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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2017 (24.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/142742 A1

(51) International Patent Classification:
G06F 21/30 (2013.01) *H04L 29/06* (2006.01)
G06F 9/44 (2006.01) *H04W 12/06* (2009.01)
G06F 21/45 (2013.01)

(21) International Application Number:
PCT/US2017/016809

(22) International Filing Date:
7 February 2017 (07.02.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/296,281 17 February 2016 (17.02.2016) US

(71) Applicant: **CARRIER CORPORATION** [US/US]; One Carrier Place, Farmington, Connecticut 06032 (US).

(72) Inventors: **GAUTHIER, Ed**; 1212 Pittsford-Victor Road, Pittsford, New York 14534 (US). **HOLM, Ben**; 1212 Pittsford-Victor Road, Pittsford, New York 14534 (US).

(74) Agent: **BARON, Eric J.**; CANTOR COLBURN LLP, 20 Church Street, 22nd Floor, Hartford, Connecticut 06103-3207 (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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, 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, ST, 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))*

[Continued on next page]

(54) Title: AUTHORIZED TIME LAPSE VIEW OF SYSTEM AND CREDENTIAL DATA

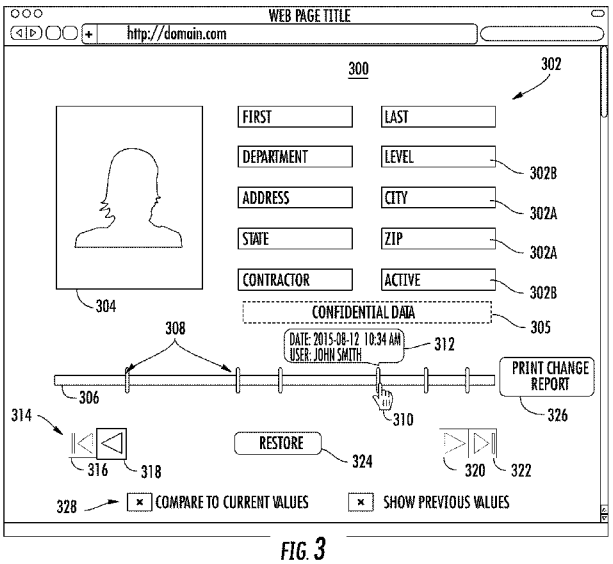

FIG. 3

(57) Abstract: A system includes a configuration management server operable to interface with a plurality of client devices via a network. The configuration management server includes a processor that is configured to track a change history of modifications to one or more records of a plurality of system data and credential data. An authorization status of a user of an access client of one of the client devices is determined. An authorized view of a selected record of the one or more records is output to the access client. One or more fields of the selected record are displayed based on the authorization status. An output of the change history of modifications to the one or more fields of the selected record to the access client is limited based on the authorization status.

WO 2017/142742 A1

Published:

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

AUTHORIZED TIME LAPSE VIEW OF SYSTEM AND CREDENTIAL DATA

DESCRIPTION OF RELATED ART

[0001] The subject matter disclosed herein relates to system configuration management, and more particularly to creating an authorized time lapse view of system and credential data.

[0002] Typically, security management systems track the present authorization of individuals to gain access to physical entry points and/or electronic systems. Security management systems can define credentials for individual users and groups of users to control access to physical locations and/or electronic data. However, such security management systems may be vulnerable to a rogue or unauthorized user changing access privileges without a means of detection. Further, in systems that track change history of security or credential data, the change history may be captured in a format that makes it difficult to determine how changes occurred over time and may provide users with change history of sensitive data that they would not otherwise be able to access.

BRIEF SUMMARY

[0003] According to an embodiment, a system includes a configuration management server operable to interface with a plurality of client devices via a network. The configuration management server includes a processor that is configured to track a change history of modifications to one or more records of a plurality of system data and credential data. An authorization status of a user of an access client of one of the client devices is determined. An authorized view of a selected record of the one or more records is output to the access client. One or more fields of the selected record are displayed based on the authorization status. An output of the change history of modifications to the one or more fields of the selected record to the access client is limited based on the authorization status.

[0004] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where a timeline control provides a user interface to select from one or more points in time when modifications to the one or more fields were made.

[0005] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where the change history of modifications include the one or more points in time when modifications to the one

or more fields were made, previous values of the one or more fields, and a modification user identifier that identifies a user who made the modifications to the one or more fields.

[0006] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where the change history of modifications is output on a user interface that displays one or more unmodified fields of the selected record in combination with the modifications to the one or more fields of the selected record.

[0007] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where visual cues of the change history of modifications to the one or more fields are output to the access client to highlight or flag changes.

[0008] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where a current instance of the selected record is restored to a previous version of the selected record from the change history of modifications to the one or more fields of the selected record based on receiving a restore request.

[0009] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where the system data includes configuration of one or more access control points of a secured environment, and the credential data includes user authorization data associated with the one or more access control points.

[0010] In addition to one or more of the features described above, or as an alternative to any of the foregoing embodiments, further embodiments could include where the change history of modifications to the one or more fields of the selected record is output as changes with respect to current values of the one or more fields or as incremental changes between sequential points in time.

[0011] According to an embodiment, a method includes tracking a change history of modifications to one or more records of a plurality of system data and credential data. An authorization status of a user of an access client is determined. An authorized view of a selected record of the one or more records is output to the access client, where one or more fields of the selected record are displayed based on the authorization status. An output of the change history of modifications to the one or more fields of the selected record to the access client is limited based on the authorization status.

[0012] Technical function of the embodiments described above includes providing an authorized time lapse view of system and/or credential data.

[0013] Other aspects, features, and techniques of the embodiments will become more apparent from the following description taken in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The subject matter is particularly pointed out and distinctly claimed in the claims at the conclusion of the specification. The foregoing and other features, and advantages of the embodiments are apparent from the following detailed description taken in conjunction with the accompanying drawings in which like elements are numbered alike in the several FIGURES:

[0015] FIG. 1 illustrates a schematic view of a system according to an embodiment;

[0016] FIG. 2 illustrates a schematic view of a change history structure according to an embodiment;

[0017] FIG. 3 illustrates a block diagram of a user interface according to an embodiment; and

[0018] FIG. 4 is a flow diagram of a method according to an embodiment.

DETAILED DESCRIPTION

[0019] Referring now to the drawings, FIG. 1 illustrates a schematic view of a system 100 according to an embodiment that can be implemented to configure access control points (e.g., physical security and/or data security) and user authorization in a secured environment. In the example depicted in FIG. 1, the system 100 includes a configuration management server 102 operable to interface with a plurality of client devices 104A-104N via a network 106. The network 106 may be any type of communications network known in the art and can include a combination of wireless, wired, and/or fiber optic links. Although only a single configuration management server 102 and three client devices 104A-N are depicted in FIG. 1, it will be understood that there can be any number of configuration management servers 102 and client devices 104A-N that can interface with each other and various networked components across the network 106. Further, one or more of the client devices 104A-N may also be the configuration management server 102.

[0020] In exemplary embodiments, the configuration management server 102 and/or client devices 104A-N can include a variety of processing devices with processing circuits and I/O interfaces, such as a keys/buttons, a touchscreen, audio input, a display device and

audio output. The configuration management server 102 and client devices 104A-N may be embodied in any type of computer device known in the art, such as a laptop, tablet computer, mobile device, personal computer, workstation, server, and the like. Accordingly, the configuration management server 102 and client devices 104A-N can include various computer/communication hardware and software technology known in the art, such as one or more processors, volatile and non-volatile memory including removable media, power supplies, network interfaces, support circuitry, operating systems, and the like.

[0021] The configuration management server 102 can include a configuration manager 108 that controls access to system data 110 and credential data 112 that may be stored in one or more files or databases. In an embodiment, the system data 110 can store configuration data for one or more access control points of a secured environment. For example, the system data 110 may establish a configuration of one or more security card (e.g., badge) readers, alarm systems, electronic locks, video surveillance systems, and the like as security data. The system data 110 can alternatively or additionally include personal information, non-security related data, location information, asset identifiers, various configuration parameters, and the like. The credential data 112 can include user authorization data associated with the one or more access control points. For example, each user that is issued an identification card or badge may be given access to select physical entry points, access to data servers, and the ability to read and/or modify settings in the system data 110 and/or the credential data 112.

[0022] In embodiments, the system data 110 includes current system data 110A and system data change history 110B. Similarly, the credential data 112 can include current credential data 112A and credential data change history 112B. The current system configuration is defined by the current system data 110A and the current credential data 112A. When one or more records of the current system data 110A are modified, a change history of modifications can be captured in the system data change history 110B. Similarly, when one or more records of the current credential data 112A are modified, a change history of modifications can be captured in the credential data change history 112B. The change history of modifications in the system data change history 110B and/or the credential data change history 112B can include, for instance, records of one or more points in time when modifications to one or more fields were made, previous values of the one or more fields, and a modification user identifier that identifies a user who made the modifications to the one or more fields.

[0023] In an alternate embodiment, change history is stored as a snapshot of data values at a point in time when the data values are saved. Using snapshots, a change history of modifications to one or more fields of a selected record can be determined by comparing records captured at different points in time, such as comparing a current record to a previous record. For example, when an update of the current system data 110A is requested, a snapshot of the current system data 110A can be copied into the system data change history 110B before changes are committed to the current system data 110A to populate a history for comparisons. Similarly, when an update of the current credential data 112A is requested, a snapshot of the current credential data 112A can be copied into the credential data change history 112B before changes are committed to the current credential data 112A.

[0024] Users of client devices 104A-N can use respective instances of access clients 114A-N to interface with the configuration manager 108 to view and/or modify the system data 110 and/or credential data 112. Users of access clients 114A-114N can each have a different authorization status that defines whether specific records or fields are available for viewing and/or editing. For instance, client device 104A may be a security desk laptop or PC, where a security guard uses access client 114A to grant temporary facility access to a visitor or contractor. Client device 104B may be a mobile computing device, where a maintenance worker uses access client 114B to install or reconfigure a physical access control point. Client device 104N may be a tablet computer, where a security manager uses access client 114N to audit the system data 110 and the credential data 112.

[0025] FIG. 2 illustrates a schematic view of a change history structure 200 according to an embodiment. The change history structure 200 illustrates a simplified example of a record 202 that may be incorporated in the current system data 110A or the current credential data 112A of FIG. 1. The record 202 includes current values 204 of one or more fields. As changes are made to the record 202, a change history 206 is created as a sequential list of change history records 206A-206N. Each of the change history records 206A-206N can include a corresponding timestamp 208 indicating when the change was made, a modification user identifier 210 indicating who made the change, and one or more previous values 212 of one or more fields that were updated. For example, if the record 202 is a record within current system data 110A, as the current values 204 are modified, the change history 206 is captured in the system data change history 110B such that the change date/time, change originator, and previous values are stored for auditing and/or restoration. Similarly, if the record 202 is a record within current credential data 112A, as the current values 204 are modified, the change history 206 is captured in the credential data change history 112B. In

an alternate embodiment, each record 202 is a snapshot of the current values 204, a timestamp 208 indicating when the record 202 was saved, and a modification user identifier 210 indicating who saved the record 202, where the record 202 can be stored in the current system data 110A or current credential data 112A as the most recently saved data and/or in the system data change history 110B or credential data change history 112B for older data.

[0026] FIG. 3 illustrates a block diagram of a user interface 300 according to an embodiment. The user interface 300 is an example that may be interactively displayed by one of the access clients 114A-N of FIG. 1. In the example of FIG. 3, the user interface 300 displays a plurality of fields 302 for a selected record, e.g., record 202 of FIG. 2. The fields 302 and associated data values can be output by the configuration manager 108 of FIG. 1. In FIG. 3, the fields 302 are from a selected record of the credential data 112 of FIG. 1; however, it will be understood that a similar user interface can be used for the system data 110 of FIG. 1. The user interface 300 may also include supplemental data 304, such as an image, a hyperlink, or other such data. A timeline control 306 on the user interface 300 allows a user to select from one or more points in time 308 when modifications to the values of one or more fields 302 were made.

[0027] A selection pointer 310 or other means can be used to highlight or select a point in time 308 to observe historical changes. Visual cues of the change history of modifications to one or more fields 302 can be output to the access client 114A-N to highlight or flag changes. For example, when selecting a point in time 308, the user interface 300 can display one or more unmodified fields 302A of the selected record in combination with the modifications to the one or more fields 302B of the selected record. Modifications can be summarized using pop-up/tooltip information bubbles 312. In some embodiments, a history of each field 302 may be viewed by moving the selection pointer 310 over the field 302.

[0028] A navigation control 314 may be used to incrementally step or jump between points in time 308 on the timeline control 306. For instance, button 316 can jump to an oldest point in time, button 318 can step sequentially through earlier points in time, button 320 can step sequentially through later points in time, and button 322 can jump to the most recent/current point in time. Other methods of navigating or stepping between points in time 308 are also contemplated. As a user navigates through points in time 308, hidden information, such as confidential data 305 that was inaccessible due to a user's authorization status remains hidden even though the confidential data 305 may be associated with the selected record. The navigation control 314 can also include a restore command 324 to

trigger restoration of a current instance of the selected record from a previous version of the selected record from the change history of modifications. A print change report command 326 may be provided to generate a report of changes on a field basis, record basis, user basis, or other basis.

[0029] The user interface 300 can further include other user selectable options 328 that modify how data changes are compared and displayed. For instance, the change history of modifications to the one or more fields 302 of the selected record can be output as changes with respect to current values of the one or more fields 302 or as incremental changes between sequential points in time 308. Further, the actual previous values may be suppressed when a history of change actions rather than data values is desired. Further options may also or alternatively be included in embodiments.

[0030] FIG. 4 illustrates a method 400 of using a fallback mobile proxy according to embodiments. The method 400 can be performed by various elements of FIGS. 1-3 and is described in reference to FIGS. 1-3. At block 402, the configuration manager 108 tracks a change history of modifications to one or more records of a plurality of system data 110 and credential data 112. At block 404, the configuration manager 108 determines an authorization status of a user of an access client 114A-N, e.g., based on group membership, department, or other authorization control. At block 406, the configuration manager 108 outputs an authorized view of a selected record of the one or more records to the access client 114A-N, where one or more fields of the selected record are displayed based on the authorization status. At block 408, the configuration manager 108 limits an output of the change history of modifications to the one or more fields of the selected record to the access client based on the authorization status.

[0031] As previously described, the configuration manager 108 can provide a timeline control 306 to a user interface 300 to select from one or more points in time 308 when modifications to the one or more fields were made. The change history of modifications can include one or more points in time when modifications to the one or more fields were made, previous values of the one or more fields, and a modification user identifier that identifies a user who made the modifications to the one or more fields. The change history of modifications can be output on a user interface 300 that displays one or more unmodified fields of the selected record in combination with the modifications to the one or more fields of the selected record. The change history of modifications to the one or more fields of the selected record may be output as changes with respect to current values of the one or more fields or as incremental changes between sequential points in time. Visual cues

of the change history of modifications to the one or more fields can be output to the access client to highlight or flag changes. A current instance of the selected record can be restored to a previous version of the selected record from the change history of modifications to the one or more fields of the selected record based on receiving a restore request.

[0032] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the embodiments. While the description of the present embodiments has been presented for purposes of illustration and description, it is not intended to be exhaustive or limited to the embodiments in the form disclosed. Many modifications, variations, alterations, substitutions or equivalent arrangement not hereto described will be apparent to those of ordinary skill in the art without departing from the scope of the embodiments. Additionally, while various embodiments have been described, it is to be understood that aspects may include only some of the described embodiments. Accordingly, the embodiments are not to be seen as limited by the foregoing description, but are only limited by the scope of the appended claims.

CLAIMS

What is claimed is:

1. A system, comprising:

a configuration management server operable to interface with a plurality of client devices via a network, the configuration management server comprising a processor that is configured to perform:

tracking a change history of modifications to one or more records of a plurality of system data and credential data;

determining an authorization status of a user of an access client of one of the client devices;

outputting an authorized view of a selected record of the one or more records to the access client, wherein one or more fields of the selected record are displayed based on the authorization status; and

limiting an output of the change history of modifications to the one or more fields of the selected record to the access client based on the authorization status.

2. The system of claim 1, wherein a timeline control provides a user interface to select from one or more points in time when modifications to the one or more fields were made.

3. The system of claim 2, wherein the change history of modifications comprises: the one or more points in time when modifications to the one or more fields were made, previous values of the one or more fields, and a modification user identifier that identifies a user who made the modifications to the one or more fields.

4. The system of any of the preceding claims, wherein the change history of modifications is output on a user interface that displays one or more unmodified fields of the selected record in combination with the modifications to the one or more fields of the selected record.

5. The system of any of the preceding claims, wherein visual cues of the change history of modifications to the one or more fields are output to the access client to highlight or flag changes.

6. The system of any of the preceding claims, wherein a current instance of the selected record is restored to a previous version of the selected record from the change history of modifications to the one or more fields of the selected record based on receiving a restore request.

7. The system of any of the preceding claims, wherein the system data comprises configuration of one or more access control points of a secured environment, and the

credential data comprises user authorization data associated with the one or more access control points.

8. The system of any of the preceding claims, wherein the change history of modifications to the one or more fields of the selected record is output as changes with respect to current values of the one or more fields or as incremental changes between sequential points in time.

9. A method comprising:

tracking a change history of modifications to one or more records of a plurality of system data and credential data;

determining an authorization status of a user of an access client;

outputting an authorized view of a selected record of the one or more records to the access client, wherein one or more fields of the selected record are displayed based on the authorization status; and

limiting an output of the change history of modifications to the one or more fields of the selected record to the access client based on the authorization status.

10. The method of claim 9, further comprising:

providing a timeline control to a user interface to select from one or more points in time when modifications to the one or more fields were made.

11. The method of claim 10, wherein the change history of modifications comprises: the one or more points in time when modifications to the one or more fields were made, previous values of the one or more fields, and a modification user identifier that identifies a user who made the modifications to the one or more fields.

12. The method of any of claims 9-11, wherein the change history of modifications is output on a user interface that displays one or more unmodified fields of the selected record in combination with the modifications to the one or more fields of the selected record.

13. The method of any of claims 9-12, wherein visual cues of the change history of modifications to the one or more fields are output to the access client to highlight or flag changes.

14. The method of any of claims 9-13, wherein a current instance of the selected record is restored to a previous version of the selected record from the change history of modifications to the one or more fields of the selected record based on receiving a restore request.

15. The method of any of claims 9-14, wherein the change history of modifications to the one or more fields of the selected record is output as changes with respect to current values of the one or more fields or as incremental changes between sequential points in time.

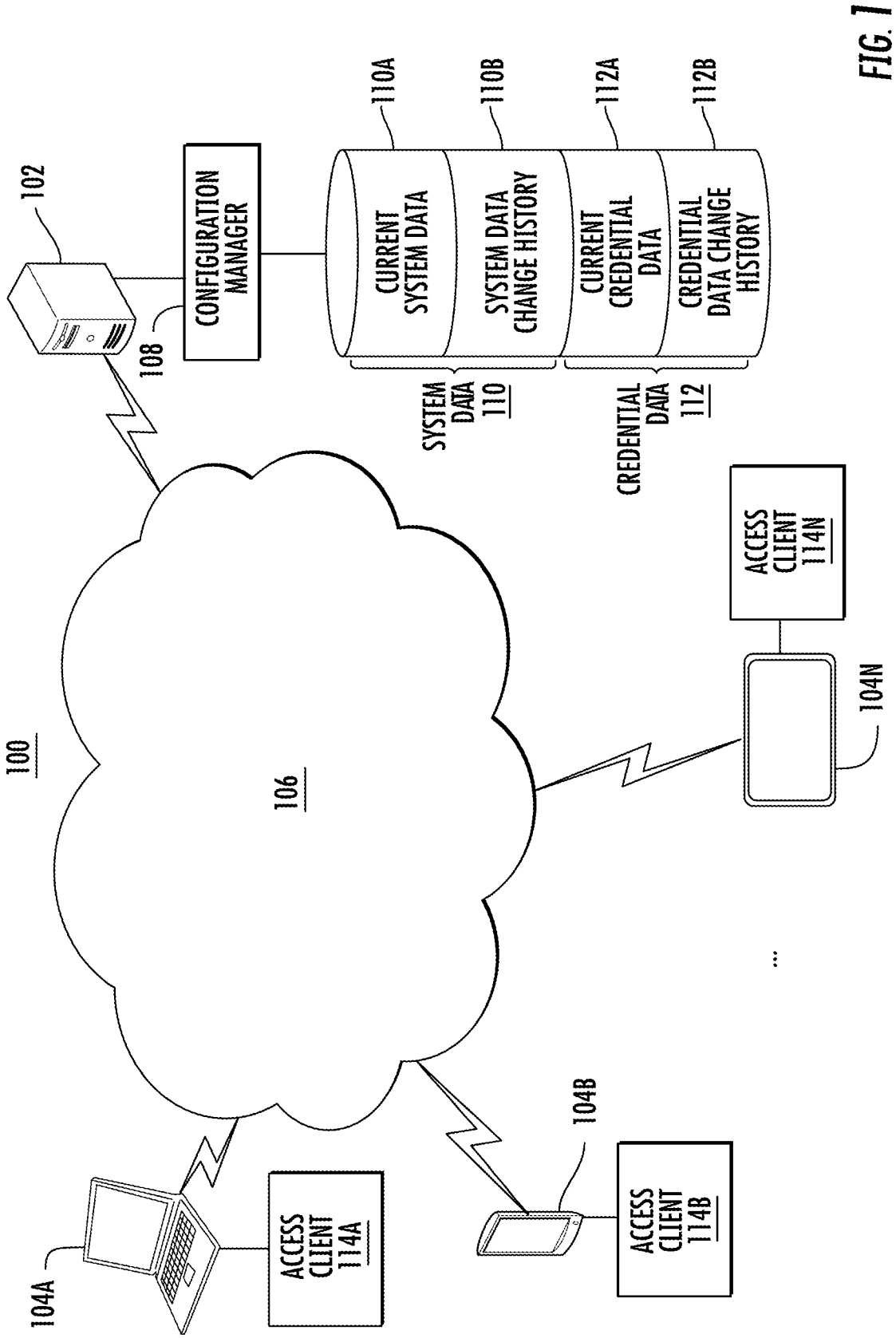
102
CONFIGURATION MANAGER
108
110A
110B
112A
112B
CURRENT SYSTEM DATA
SYSTEM DATA CHANGE HISTORY
CURRENT CREDENTIAL DATA
CREDENTIAL DATA CHANGE HISTORY
SYSTEM DATA 110
CREDENTIAL DATA 112
100
106
ACCESS CLIENT 114N
104N
104A
ACCESS CLIENT 114A
104B
ACCESS CLIENT 114B

FIG. 1

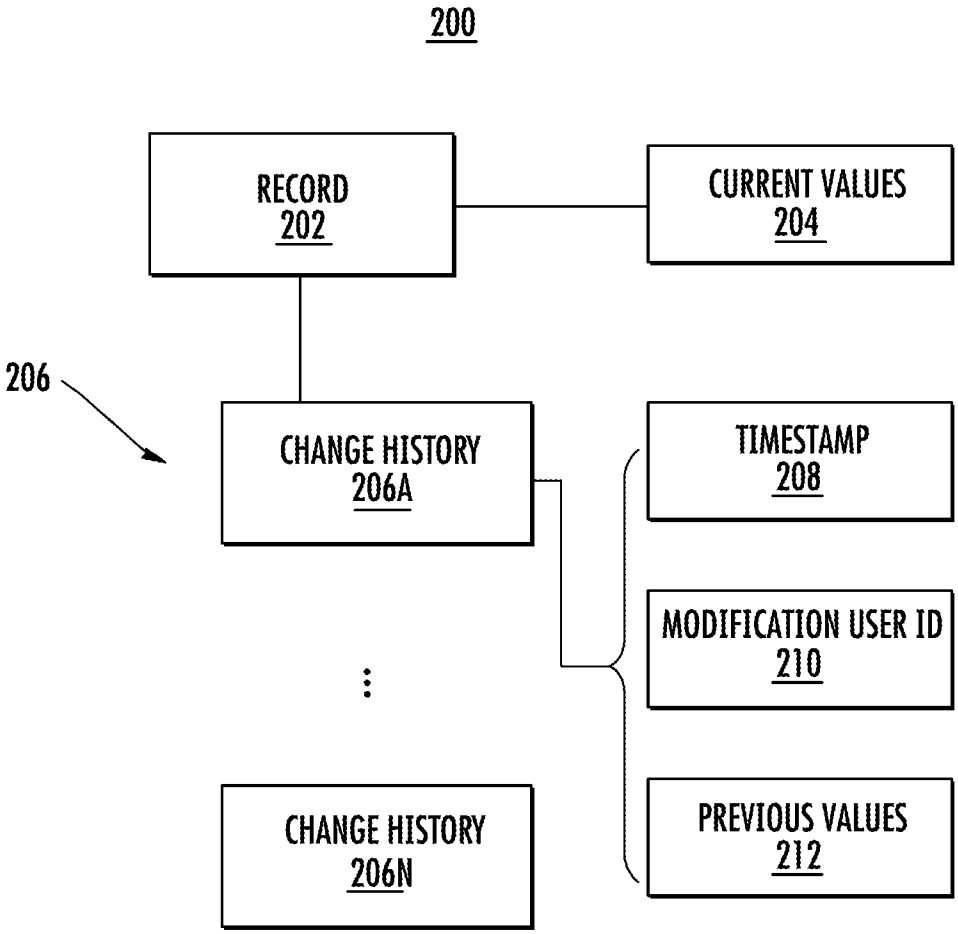
200
RECORD
202
CURRENT VALUES
204
206
CHANGE HISTORY
206A
TIMESTAMP
208
MODIFICATION USER ID
210
CHANGE HISTORY
206N
PREVIOUS VALUES
212

FIG. 2

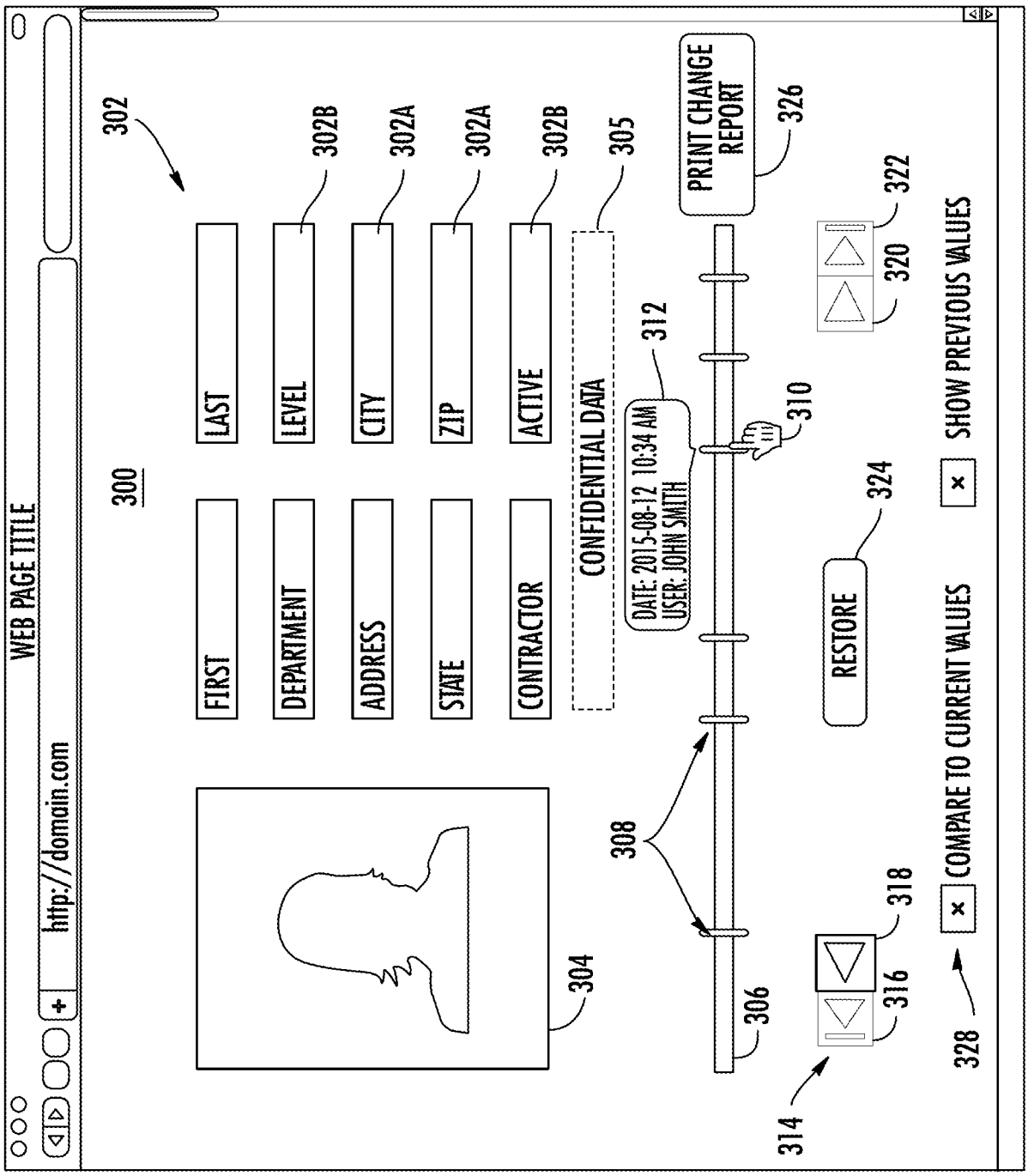
WEB PAGE TITLE
http://domain.com
300
302
FIRST
LAST
DEPARTMENT
LEVEL
ADDRESS
CITY
STATE
ZIP
CONTRACTOR
ACTIVE
CONFIDENTIAL DATA
302B
302A
302A
302B
305
304
308
306
DATE: 2015-08-12 10:34 AM
USER: JOHN SMITH
312
310
PRINT CHANGE REPORT
326
322
320
RESTORE
324
318
316
314
328
COMPARE TO CURRENT VALUES
SHOW PREVIOUS VALUES

FIG. 3

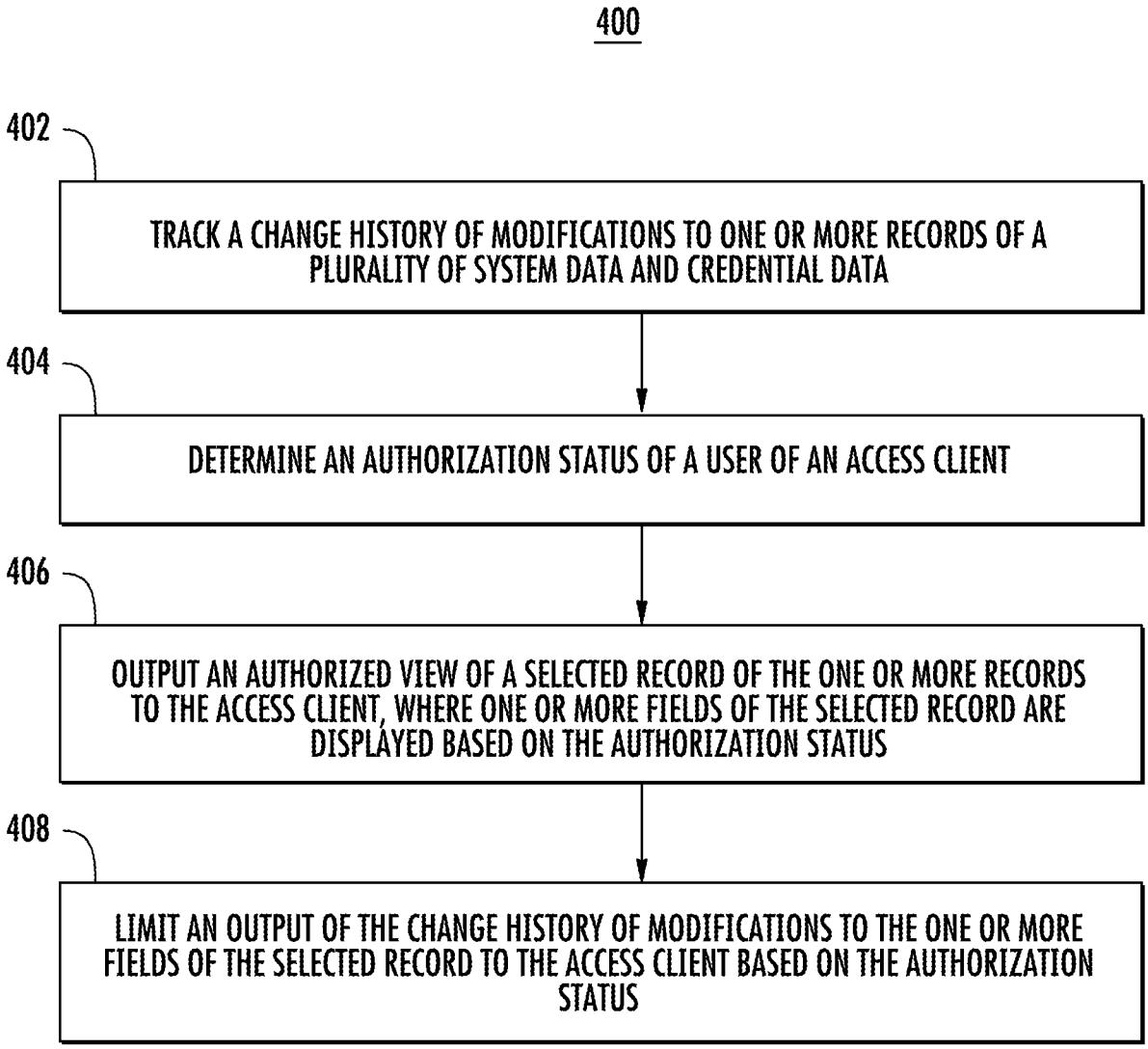
400
402
TRACK A CHANGE HISTORY OF MODIFICATIONS TO ONE OR MORE RECORDS OF A PLURALITY OF SYSTEM DATA AND CREDENTIAL DATA
404
DETERMINE AN AUTHORIZATION STATUS OF A USER OF AN ACCESS CLIENT
406
OUTPUT AN AUTHORIZED VIEW OF A SELECTED RECORD OF THE ONE OR MORE RECORDS TO THE ACCESS CLIENT, WHERE ONE OR MORE FIELDS OF THE SELECTED RECORD ARE DISPLAYED BASED ON THE AUTHORIZATION STATUS
408
LIMIT AN OUTPUT OF THE CHANGE HISTORY OF MODIFICATIONS TO THE ONE OR MORE FIELDS OF THE SELECTED RECORD TO THE ACCESS CLIENT BASED ON THE AUTHORIZATION STATUS

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/016809

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/30 G06F9/44 G06F21/45 H04L29/06 H04W12/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/016521 A1 (KIGO KENICHIRO [JP]) 20 January 2011 (2011-01-20)	1,9
Y	figure 5 paragraph [0023] paragraph [0042] paragraph [0044]	2-8, 10-15

Y	US 2011/083088 A1 (CISLER PAVEL [US] ET AL) 7 April 2011 (2011-04-07)	2-8, 10-15
A	figure 4b paragraph [0019] paragraph [0062] paragraph [0046]	1,9

A	US 2015/254453 A1 (SUGIYAMA TOSHIHARU [JP]) 10 September 2015 (2015-09-10) paragraph [0090] paragraph [0093]	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2017	20/04/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Caragata, Daniel

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/016809

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011016521 A1	20-01-2011	CN 101958794 A	26-01-2011
		JP 5413011 B2	12-02-2014
		JP 2011022942 A	03-02-2011
		US 2011016521 A1	20-01-2011
US 2011083088 A1	07-04-2011	EP 2054801 A1	06-05-2009
		HK 1131233 A1	20-11-2015
		US 2008034327 A1	07-02-2008
		US 2011083088 A1	07-04-2011
		WO 2008019248 A1	14-02-2008
US 2015254453 A1	10-09-2015	JP 5568696 B1	06-08-2014
		JP 2015170210 A	28-09-2015
		US 2015254453 A1	10-09-2015