

Security Administration

Overview

Project Gateway provides a security implementation that is designed specifically for the needs of a project management environment

This security implementation is based on the Author level security capabilities of Lotus Domino.

As a general rule, all users of the database should be given author level access.

The security model is divided into two major categories, security for automatically generated documents (project assignments, project and participant profiles) and security for manually created documents (project documents, issues, discussion, news, scope changes, etc.).

Security for Manually Generated Documents

In general whenever you create an issue, risk, scope change, status report, or project document, you have the option to control the set of people who can subsequently modify or read that document.

Rather than selecting or entering individual names, Project Gateway provides a grouping concept called a Team Profile. A Team Profile is a repository document that defines a list of users and a team name.

The team name can be selected whenever a document is created or edited to define the users allowed to read or edit that document. If the membership of the team changes, all the documents referencing that team will be updated automatically.

Since all team members are subject to the access control list of the database, there are no additional tasks created for the Notes administrators when teams are used.

In Project Gateway 6, a project can specify a default team to be used for any new documents created for the project. This makes it quite simple to restrict project information to a designated working group.

Teams are discussed in more detail in the Repository User Guide.

Security for Automatically Generated Documents

When a project plan is imported by Project Gateway, a series of documents are created.

- Project Profile document
- Participant Profile documents (for new participants not previously part of any project)
- Assignment documents
- Chart Definition documents
- News document

Each of these documents is given an edit access list during the import process. This list identifies those individuals who can edit the document.

Note that the exact same rules apply when these documents are manually created.

User ID fields in Project and Participant Profiles

The Project Profile document contains a field labeled "**UserID for Project Manager.**" This field should be set to contain the user name of the person acting as the project manager and any other people who should have the right to act in this capacity. The persons listed here will have the right to modify the Project Profile (including changing the UserID) and to modify any assignment document associated with the project.

The Participant Profile document also contains a field labeled "**UserID for Participant.**" This field should be set to contain the user name of the person represented by this Profile and any other people who should be able to act as representatives of that person. The people listed here will have the right to modify the Participant Profile (including to change the UserID field) and to modify any assignment documents of this participant.

Although the Participant name and the name in the UserID field may be identical, this is not required. The UserID field must contain a name from the Notes address book that is included in the Access Control List of the database. The Participant name will be the name used in the project management application for this person.

Note: Whenever we refer to UserIDs in Project Gateway, we are really referring to the entries found in the Name and Address book. Web Users will normally be in the Name and Address book also, even though they will not have a NotesID file or Notes Client license.

Adding a Project to an existing Repository

The Project Profile UserID will be initialized to the UserName of the creator. The Project Profile itself will be editable by that person plus the roles of [PGADMIN] and [PGMASTER].

The UserID fields of New Participant Profiles created during import (if any) will be initialized to the UserName of the creator. These new Participant Profiles will be editable by that person plus the roles of [PGADMIN] and [PGMASTER].

Each assignment document will be editable by the UserName of the creator and the UserID from the assigned participants Participant Profile. Assignments will also be editable by the roles of [PGADMIN] and [PGMASTER].

If the advanced security option "Full Security" is enabled in the Field Map Document, then both Edit access and Reader access will be limited to the set of people defined for the assignment. This means that the assignment will be invisible to all others.

Chart Definition and News documents will be give access to the UserName of the creator and to the roles of [PGADMIN] and [PGMASTER].

Using Synchronize Update Notes

The UserID of New Participant Profiles created during synchronization (if any) will be initialized to the UserName of the creator. These new Participant Profiles will be editable by that person plus the roles of [PGADMIN] and [PGMASTER].

Access to every assignment created or modified during synchronization will be set to include those people listed in the UserID field of the Project Profile, plus those people listed in the UserID field of the Participant Profile plus the roles of [PGADMIN] and [PGMASTER].

If the advanced security option "Full Security" is enabled in the Field Map Document, then both Edit access and Reader access will be limited to the set of people defined for the assignment. This means that the assignment will be invisible to all others.

Chart Definition and News documents will be give access to those persons listed in the UserID of the Project Profile of the creator and to the roles of [PGADMIN] and [PGMASTER].

Maintaining Assignment Security

Since assignments are supposed to be accessible to the Project Manager and the Participant, the assignment documents must be updated when changes are made to the UserID lists in the corresponding Project and Participant Profiles.

This update can be done at any time by running the "Admin\Update Organization" agent from the Agent Menu. The update will be done automatically by the "Maintain Organization" agent that should be scheduled for periodic operation (usually nightly).

Note that after the UserID of a Project or Participant Profile is changed and before the agent has run, the newly listed people will not have edit access to their assignments and any recently delisted people will still have access.

ROLES: [PGADMIN] and [PGMASTER]

The PGADMIN role should be assigned only to those people who should be able to modify Profiles. These people may be need to set UserIDs when new participants have been created and when people leave the organization.

The PGMASTER role should be assigned to the Notes ID used to sign the agents running in the database. This gives the agents the rights to make changes to the security settings.

Timesheet Security

The Timesheet facility implements a special security model using information provided in the Timesheet Profile section of the Participant Profile. When a Timesheet is created, its editing rights are set from the Participant data existing at that time. The editing rights cannot be changed later.

Edit Rights

The following people will be able to edit a particular Timesheet.

1. Those people listed in the UserID list of the Participant Profile
2. The author of the Timesheet (who must in turn be listed in the "People who can create timesheets" section of the Participant Profile in order to be allowed to create the Timesheet). If this section is empty, anyone can create a Timesheet for that participant. Note: Only names can be used, Groups are not supported in this context.
3. Those people listed in the "People who can approve Timesheet" section of the Participant Profile.
4. The special roles [PGADMIN] and [PGMASTER].

Read Rights

A timesheet can be read only by someone authorized to edit it. This means that, when you look at a view that includes timesheets, you will see only those that you have the right to modify. The generally means that you can see only your own timesheets.

Security in Web Operation

When accessing the database using the Web browser, the security system operates exactly as described. You will only be able to see documents for which you have read access and you will only be able to modify documents for which you have edit access.

To enter user names into the UserID fields of the profile documents or into the Team Profile form, you should enter the name exactly as it appears on the Repository Center home page after logging into the database or as your full Notes User ID name if you have one. If you do not spell it correctly, that person will not have access. There are some sites where a person will have a different web user id from the same person's note's user id. In this case you must enter both ids into the UserID fields in Project, Participant and Team Profiles in order to always have access from both clients.

Since you cannot run agents directly from the browser, changes made in security lists will not be implemented until the time that the server agents are scheduled for operation. This frequency is controlled by the database manager.

When you upload a new project using the ProjectWeb Publication form, the project profile UserID will be set by default as your current login name. If this should be different, you must put the correct name into the publication form before submitting it.

When entering more than one name into a security list, put a comma between each entry.