

Understanding Repository Security

Overview

The Repository is designed to provide a secure environment for the management of projects where one user cannot accidentally affect the work of others. It is also intended to promote a high degree of collaboration by sharing information freely.

Database Access Control

The outer layer of security is provided by the access control list of the database which limits who can open the database and what kind of changes they can make. All project users, including the project managers, should be designated as "authors" in the database. A few individuals should also be assigned the special role of [PGADMIN] which allows them to make changes in all documents.

Note that Project Managers should not be [PGADMIN]'s because it will defeat some of the normal protection the system provides from accidental data loss.

Information Access Control

There are four classes of information in the repository. These are Projects & Assignments, Timesheets, Profile documents and Information documents.

Projects and Assignments

Most of which are created using planning tools such as Microsoft Project. The security of these documents can take two forms. Normal security means that these documents can be seen by all users, but can only be modified by the person assigned and the project manager of that project. The more stringent security mode means that the assignments are only visible to the participant and the project manager, no one else can see the assignment.

The security for these documents is setup automatically using the User ID information stored in the project and participant profiles. Thus it is important to setup the profiles correctly.

Timesheets

These have security and approval properties set for each participant. In general, only a predefined named list of people can create a Timesheet for a participant. In Project Gateway 5.1 and later, Timesheets can only be seen by people who have the right to modify them. So while you can see your own Timesheets when you look into the database, you will not generally be able to see Timesheets belonging to others.

Profile Documents

Profile documents define the structure of the system. There are 5 kinds of profiles, Project, Program, Participant, Organization, and Team.

Profiles are normally visible to everyone, but can only be modified by the specific named managers identified within each profile.

General Documents

This class includes Project Documents, Issues, Risks, Discussion, Scope Change, and Status Report documents that are routinely created and used by participants and managers alike.

These documents are always manually created by database users. When created the author has the choice to limit both editing and reading. These limits can be changed later, but only by someone who has the right to modify the document.

Limiting reading means that the document is invisible to people who are not on the reader list for that document, even though they may have Editor, Designer or Manager rights to the database. When a document is hidden, the view categories may still appear, but nothing will be displayed when they are expanded. This can be confusing unless you have used other Notes applications with read limited documents.

Limiting editing restricts the set of people who can modify the document once it has been created. Note that the author can always modify the document.

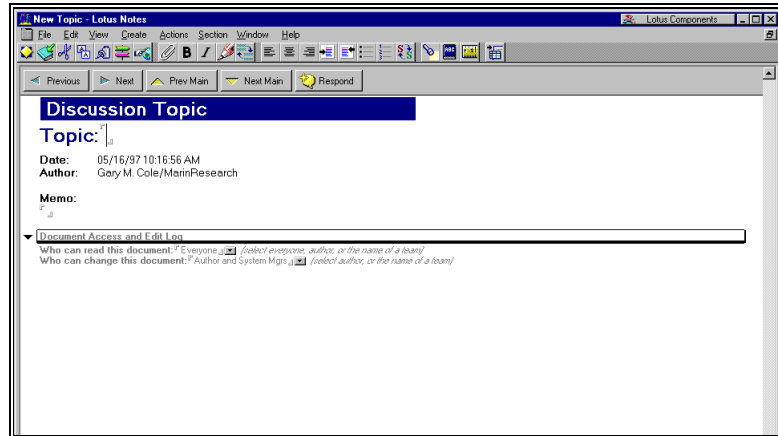
The security of these documents can be individually defined by the creators of the document. In general, the creator and the project manager will be able to edit them (for documents that are associated with specific projects), but everyone will be able to read them. This is discussed in more detail in the next section.

The default visibility for these documents can be preset on a project by project basis using the project policy controls found in each project profile.

Document Access Section

Document access is controlled by two keyword selections located in the Access Control section of these documents. When the document is created or is being edited, these fields may be modified to set the security for future access.

Here is an example as seen in the discussion topic form.



Who can read this document:

When a project related document is created, this field will be preset to "Default". This means that, if the project has specified a reader team, then that team will be assigned, otherwise the Everyone will be used

The options vary somewhat from based upon the document type, but choices generally include "Everyone", "Author & System Mgr" on documents that are not project specific, or to "Author & Project & System Mgr" on documents that are project specific, and the names of all Team Profiles.

Who can modify this document:

This field will be set by default to "Author & System Mgr" on documents that are not project specific, or to "Author & Project & System Mgr" on documents that are project specific. It can also be set to the name of a Team Profile.

Note that anyone who can modify a document automatically has the right to read it, even if they are not part of the reader list or team.

Teams and Team Profiles

A *Team* is a named list of people. This list is created and maintained in a document called a Team Profile. Once a team profile has been created, other documents can use the team to control read or edit access by selecting the name of the team in the document access control fields.

When a team is specified in the "Who can read..." field, only those people who are listed in the Team Profile, and the editors of that document, will be able to see the document in the database. The document will be invisible to everyone else except someone with the role of [PGMASTER].

When a team is specified in the "Who can modify..." field, only those people who are listed in the Team Profile will be able to change the document.

Composing a Team Profile

This document can be created using the "Create a Team Profile" item on the Participants Navigator. This will prompt you to choose the type of team profile form to be used. There are two types of team profiles known simply as Type I and Type II.

Type I Team Profiles allow you to define a team by specifying the name of an organization and/or entering the names of specific people.

Using an organization name means that all members of that organization and its sub-organizations will be members of the team.

Using a named list allows you to select any users without regard to the organization structure. This is convenient when working in a Notes client because you can select names directly from the address book just as you would for an email. However this address list is not available to web users. They must then type names in correctly to use the form.

Type II Team Profiles allow you to define a team by selecting from a checklist of participant names. This works for both Notes and Web users because there is no typing required, but all members of the team must have participant profiles in the database.

Creating a Type I Team Profile (Notes)

1. Click on "create a new team profile" item on the Participants Navigator.
2. Select Type I
3. Enter a name for the new team that is not already used. If you pick an existing name, an error will appear when you close the document.
4. You may specify an Organization name from the list provided. If you do, all the members of the organization will be made members of the team.
5. You may list members individually by putting their names in one of the grid fields (which can each contain multiple entries). Note: In the list, you may enter User Names, Notes Groups, or Notes Roles.
6. Adjust the document access controls (see below.)
7. Close and save the new team profile.

Creating a Type II Team Profile (Notes)

1. Click on "create a new team profile" item on the Participants Navigator.
2. Select Type II
3. Enter a name for the new team that is not already used. If you pick an existing name, an error will appear when you close the document.
4. Press the "Select Participants" action.

5. This will display a series of dialog boxes containing columns of participant names and checkboxes. Click the participants to be included and press OK to go on to the next page of names until done.
6. Adjust the document access controls (see below).
7. Close and save the team profile.

Creating a Type I Team Profile (Web)

1. Click on "create a new team profile" item on the Participants Navigator.
2. The "Create a New Team" page will appear. Select the team profile format and press Submit.
3. Enter a name for the new team that is not already used. If you pick an existing name, an error will appear when you close the document.
4. You may specify an Organization -- all the members of the organization will be made members of the team.
5. You may list members individually by putting their names in one of the grid fields (which can each contain multiple entries separated by commas). Note: In the list, you may enter User Names, Notes Groups, or Notes Roles.
6. Adjust the document access controls (see below).
7. Close and save the new team profile.

Creating a Type II Team Profile (Web)

1. Click on "create a new team profile" item on the Participants Navigator.
2. Select Type II
3. Enter a name for the new team that is not already used. If you pick an existing name, an error will appear when you close the document.
4. Adjust the document access controls (see below.)
5. Press Submit.
6. The first Team Selection Form will appear. It will display the first 100 participant names and checkboxes. Click the participants to be included. Press Go to continue to the next page and repeat until all names have been presented to you. When the last participants have been displayed, the team profile document will be redisplayed for your review.

Document Access for Team Profiles

The Team Profile itself can be secured. By default, the profile can be seen by anyone and edited only by its members. You can however, make the profile visible only to the members of this team or allow it to be edited by all members of the team.

When you limit read access to members of the team, the team profile itself cannot be seen by anyone else. That, in turn, means that it cannot be used to secure another document (issue, discussion, etc.) except when that document is being created or edited by a member of the team.

Teams provide a very convenient way to allow a set of people to work together in the database without their work being visible to anyone else. For example, if a team member writes an issue item and limits reading to the team, then only team members will see it when they display the issues view. The same applies to risks, news, scope changes, discussions as well as project documents.

Maintaining Team Access Control

When the members of a Team are changed, either by editing the Team Profile or by changing the membership of an organization that is part of a team profile, the documents that are secured to that team must be updated. This is necessary because the document access lists are maintained in the individual documents.

Three scheduled system agents, "Maintain Team Organizations", "Maintain Team Participants" and "Maintain Access Control" should be scheduled for periodic operation in any database that uses Teams. The first will update the Type I Team Profiles when participants are added or removed from Organizations. The second will update Type II team profiles when the user ids of the team members change. The third will update any document that uses a team in its read or edit access lists when the list in the corresponding Team Profile has been modified. Since these are usually scheduled for nightly operation, changes in Team Profiles may not take effect until the next day for existing documents.

Note: If you have the right to modify a document, you can update its team members immediately by editing the document and then saving it. This will cause the document to reset the edit and read lists to the current contents of those lists in the named team profiles.