

Claims

1. A system comprising at least one client device, and at least one server device executing a server-side process of a web application,

the at least one client device including a first processing system having at least one hardware processor, the first processing system being configured to execute a first client application providing a first client-side portion of the web application and a second client application providing a second client-side portion of the web application, wherein the first client application is a browser application and the second client application is a native application,

the at least one server including a second processing system having at least one hardware processor, the second processing system being configured to execute the server-side portion of the web application and to perform operations comprising:

in response to a first access request received from the first client application, causing the first client application to perform a sign-on process prior to accessing application data provided by the server-side portion of the web application;

generating, in relation to the performed sign-on process, a first session, wherein the first client application is subsequently provided access to said application data using the first session;

when a second request is received from the second client application, determining, using at least one identifier included in the second request and a browser type associated with the second request, whether the first session is useable by the second client application to access said application data;

in the event that it is determined that the first session is useable by the second client application to access said application data, providing the second client application with access to the application data using the first session;

in the event that it is determined that the first session is not useable by the second client application to access said application data, causing the second client application to perform a sign-on process prior to accessing the application data, and subsequent to the second client application performing the sign-on process, providing the

second client application access to the application data using a second session generated in relation to the sign-on process performed by the second client application;

generating, in relation to a sign-on by an instance of either the first client application or the second client application executing on another client device, a third session, wherein said instance executing on said another device is subsequently provided access to said application data using the third session; and

in response to generating the third session, deactivating the first session and preventing access to the application data by the first client application and the second client application executing on the first client device.

2. The system according to claim 1, wherein the determining includes determining whether a value corresponding to the identifier is stored in a memory of the at least one server device in association with at least one of a plurality of session records.

3. The system according to claim 2, wherein the determining further comprises: identifying a corresponding previously stored entitlement associated with the web application,

wherein the determining is further based upon the identified entitlement.

4. The system according to claim 1, wherein the first processing system is further configured to:

determine, by the second client application, one or more candidate browser controls for use by the second client application to communicate with the server-side portion of the web application;

transmitting by the second client application to the server device, a first instance of the second request, wherein the first instance corresponds to a first selected one of the one or more candidate browser controls;

based upon a response received to the transmitted first instance of the second request, determining, by the second client application, whether to access the application

data, or to transmit a second instance of the second request, wherein the second instance corresponds to another one of the one or more candidate browser controls.

5. The system according to claim 4, wherein (a) when a browser type of the first client application is the same as a browser type of the first selected one of the one or more candidate browser controls, the response received indicates a presence of the first session, and (b) when the browser type of the first client application is different from the browser type of the first selected one of the one or more candidate browser controls, the response received represents a failure to find an existing session usable by the second client application.

6. The system according to claim 5, wherein the first processing system is further configured to:

when the response received indicates the presence of the first session, and a browser type of a currently selected one of the one or more candidate browser controls is different from a predetermined browser type, obtain a first session identifier that is included in the response;

instantiate a browser control of the predetermined browser type; and
access the application data using the instantiated browser control of the predetermined browser type and using the first session identifier.

7. The system according to claim 5, wherein the first processing system is further configured to:

after having transmitted one or more instances of the second request, in relation to a response received for an instance of the second request, perform-the sign-on by the second client application.

8. The system according to claim 1, wherein the second processing system is further configured to:

responsive to receiving an instance of the second request, determine whether the first session corresponds to a browser type currently associated with the second request;

if the determining determines that the first session corresponds to a browser type currently associated with the second request, return to the second client application a first session identifier associated with the first session; and

if the determining determines that the first session does not correspond to the browser type currently associated with the second request, return to the second client application an indication that no session usable by the second client application was found.

9. A server device including at least one hardware processor configured to execute a server-side portion of a web application and to perform operations comprising:

in response to a first access request received from a first client application having a first client-side portion of the web application, causing the first client application to perform a sign-on process prior to accessing application data provided by the server-side portion of the web application, wherein the first client application is a browser application;

generating, in relation to the performed sign-on process, a first session, wherein the first client application is subsequently provided access to said application data using the first session;

when a second request is received from a second client application having a second client-side portion of the web application, determining, using at least one identifier included in the second request and a browser type associated with the second request, whether the first session is useable by the second client application to access said application data, wherein the second client application is a native application;

in the event that it is determined that the first session is useable by the second client application to access said application data, providing the second client application with access to the application data using the first session;

in the event that it is determined that the first session is not useable by the second client application to access said application data, causing the second client application to perform a sign-on process prior to accessing the application data, and subsequent to the second client application performing the sign-on process, providing the second client application access to the application data using a second session generated in relation to the sign-on process performed by the second client application;

generating, in relation to a sign-on by an instance of either the first client application or the second client application executing on another client device, a third session, wherein said instance executing on said another device is subsequently provided access to said application data using the third session; and

in response to generating the third session, deactivating the first session and preventing access to the application data by the first client application and the second client application executing on the first client device.

10. The server device according to claim 9, wherein the at least one processor is further configured to:

responsive to receiving an instance of the second request, determine whether the first session corresponds to a browser type currently associated with the second request;

if the determining determines that the first session corresponds to a browser type currently associated with the second request, return to the second client application a first session identifier associated with the first session; and

if the determining determines that the first session does not correspond to the browser type currently associated with the second request, return to the second client application an indication that no session usable by the second client application was found.

11. A method performed by a server device including at least one processor, the method comprising:

executing a server-side portion of a web application;

in response to a first access request received from a first client application having a first client-side portion of the web application, causing the first client application to perform a sign-on process prior to accessing application data provided by the server-side portion of the web application, wherein the first client application is a browser application;

generating, in relation to the performed sign-on process, a first session, wherein the first client application is subsequently provided access to said application data using the first session;

when a second request is received from a second client application having a second client-side portion of the web application, determining, using at least one identifier included in the second request and a browser type associated with the second request, whether the first session is useable by the second client application to access said application data, wherein the second client application is a native application;

in the event that it is determined that the first session is useable by the second client application to access said application data, providing the second client application with access to the application data using the first session;

in the event that it is determined that the first session is not useable by the second client application to access said application data, causing the second client application to perform a sign-on process prior to accessing the application data, and subsequent to the second client application performing the sign-on process, providing the second client application access to the application data using a second session generated in relation to the sign-on process performed by the second client application;

generating, in relation to a sign-on by an instance of either the first client application or the second client application executing on another client device, a third session, wherein said instance executing on said another device is subsequently provided access to said application data using the third session; and

in response to generating the third session, deactivating the first session and preventing access to the application data by the first client application and the second client application executing on the first client device.

12. A non-transitory computer-readable storage medium, having stored thereon program instructions which, when executed by a computer of a server device, causes the server device to perform operations comprising:

executing a server-side portion of a web application;

in response to a first access request received from a first client application having a first client-side portion of the web application, causing the first client application to perform a sign-on process prior to accessing application data provided by the server-side portion of the web application, wherein the first client application is a browser application;

generating, in relation to the performed sign-on process, a first session, wherein the first client application is subsequently provided access to said application data using the first session;

when a second request is received from a second client application having a second client-side portion of the web application, determining, using at least one identifier included in the second request and a browser type associated with the second request, whether the first session is useable by the second client application to access said application data;

in the event that it is determined that the first session is useable by the second client application to access said application data, providing the second client application with access to the application data using the first session;

in the event that it is determined that the first session is not useable by the second client application to access said application data, causing the second client application to perform a sign-on process prior to accessing the application data, and subsequent to the second client application performing the sign-on process, providing the second client application access to the application data using a second session generated in relation to the sign-on process performed by the second client application;

generating, in relation to a sign-on by an instance of either the first client application or the second client application executing on another client device, a third

session, wherein said instance executing on said another device is subsequently provided access to said application data using the third session; and

in response to generating the third session, deactivating the first session and preventing access to the application data by the first client application and the second client application executing on the first client device.

13. A client device including at least one hardware processor configured to execute a first client application which is a browser application providing a first client-side portion of a web application and a second client application which is a native application providing a second client-side portion of the web application, and to perform operations comprising:

performing, by the first client application having transmitted a first request to a server-side portion of the web application, a sign-on to the server-side portion of the web application, and subsequent to the performed sign-on accessing application data from the server-side portion of the web application using a first session generated in relation to the performed sign-on;

transmitting by the second client application to the server device, a second request including a selected one of one or more candidate browser controls for use by the second client application to communicate with the server-side portion of the web application; and

based upon a response received to the transmitted second request, determining, by the second client application, whether to access application data of the server-side portion of the web application, or to transmit another instance of the second request,

wherein the server-side portion of the web application is configured to:

when the second request is received from the second client application, determining, using at least one identifier included in the second request and a browser type associated with the second request, whether the first session is useable by the second client application to access said application data;

in the event that it is determined that the first session is useable by the second client application to access said application data, providing the second client application with access to the application data using the first session; and

in the event that it is determined that the first session is not useable by the second client application to access said application data, causing the second client application to perform a sign-on process prior to accessing the application data, and subsequent to the second client application performing the sign-on process, providing the second client application access to the application data using a second session generated in relation to the sign-on process performed by the second client application;

generating, in relation to a sign-on by an instance of either the first client application or the second client application executing on another client device, a third session, wherein said instance executing on said another client device is subsequently provided access to said application data using the third session; and

in response to generating the third session, deactivating the first session and preventing access to the application data by the first client application and the second client application executing on the client device.

14. The client device according to claim 13, wherein (a) when a browser type of the first client application is the same as a browser type of the selected one of the one or more candidate browser controls, the response received indicates a presence of the first session, and (b) when the browser type of the first client application is different from the browser type of the selected one of the one or more candidate browser controls, the response received represents a failure to find an existing session usable by the second client application.

15. The client device according to claim 14, the at least one hardware processor is further configured to:

when the response received indicates the presence of the first session, and a browser type of the selected one of the one or more candidate browser controls is different from a predetermined browser type, obtain a first session identifier that is included in the response;

 instantiate a browser control of the predetermined browser type; and

 access the application data using the instantiated browser control of the predetermined browser type and using the first session identifier.