(12) STANDARD PATENT (11) Application No. **AU 2014259659 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Time-based configuration policy toggling

(51) International Patent Classification(s)
H04W 24/00 (2009.01)

(21) Application No: **2014259659** (22) Date of Filing: **2014.05.02**

(87) WIPO No: **WO14/179743**

(30) Priority Data

(31) Number	(32) Date	(33) Country
13/875,414	**2013.05.02**	**US**

(43) Publication Date: **2014.11.06**
(44) Accepted Journal Date: **2016.07.28**

(71) Applicant(s)
AirWatch LLC

(72) Inventor(s)
Dabbiere, Alan;Marshall, John;Stuntebeck, Erich

(74) Agent / Attorney
FB Rice, Level 14 90 Collins Street, Melbourne, VIC, 3000

(56) Related Art
US 2012/0023554 A1
US 2013/0040604 A1
US 2010/0317371 A1
US 2010/0318701 A1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 November 2014 (06.11.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/179743 A1

(51) International Patent Classification:
H04W 24/00 (2009.01)

(21) International Application Number:
PCT/US2014/036657

(22) International Filing Date:
2 May 2014 (02.05.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/875,414 2 May 2013 (02.05.2013) US

(71) Applicant: **SKY SOCKET, LLC** [US/US]; 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338 (US).

(72) Inventors: **DABBIERE, Alan**; 1100 Dogwood Drive, McLean, VA 22101 (US). **MARSHALL, John**; 943 Peachtree St. NE, #706, Atlanta, GA 30309 (US). **STUNTEBECK, Erich**; 3317 Chastain Ridge Drive, Marietta, GA 300066 (US).

(74) Agent: **DIRICO, John**; 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,

[Continued on next page]

(54) Title: TIME-BASED CONFIGURATION POLICY TOGGLING

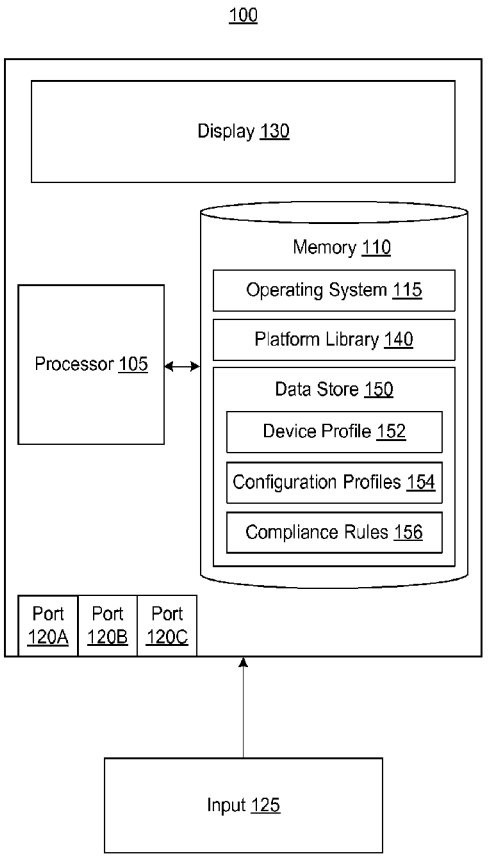

Figure 1

(57) Abstract: Time-based configuration profile toggling may be provided. Configuration profiles associated with user devices may be identified, determinations of whether the user devices are authorized to enable the configuration profiles on the user devices may be made based at least in part on time constraints, and the configuration profiles may be enabled on the user devices if the time constraints are satisfied.

WO 2014/179743 A1

OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TITLE

TIME-BASED CONFIGURATION PROFILE TOGGLING

RELATED APPLICATION

[0001] This application is a PCT Application claiming priority to US Application No. 13/875,414, entitled "TIME-BASED CONFIGURATION PROFILE TOGGLING," filed on May 02, 2013. The patent application identified above is incorporated by reference herein in its entirety.

BACKGROUND

[0002] In some situations, user devices may have access to one or more configuration profiles that may be enabled on the user devices. The configuration profiles may, for instance, configure the user device for personal and/or business use, such as configuring email accounts, applications, hardware features, software features and/or the like. Conventional approaches of using such persona-specific configuration profiles include providing a user device with access to only one of either personal configuration profiles or business configuration profiles to control which persona is enabled on the user device at the proper time. For instance, an Information Technology (IT) administrator may manually enable a set of business configuration profiles on a user device owned by the business upon hiring a new employee that will use such user device for tasks related to the business. The IT administrator may further, upon an authorized condition, disable the business configuration profiles on the user device and enable the personal configuration profiles on the user device to allow the employee to use the user device for tasks related to the employee's personal affairs.

[0002a] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each claim of this application.

[0002b] Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

SUMMARY

[0003a] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is this Summary intended to limit the scope of the claimed subject matter.

[0003b] Some embodiments relate to a method for providing time-based configuration profile toggling, the method being executed by a server comprising at least one memory storage and at least one processor coupled to said memory storage, the method comprising:

receiving a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identifying at least one configuration profile associated with said user device, in response to receiving the request from said user device;

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user device;

instructing said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile; and

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

[0003c] Some embodiments relate to a non-transitory computer-readable medium which stores a set of instructions that when executed by a server comprising at least one memory storage and at least one processor coupled to said memory storage, performs a method executed by the set of instructions comprising:

receiving a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identifying at least one configuration profile enabled on the user device, in response to receiving the request from said user device;

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user device;

instructing said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile; and

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

[0003d] Some embodiments relate to a server comprising:

at least one memory storage; and

at least one processor coupled to said memory storage, wherein said processor is configured to:

receive a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identify at least one configuration profile associated with said user device, in response to receiving the request from said user device;

determine whether said user device is authorized to enable said configuration profile on said user device based at least in part on whether a current time associated with said

user device complies with at least one compliance rule specifying at least one time period when said user device is authorized to enable said configuration profile on said user device;

instruct said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device; and

instruct said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

[0004] Time-based configuration profile toggling may be provided. A user device may be instructed to enable a configuration profile if it is determined that the user device is authorized to enable the configuration profile based at least in part on a current time associated with the user device. Additionally, a user device may be instructed to disable a configuration profile if it is determined that the user device is not authorized to enable the configuration profile based at least in part on a current time associated with the user device. A user device may thereby be, for instance, instructed to toggle between personal configuration profiles and business configuration profiles based on a configured workday. More specifically, the user device may be instructed to enable business configuration profiles at the beginning of the workday, disable personal configuration profiles at the beginning of the workday, enable personal configuration profiles at the end of the workday, and disable business configuration profiles at the end of the workday.

[0005] It is to be understood that both the foregoing general description and the following detailed description are examples and explanatory only, and should not be considered to restrict the disclosure's scope, as described and claimed. Further,

features and/or variations may be provided in addition to those set forth herein. For example, embodiments of the disclosure may be directed to various feature combinations and sub-combinations described in the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Many aspects of the present disclosure can be better understood with reference to the following diagrams. The drawings are not necessarily to scale. Instead, emphasis is placed upon clearly illustrating certain features of the disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views. In the drawings:

[0007] FIG. 1 is a block diagram of a user device;

[0008] FIG. 2 is a block diagram of an operating environment; and

[0009] FIG. 3 is a flow chart illustrating a method for providing time-based configuration profile toggling.

DETAILED DESCRIPTION

[0010] The following Detailed Description refers to the accompanying Drawings. Wherever possible, the same reference numbers are used in the Drawings and the following Detailed Description to refer to the same or similar elements. While embodiments of the disclosure may be described, modifications, adaptations, and other implementations of the disclosure are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the Drawings without departing from the spirit and scope of the disclosure. The methods described herein may be also modified by substituting, reordering, or adding stages to the methods

without departing from the spirit and scope of the disclosure. Accordingly, the following Detailed Description does not limit the disclosure; instead, the proper scope of the disclosure is defined by the appended Claims.

[0011] Time-based configuration profile toggling may be provided. To reduce the cost of ownership of user devices and cellular and/or data service charges associated with use of such user devices, a business may implement a "bring your own device" (BYOD) policy to allow an employee to use her personal device to access business resources rather than provide the employee with a business owned user device for such purpose. To support such a BYOD policy, a user device administrator (i.e. IT administrator) may manage a group of personally owned user devices, via a management application executed by a management server in communication with the user devices over a network, to provide the user devices with secure access to business resources.

[0012] The user device administrator may enroll user devices into the management system to monitor the user devices for security vulnerabilities and to configure the user devices for secure access to business resources. The user device administrator may create and/or configure at least one configuration profile via a user interface provided by the management system. A configuration profile may comprise a set of instructions and/or settings that configure the operations and/or functions of a user device, which may ensure the security of the accessed resources. The user device administrator may, for instance, configure a business email configuration profile by specifying the network address and access credentials of a business email account that the users of the user devices are authorized to access. Other configuration policies

may include, but are not limited to, hardware, software, application, function, cellular, text message, and data use restrictions, which may be based at least in part on the current time and/or location of the restricted user device. The user device administrator may thereafter deploy the configuration profiles to specific user devices, such as to groups of user devices of employees with similar roles, privileges and/or titles.

[0013] The user devices may also have access to personal configuration profiles that may be created by the users of the user devices. The user devices may, for instance, have access to a personal email configuration profile that was created by a user of the user device to provide access to her personal email account. Thus, a user device enrolled in a BYOD management system may have more than one configuration profile for a given use of the user device, such as a personal email configuration profile and a business email configuration profile that are both used for accessing email accounts on the user device.

[0014] Time-based configuration profile toggling may be provided, which may ensure the security of business resources and/or to ensure the productivity of employee users of user devices with access to business resources. User devices may be instructed to enable certain configuration profiles and/or disable certain configuration profiles based at least in part on the current time associated with the user devices. More specifically, user devices may be instructed to toggle between personal configuration profiles and business configuration profiles based on a configured workday. The user device administrator may instruct the user devices to enable and/or disable certain configuration profiles via an agent application executed on the user devices, which may be installed on the user devices upon enrollment into the BYOD

management system. Alternatively, the user device administrator may instruct the user devices to enable and/or disable certain configuration profiles via application programming interface (API) calls to the operating system of the user devices, which may be remotely transmitted from the management system to the user devices over a cellular and/or data network.

[0015] In any case, the user devices may be instructed to enable and/or disable certain configuration profiles according to authorization rights specified by the user device administrator, such as time-based authorization rights. For example, a BYOD policy may specify that user devices enrolled in the BYOD management system are authorized for personal use outside of the workday and are authorized for business use during the workday. To implement such a policy, a user device administrator may instruct the user devices to toggle between personal configuration policies and business configuration policies based on the current time associated with the user device. The current time may be based on the current time at the current location of the user device, which may be determined by GPS, Wi-Fi, cellular network tower triangulation, etc., or may be based on the current time at a configured primary location associated with the user device, which may be the primary office location of an employee user of the user device. As an example, time-based configuration profile toggling may be provided by instructing a user device to enable business configuration profiles and disable personal configuration profiles while the current time is between 9AM and 5PM at the current location of the user device, and to disable business configuration profiles and enable personal configuration profiles while the current time is between 5PM and 9AM at the current location of the user device.

[0016] Additionally, location-based configuration profile toggling may be provided, which may ensure the security of business resources and/or to ensure the productivity of employee users of user devices with access to business resources. User devices may be instructed to enable certain configuration profiles and/or disable certain configuration profiles based at least in part on the current location associated with the user devices. More specifically, user devices may be instructed to toggle between personal configuration profiles and business configuration profiles based on a configured office location. The user device administrator may instruct the user devices to enable and/or disable certain configuration profiles via an agent application executed on the user devices, which may be installed on the user devices upon enrollment into the BYOD management system. Alternatively, the user device administrator may instruct the user devices to enable and/or disable certain configuration profiles via application programming interface (API) calls to the operating system of the user devices, which may be remotely transmitted from the management system to the user devices over a cellular and/or data network.

[0017] In any case, the user devices may be instructed to enable and/or disable certain configuration profiles according to authorization rights specified by the user device administrator, such as location-based authorization rights. For example, a BYOD policy may specify that user devices enrolled in the BYOD management system are authorized for personal use outside of the workplace and are authorized for business use inside the workplace. To implement such a policy, a user device administrator may instruct the user devices to toggle between personal configuration policies and business configuration policies based on the current location associated

with the user device, which may be determined by GPS, Wi-Fi, cellular network tower triangulation, and/or the like. As an example, location-based configuration profile toggling may be provided by instructing a user device to enable business configuration profiles and disable personal configuration profiles when the current location of the user device is within a configured office location, and to disable business configuration profiles and enable personal configuration profiles when the current location of the use device is outside the configured office location.

[0018] Fig. 1 is a block diagram of a user device 100, which may comprise a smart phone, cellular telephone, personal digital assistant, tablet computer system, web pad, laptop computer, desktop computer, set-top box, music player, game console, and/or another device with like capability. User device 100 may comprise a processor 105 and a memory 110. Depending on the configuration and type of device, memory 110 may comprise, but is not limited to, volatile (e.g. random access memory (RAM)), non-volatile (e.g. read-only memory (ROM)), flash memory, or any combination. Memory 110 may store executable programs and related data components of various applications and modules for execution by user device 100. Memory 110 may be coupled to processor 105 for storing configuration data and operational parameters, such as commands that are recognized by processor 105.

[0019] Basic functionality of user device 100 may be provided by an operating system 115 contained in memory 100. One or more programmed software applications may be executed by utilizing the computing resources in user device 100. Applications stored in memory 110 may be executed by processor 105 (e.g., a central processing unit or digital signal processor) under the auspices of operating system 115. For

example, processor 105 may be configured to execute applications such as web browsing applications, email applications, instant messaging applications, and/or other applications capable of receiving and/or providing data.

[0020] Data provided as input to and generated as output from the application(s) may be stored in memory 110 and read by processor 105 from memory 110 as needed during the course of application program execution. Input data may be data stored in memory 110 by a secondary application or other source, either internal or external to user device 100, or possibly anticipated by the application and thus created with the application program at the time it was generated as a software application program. Data may be received via any of a plurality of communication ports 120(A)-(C) of user device 100. Communication ports 120(A)-(C) may allow user device 100 to communicate with other devices, and may comprise components such as an Ethernet network adapter, a modem, and/or a wireless network connectivity interface. For example, the wireless network connectivity interface may comprise one and/or more of a PCI (Peripheral Component Interconnect) card, USB (Universal Serial Bus) interface, PCMCIA (Personal Computer Memory Card International Association) card, SDIO (Secure Digital Input-Output) card, NewCard, Cardbus, a modem, a wireless radio transceiver, and/or the like.

[0021] User device 100 may also receive data as user input via an input component 125, such as a keyboard, a mouse, a pen, a stylus, a sound input device, a touch input device, a capture device, etc. A capture device may be operative to record user(s) and capture spoken words, motions and/or gestures, such as with a camera

and/or microphone. The capture device may comprise any speech and/or motion detection device capable of detecting the speech and/or actions of the user(s).

[0022] Data generated by applications may be stored in memory 110 by the processor 105 during the course of application program execution. Data may be provided to the user during application program execution by means of a display 130. Consistent with embodiments of this disclosure, display 130 may comprise an integrated display screen and/or an output port coupled to an external display screen.

[0023] Memory 110 may also comprise a platform library 140. Platform library 140 may comprise a collection of functionality useful to multiple applications, such as may be provided by an application programming interface (API) to a software development kit (SDK). These utilities may be accessed by applications as necessary so that each application does not have to contain these utilities thus allowing for memory consumption savings and a consistent user interface.

[0024] Furthermore, embodiments of this disclosure may be practiced in conjunction with a graphics library, other operating systems, or any other application program and is not limited to any particular application or system. The devices described with respect to the Figures may have additional features or functionality. For example, user device 100 may also include additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape (not shown).

[0025] User device 100 may store in a data store 150 a device profile 152. Device profile 152 may comprise one or more indications of the state of user device 100. For instance, device profile 152 may represent hardware specifications of user

device 100, version and configuration information of various software program and hardware components installed on user device 100, data transmission protocols enabled on user device 100, version and usage information of various resources stored on user device 100, and/or any other attributes associated with the state of user device 100. The device profile 152 may further comprise data indicating a date of last virus scan of user device 100, a date of last access by an IT representative, a date of last service by the IT representative, and/or any other data indicating maintenance and usage of user device 100. Moreover, the device profile 152 may comprise indications of the past behavior of associated users, such as resources accessed, charges for resource accesses, and the inventory accessed from such resources. Furthermore, device profile 152 may indicate a current location associated with user device 100 and/or a current time associated with user device 100. Device profile 152 may, for example, comprise data accessible to user device 100 via functions of user device 100, such as GPS location data, and/or via remote services communicatively coupled to user device 100, such as current time data provided by a remote time service.

[0026] User device 100 may also store one or more configuration profiles 154 in data store 150. Configuration profiles 154 may comprise settings, plug-ins, configuration files and/or other data capable of configuring, controlling, and/or influencing the operations and/or functions of user device 100. Configuration profiles 154 may specify how user device 100 may perform certain functions of the user device 100, such as a camera, touchscreen, microphone or other function provided by user device 100. Configuration profiles 154 may, for example, comprise configuration profiles 154 specific to Apple iOS, Apple OSX, Samsung KNOX, Samsung SAFE,

Google Android, Windows Mobile, Windows 8, Blackberry 10, Symbian, and/or other user device 100 operating systems 115. Configuration profiles 154 may utilize an application programming interface (API) to communicate the specifications and/or requirements of the configuration profiles 154 to operating system 115 of user device 100.

[0027] Configuration profiles 154 may also specify a series of authorized sub functions that user device 100 may perform in response to a request to perform certain unauthorized functions of user device 100. Such configuration profiles 154, or macros, may provide similar and/or equivalent functions to requested functions through a series of authorized sub-functions of user device 100. In some embodiments, configuration profiles 154 may specify that user device 100 may enable a data network calling function when a cellular network calling function is disabled on user device 100 and a request to perform such cellular network calling function is received by user device 100. For example, user device 100 may interface with a Voice-over-Internet Protocol (VoIP) provider, such as Skype, may create a VoIP account and/or enroll into a group account associated with the user device 100, and may download, install, and execute a VoIP application. In other embodiments, configuration profiles 154 may specify that user device 100 may interface with a cellular network carrier and/or provider to enable an international calling plan when the user device 100 is located outside of the United States and a request to perform a cellular network calling function is received by user device 100. In further embodiments, configuration profiles 154 may specify that user device 100 may enable a data network messaging function when a short message service (SMS) messaging function is disabled on user device 100 and a request to

perform such SMS messaging function is received by user device 100. For instance, user device 100 may interface with an application store associated with the user device 100 and may download, install, and execute a data messaging application, such as Apple iMessage, Blackberry Messenger, and/or the like.

[0028] Configuration profiles 154 may comprise personal configuration profiles 154. Personal configuration profiles 154 may comprise configuration profiles 154 created by a user of user device 100 by configuring certain personal data, personal applications, personal software features, and/or personal hardware features of user device 100. Personal configuration profiles 154 may, for example, comprise configuration profiles 154 that provide access to a personal email account.

[0029] Configuration profiles 154 may further comprise business and/or enterprise configuration profiles 154. Business configuration profiles 154 may comprise configuration profiles 154 created by a user device 100 administrator of user device 100 by configuring certain business data, business applications, business software features, and/or business hardware features of user device 100. Business configuration profiles 154 may be configured by a user device 100 administrator via a management server 210 and, thereafter, distributed to the user device 100 via a network 240 transmission. Business configuration profiles 154 may, for example, configuration profiles 154 that provide access to a business file repository.

[0030] Moreover, user device 100 may store one or more compliance rules 156. Compliance rules 156 may specify conditions and/or events required for user device 100 to perform certain functions on user device 100. In some embodiments, compliance rules 156 may specify that user device 100 must satisfy and/or comply with

a single condition for user device 100 to be authorized to perform certain functions of user device 100 associated with the compliance rules 156. For instance, compliance rules 156 may require that user device 100 is associated with a current time that is within an authorized time period specified by such compliance rules 156 in order for user device 100 to be authorized to perform certain functions of user device 100. More specifically, compliance rules 156 may specify that user device 100 is authorized to access a business email account while the system clock of user device 100 is within a configured workday and is not authorized to access the business email account while the system clock of user device 100 is outside of the configured workday.

[0031] In some embodiments, compliance rules 156 may specify that user device 100 must satisfy and/or comply with more than one condition for user device 100 to be authorized to perform certain functions of user device 100 associated with the compliance rules 156. For example, compliance rules 156 may specify that user device 100 must be associated with a "safe zone" location to perform certain functions of user device 100, which may require that both a GPS sensor of user device 100 indicates that user device 100 is currently located within the safe zone and a Wi-Fi network access point associated with the safe zone is communicatively coupled to and/or enrolled with the Wi-Fi network access point.

[0032] In some embodiments, compliance rules 156 may specify that user device 100 and another computing device, similar to and/or identical to user device 100, satisfy and/or comply with one or more conditions for user device 100 to be authorized to perform certain functions of user device 100 associated with the compliance rules 156. Compliance rules 156 may require that user device 100 be located within

proximity of and/or be communicatively coupled to a secondary user device 100 and that both user devices 100 be located within an authorized location in order to perform certain functions of user device 100. As an example, compliance rules 156 may specify that user devices 100 associated with nurses may only access medical records of patients while the user devices 100 associated with the nurses are located within 10 feet of user devices 100 associated with such patients and both the user devices 100 associated with nurses and user devices 100 associated with patients are located within examination rooms specific to the patients' appointments.

[0033] In some embodiments, compliance rules 156 may be granular such that user device 100 may be authorized to perform different functions depending on how many of the conditions of the compliance rules 156 are satisfied by user device 100. For example, user device 100 may be authorized to access a business contact list on user device 100 if a GPS sensor on user device 100 indicates that user device 100 is located within the business's office location, but user device 100 may be prohibited from sending a business email until it is confirmed that user device 100 is located within a "safe zone" by being communicatively coupled to a Wi-Fi network access point associated with the business's office location.

[0034] In any case, compliance rules 156 may be associated with configuration profiles 154 such that compliance rules 156 may determine whether user device 100 is authorized to enable configuration profiles 154 on user device 100. For instance, compliance rules 156 may specify that certain configuration profiles 154 may only be enabled on user device 100 while a current time associated with user device 100 is within an authorized time period specified by compliance rules 156, as within a

configured workday. User device 100 may receive configuration profiles 154 and compliance rules 156 from a user device 100 management service communicatively coupled to user device 100. User device 100 may receive a distribution of configuration profiles 154 and compliance rules 156 from a user device 100 management service "over the air," such as via a data network 240.

[0035] An agent application on user device 100 may determine whether compliance rules 156 are satisfied, for instance, by determining whether device profile 152 satisfies compliance rules 156. For instance, agent application may determine whether device profile 152 specifies that the current time associated with user device 100 is within a configured workday specified by compliance rules 156. Alternatively, user device 100 may transmit all and/or a portion of device profile 152 to a user device 100 management service that may determine whether user device 100 satisfies compliance rules 156. In any case, user device 100 may be authorized and/or instructed to perform functions of user device 100 according to the specifications of configuration profiles 154 in response to a determination that user device 100 complies with compliance rules 156 associated with such configuration profiles 154.

[0036] Figure 2 is a block diagram view of an operating environment 200 comprising user device 100 in communication with a management server 210 via a network 240. The management server 210 may comprise, for example, cloud-based solutions, server computers and/or any other system providing user device 100 management capability. For purposes of convenience, the management server 210 is referred to herein in the singular, although it is understood that a plurality of servers may be employed in the arrangements as descried herein. Furthermore, in some

embodiments, multiple management servers 210 may operate on the same server computer. The components executed on the management server 210, for example, may comprise various applications, services, processes, systems, engines, or functionality not disclosed in detail herein.

[0037] The management server 210 may comprise a configuration profile store 220 comprising a plurality of configuration policies 154 that may be applicable to user device 100, as described herein. The management server 210 may further comprise a compliance rule store 230 comprising a plurality of compliance rules 156. While the configuration profile store 220 and compliance rule store 230 are shown as within the management server 210, the configuration profile store 220 and compliance rule store 230 may alternately be within the user device 100 and/or remotely located on a file server and may be remotely updated periodically by management server 210 according to common over-the-air (OTA) updating methods.

[0038] As described herein, requests and/or attempts by user device 100 to perform certain functions on user device 100 may require user device 100 to be in compliance with compliance rules 156 stored, which may be stored in compliance rule store 220. Further, if the user device 100 complies with compliance rules 156 associated with the requested functions of user device 100, user device 100 may provide the functions in accordance with configuration profiles 154, which may be stored in configuration profile store 220. Depending on the sensitivity of a given functionality, different compliance rules 156 may be necessary to ensure that the functionality is adequately restricted. Some functionality may only require ensuring that the proper user is requesting the functionality. Other resources may require compliance with more

stringent authorization rules, such as determining whether the functionality is restricted during certain time windows. Accordingly, user device 100 and/or management server 210 may be operative to determine whether a user of user device 100 is authorized to perform requested functionality upon the user's request to perform such functionality.

[0039] In some embodiments, an agent application 250 executed on user device 100 may make the compliance determination based on a device profile 152, user credentials, and/or user preferences. For instance, the agent application 250 may monitor calls by applications, such as a web browser 252, an e-mail client 254, and/or a secure application 256, on user device 110 to the operating system 115 of user device 100 to determine whether user device 110 seeks to perform functionality associated with a given compliance rule 156. Additionally, the agent application 250 on user device 100 may approve and/or deny the associated functionality requests. For instance, the agent application 250 may instruct operating system 115 on user device 100 to enable certain configuration profiles 154 on user device 100 in response to a determination that user device 100 is authorized to enable the configuration profiles 154 on the user device 100 based at least in part on the current time associated with user device 100 and compliance rules 156 associated with such configuration profiles 154 specifying at least one time period when the user device is authorized to enable such configuration profiles 154.

[0040] While agent application 250 is depicted as a single application on user device 100 capable of determining whether user device 100 is authorized to perform functions of the user device 100, agent application 250 may comprise applications, plug-ins, application wrappers, and/or software developer kits (SDK) specific to certain

functionality of user device 100. Accordingly, user device 100 may store a multitude of function-specific agent applications 250 that collectively communicate with operating system 115 of user device 100 and/or management server 210.

[0041] In some embodiments, the agent application 250 executed on user device 100 may rely on management server 210 to determine whether a given functionality request on user device 100 is authorized according to the compliance rules 156. For instance, the agent application may transmit a functionality request, a device profile 152, user credentials, and/or user preferences to management server 210 so that management server 210 may determine whether user device 110 seeks to perform functions of user device 100 that may violate certain compliance rules 156 associated with the functions. Additionally, management server 210 may approve and/or deny the associated functionality requests. For instance, the management server 210 may instruct operating system 115 on user device 100, via agent application 250 on user device 100, to disable certain configuration profiles 154 on user device 100 in response to a determination that user device 100 is not authorized to enable the configuration profiles 154 based at least in part on the current time associated with user device 100 and compliance rules 156 associated with such configuration profiles 154 specifying at least one time period when the user device is not authorized to enable such configuration profiles 154.

[0042] The network 240 may comprise, for example, any type of wired and/or wireless network such as a wireless local area network (WLAN), a wireless wide area network (WWAN), Ethernet, fiber-optic network, and/or any other type of wired and/or wireless network now known or later developed. Additionally, the network 240 may be

or include the Internet, intranets, extranets, microwave networks, satellite communications, cellular systems, PCS, infrared communications, global area networks, or other suitable networks, etc., or any combination of such networks 240.

[0043] Figure 3 is a flow chart setting forth the general stages involved in a method 300 consistent with embodiments of this disclosure for providing time-based configuration profile toggling. Method 300 may be implemented using elements of operating environment 200 as described above. Ways to implement the stages of method 300 will be described in greater detail below.

[0044] Method 300 may begin at starting block 305 and proceed to stage 310 where configuration profiles 154 associated with one or more user devices 100 are identified. In some embodiments, method 300 may proceed to stage 310 in response to the user devices 100 receiving a request to perform certain functions on the user devices 100 that may be associated with such configuration profiles 154. In other embodiments, method 300 may proceed to stage 310 in response to the user devices 100 identifying configuration profiles 154 that are currently enabled on the user devices 100. For instance, an agent application 250 on the user devices 100 may periodically query the user device 100 to determine whether any configuration profiles 154 are enabled on the user devices 100.

[0045] In some embodiments, a user device 100 may query the data store 150 of user device 100 to determine whether any configuration profiles 154 are associated with the user device 100. In other embodiments, management server 210 may query the configuration profile store 220 to determine whether any configuration profiles 154 stored within configuration profile store 220 are associated with a given user device

100. In yet further embodiments, user device 100 and/or management server 210 may query a remote file server to determine whether any configuration profiles 154 stored within the remote file server are associated with user device 100.

[0046] From stage 310, method 300 may advance to stage 315 where a current time associated with the user devices 100 is identified. In certain embodiments, compliance rules 156 associated with the configuration profiles 154 may specify that a current time associated with the user devices 100 must fall within certain authorized time windows for the user device 100 to be authorized to enable the identified configuration profiles 156. In some embodiments, user devices 100 may query the user devices 100 to identify the current system time of the operating systems 115 of user devices 100, may query a network 240 communicatively coupled with the user devices 100 to identify the current network time of the network 240, and/or may query other services communicatively coupled to the user devices 100 that may provide an indication of a current time associated with the user devices 100. In other embodiments, the user devices 100 may determine the current location of the user devices 100 and may identify the current time associated with user devices 100 based at least in part on the current location of the user devices 100 and the time zone applicable to such current location of the user devices 100. For example, the user devices 100 may determine the current location of the user devices 100 via GPS, cell tower triangulation, network access points such as Wi-Fi hotspots, near field communication (NFC), and/or the like. In yet further embodiments, management server 210 may identify the current time associated with user device 100 by identifying a configured “home” location associated with user device 100, such as the primary office

location associated with the user of user device 100, and determining the current time at such configured "home" location associated with user device 100.

[0047] From stage 315, method 300 may advance to stage 320 where method 300 determines whether the user devices 100 are authorized to enable the identified configuration profiles 154 on the user devices 100 based at least in part on the identified current time associated with the user devices 100. In some embodiments, an agent application 250 on the user devices 100 may determine whether the current time associated with user devices 100 falls within at least one authorized time period specified by the configuration profiles 154. In other embodiments, management server 210 may determine whether the current time associated with user device 100 falls within at least one authorized time period specified by the configuration profiles 154. In yet a further embodiment, user devices 100 and/or management server 210 may transmit the identified configuration profiles 154 and identified current times associated with the user devices 100 to a remote compliance service that may determine whether the current time associated with the user devices 100 falls within at least one authorized time period specified by the configuration profiles 154 and may return a response to the user devices 100 and/or management server 210.

[0048] If it is determined that the user devices 100 are authorized to enable the identified configuration profiles 154 on the user devices 100 based at least in part on the identified current time associated with the user devices 100, method 300 may advance to stage 325 where the user devices 100 may enable the configuration profiles 154 on the user devices 100. In some embodiments, the user devices 100 may enable the configuration profiles 154 on the user devices 100 by instructing the operating systems

115 of the user devices 100 to one or more of download, install, activate, and execute the identified configuration profiles 154 on the user devices 100. In other embodiments, management server 210 may transmit instructions to the operating systems 115 of the user devices 100 to one or more of download, install, activate, and execute the identified configuration profiles 154 on the user devices 100. Method 300 may then end at stage 335.

[0049] If, however, it is determined that the user devices 100 are not authorized to enable the identified configuration profiles 154 on the user devices 100 based at least in part on the identified current time associated with the user devices 100, method 300 may advance to stage 330 where the user devices 100 may disable the configuration profiles 154 on the user devices 100. In some embodiments, the user devices 100 may disable the configuration profiles 154 on the user devices 100 by instructing the operating systems 115 of the user devices 100 to one or more of delete, uninstall, deactivate, and terminate the execution of the identified configuration profiles 154 on the user devices 100. In other embodiments, management server 210 may transmit instructions to the operating systems 115 of the user devices 100 to one or more of delete, uninstall, deactivate, and terminate the execution of the identified configuration profiles 154 on the user devices 100. Method 300 may then end at stage 335.

[0050] An embodiment consistent with the disclosure may comprise a method for providing time-based configuration profile toggling. The method may comprise identifying at least one configuration profile associated with at least one user device, determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user

device, and enabling said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device based at least in part on said current time associated with said user device.

[0051] Another embodiment consistent with the disclosure may comprise a non-transitory computer-readable medium for providing time-based configuration profile toggling. The non-transitory computer-readable medium may store a set of instructions that when executed perform a method executed by the set of instructions. The method may comprise identifying at least one configuration profile enabled on at least one user device, determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user device, and disabling said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device based at least in part on said current time associated with said user device.

[0052] Yet another embodiment consistent with the disclosure may comprise a system for providing time-based configuration profile toggling. The system may comprise a memory storage and a processing unit coupled to the memory storage. The processing unit may be operative to identify at least one configuration profile associated with at least one user device, determine whether said user device is authorized to enable said configuration profile on said user device based at least in part on whether a current time associated with said user device complies with at least one compliance rule specifying at least one time period when said user device is authorized to enable said

configuration profile on said user device, and enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device based at least in part on said current time associated with said user device.

[0053] The embodiments and functionalities described herein may operate via a multitude of computing systems, including wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, tablet or slate type computers, laptop computers, etc.). In addition, the embodiments and functionalities described herein may operate over distributed systems, where application functionality, memory, data storage and retrieval and various processing functions may be operated remotely from each other over a distributed computing network, such as the Internet or an intranet. User interfaces and information of various types may be displayed via on-board computing device displays or via remote display units associated with one or more computing devices. For example user interfaces and information of various types may be displayed and interacted with on a wall surface onto which user interfaces and information of various types are projected. Interaction with the multitude of computing systems with which embodiments of this disclosure may be practiced include, keystroke entry, touch screen entry, voice or other audio entry, gesture entry where an associated computing device is equipped with detection (e.g., camera) functionality for capturing and interpreting user gestures for controlling the functionality of the computing device, and the like. The Figures above and their associated descriptions provide a discussion of a variety of operating environments in which embodiments of this disclosure may be practiced. However, the devices and systems illustrated and discussed with respect to

the Figures are for purposes of example and illustration and are not limiting of a vast number of computing device configurations that may be utilized for practicing embodiments of this disclosure as described herein.

[0054] The term computer readable media as used herein may include computer storage media. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. System memory, removable storage, and non-removable storage are all computer storage media examples (i.e., memory storage.) Computer storage media may include, but is not limited to, RAM, ROM, electrically erasable read-only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store.

[0055] The term computer readable media as used herein may also include communication media. Communication media may be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and includes any information delivery media. The term “modulated data signal” may describe a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and

wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media.

[0056] A number of applications and data files may be used to perform processes and/or methods as described above. The aforementioned processes are examples, and a processing unit may perform other processes. Other programming modules that may be used in accordance with embodiments of this disclosure may include electronic mail, calendar, and contacts applications, data processing applications, word processing applications, spreadsheet applications, database applications, slide presentation applications, drawing or computer-aided application programs, etc.

[0057] Generally, consistent with embodiments of this disclosure, program modules may include routines, programs, components, data structures, and other types of structures that may perform particular tasks or that may implement particular abstract data types. Moreover, embodiments of the disclosure may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, mainframe computers, and the like. Embodiments of this disclosure may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0058] Furthermore, embodiments of this disclosure may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated

electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. Embodiments of this disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to mechanical, optical, fluidic, and quantum technologies. In addition, embodiments of the disclosure may be practiced within a general purpose computer or in any other circuits or systems.

[0059] Embodiments of this disclosure may, for example, be implemented as a computer process and/or method, a computing system, an apparatus, device, or appliance, and/or as an article of manufacture, such as a computer program product or computer readable media. The computer program product may be a computer storage media readable by a computer system and encoding a computer program of instructions for executing a computer process. The computer program product may also be a propagated signal on a carrier readable by a computing system and encoding a computer program of instructions for executing a computer process. Accordingly, the present disclosure may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.). In other words, embodiments of the present disclosure may take the form of a computer program product on a computer-usable or computer-readable storage medium having computer-usable or computer-readable program code embodied in the medium for use by or in connection with an instruction execution system. A computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the

program for use by or in connection with the instruction execution system, apparatus, or device.

[0060] The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific computer-readable medium examples (a non-exhaustive list), the computer-readable medium may include the following: an electrical connection having one or more wires, a portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disc read-only memory (CD-ROM). Note that the computer-usable or computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

[0061] Embodiments of this disclosure may be practiced via a system-on-a-chip (SOC) where each and/or many of the elements described above may be integrated onto a single integrated circuit. Such an SOC device may include one or more processing units, graphics units, communications units, system virtualization units and various application functionalities, all of which may be integrated (or "burned") onto the chip substrate as a single integrated circuit. When operating via an SOC, the functionality, described herein, with respect to training and/or interacting with any

element may operate via application-specific logic integrated with other components of the computing device/system on the single integrated circuit (chip).

[0062] Embodiments of this disclosure are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0063] While certain embodiments have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

[0064] Embodiments of the present disclosure, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed

substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0065] While certain embodiments of the disclosure have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

[0066] All rights including copyrights in the code included herein are vested in and the property of the Assignee. The Assignee retains and reserves all rights in the code included herein, and grants permission to reproduce the material only in connection with reproduction of the granted patent and for no other purpose.

[0067] While the specification includes examples, the disclosure's scope is indicated by the following claims. Furthermore, while the specification has been described in language specific to structural features and/or methodological acts, the claims are not limited to the features or acts described above. Rather, the specific features and acts described above are disclosed as example for embodiments of the disclosure.

2014259659 04 Jul 2016

CLAIMS:

1. A method for providing time-based configuration profile toggling, the method being executed by a server comprising at least one memory storage and at least one processor coupled to said memory storage, the method comprising:

receiving a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identifying at least one configuration profile associated with said user device, in response to receiving the request from said user device;

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user device;

instructing said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile; and

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

2. The method of claim 1, wherein said configuration profile associated with said user device is associated with at least one of the following: business data, business applications, business software features, and business hardware features.

3. The method of claim 1 or claim 2, wherein said configuration profile associated with said user device is associated with at least one of the following: personal data, personal applications, personal software features, and personal hardware features.

4. The method of any one of claims 1 to 3, wherein determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on said current time associated with said user device comprises determining whether said current time associated with said user device complies with at least one

compliance rule specifying at least one time period when said user device is authorized to enable said configuration profile on said user device.

5. The method of any one of claims 1 to 4, further comprising:

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current location associated with said user device; and,

instructing said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device based at least in part on said current location associated with said user device.

6. The method of claim 5, wherein determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on said current location associated with said user device comprises determining whether said current location associated with said user device complies with at least one compliance rule specifying at least one location where said user device is authorized to enable said configuration profile on said user device.

7. The method of claim 5 or claim 6, further comprising:

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device based at least in part on said current location associated with said user device.

8. A non-transitory computer-readable medium which stores a set of instructions that when executed by a server comprising at least one memory storage and at least one processor coupled to said memory storage, performs a method executed by the set of instructions comprising:

receiving a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identifying at least one configuration profile enabled on the user device, in response to receiving the request from said user device;

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current time associated with said user device;

instructing said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile; and

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

9. The non-transitory computer-readable medium of claim 8, wherein said configuration profile associated with said user device is associated with at least one of the following: business data, business applications, business software features, and business hardware features.

10. The non-transitory computer-readable medium of claim 8 or claim 9, wherein said configuration profile associated with said user device is associated with at least one of the following: personal data, personal applications, personal software features, and personal hardware features.

11. The non-transitory computer-readable medium of any one of claims 8 to 10, further comprising:

determining whether said user device is authorized to enable said configuration profile on said user device based at least in part on a current location associated with said user device; and,

instructing said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said

configuration profile on said user device based at least in part on said current location associated with said user device.

12. The non-transitory computer-readable medium of claim 11, further comprising:

instructing said user device to enable at least one configuration profile that said user device is authorized to enable based at least in part on said current location associated with said user device.

13. A server comprising:

at least one memory storage; and

at least one processor coupled to said memory storage, wherein said processor is configured to:

receive a request from at least one Bring Your Own Device, BYOD, user device to perform a function on said user device;

identify at least one configuration profile associated with said user device, in response to receiving the request from said user device;

determine whether said user device is authorized to enable said configuration profile on said user device based at least in part on whether a current time associated with said user device complies with at least one compliance rule specifying at least one time period when said user device is authorized to enable said configuration profile on said user device;

instruct said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device; and

instruct said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device.

14. The server of claim 13, wherein said configuration profile associated with said user device is associated with at least one of the following: business data, business applications, business software features, and business hardware features.

15. The server of claim 13 or claim 14, wherein said configuration profile associated with said user device is associated with at least one of the following: personal data, personal applications, personal software features, and personal hardware features.

16. The server of any one of claims 13 to 15, wherein said processor is further configured to:

determine whether said user device is authorized to enable said configuration profile on said user device based at least in part on whether a current location associated with said user device complies with at least one compliance rule specifying at least one location where said user device is authorized to enable said configuration profile on said user device; and,

instruct said user device to enable said configuration profile on said user device in response to a determination that said user device is authorized to enable said configuration profile on said user device based at least in part on said current location associated with said user device.

17. The server of claim 16, wherein said processor is further configured to:

instruct said user device to disable said configuration profile on said user device in response to a determination that said user device is not authorized to enable said configuration profile on said user device based at least in part on said current location associated with said user device.

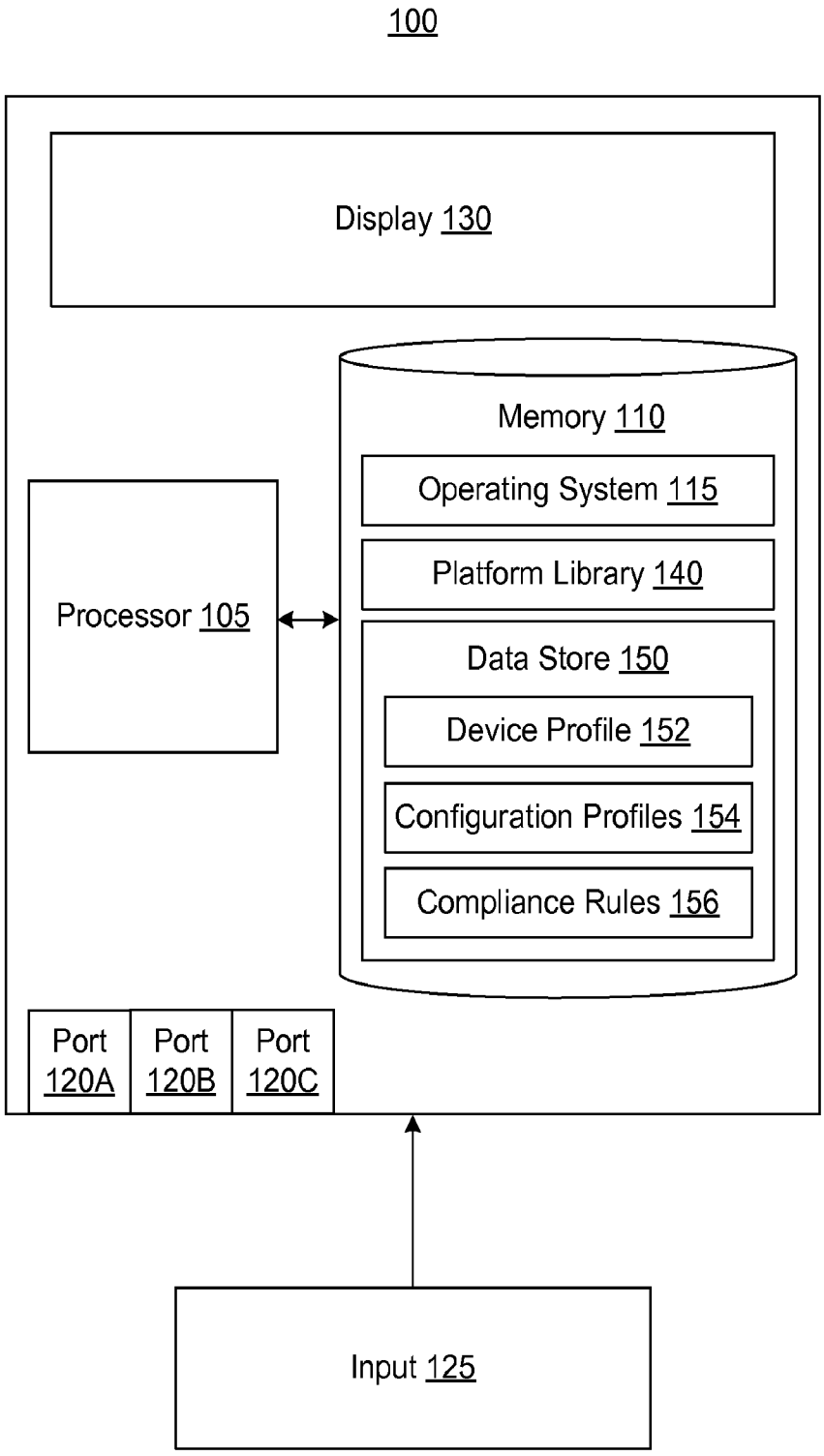
100
Display 130
Memory 110
Operating System 115
Platform Library 140
Processor 105
Data Store 150
Device Profile 152
Configuration Profiles 154
Compliance Rules 156
Port 120A
Port 120B
Port 120C
Input 125

Figure 1

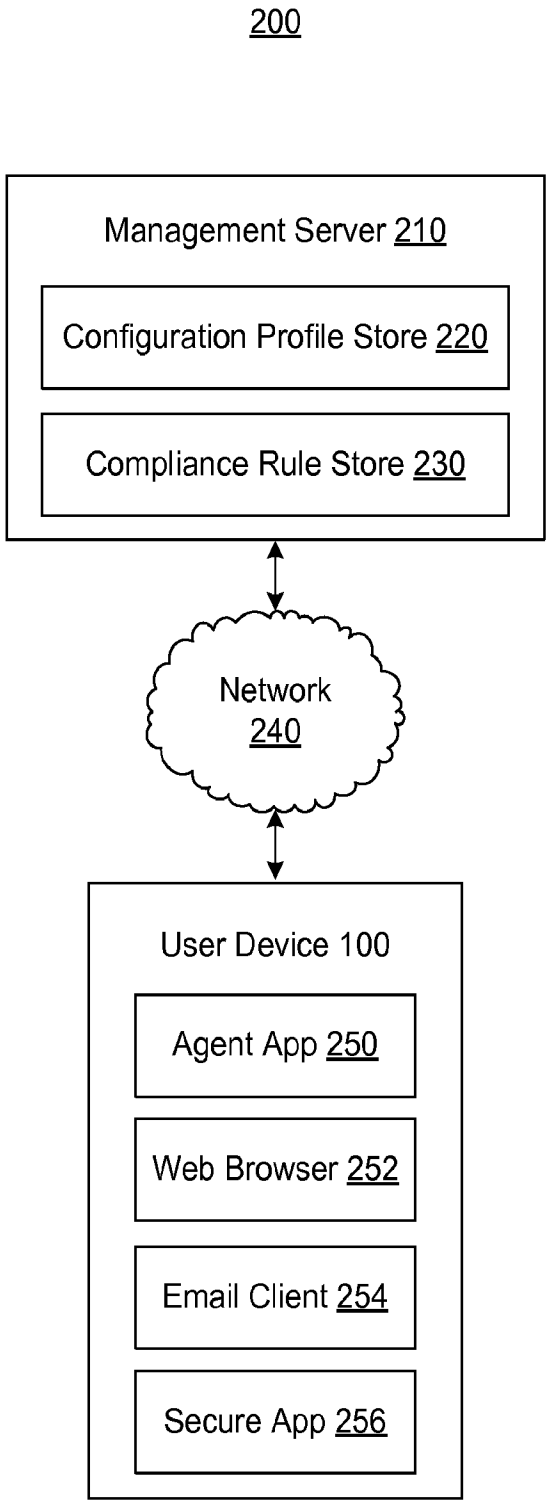
200
Management Server 210
Configuration Profile Store 220
Compliance Rule Store 230
Network 240
User Device 100
Agent App 250
Web Browser 252
Email Client 254
Secure App 256

Figure 2

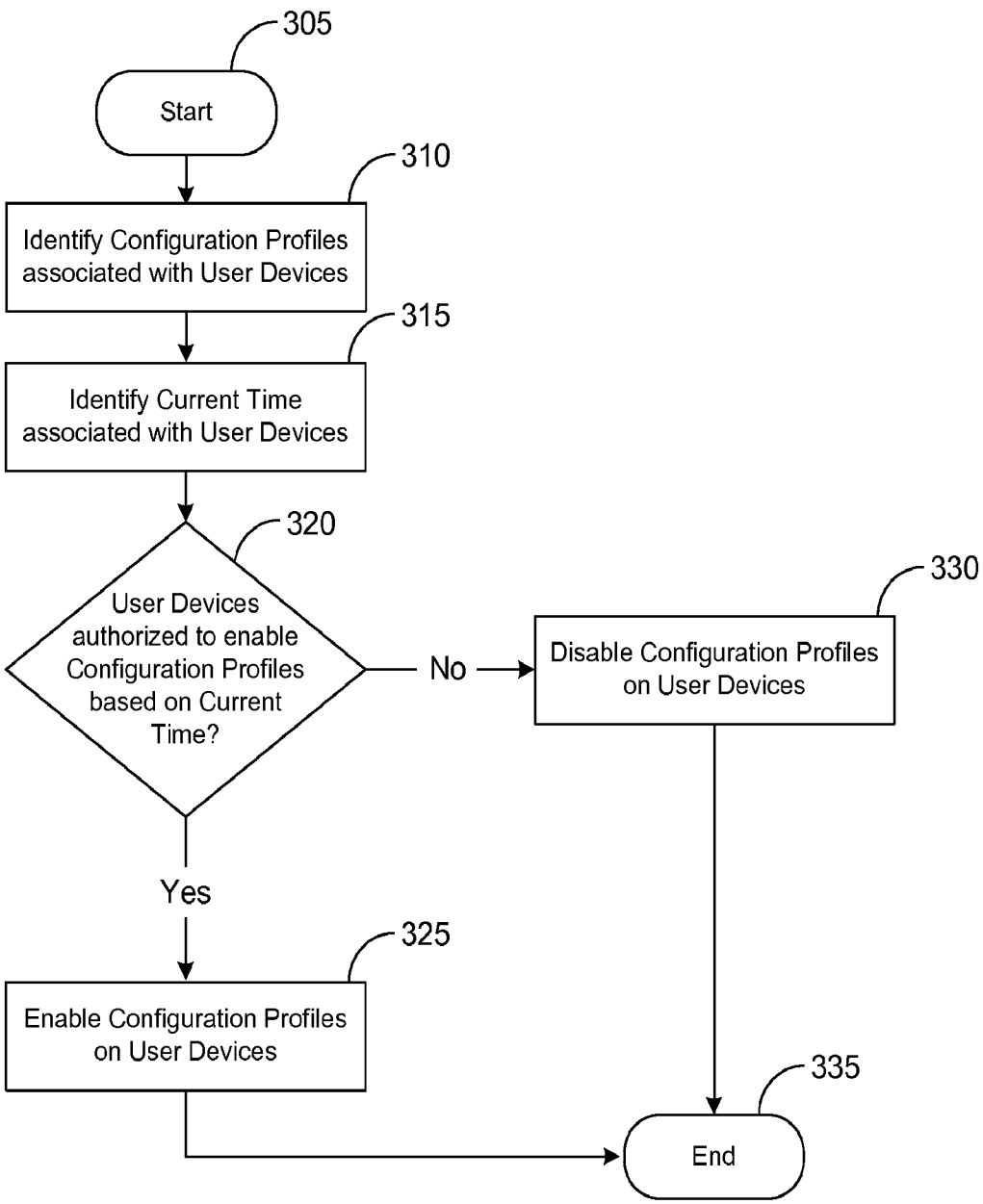
300
305
Start
310
Identify Configuration Profiles associated with User Devices
315
Identify Current Time associated with User Devices
320
User Devices authorized to enable Configuration Profiles based on Current Time?
No
330
Disable Configuration Profiles on User Devices
Yes
325
Enable Configuration Profiles on User Devices
335
End

Figure 3