Best Practices Enforced by Group Administration

The Series25 Group Administration tool handles permissions in a clean and straightforward way. In order to make this possible, certain best practices are enforced when you use Group Administration.

In order to edit the group's security in the Groups tool, it must meet the following minimum security requirements. If they are not met, you will be prompted to automatically update them before continuing.

Object Security **Viewing Rights**:

- Events
- Cabinets
- Folders
- Locations
- Resources
- Organizations

Object Security Edit, Delete, Copy Rights:

- Event Drafts
- Event Resources
- Event Locations

Other

- View rights for layout and image Master Definitions
- View rights for contacts

If a group needs more than this (for example, the ability to create events) then you will have a chance to set higher permissions later.

These are the best practices for security in 25Live, and you will not be able to use the Group Administration tool without following them. Please see our recommendations below if you are accustomed to different permissions.

Why do we enforce these best practices?

As Series25 evolved over time, more and more settings were added to handle increasingly complex permissions. The combinations of these settings could be unpredictable and even contradictory. In addition, the average scope of Series25 on campus has grown as 25Live is used by greater numbers of users with increasingly diverse requirements. All of this put a great burden on administrators to know how to correctly configure their environments and follow best practices.

With the development of the Group Administration tool we decided to make administrators' jobs easier by bringing certain permissions up to a specific minimum level. This allowed us to accomplish the following goals:

- The new tool should support the same range of use cases for 25Live without eliminating functionality.
- All permissions should be configurable using simple "yes/no" questions regarding a user's permissions.

- As an event scheduling application, 25Live should allow all users to see and search for events.
- Object Level Security should be mandatory to allow a more precise configuration of event, location, organization, and resource visibility.

Most institutions are already following the best practices described by these goals, but if you're reading this page it's probably because one of your security groups wasn't. If you want to know how to adapt your settings to achieve the same functionality as before while meeting best practices, read the following section.

Adjusting Your Configurations to Accommodate Best Practices

Here is a list of all the minimum permissions enforced by Group Administration, along with tips to achieve the same functionality if you are used to having lower permissions.

Permission	Minimum Enforced	Tips
Event Drafts	View, edit, create, and copy	To prevent users from creating or editing drafts, configure their allowed event states.
Events	View Only (or higher)	This permission should not be removed. If users aren't viewing events, why are they using 25Live?
Folders, Cabinets	View Only (or higher)	Viewing folders and cabinets is necessary to allow users to view the events contained within. Use object security to hide specific folders and cabinets if desired.
Location/Organization/Resource Access	View Only (or higher)	To prevent users from viewing specific locations, organizations, or resources, use object security.
Layouts and Images	Access for abridged groups OR Basic: *View All Location Master Definitions (Not Just Abridged List)*	In order to ensure smooth operation of location requests, we require that any layouts and their images are visible to all users. Make sure that these Master Definitions are available to users with abridged access OR that users have the following security permission set to **Yes** in Group Administration: Basic: *View All Location Master Definitions (Not Just Abridged List).*
View Contacts	View Contacts	This is necessary for Contact Details pages in 25Live. Users will need the following security setting in Group Administration set to **Yes**: Basic: *View Contacts.*
Event Resource and Event Location	Full Control	To prevent users from assigning locations or resources in the event form, use event form configurations.