

Secure Collaboration Environments

November 2008

Experience Revolutionary Collaboration

CollabraSpace
180 Admiral Cochrane Drive
Suite 525
Annapolis, MD 21401
410.224.4343
www.collabraspace.com

Executive Summary

Many organizations interested in collaboration or information sharing environments have to balance the need for increased efficiencies with their need or desire to protect information. Users need to be sure that the person(s) they are collaborating with are in fact who they say they are. In addition, sensitive information may need to be shared in real-time with a limited set of users, yet ensure that the information does not spill into the rest of the user community. Organizations that have successfully deployed collaborative work environments have leveraged products that have been designed with a flexible security structure for the enterprise.

CollabraSuite is designed to operate in a secure enterprise environment. It leverages the J2EE security model for providing identification, authentication, and authorization. CollabraSuite provides full auditing and metric reporting on all collaborative activities. In addition to the operating environment, the collaborative environment contains access controls allowing users to share information with their peers or other community members while protecting that same information from those who are not part of the specific group or community.

The CollabraSuite virtual environment is structured as a campus consisting of buildings, floors, and rooms. CollabraSuite also supports multiple campuses that allow users to move between campuses. In this scenario, users enter the campus as individuals who can roam anywhere in the campus that has not been restricted. Users can be added to groups and with permission can then access other remote campuses. Privileges may also be added to a user so that an individual user may access restricted space within the same campus.

Document repositories, in the form of a file cabinet, are located in each room. Users can choose to control access to folders or documents by adding read/write permissions or may leave the folders or documents open for all to share.

The CollabraSuite environment is typically administered by corporate-wide system administrators. Additional administrators may be assigned at any level of the campus structure, which includes the campus, building, floor or room, to protect specific areas within the collaborative environment.

The collaborative environment can be tailored to any community or group. A community may decide to leave their space open for all to enter and view. Other groups may decide to leave their room open but restrict access to certain folders or documents. Other groups may completely restrict access to their environment to all but a select few.

Security Infrastructure

CollabraSuite can leverage the SSL/TLS protocols between the server and client to ensure secure communications. Because authentication is performed by the J2EE application server, CollabraSuite can take advantage of existing LDAP servers, PKI infrastructures and single sign-on solutions to seamlessly tie into corporate authentication services.

Additional details on configuring security can be found in the CollabraSuite Developer's Guide.



CollabraSpace

Revolutionary Collaboration

www.collabraspace.com

Room Access

The campus, building, floor, or room can be locked down for access only by specific users or groups. This restriction occurs at the highest level and flows down to all its children. Thus, if a campus was restricted, all buildings, floors, and rooms created in the campus would carry the same restrictions.

Users or groups may be assigned specific access to a certain campus or location within the campus. For access to any remote campus, a user must be placed into a group and must be accepted by the system administrator of the remote campus. Users or groups who have been granted privileges to enter the campus have access to all the buildings, floors, and rooms in the campus that have not been further restricted.

Folders and Documents

Document management is performed at the user and/or group level. Any user can add restrictions to any folder, file, or document that has not been previously restricted. Restrictions include read/write privileges where only the entitled users would even see that the folder or document is contained in a room's file cabinet. This provides additional access controls on documents and folders beyond the access controls to the room itself. Therefore, even if a room has been restricted to a certain group or users, further restrictions can be added on a folder or document.

Detailed instructions for adding or removing restrictions on documents and folders are provided in the CollabraSuite User's Guide.

Administration

CollabraSuite Administrators can be assigned at any level within the structure as well. If a building was restricted, the community or group could assign its own administrators to administer all of the functions within the building. Building administration functions include adding or deleting floors and rooms as well as modifying the permissions for those floors and rooms. However, these system administrators would not have any control over other buildings within the campus or other campuses.

Details on how to assign administrators, set up a remote campus, organize groups, or perform any other administrative function are described in the CollabraSuite Administrator's Guide.

Designing a Secure Environment

Since a secure space can be accommodated at any level of the virtual structure, a user group or community should first decide on the overall structure for their organization. A large scale community with multiple organizations and subgroups may have a need for its own campus. A smaller group, who needs a secure space to share information on a specific event or series of events, may find a restricted room adequate for their purposes.

A Remote Campus is a collaborative environment designed as a stand alone structure. Users from a remote campus can enter other campuses for which they have been authorized. Administrators can set up their own campus so that only their selected users can enter. A remote campus must identify system administrators to perform the administrative



CollabraSpace
Revolutionary Collaboration

www.collabraspace.com

functions for their campus. As an additional security layer, users from other campuses must be accepted by the administrator of the remote campus prior to gaining access to a specific campus.

The administrators identified by a community or group for their remote campus or other secure space will control all access to the restricted space. Further thought should be given to the addition of CollabraSuite administrators to deal with issues that room or campus administrators may not be familiar with. It is possible that these administrators may need to sign special documents, such as non-disclosure agreements, to protect the contents of individual rooms or campuses.



CollabraSpace
Revolutionary Collaboration

www.collabraspace.com