invention. Policy server 130 has the ability to communicate over network 110. As an example, policy server 130 may provide an enforcement policy to mobile device 120 over network 110. In an embodiment, policy server may encrypt an enforcement policy using any well known encryption technique or technology before it is provided to mobile device 120 over network 110.

Mobile Device

[0029] FIG. 2 is an architecture diagram of a mobile device 120 according to an embodiment of the invention.

[0030] Mobile device 120 includes enforcement monitor 220, enforcement policy 230, enforcement device driver 240, device operating system 210, user application(s) 202A-N, and operating system interface 206. Mobile device 120 may further include internet controls 250, messaging configuration 252, network connection 254, camera device 256, Bluetooth device 258 and external data store 270 which may be connected to mobile device 120. Mobile device 120 can include other functional modules, and/or combinations or sub-combinations of the modules described herein.

[0031] Mobile device 120 may receive enforcement policy 230 from policy server 130 over network 110. Enforcement policy 230 could also be pre-installed, manually installed or installed through any other method. As an example, not intended to limit the invention, mobile device 120 may

receive enforcement policy 230 from policy server through a message transmitted using the short messaging service (SMS). SMS is known to persons skilled in the art as a method to transmit short messages to mobile devices across wireless networks.

[0032] User application(s) 202A-N may be any type of applications that can be instantiated on mobile device 120 by user 150. Such an application includes, but is not limited to, a word processing application, a spread sheet application, a mail application, a financial application, a browser and forms of voice, video and multimedia applications or any other application that makes use of data.

[0033] Device operating system 210 may be any operating system that may be used for operation of mobile device 120. As an example, but without limitation, device operating system 210 may be the Palm or the Windows CE operating system, or an operating system based on Linux. These examples are illustrative and are not intended to limit the invention. User 150 may interact with device operating system 210 using operating system user interface 206.

[0034] Enforcement policy 230 may include information regarding resources on a mobile device that can be controlled by administrator 102. Furthermore, enforcement policy 230 may describe how features of mobile device 120 may be set, configured or disabled. Exemplary resources or features that may be controlled by enforcement policy 230, include, but are not limited to:

- [0035]** 1. Cellular Network Connections
- [0036]** 2. Internet Connections and Security Configuration
- [0037]** 3. Infrared Ports
- [0038]** 4. WiFi Connections
- [0039]** 5. Microphones
- [0040]** 6. Device Cameras
- [0041]** 7. Device Memory Expansion Slots
- [0042]** 8. Device USB Connectivity
- [0043]** 9. Device Bluetooth Connectivity
- [0044]** 10. Owner Information for Device
- [0045]** 11. Email and Text Messaging Configuration

[0046] Additionally, enforcement policy 230 may control or enforce internet controls 250, messaging configuration 252, network connection 254, camera device 256, Bluetooth device 258 and external data store 270.

[0047] Internet controls 250 may include controls which may regulate access to certain sites on the Internet or control a manner in which mobile device 120 connects to the Internet or other networks.

[0048] Messaging configuration 252 may include information on how messages are transmitted and received by mobile device 120. For example, messaging configuration 252 may prevent user 150 from sending messages to a certain group of users associated with network 110.

[0049] Network connection 254 may include one or more connections used by mobile device 120 to access network 110. Enforcement policy 230, for example, may prevent user 150 from accessing network 110 by controlling or restricting access to network connection 254.

[0050] Camera device 256 may include any device used to obtain digital images. Enforcement policy 230 may be configured in a way as to prevent or allow user 150 from using camera device 256.

[0051] Bluetooth device 258 may include any device used to transmit or receive data using the Bluetooth protocol. Bluetooth is known to persons skilled in the art as a wireless protocol used to connect devices over a short range.

[0052] Enforcement policy 230 may control other functions and capabilities of mobile device 120, and the extent of such control is limited only by such functionality and capability of the mobile device 120.

[0053] In an embodiment, enforcement policy 230 is stored in an encrypted state on mobile device 120. As an example, policy server 130 may encrypt enforcement policy 230 created by administrator 102 before it is provided to mobile device 120. Encryption of enforcement policy 230 may prevent user 150 from modifying enforcement policy 230.

[0054] In an embodiment, not intended to limit the invention, enforcement policy 230 is encrypted using FIPS 140-2 compliant encryption. FIPS 140-2 is known to persons skilled in the art and is a U.S. government computer security standard used to accredit cryptographic modules. Some of the cryptographic algorithms used are triple DES (3DES) and advanced encryption standard (AES). However, the invention could alternatively employ any well known encryption algorithm process or technique.

Enforcement Device Driver

[0055] Enforcement device driver 240 intercepts requests for resources made by user 150 and/or user application(s) 202A-N and checks encrypted enforcement policy 230 to authorize or deny such requests. In an example, enforcement device driver 240 may restrict user 150 from taking photographs using camera device 256 by preventing requests from user 150 from being passed onto camera device 256.

[0056] Operation of enforcement device driver 240 according to an embodiment of the invention will now be described in detail with reference to flowchart 300 in FIG. 3.

[0057] In step 302, enforcement device driver 240 detects a request to access a resource associated with mobile device 120. As an example, a resource may include network connection 254 or camera device 256.

[0058] In step 304, enforcement device driver 240 intercepts the request detected in step 302.

[0059] In step 306, enforcement device driver 240 checks whether the request detected in step 302 is authorized based on enforcement policy 230. If the request is authorized, step 310 is performed. If the request is not authorized, step 308 is performed.

[0060] In step 310, enforcement device driver 240 allows user 150 or application 202 to access a resource per the request detected in step 302.

[0061] Returning to step 306, if the request is not authorized, step 308 is performed and enforcement device driver 230 prevents user 150 or application 202 from accessing the requested resource.

[0062] In this way, enforcement device driver 240 controls access to resources of mobile device 120 based on enforcement policy 230.

Enforcement Monitor

[0063] Enforcement monitor 220 monitors user applications 202A-N and any other operation that may be automatically invoked or instantiated by user 150. In an embodiment, enforcement monitor 220 may prevent user 150 from running applications which are "black-listed" or blocked by administrator 102. For example, enforcement monitor 220 may prevent user 150 from running gaming applications on mobile device 120.

[0064] In an embodiment, enforcement monitor 220 actively monitors settings associated with resources that are enforced by enforcement policy 230. If enforcement monitor 220 detects a change in the settings, enforcement monitor 220

may re-apply settings that are included in enforcement policy 230. Enforcement monitor 220 monitors enforcement policy 230 regardless of whether mobile device 220 is "online" and connected to network 110 or "offline" and disconnected from network 110.

[0065] Operation of enforcement monitor 220 according to an embodiment of the invention will now be described in detail with reference to flowchart 400 in FIG. 4.

[0066] In step 402, enforcement monitor 220 begins monitoring resources associated with mobile device 120. For example, enforcement monitor 220 may monitor user application(s) 202A-N instantiated by user 150 when mobile device 120 is powered on.

[0067] In step 404, enforcement monitor 220 checks if settings enforced by enforcement policy 230 have changed. If settings have not changed, method 400 returns to step 402. If settings enforced by enforcement policy 230 have changed, step 406 is performed.

[0068] In step 406, enforcement monitor 220 checks if the change in settings is authorized. For example, enforcement monitor 220 may read enforcement policy 230 to check if the change in settings is authorized. If the change in settings is not authorized, step 410 is performed. If a change in settings is authorized, step 408 is performed.

[0069] In step 408, enforcement monitor 220 allows the change in settings and method 400 proceeds to step 402.

[0070] Returning to step 406, if the change was not authorized, enforcement monitor 220 in step 410 returns the settings to a state determined by enforcement policy 230 or a state desired by administrator 103 and method 400 proceeds to step 402.

[0071] In this way, enforcement monitor 220 monitors and enforces settings associated with mobile device 120 regardless of whether mobile device 120 is "offline" or "online".

Encryption and Decryption of Enforcement Policy

[0072] In an embodiment, enforcement policy 230 stored in an encrypted form is decrypted when it is read by enforcement device driver 240 or enforcement monitor 220. Enforcement policy 230 is then stored back in an encrypted form on mobile device 120 in real time without any separate input from user 150 or user application(s) 202A-N.

[0073] A process illustrating real time encryption and decryption of enforcement policy 230 according to an embodiment of the invention will now be described in detail with reference to flowchart 500 in FIG. 5.

[0074] In step 502, enforcement device driver 240 reads encrypted enforcement policy 230. Enforcement policy 230 may be read, for example, when user 150 is requesting access to a resource associated with mobile device 120.

[0075] In step 504, enforcement device driver 240 decrypts mobile device settings included in encrypted enforcement policy 230. As an example, such settings may be set by an administrator 102 to control access to resources associated with mobile device 102.

[0076] In step 506, enforcement device driver 240 stores decrypted mobile device settings in memory associated with mobile device 120.

[0077] In step 508, enforcement device driver 240 uses decrypted mobile device settings in enforcement policy 230.

[0078] In step 510, enforcement device driver 240 checks if the use of enforcement policy 230 is complete. If the use of enforcement policy 230 is complete, step 514 is performed. If the use of enforcement policy 230 is not complete, step 512 is performed.

[0079] In step 512, decrypted settings associated with enforcement policy 230 are kept in memory of mobile device 120 and method 500 proceeds to step 506.

[0080] Returning to step 510, if the use of enforcement policy 230 is complete, the decrypted settings are removed from memory in step 514.

[0081] In this way, enforcement policy 230 and any settings associated with enforcement policy 230 are encrypted and decrypted in real time without any input from user 150. It is noted that the invention may be used with any well known encryption and decryption technique and algorithms.

Exemplary Control of Bluetooth Device

[0082] In some cases, administrator 102 configure enforcement policy 230 in a manner that allows use of Bluetooth device 258 for voice communication but blocks any form of data transfer over Bluetooth device 258 by user 150.

[0083] An exemplary process illustrating control of Bluetooth device 258, according to an embodiment of the invention will now be described in detail with reference to flowchart 600 in FIG. 6.

[0084] In step 602, user 150 accesses Bluetooth device 258 through user application(s) 220A-N.

[0085] In step 604, enforcement device driver 240 checks if Bluetooth device 258 is intended to be used for voice communication. If Bluetooth device 258 is to be used for voice communication step 606 is performed. If Bluetooth device 258 is not to be used for voice communication, step 608 is performed.

[0086] In step 606, enforcement device driver 240 allows user 150 to proceed with use of Bluetooth device 258.

[0087] Returning to step 606, if the device is not to be used for voice communication, enforcement device driver 240 checks if Bluetooth device 258 is used for data transfer in step 608. If Bluetooth device 258 is not used for data transfer, step 610 is performed. If Bluetooth device 258 is used for data transfer, step 612 is performed.

[0088] In step 610, enforcement device driver 240 identifies purpose of use of mobile device 240 and prompts user 150. As an example, user 150 may be prompted to provide additional input to mobile device 120 regarding the user 150's intended use of the Bluetooth functionality.

[0089] Returning to step 608, if Bluetooth device 258 is to be used for data transfer, step 612 is performed, wherein enforcement device driver 240 prevents user 150 from using Bluetooth device 258 for data transfer.

[0090] In this way, enforcement device driver 240 allows user 150 to use Bluetooth device 258 for voice communication, but blocks user 150 from using Bluetooth device 258 for data transfer.

[0091] It is noted that such enforcement policy for Bluetooth functionality is provided herein for illustrative purposes only and is not limiting. Other embodiments may employ different Bluetooth enforcement policies.

Exemplary Control of External Data Store

[0092] In some cases, administrator 102 may configure enforcement policy 230 to prevent use of external data store 270 by user 150. This may be necessary to prevent private or confidential data from being copied onto external data store 270 from mobile device 120.

[0093] A process illustrating control of external data store 270 according to an embodiment of the invention will now be described in detail with reference to flowchart 700 in FIG. 7.

[0094] In step 702, enforcement device driver 240 detects external data store 270. As an example, external data store 270

may be detected when user 150 inserts an external data store such as an SD card into mobile device 120.

[0095] In step 704, enforcement device driver checks if use of external data store 270 is allowed by enforcement policy 230. If the use of external data store is allowed by enforcement policy 230, step 710 is performed, wherein enforcement device driver 240 allows mobile device 120 to use external data store 270. For example, user 150 may be able to access data stored in external data store 270 using mobile device 120.

[0096] Returning to step 706, if addition of external data store is not allowed by enforcement policy 230, then step 708 is performed and enforcement device driver 240 does not allow mobile device 120 to use external data store 270.

[0097] It is noted that such enforcement policy for external data store functionality is provided herein for illustrative purposes only and is not limiting. Other embodiments may employ different external data store enforcement policies.

Example Computer Embodiment

[0098] In an embodiment of the present invention, the system and components of embodiments described herein are implemented using well known computers, such as computer 802 shown in FIG. 8. For example, policy server 130 or mobile device 120 can be implemented using computer(s) 802.

[0099] The computer 802 can be any commercially available and well known computer capable of performing the functions described herein, such as computers available from International Business Machines, Apple, Sun, HP, Dell, Compaq, Digital, Cray, etc.

[0100] The computer 802 includes one or more processors (also called central processing units, or CPUs), such as a processor 806. The processor 806 is connected to a communication bus 804.

[0101] The computer 802 also includes a main or primary memory 808, such as random access memory (RAM). The primary memory 808 has stored therein control logic 828A (computer software), and data.

[0102] The computer 802 also includes one or more secondary storage devices 810. The secondary storage devices 810 include, for example, a hard disk drive 812 and/or a removable storage device or drive 814, as well as other types of storage devices, such as memory cards and memory sticks. The removable storage drive 814 represents a floppy disk drive, a magnetic tape drive, a compact disk drive, an optical storage device, tape backup, etc.

[0103] The removable storage drive 814 interacts with a removable storage unit 816. The removable storage unit 816 includes a computer useable or readable storage medium 824 having stored therein computer software 828B (control logic) and/or data. Removable storage unit 816 represents a floppy disk, magnetic tape, compact disk, DVD, optical storage disk, or any other computer data storage device. The removable storage drive 814 reads from and/or writes to the removable storage unit 816 in a well known manner.

[0104] The computer 802 also includes input/output/display devices 822, such as monitors, keyboards, pointing devices, etc.

[0105] The computer 802 further includes a communication or network interface 818. The network interface 818 enables the computer 802 to communicate with remote devices. For example, the network interface 818 allows the computer 802 to communicate over communication networks or mediums 824B (representing a form of a computer useable or readable medium), such as LANs, WANs, the Internet, etc. The network interface 818 may interface with remote sites or networks via wired or wireless connections.

[0106] Control logic 828C may be transmitted to and from the computer 802 via the communication medium 824B. More particularly, the computer 802 may receive and transmit carrier waves (electromagnetic signals) modulated with control logic 830 via the communication medium 824B.

[0107] Any apparatus or manufacture comprising a computer useable or readable medium having control logic (software) stored therein is referred to herein as a computer program product or program storage device. This includes, but is not limited to, the computer 802, the main memory 808, secondary storage devices 810, the removable storage unit 816 and the carrier waves modulated with control logic 830. Such computer program products, having control logic stored therein that, when executed by one or more data processing devices, cause such data processing devices to operate as described herein, represent embodiments of the invention.

[0108] The invention can work with software, hardware, and/or operating system implementations other than those described herein. Any software, hardware, and operating system implementations suitable for performing the functions described herein can be used.

CONCLUSION

[0109] It is to be appreciated that the Detailed Description section, and not the Summary and Abstract sections, is intended to be used to interpret the claims. The Summary and Abstract sections may set forth one or more but not all exemplary embodiments of the present invention as contemplated by the inventor(s), and thus, are not intended to limit the present invention and the appended claims in any way.

[0110] The present invention has been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.

[0111] The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments, without undue experimentation, without departing from the general concept of the present invention. Therefore, such adaptations and modifications are intended to be within the meaning and range of equivalents of the disclosed embodiments, based on the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by the skilled artisan in light of the teachings and guidance.

[0112] The breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What is claimed is:

1. A method of controlling access to resources in a mobile device, comprising:

intercepting a request to access one or more resources of said mobile device;
authorizing said request based on an enforcement policy;
and
controlling access to said resources based on said authorizing step.

2. The method of claim 1, wherein said authorizing step comprises:

applying said enforcement policy.

3. The method of claim 2, wherein said enforcement policy is encrypted.

4. The method of claim 2, wherein said applying step comprises:

decrypting said enforcement policy to obtain a decrypted enforcement policy;

storing said decrypted enforcement policy in memory; and
using said decrypted enforcement policy to control access to said resources;

wherein said decrypted enforcement policy is removed from memory after said using step is completed.

5. A method of maintaining a desired state on a mobile device, comprising:

monitoring one or more settings associated with a plurality of user applications or device resources;

detecting a change in said settings; and

restoring said settings to a desired state wherein said desired state is based on an enforcement policy.

6. A system for controlling access to resources in a mobile device, comprising:

an enforcement policy that includes one or more settings to control access to resources associated with said mobile device;

an enforcement device driver that intercepts requests to access said resources; and

an enforcement monitor that monitors said settings, wherein said enforcement monitor returns said settings to a desired state if said settings have been changed in a manner that is not authorized.

7. The system of claim 6, wherein said mobile device is offline.

8. The system of claim 6, wherein said enforcement policy is encrypted.

9. The system of claim 6, wherein said desired state is determined by an administrator.

10. The system of claim 6, wherein said enforcement monitor monitors a plurality of user applications.

11. A computer program product having control logic stored therein, said control logic enabling a processor to control access to resources in a mobile device, said control logic comprising:

intercepting means for enabling a processor to intercept a request to access one or more resources associated with said mobile device;

authorizing means for enabling a processor to authorize said request based on an enforcement policy; and

controlling means for enabling a processor to control access to said resources.

* * * * *