How Security and Policy Settings Work Together

After you have a basic understanding of the policy and security settings that impact your Series25 suite, it is then important to recognize how these elements interact with one another to help you maintain granular control over scheduling practices across your institution.

Proper security setup can...

- assure correct data maintenance by the proper people
- help enforce your business processes
- streamline event scheduling for schedulers and requestors

Alternatively, a haphazard security setup can be a recipe for angry schedulers, unintended results, and potential data disasters.

When we talk about security, we largely mean:

- Functional Security (FS)
- Object Security (OS)
- Assignment Policy (AP)
- Notification Policy (NP)

In addition to those four items, Event Form settings also play a big part in what users can and cannot do. Below, we'll go over the basics of how these five elements work together.

How Functional Security and Object Security Interact

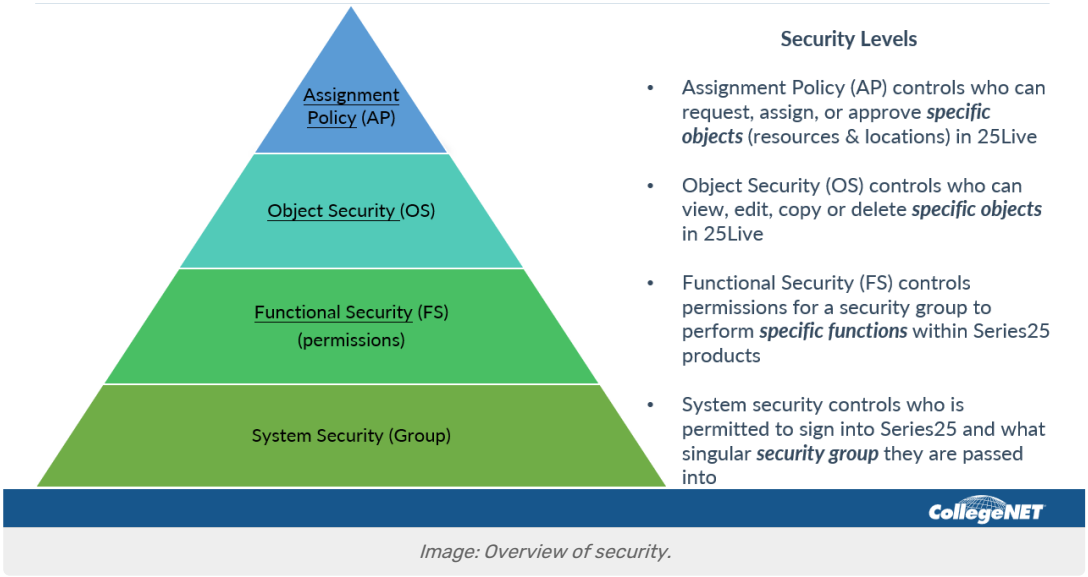

Image: Overview of security.

Functional Security (FS) applies to the general actions a security group can perform across Series25, including actions performed on objects. These are "big picture" settings, which is why it is best practice to set up FS before setting up Object Security.

Object Security (OS) determines whether specific objects (Events, Locations, Resources, Organizations, and Reports) can be viewed, edited, copied, or deleted by a security group. This gives you granular control over each object.

For example, where FS may grant a security group permission to edit events *in general*, OS will go a step further to specify *which* individual events they can edit and which ones they can't. And, while a security group might have the OS rights to delete, that ability can still be restricted by FS.

How Object Security and Assignment Policy Interact

Similar to Object Security, Assignment Policy (AP) applies to individual objects, but only locations and resources are affected. AP determines whether and when users can request, assign, unassign, or approve location and resource assignments.

Between these two types of rights, OS takes precedence. For example, if a user has **request** rights to a location but they aren't allowed to **view** that location, the system will not allow them to make a request.

How Assignment Policy and Notification Policy Interact

Notification Policy (NP) controls notifications, which are workflow tasks that appear in a user's task list alongside assignment requests and To Dos. Where Assignment Policy determines who can request and assign objects, NP determines who gets notified when these actions take place. In other words, the AP **Assign** action actually results in the assignment of the location or resource to the event whereas an NP **Approve** action results in a notification to interested parties.

How Security Settings, Policy Settings, and Event Form Configurations Interact

With custom Event Form Presentations, security groups can have separate forms when creating or editing events, each with its own hidden, required, and customized fields, default schedulers, and time restrictions. Then, Event Quotas can be added—limiting how many event reservations can be made by a user or organization.

To create an event, users would need event creation Functional Security rights. Then, if they wanted resources or locations attached to the event, they would need the Object Security rights to view those objects, and the Assignment Policy rights to request/assign those objects. Before interested parties can be contacted, Notification Policies must to be setup. Thus, Event Form configurations are typically set up last—after all other security and policy settings are in place.