METHOD, APPARATUS AND COMPUTER PROGRAM PRODUCT FOR MANAGING ACCESS TO A SOCIAL NETWORK SERVICE

BACKGROUND OF THE INVENTION

[0001] The present invention relates to social network services and more particularly to managing access to social network services.

[0002] Social networking sites such as, for example, Facebook, MySpace, Twitter, etc., provide an extremely cost-effective means for organisations to engage their customers and stakeholders.

[0003] There are however a number of challenges faced by these organisations in their use of social networking services.

[0004] One such challenge relates to user account management. Some organisations employ a single user account for the entire organisation. Others have multiple user accounts to support multiple products, brands or departments within the organisation. To maintain control, the one or more accounts of an organisation are typically administered by a single user. However, this results in a bottleneck in the engagement of customers and stakeholders on social networking platforms and additionally in the case of multiple accounts, duplication and wastage of resources.

[0005] Furthermore, because social networking platforms were not designed to be utilised by organisations for engaging and reaching out to their customers and

stakeholders, social network services lack access control features that restrict the actions a user is allowed to perform on a social networking site. Such services also lack the necessary tracking, logging and audit trail features that organisations commonly require of their corporate applications. Consequently, it is a challenge for organisations to ensure staff compliance with corporate policies when accessing social network services. It is also a challenge to carry out audit checks on social network service usage.

[0006] There is thus a need for a social network service access management system for organisations.

SUMMARY OF THE INVENTION

[0007] Accordingly, in a first aspect, the present invention provides a computer-implemented method for managing access to a social network service. The method includes receiving a request from a sub account and transmitting the request to the social network service for processing. The sub account is associated with a primary account of an organisation.

[0008] In a second aspect, the present invention provides a device for managing access to a social network service. The device includes a processor and a memory coupled to the processor. The processor is configured to receive a request from a sub account and transmit the request to the social network service for processing. The sub account is associated with a primary account of an organisation.

[0009] In a third aspect, the present invention provides a computer program product including a computer usable medium having a computer readable program. The computer readable program when executed on a computer causes the computer to receive a request from a sub account and transmit the request to the social network service for processing. The sub account is associated with a primary account of an organisation.

[0010] Other aspects and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The following detailed description of preferred embodiments of the invention will be better understood when read in conjunction with the appended drawings. The present invention is illustrated by way of example and is not limited by the accompanying figures, in which like references indicate similar elements.

[0012] FIG. 1 is a schematic block diagram of a social network service access management system in accordance with an embodiment of the present invention;

[0013] FIG. 2 is a schematic flow diagram of a method for managing access to a social network service in accordance with an embodiment of the present invention;

[0014] FIG. 3 is a schematic flow diagram of a method for providing a notification generated by a social network service to one or more relevant sub accounts in accordance with an embodiment of the present invention; and

[0015] FIG. 4 is a schematic block diagram of a device for managing access to a social network service in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0016] The detailed description set forth below in connection with the appended drawings is intended as a description of presently preferred embodiments of the invention, and is not intended to represent the only forms in which the present invention may be practiced. It is to be understood that the same or equivalent functions may be accomplished by different embodiments that are intended to be encompassed within the scope of the invention. In the drawings, like numerals are used to indicate like elements throughout.

[0017] Referring now to FIG. 1, a social network service access management system 10 is shown. The system 10 includes a corporate network 12 of an organisation and a device 14 for managing access to a social network service 16. The organisation is registered with the social network service 16 and has a primary account 18 with the social network service 16. Each user of the corporate network 12 is issued or assigned a sub account 20 that is associated with the primary account 18 of the organisation. In the

embodiment shown, the device 14 is provided in a demilitarised zone (DMZ) 22 and a firewall 24 is provided between the corporate network 12 and the device 14. However, it should be understood by persons of ordinary skill in the art that the present invention is not limited by the location of the device 14. For example, in an alternative embodiment, the device 14 may be sited with the corporate network 12 behind the firewall 24.

[0018] The device 14 functions as a gateway or proxy between the corporate network 12 and the primary account 18 of the organisation, thereby ensuring that all access by users of the corporate network 12 to the primary social network service account 18 of the organisation is regulated. All user actions relating to the primary account 18 of the organisation including viewing, posting, deleting, editing and sending of posts, messages and any other information can only be performed via the device 14. Users of the corporate network 12 are not able to perform any action relating to the primary account 18 of the organisation directly via an interface of the social network service 16.

[0019] In order to control and manage access to the primary social network service account 18 of the organisation, one or more of a plurality of access rights is assigned to each of the sub accounts 20 based on user profiles and roles within the organisation. Examples of the access rights that may be assigned include, but are not limited to, permission to access, create and/or delete tabs or sections, permission to access, read, create, edit and/or delete events, permission to access, read and/or

write postings on walls, permission to access, read and/or write status messages, and permission to access, read and/or write messages in an inbox.

[0020] The assigned access rights or permission settings determine the objects and/or connections each of the sub accounts 20 is able to access on the social network service 16 and the actions (e.g., create, edit, delete, read only, etc.) the sub account 20 is able to perform. For example, if one of the sub accounts 20 is authorized for read-only access, that sub account 20 will only be able to read posts/comments/messages only.

[0021] Varying levels of access rights may be set for the sub accounts 20. Each sub account 20 may be assigned different access rights.

[0022] The access rights and permission settings for the sub accounts 20 may be configured via the social network service access management device 14. Alternatively, the configuration of the access rights and permission settings may be linked to and carried out via an external Authentication, Authorization and Accounting (AAA) device such as, for example, Active Directory by Microsoft® or a third-party RADIUS server.

[0023] Referring now to FIG. 2, a method 50 for managing access to the social network service 16 will be described. The method 50 begins at step 52 when a request is received by the social network service access management device 14 from a sub account 20 associated with the primary account 18 of the organisation. The request may be a post, message

or comment, etc. and may be made by a user via a web interface. The primary account 18 may be required to log in to the social network service 16 when the request is received. In one embodiment, the log in is performed using OAuth 2.0 or other similar authorization methods.

[0024] If the request is a write request, a sub account identifier is appended to the write request at step 54. This allows users of the social network service 16 to identify the sub account 20 responsible for information shared via the primary account 18 of the organisation. In one embodiment, the write request is automatically tagged and appended with a digital signature of the user. The digital signature is forwarded with the write request to the social network service 16 and is uploaded to the social network platform. An exemplary post and an exemplary message with a sub account identifier appended are shown below.

[0025] Exemplary Post

> **[Organisation's Primary Account Name]** ABC Company; **[Content]** Our company is currently looking into expanding our sales & marketing team. Potential candidates for the position of sales manager should minimally have a degree from a reputable university and at least 2-3 years' of relevant experience; **[Digital signature]** Posted by Melissa Lee - HR, melissa@abc.com, 6555-5555

[0026] Exemplary Message

[Organisation's Primary Account Name] ABC Company
[Message] Hi, this is a test email
[Digital signature] Message from Melissa Lee - HR, melissa@abc.com, 6555-5555

[0027] The digital signature may be pre-assigned to the sub account 20 of the user or entered on-the-fly by the user and/or a system administrator.

[0028] At step 56, a determination is made if the request is related or linked to an existing object or connection of the social network service 16. The request is deemed to have a parent object or connection if it is, for example, a reply or response to an existing post, message, comment, or event, etc.

[0029] If at step 56, a determination is made that the request is related to an existing object or connection of the social network service 16, the request is tagged with an identifier corresponding to the existing object or connection at step 58. In other words, the request is tagged with the same unique identifier (ID) as its parent object or connection. This allows the social network service access management device 14 to determine which existing object or connection of the social network service 16 the request should be forwarded to since the unique ID of the request is the same as the unique ID of the parent object or connection.

[0030] If at step 56, a determination is made that the request is not related to an existing object or connection of the social network service 16 (i.e., the request does

not have a parent object or connection – it is a new post, message, comment, or event, etc.), the method 50 proceeds directly to step 60.

[0031] At step 60, details of the request are stored in a database associated with the social network service access management device 14. The details of the request stored in the database include the content of the post, message or comment, a user name, a user ID, a date/time stamp, any tagged or assigned identifiers, etc. Consequently, all user actions are captured and logged by the social network service access management device 14. User accounts/permission, activities/history logs, message posting/reply logs, object/connection properties, etc. may be monitored with the data stored in the database. The database may be provided within or separately from the social network service access management device 14.

[0032] The request is transmitted to the social network service 16 for processing at step 62. If the request is not related to an existing object or connection of the social network service 16, the request is processed by the social network service 16 as a new object or connection and a new identifier is generated by the social network service 16 for the new object or connection. The new identifier generated by the social network service 16 is transmitted back to the social network service access management device 14 where it is tagged to the request and stored with the other details of the request in the database associated with the social network service access management device 14.

[0033] The processing of the request by the social network service 16 may include creating a new post, message, comment or event, etc., or deleting an existing post, message, comment or event, etc. Posts, messages, comments, threads, etc. are regarded as objects and connections by the social network service 16 and all of them have their own unique ID, data and properties. Examples of object properties of a thread in a message thread and a comment are shown below.

[0034] Object properties of a thread in a message thread

Name	**Description**	**Permissions**	**Returns**
id	The unique ID for this message thread	read_mailbox	A JSON string
snippet	Fragment of the thread for use in thread lists	read_mailbox	A JSON string
updated_time	Timestamp of when the thread was last updated	read_mailbox	A JSON string containing a IETF RFC 3339 datetime
message_count	Number of messages in the thread	read_mailbox	An integer
unread_count	Number of unread messages in the thread	read_mailbox	An integer
tags	Thread tags	read_mailbox	A list of JSON strings

[0035] Object properties of a comment

Name	Description	Permissions	Returns
id	The Facebook ID of the comment	Available to everyone on Facebook by default	A JSON string
created_time	The timedate the comment was created	Available to everyone on Facebook by default	A JSON string containing a IETF RFC 3339 datetime
message	The comment text	Available to everyone on Facebook by default	A JSON string
from	The user that created the comment	Available to everyone on Facebook by default	A JSON object containing the id and name of the creating user
likes	The number of times this comment was liked	Available to everyone on Facebook by default	A JSON string

[0036] In a preferred embodiment after the request is processed at step 62 by the social network service 16, properties of objects and/or connections generated by the social network service 16 are stored in the database at step 64. This data/information is obtained via the

Application Programming Interface (API) of the social network service 16.

[0037] Request details stored in the database may be compared against object and/or connection properties of the social network service 16 stored in the database at step 66 to determine if any unauthorised access has been made to the primary account 18 of the organisation. For example, if a post is made directly to the social network service 16 without going through the social network service access management device 14, the stored details of all the requests made through the social network service access management device 14 will not tally with the stored details of all the objects/connections of the social network service 16 in the database as there will be a missing corresponding record in the request database. Whilst it is also possible to determine if any unauthorised access has been made to the primary account 18 of the organisation by comparing stored details of the requests made directly with objects and/or connections of the social network service 16 without storing the latter in the database, it is more efficient and practical and therefore preferable to store the properties of objects and/or connections generated by the social network service 16 in the database as otherwise internet connectivity needs to be up and multiple requests for details from the social network service 16 are required whenever a comparison needs to be made.

[0038] An audit trail or audit log of all actions carried out by one of the sub accounts 20 may be generated at step 68 with request details and object and/or connection properties of the social network service stored

in the database. The audit trail or audit log is generated by drawing on and matching the information stored in the database. The generated reports may be viewed online or output via report generating tools or software.

[0039] The social network service 16 may generate an alert, update or other form of notification whenever there is a new post, message, or reply, etc. made to the primary account 18. The notification may be provided at step 70 to one or more relevant sub accounts based on user profiles and roles within the organisation. The notification may be sent to the relevant users via, for example, email, webchat, instant messaging (IM) bot, or a smartphone application, etc.

[0040] Referring now to FIG. 3, a method 100 for providing a notification generated by the social network service 16 to one or more relevant sub accounts 20 is shown. The method 100 begins at step 102 when a notification is received by the social network service access management device 14 from the social network service 16. The received notification may be stored in the database of the social network service access management device 14.

[0041] At step 104, objects and/or connections associated with the notification are compared against request details and object and/or connection details stored in the database of the social network service access management device 14 to determine a relevance of the notification to the sub accounts 20 associated with the primary account 18 of the organisation. One or more of the

sub accounts 20 may be deemed relevant if the sub account 20 is authorised to receive alerts or notifications for the objects and/or connections associated with the notification (e.g., if a user of the sub account 20 has been granted access rights to a tab, section, page or application, etc.), or if a user of the sub account 20 has contributed any post, message, or comment, etc. on the objects and/or connections associated with the notification.

[0042] Once the one or more relevant sub accounts 20 are identified, the notification is transmitted to the one or more relevant sub accounts 20 at step 106.

[0043] Referring now to FIG. 4, a schematic block diagram of an exemplary embodiment of the social network service access management device 14 is shown. In the embodiment shown, the device 14 is a server including a processor 150 and a memory 152 coupled to the processor 150 via a bus 154. The processor 150 is configured to implement the methods 50 and 100 described above. As server computers are well known to those of ordinary skilled in the art, a detailed description of the hardware configuration of the device 14 is not required for a complete understanding of the present invention.

[0044] The device 14 may run on a Linux or Windows operating system with a database (e.g. MySQL) and an application/web server (e.g. Glassfish, Apache) installed either on the same or a separate server. The database keeps track of user accounts/permission, activities/history logs, message posting/reply logs, etc.

[0045] As is evident from the foregoing discussion, the present invention provides a holistic solution for organisations to connect to social networking platforms, leveraging on their reach and prevalence to serve as an extension of an organisation's customer relationship management (CRM), public/corporate relations activities, sales and marketing activities, pre/post-sales support functions, etc. This results in increased productivity, improved compliance, better access control and accountability. The present invention may be used to help organisations achieve their corporate governance, compliance, audit and accountability objectives. The present invention may be implemented as a server/appliance-based solution or software-only solution. In one embodiment, the present invention may be provided as a single web interface to consolidate all the feeds from multiple social networking sites.

[0046] The description of the preferred embodiments of the present invention have been presented for purposes of illustration and description, but are not intended to be exhaustive or to limit the invention to the forms disclosed. It will be appreciated by those skilled in the art that changes could be made to the embodiments described above without departing from the broad inventive concept thereof. It is understood, therefore, that this invention is not limited to the particular embodiments disclosed, but covers modifications within the scope of the present invention as defined by the appended claims.

[0047] Further, unless the context clearly requires otherwise, throughout the description and the claims, the

words "comprise", "comprising" and the like are to be construed in an inclusive as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to".

CLAIMS

1. A method for managing access to a social network service, the method comprising:

receiving a request from a sub account, wherein the sub account is associated with a primary account of an organisation; and

transmitting the request to the social network service for processing.

2. The method of claim 1, further comprising appending a sub account identifier to a write request.

3. The method of claim 1, further comprising storing details of the request in a database.

4. The method of claim 3, further comprising storing properties of objects and/or connections generated by the social network service in the database.

5. The method of claim 4, further comprising comparing request details stored in the database against object and/or connection properties of the social network service stored in the database to determine if any unauthorised access has been made to the primary account of the organisation.

6. The method of claim 4, further comprising generating an audit trail of the sub account with request details and object and/or connection properties of the social network service stored in the database.

7. The method of claim 1, further comprising determining if the request is related to an existing object or connection of the social network service.

8. The method of claim 7, further comprising tagging the request with an identifier corresponding to the existing object or connection if a determination is made that the request is related to an existing object or connection of the social network service.

9. The method of claim 1, further comprising assigning one or more of a plurality of access rights to the sub account.

10. The method of claim 1, further comprising providing a notification generated by the social network service to one or more relevant sub accounts associated with the primary account of the organisation.

11. The method of claim 10, wherein the step of providing the notification generated by the social network service to the one or more relevant sub accounts comprises:

receiving the notification from the social network service;

comparing objects and/or connections associated with the notification against request details and object and/or connection details stored in the database to determine a relevance of the notification to a plurality of sub accounts associated with the primary account of the organisation; and

transmitting the notification to the one or more relevant sub accounts.

12. A device for managing access to a social network service, the apparatus comprising:

a processor configured to:

receive a request from a sub account, wherein the sub account is associated with a primary account of an organisation; and

transmit the request to the social network service for processing; and

a memory coupled to the processor.

13. The device of claim 12, wherein the processor is further configured to append a sub account identifier to a write request.

14. The device of claim 12, wherein the processor is further configured to store details of the request in a database.

15. The device of claim 12, wherein the processor is further configured to store properties of objects and/or connections generated by the social network service in the database.

16. The device of claim 12, wherein the processor is further configured to provide a notification generated by the social network service to one or more relevant sub accounts associated with the primary account of the organisation based on user profiles and roles within the organisation.

17. A computer program product comprising a computer usable medium having a computer readable program, wherein the computer readable program when executed on a computer causes the computer to:

receive a request from a sub account, wherein the sub account is associated with a primary account of an organisation; and

transmit the request to the social network service for processing.

18. The computer program product of claim 17, wherein the computer readable program further causes the computer to append a sub account identifier to a write request.

19. The computer program product of claim 17, wherein the computer readable program further causes the computer to store details of the request in a database.

20. The computer program product of claim 17, wherein the computer readable program further causes the computer to store properties of objects and/or connections generated by the social network service in the database.