CLAIMS

1. A computer-implemented method for access token scope limiting, the computer-implemented method comprising:

presenting, by a computer, an access token received from a client containing a list of scopes to an authorization application programming interface of the computer, each scope contained in the list of scopes defining a permission to access a particular protected resource hosted by a resource server; and

returning, by the computer, a new access token to the client containing a decreased number of scopes using a scope alias in response to the authorization application programming interface requesting the decrease in the number of scopes in the list of scopes, the scope alias representing a plurality of specific scopes from the list of scopes contained in the presented access token , wherein the scope alias maintains a same level of access permissions for the access token as the list of scopes that the scope alias represents.

2. The computer-implemented method of claim 1, further comprising:

receiving, by the computer, an access token request with an authorization code and a client identifier from the client via a network;

determining, by the computer, whether scopes are specified in the access token request based on an analysis of the access token request; and

responsive to the computer determining that scopes are specified in the access token request based on the analysis, identifying, by the computer, a set of scopes specified in the access token request to form a set of specified scopes.

3. The computer-implemented method of claim 2 further comprising:

expanding, by the computer, each scope alias included in the set of specified scopes to form an expanded set of specified scopes; and

expanding, by the computer, all scope aliases included in authorized scopes (i) corresponding to the client identifier and (ii) retrieved from storage to form an expanded set of authorized scopes.

4. The computer-implemented method of claim 3 further comprising:

generating, by the computer, an intersection between the expanded set of specified scopes and the expanded set of authorized scopes; and

identifying, by the computer, a number of valid scopes corresponding to the access token request by the client based on the intersection between the expanded set of specified scopes and the expanded set of authorized scopes.

5. The computer-implemented method of claim 4 further comprising:

decreasing, by the computer, the number of valid scopes corresponding to the access token request using a number of predefined scope aliases, each of the number of predefined scope aliases representing a collection of two or more client-specified individual scopes;

generating, by the computer, the new access token for the client using the number of predefined scope aliases and any remaining valid scopes corresponding to the access token request not included in at least one of the number of predefined scope aliases; and

sending, by the computer, the new access token to the client via the network.

6. The computer-implemented method of claim 5 further comprising:

receiving, by the computer, a request to grant access to a protected resource hosted by a resource server along with the access token of the client that includes one or more scopes from the resource server via the network;

expanding, by the computer, each scope alias included in the one or more scopes of the access token to form an expanded set of access token scopes; and

determining, by the computer, whether the expanded set of access token scopes contains a scope that grants access to the protected resource.

7. The computer-implemented method of claim 6 further comprising:

responsive to the computer determining that the expanded set of access token scopes does not contain a scope that grants access to the protected resource, sending, by the computer, an indication to the resource server that access to the protected resource by the client is denied.

8. The computer-implemented method of claim 6 further comprising:

responsive to the computer determining that the expanded set of access token scopes does contain a scope that grants access to the protected resource, retrieving, by the

computer, a set of authorization policies corresponding to the protected resource hosted by the resource server; and

determining, by the computer, whether the set of authorization policies grants access to the protected resource by the client.

9. The computer-implemented method of claim 8 further comprising:

responsive to the computer determining that the set of authorization policies does not grant access to the protected resource by the client, sending, by the computer, a deny indication to the resource server that access to the protected resource by the client is denied; and

responsive to the computer determining that the set of authorization policies does grant access to the protected resource by the client, sending, by the computer, a grant indication to the resource server that access to the protected resource by the client is granted.

10. The computer-implemented method of claim 1 further comprising:

receiving, by the computer, a refresh token containing a list of scopes corresponding to an existing access token of the client along with a request for the new access token specifying a limited set of scopes from the client via a network, the limited set of scopes specific to a particular set of protected resources that the client wants to access;

expanding, by the computer, each scope alias included in the list of scopes of the refresh token to form an expanded set of refresh token scopes; and

expanding, by the computer, each scope alias included in the limited set of scopes specified in the request for the new access token to form an expanded set of specified scopes.

11. The computer-implemented method of claim 10 further comprising:

generating, by the computer, an intersection between the expanded set of refresh token scopes and the expanded set of specified scopes; and

identifying, by the computer, a number of valid scopes corresponding to the request for the new access token based on the intersection between the expanded set of refresh token scopes and the expanded set of specified scopes.

12. The computer-implemented method of claim 11 further comprising:

decreasing, by the computer, the number of valid scopes corresponding to the request for the new access token using one or more predefined scope aliases, each of the one or more predefined scope aliases representing a collection of two or more client-specified individual scopes;

generating, by the computer, the new access token for the client using the one or more predefined scope aliases and any remaining valid scopes corresponding to the request for the new access token that were not included in the one or more predefined scope aliases; and

sending, by the computer, the new access token to the client via the network.

13. A computer system for access token scope limiting, the computer system comprising:

a bus system;

a storage device connected to the bus system, wherein the storage device stores program instructions; and

a processor connected to the bus system, wherein the processor executes the program instructions to:

present an access token received from a client containing a list of scopes to an authorization application programming interface, each scope contained in the list of scopes defining a permission to access a particular protected resource hosted by a resource server; and

return a new access token to the client containing a decreased number of scopes using a scope alias in response to the authorization application programming interface requesting the decrease in the number of scopes in the list of scopes, the scope alias representing a plurality of specific scopes from the list of scopes contained in the presented access token, wherein the scope alias maintains a same level of access permissions for the access token as the list of scopes that the scope alias represents.

14. The computer system of claim 13, wherein the processor further executes the program instructions to:

receive an access token request with an authorization code and a client identifier from the client via a network;

determine whether scopes are specified in the access token request based on an analysis of the access token request; and

identify a set of scopes specified in the access token request to form a set of specified scopes in response to determining that scopes are specified in the access token request based on the analysis.

15. The computer system of claim 14, wherein the processor further executes the program instructions to:

expand each scope alias included in the set of specified scopes to form an expanded set of specified scopes; and

expand all scope aliases included in authorized scopes (i) corresponding to the client identifier and (ii) retrieved from storage to form an expanded set of authorized scopes.

16. The computer system of claim 15, wherein the processor further executes the program instructions to:

generate an intersection between the expanded set of specified scopes and the expanded set of authorized scopes;

identify a number of valid scopes corresponding to the access token request by the client based on the intersection between the expanded set of specified scopes and the expanded set of authorized scopes;

decrease the number of valid scopes corresponding to the access token request using a number of predefined scope aliases, each of the number of predefined scope aliases representing a collection of two or more client-specified individual scopes;

generate the new access token for the client using the number of predefined scope aliases and any remaining valid scopes corresponding to the access token request not included in at least one of the number of predefined scope aliases; and

send the new access token to the client via the network.

17. A computer program product for access token scope limiting, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a computer to cause the computer to perform a method of:

presenting, by the computer, an access token received from a client containing a list of scopes to an authorization application programming interface of the computer, each scope contained in the list of scopes defining a permission to access a particular protected resource hosted by a resource server; and

returning, by the computer, a new access token to the client containing a decreased number of scopes using a scope alias in response to the authorization application programming interface requesting the decrease in the number of scopes in the list of scopes, the scope alias representing a plurality of specific scopes from the list of scopes contained in the presented access token, wherein the scope alias maintains a same level of access permissions for the access token as the list of scopes that the scope alias represents.

18. The computer program product of claim 17, further comprising:

receiving, by the computer, an access token request with an authorization code and a client identifier from the client via a network;

determining, by the computer, whether scopes are specified in the access token request based on an analysis of the access token request; and

responsive to the computer determining that scopes are specified in the access token request based on the analysis, identifying, by the computer, a set of scopes specified in the access token request to form a set of specified scopes.

19. The computer program product of claim 18 further comprising:

expanding, by the computer, each scope alias included in the set of specified scopes to form an expanded set of specified scopes; and

expanding, by the computer, all scope aliases included in authorized scopes (i) corresponding to the client identifier and (ii)retrieved from storage to form an expanded set of authorized scopes.

20. The computer program product of claim 19 further comprising:

generating, by the computer, an intersection between the expanded set of specified scopes and the expanded set of authorized scopes; and

identifying, by the computer, a number of valid scopes corresponding to the access token request by the client based on the intersection between the expanded set of specified scopes and the expanded set of authorized scopes.

21. The computer program product of claim 20 further comprising:

decreasing, by the computer, the number of valid scopes corresponding to the access token request using a number of predefined scope aliases, each of the number of predefined scope aliases representing a collection of two or more client-specified individual scopes;

generating, by the computer, the new access token for the client using the number of predefined scope aliases and any remaining valid scopes corresponding to the access token request not included in at least one of the number of predefined scope aliases; and

sending, by the computer, the new access token to the client via the network.

22. The computer program product of claim 21 further comprising:

receiving, by the computer, a request to grant access to a protected resource hosted by a resource server along with the access token of the client that includes one or more scopes from the resource server via the network;

expanding, by the computer, each scope alias included in the one or more scopes of the access token to form an expanded set of access token scopes; and

determining, by the computer, whether the expanded set of access token scopes contains a scope that grants access to the protected resource.

23. The computer program product of claim 22 further comprising:

responsive to the computer determining that the expanded set of access token scopes does not contain a scope that grants access to the protected resource, sending, by the computer, an indication to the resource server that access to the protected resource by the client is denied.

24. The computer program product of claim 23 further comprising:

responsive to the computer determining that the expanded set of access token scopes does contain a scope that grants access to the protected resource, retrieving, by the computer, a set of authorization policies corresponding to the protected resource hosted by the resource server; and

determining, by the computer, whether the set of authorization policies grants access to the protected resource by the client.

25. The computer program product of claim 24 further comprising:

responsive to the computer determining that the set of authorization policies does not grant access to the protected resource by the client, sending, by the computer, a deny indication to the resource server that access to the protected resource by the client is denied; and

responsive to the computer determining that the set of authorization policies does grant access to the protected resource by the client, sending, by the computer, a grant indication to the resource server that access to the protected resource by the client is granted.