25Live Security Administration Guide

The 25Live Administration Utility

The security administration tasks you can perform

The 25Live Administration Utility is used to set up and maintain the security of your 25Live environment. The Utility allows you to perform the following security administration tasks:

- Set object security permissions for specific events, folders, cabinets, locations, resources, organizations, and reports for each 25Live security group
- Set default object security for event drafts, locations, resources, organizations, and reports for each 25Live security group
- Set assignment policies for specific locations and resources for each 25Live security group
- Set notification policies for specific locations, resources, organizations, event types, and event requirements
- Manage and add 25Live security groups and set the functional security permissions of each
- Manage and add 25Live users
- View locked 25Live items and remove locks
- See which users are currently signed into 25Live

The 25Live Administration Utility is also used to:

- Set up and manage 25Live data. For information, see the *25Live Data Administration Guide* available by clicking Help and choosing "Data Administration."
- Set up and manage 25Live event pricing. For information see the *25Live Event Pricing Guide* available by clicking Help and choosing "Event Pricing."
- Access and run the Schedule25 Optimizer. For information, see the *Schedule25 Optimizer User Guide* available by clicking Help and choosing "Schedule25 Optimizer User Guide."
- Integrate custom reports into the 25Live environment. For information, see the *25Live Custom Report Integration* document available by clicking Help and choosing "Custom Report Integration."

Utility security administration tabs

The 25Live Administration Utility provides the following security administration tabs:

- Events
- Locations
- Resources
- Contacts
- Organizations
- Reports
- Security

Events

The **Events** tab provides functionality to allow you to:

- Set object security access permissions to specific events, folders, and cabinets by 25Live security groups
- Set default object security access to event drafts by 25Live security groups
- Define event requirement and event type notification policies

This tab also allows you to perform the following data-related tasks as described in the *25Live Data Administration Guide*:

- Maintain event master definitions
- Create and maintain the Event Type Hierarchy
- Create and manage cabinets and folders
- Bind back-to-back events
- Complete vCalendar To Do's for multiple classes and export the classes to your SIS
- Delete events
- Export data to X25
- View Series25 import messages

Locations

The **Locations** tab provides functionality to allow you to:

- Set object security access permissions, assignment policies, and notification policies for specific locations by 25Live security groups
- Set default object security and assignment policy access to locations by 25Live security groups

This tab also allows you to perform the following data-related tasks as described in the 2*5Live Data Administration Guide*:

- Maintain location master definitions
- Add, copy, edit, and delete locations
- Remove pending location reservations

Resources

The **Resources** tab provides functionality to allow you to:

- Set object security access permissions, assignment policies, and notification policies for specific resources by 25Live security groups
- Set default object security and assignment policy access to resources by 25Live security groups

This tab also allows you to perform the following data-related tasks as described in the 2*5Live Data Administration Guide*:

- Maintain resource master definitions
- Add, copy, edit, and delete resources
- Remove pending resource reservations

Contacts

The **Contacts** tab provides functionality to allow you to:

- Add and manage 25Live users
- Activate and deactivate 25Live users
- See which users are currently logged into 25Live

This tab also allows you to perform the following data-related tasks as described in the *25Live Data Administration Guide*:

- Maintain the Contact Custom Attributes master definition
- Add, copy, edit, and delete contacts

Organizations

The **Organizations** tab provides functionality to allow you to:

- Set object security access permissions and notification policies for specific organizations by 25Live security groups
- Set default object security access to organizations by 25Live security groups

This tab also allows you to perform the following data-related tasks as described in the *25Live Data Administration Guide*:

- Maintain organization master definitions

- Add, copy, edit, and delete organizations

Reports

The **Reports** tab provides functionality to allow you to:

- Set object security access permissions to specific reports by 25Live security groups
- Set default object security access to reports by 25Live security groups

Security

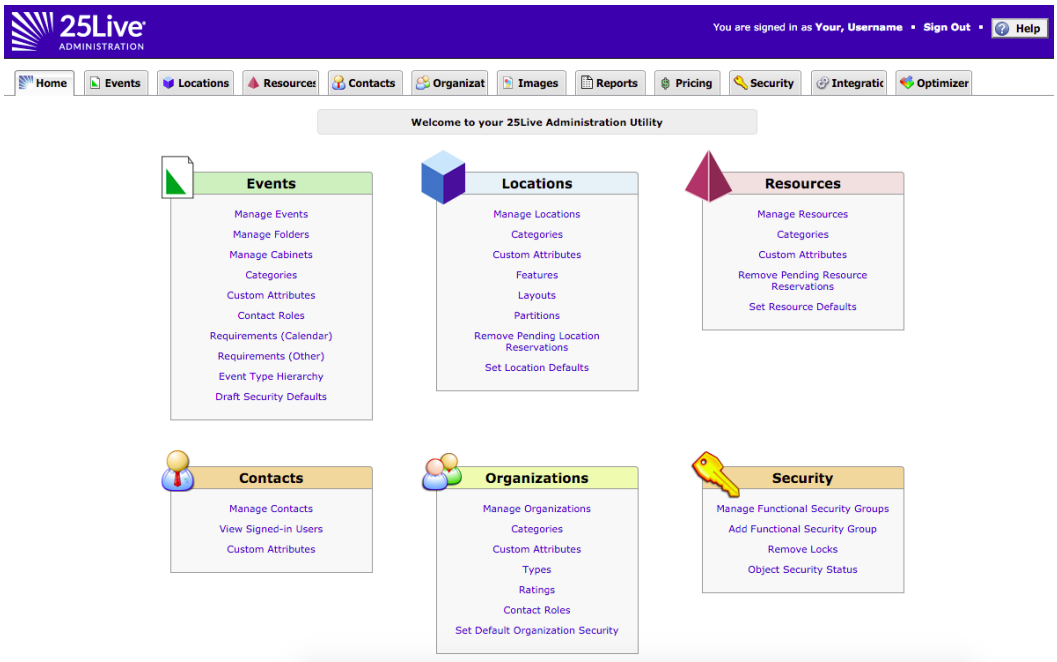
The **Security** tab provides functionality to allow you to:

- Manage the functional security rights of 25Live security groups
- Add 25Live security groups and set their functional security rights
- View locked 25Live items and remove locks
- Turn object security “on” and “off” in your Series25 environment

Accessing the Administration Utility

Your ability to access the 25Live Administration Utility and use its functionality is controlled by the functional and object security permissions of the 25Live security group to which you belong. For example, if your security group has permission to manage the object security, assignment policies, and notification policies of specific locations, only those locations will appear in your view of the Administration Utility.

1. Enter your 25Live URL followed by "/admin.html" in your browser and click <Enter>.
2. On the Administration Utility sign in page, enter your 25Live username and password.
3. Click Sign In.



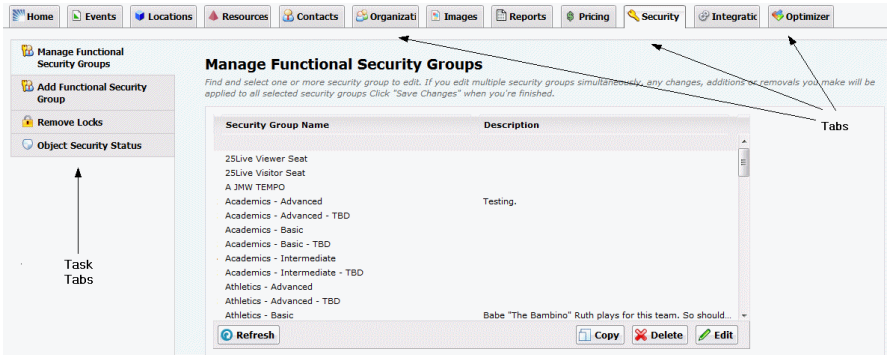
Using the Administration Utility

The Administration Utility is very easy to use.

1 From the Home tab, click the security administration task you want to perform from the Events, Locations, Resources, Contacts, Organizations, Reports, and Security options.
or
From the Events, Locations, Resources, Contacts, Organizations, Reports, or Security tab, click the security administration task you want to perform.

Either of these actions opens the selected task page with the appropriate task tab selected on the left.

Security > Manage Functional Security Groups example:



2 Perform the task. Basic instructions for doing so are provided below the task name in the Administration Utility. This document contains detailed instructions and guidelines for performing each task.

3 Save your work by clicking the appropriate button at the bottom of the page.

Accessing previous versions of this guide

If you're using an earlier release of 25Live and want to access the Security Administration Guide for that release do the following:

1. Access the 25Live Documentation page of Customer Resources: http://knowledge25.collegenet.com/display/CustomerResources/25Live+Documentation
2. Scroll to the bottom of the page and click the link for the 25Live release you're using to access the document archive for that release.
3. Click the appropriate link.

25Live Security Overview

Comprehensive security control

25Live Administration Utility security functionality provides powerful tools you can use to control user access to functional areas of 25Live and the 25Live Administration Utility, and to individual locations, resources, organizations, cabinets, folders, events, and reports.

The security controls you can set are designed to meet the needs of your institution, whether large or small, centralized or decentralized, single- or multi-campus. You can control:

- What parts of 25Live schedulers and other users can access
- What 25Live data—contact, organization, event, interface, master definition, report, resource, security, location, system definition, communication—users can access, use, and/or act on
- Who can create and edit events
- Who can assign locations and resources to events and when
- Which event cabinets and folders schedulers can view and/or schedule events in
- Which reports users can access and generate, and who can manage standard and custom reports
- Who is notified when events of a certain type are created or certain actions are taken on an event

The "building blocks" of control

Four building blocks

There are four major "building blocks" of security control. All are required to effectively use 25Live.

- System security
- Functional security
- Assignment policies
- Object security

In addition to these, you can define notification policies. See "Notification Policies"

System Security

System security controls access to the 25Live application. Access is limited to "active" 25Live users via unique user ID and password. System security is the most basic building block of control in 25Live.

Functional Security

Functional security controls access to functional areas of 25Live, such as whether or not a user can access the event search function or run reports. Functional security is the most basic building block of usage control in 25Live.

Assignment Policies

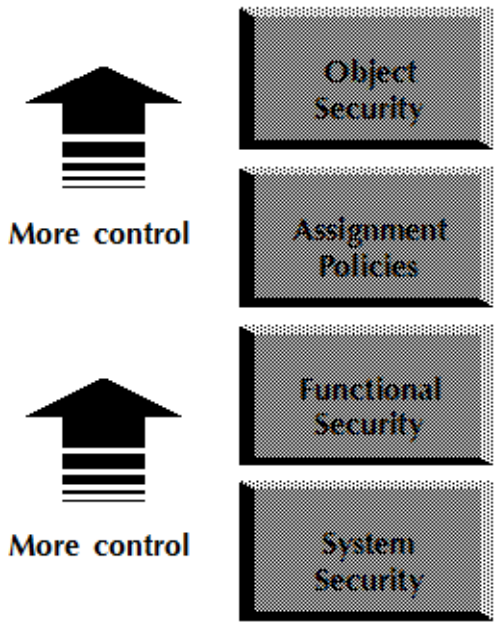
Assignment policies control for each location and resource who can assign it to events and when it can be assigned to events.

Object Security

Object security controls access to individual events, event drafts, locations, resources, organizations, cabinets, folders, and reports, and, for locations and resources, the events they're assigned to.

The building blocks build on each other

Security "building blocks" build upon each other, each providing an additional level of control.



Classes of 25Live users

There are two general classes of 25Live users: Viewers and Users.

Viewers

25Live Viewers have restricted view-only access to events, locations, resources, and organizations as controlled by the 25Live Viewer Seat, which is the "generic" 25Live user for this user class. Viewers have no 25Live sign-on privileges and no ability to personalize their 25Live user experience.

Users

25Live Users have access to potentially all levels of functionality and objects (event drafts, events, locations, resources, organizations, and reports) in 25Live, as defined by the access permissions of the 25Live security group to which they belong, and they have the ability to personalize their 25Live user experience. Users are further divided into specific 25Live security groups (see "Security groups").

Typical activities by user class

Typical 25Live activities for each of these user classes are listed below.

	25Live Viewer	25Live User
View event, location, and resource lists	✓	✓
View calendars and location/resource availability grids	✓	✓
View event, location, and resource details	✓	✓
Submit event drafts, or create events and save them to the Series25 database		✓
Run reports		✓
Receive and respond to assignment policy tasks		✓
Set user preferences		✓

	25Live Viewer	25Live User
Star important or favorite events, locations, and resources		✓

Security groups

Definition

A ***security group*** is comprised of one or more 25Live users with the same set of functional security, assignment policy, and object security permissions.

Default security groups

25Live comes with two default security groups, System Administrators (-1) and Default Users (-2). The System Administrators group has full rights to all system functions and objects. You can't change the functional or object rights of this security group, but you can add and change its members. The Default Users group typically becomes the default group for LDAP or Shibboleth authentication.

25Live security group templates

The 25Live Administration utility comes with several security group "templates" that each have functional security settings most common to a particular group of users. The templates reflect best security practices, and are to be used as guides in setting up your security groups. You may, however, have more or fewer security groups depending on your needs, and the functional access settings of each can be different than the recommendations reflected in each template. See "25Live security group templates"

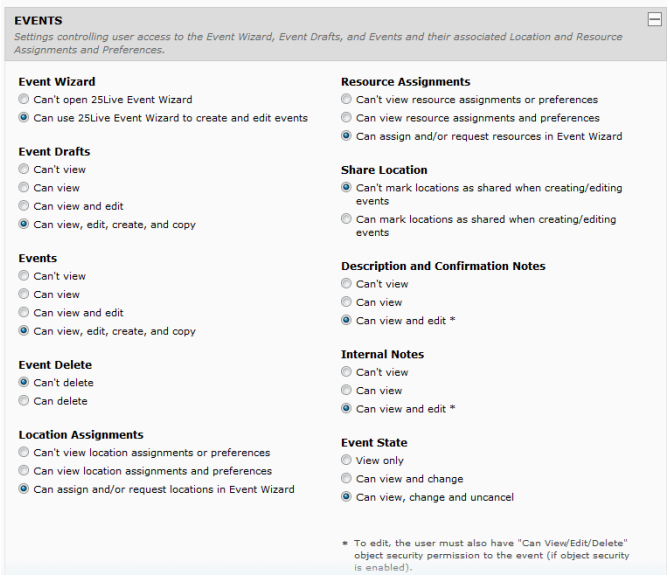
Access levels

Definition

Access levels define how much access a security group has in each functional area of 25Live (as controlled by functional security), which locations and resources they can assign to events (as controlled by assignment policies), and which objects—locations, resources, organizations, reports, cabinets, folders, events, and event drafts—they can access and possibly act on (as controlled by object security).

Functional security access levels

Functional security access levels control access to the various functional areas of 25Live, as shown in this Events functional security example:



Functional security example

The following example shows how the functional security access levels of three groups of users—those in the Events Office, Athletics Office, and Registrar's Office—affect their access to 25Live event pricing functionality.

This group...	Has this functional access level for event pricing...	Which means that members of the group...
Events Office	Event Details Pricing: Can view, edit, and create	Can view, create, and edit event pricing information in event details.
Athletics Office	Event Details Pricing: Can view	Can view event pricing information in event details.
Registrar's Office	Event Details Pricing: Can't view	Can't access event pricing functions in event details. They're "hidden."

Assignment policy access levels

Assignment policy access levels control the ability to request assignment of or assign a particular location or resource to events.

Assign, Unassign, Approve	Allows users in the security group to assign and unassign the location or resource, and receive and act on assignment requests in their 25Live Task List.
Assign/ Unassign	Allows users in the security group to assign and unassign the location or resource.
Request/ Unassign	Allows users in the security group to request assignment of the location or resource, and unassign it.
Request	Allows users in the security group to request assignment of the location or resource, but not assign it themselves or unassign it.

Assignment policy example

The following example shows how the assignment policy access levels of three groups of users—those in the Events Office, Athletics Office, and Registrar's Office—affect their ability to assign two locations.

This group...	Has this assignment policy access level for location BCC101...	And this assignment policy access level for location Gym 2...	Which means that members of the group...
Events Office	Assign/Unassign	Request	Can assign and unassign BCC101. Can request assignment of Gym 2, but can't assign or unassign it.
Athletics Office	Request	Assign/Unassign/Approve	Can request assignment of BCC101, but can't assign or unassign it. Can assign, unassign, and act on assignment requests for Gym 2.

This group...	Has this assignment policy access level for location BCC101...	And this assignment policy access level for location Gym 2...	Which means that members of the group...
Registrar's Office	Assign/Unassign	Request/Unassign	Can assign and unassign BCC101. Can request assignment of and unassign Gym 2, but can't assign it.

Note Assignment policies are not enforced for event drafts.

Assignment policy exceptions

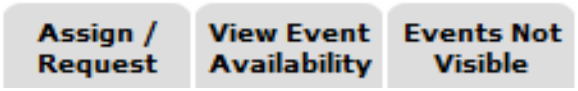
You can create assignment policy exceptions for particular security groups that have a different access level than the standard one defined for each group. In the example above, for instance, you could create an exception that gives the Events Office security group Assign/Unassign privileges to Gym 2 just during Homecoming week.

Object security access levels

Object security access levels control the ability to access and act on a specific location, resource, organization, event, folder, cabinet, or report.

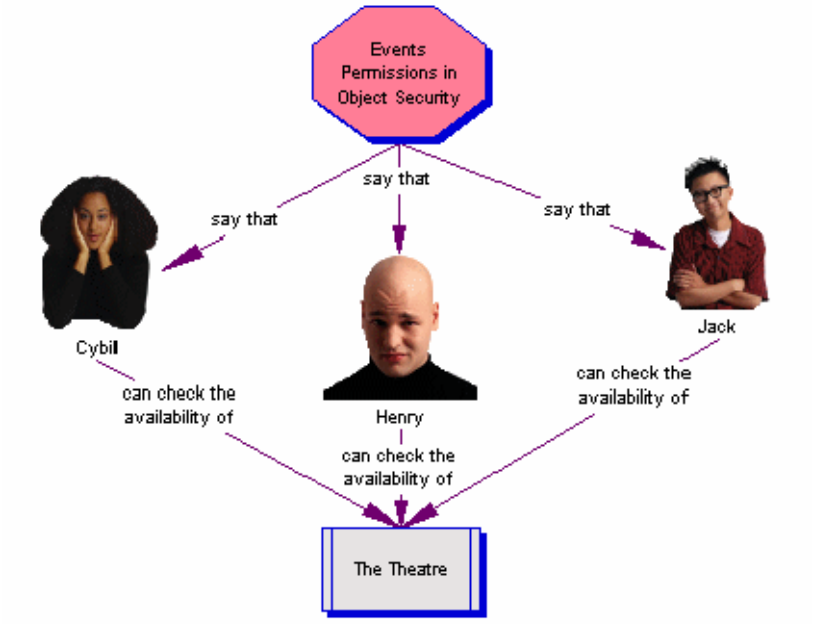
Edit, Delete, Copy	Allows users in the security group to edit, delete, and copy the object.
Edit	Allows users in the security group to edit the object.
View Only	Allows users in the security group to view the object.
Not Visible	Hides the object from the security group's view.

Locations and resources have these additional Events object security access levels that control the ability to see the events a particular location or resource is assigned to and potentially assign the location or resource to events or request its assignment.



Assign/ Request	Allows users in the security group to see the events the location or resource is assigned to, run reports on the location or resource, and potentially assign the location or resource to events or request its assignment. **Note:** The ability to actually assign the location or resource to events is controlled by the assignment policy of the location or resource, not this setting. See "Assignment policy access levels"
View Event Availability	Allows users in the security group to see the availability of the location or resource and the events the location or resource is assigned to, and to run reports on the location or resource.
Events Not Visible	Prevents users in the security group from seeing the availability of the location or resource and the events the location or resource is assigned to, and from running reports on the location or resource.

In this example, Events object security access to the Theatre has been set to View Event Availability for the security group of which Cybil, Henry, and Jack are members.



Key Concept

Event Object "Ownership"

The user who creates an event with an event state of Tentative or Confirmed has full "Edit, Delete, Copy" access to the event independent of the object security setting on the event for their security group. This remains the case unless another user with "Edit, Delete, Copy" object security access to the event "takes ownership" of it, in which case the object security access to the event by the event creator reverts to that of their security group.

This is not the case for other objects controlled by object security—cabinets, folders, locations, resources, organizations, and reports—where the object security access of the object creator's security group determines that user's access to the object.

Object security example

The following example shows how object security access to two locations for each of three groups of users—those in the Events Office, Athletics Office, and Registrar's Office—affects their ability to access those locations and the events they're assigned to in 25Live. Functional security access has been set appropriately for all three groups.

This group...	Has these object security access levels for location BCC101...	And these object security access levels for location Gym 2...	Which means that members of the group...
Events Office	View Only View Event Availability	Not Visible Events Not Visible	Can access and view BCC101, and see the events BCC101 is assigned to. Can't access Gym 2 or see the events Gym 2 is assigned to. Gym 2 won't appear in 25Live for members of this group.
Athletics Office	Not Visible Events Not Visible	Edit Assign/Request	Can't access BCC101 or see the events BCC101 is assigned to. BCC101 won't appear in 25Live for members of this group. Can access and edit Gym 2, see the events Gym 2 is assigned to, and potentially assign or request assignment of Gym 2 if they have appropriate assignment policy permissions to Gym 2. See "Object security and assignment policy interdependencies"

This group...	Has these object security access levels for location BCC101...	And these object security access levels for location Gym 2...	Which means that members of the group...
Registrar's Office	Edit, Delete, Copy Assign/Request	View Only View Event Availability	Can access, edit, and copy BCC101. If their functional security access for Location Delete is "Can delete," they can also delete BCC101. Can see the events BCC101 is assigned to and potentially assign or request assignment of BCC101 if they have appropriate assignment policy permissions to BCC101. See "Object security and assignment policy interdependencies". Can view Gym 2 and see the events Gym2 is assigned to.

Object security exceptions

You can create object security exceptions for particular security groups that have a different access level than the standard one defined for each group. In the example above, for instance, you could create an exception that gives the Events Office security group Assign/Request privileges to Gym 2 just during Homecoming week.

Functional and object security interdependencies

Key Concept

A security group must have at least "Can view" access to a functional area before any related object security access is applied.

For example, if a security group's functional Resource Access is "Can't view, Resources tab doesn't appear in 25Live" and its object access to the DVD Player resource is "Edit," the security group members won't see any resources in 25Live, including the DVD Player.

The object access a security group has to a particular object overrides the functional access it has to the related functional area, if the security group has at least "Can view" access to the functional area.

For example, if a security group's functional Locations Access is "Can view, Locations tab appears in 25Live" and its object access to location BCC101 is "Not Visible," the security group members won't see BCC101 in 25Live.

Object security and assignment policy interdependencies

Key Concept

To be able to request assignment of a particular location or resource for events, a security group's Events object security permission to the location or resource must be "Assign/Request" and their assignment policy permission must be "Request" or "Request/Unassign."

To be able to assign a particular location or resource to events, a security group's Events object security permission to the location or resource must be "Assign/Request" and their assignment policy permission must at minimum be "Assign/Unassign."

To be able to act on assignment requests from other users, a security group's Events object security to the location or resource must be "Assign/Request" and their assignment policy permission must be "Assign/Unassign/Approve."

Request/Approve example

Scenario

Mary is a scheduler in the Athletics Office. She's a member of the Athletics Office security group. As defined by the group's location assignment policies and object security, Mary can use 25Live to:

- Create events in her own Athletic folder in the Special Events cabinet and view (but not change) events in the rest of the cabinet.
- Assign all athletic locations to events.
- See what events are happening in all the other locations on campus, but not assign any of those locations to events.

Mary is occasionally asked by the Athletic Department staff to schedule a meeting in MEETROOM, one of the campus meeting rooms. Mary can't assign MEETROOM, but she can create an event and initiate an assignment request for it. That assignment request is sent to Jane.

Jane is the secretary to the president and controls all of the meeting rooms in the administration building, including MEETROOM. She's a member of the President's Office security group. As defined by the group's location assignment policies and object security, Jane can use 25Live to:

- Create events in the President's Office folder in the Special Events cabinet and view (but not edit) events in the rest of the cabinet.
- Assign MEETROOM and all other locations in the administration building to events.

Jane occasionally receives assignment requests for MEETROOM from Mary via her 25Live Task List. Jane decides whether or not to assign MEETROOM to Mary's events. When she assigns it or denies the request, Mary sees that in her own 25Live Task List.

Minimum functional security required

The following table shows the minimum functional security that must be in place for Mary to be able to create an event, check the availability of MEETROOM, and have the assignment request sent to Jane, and for Jane to complete the request (either assign MEETROOM or deny the request).

Functional Security Permission	Athletics Office (Mary's) Access	President's Office (Jane's) Access
Events: Event Wizard	Can use 25Live Event Wizard to create and edit events	Can use 25Live Event Wizard to create and edit events

Functional Security Permission	Athletics Office (Mary's) Access	President's Office (Jane's) Access
Events: Events	Can view, edit, create, and copy	Can view, edit, create, and copy
Events: Location Assignments	Can view location assignments and preferences	Can assign and/or request locations in the Event Wizard
Tasks, Reports, and Email: Task List	Can view and act on task items	Can view and act on task items
Locations: Location Access	Can view, Locations tab appears in 25Live	Can view, Locations tab appears in 25Live

Object security on MEETROOM

Both Mary and Jane must be able to see MEETROOM (controlled by Object object security) and run an availability check on MEETROOM (controlled by Events object security).

Object Security Permission	Athletics Office (Mary's) Access	President's Office (Jane's) Access
Object	View Only	Edit, Delete, Copy
Events	Assign/Request	Assign/Request

Location Assignment Policy for MEETROOM

Mary can't assign MEETROOM to events, but she can request its assignment. Jane can respond to assignment requests for MEETROOM and assign it to events.

Athletics Office (Mary's) Access	President's Office (Jane's) Access
Request	Assign/Unassign/Approve

Object security on the Athletics Office folder and the events in it

Mary must be able to create events in the Athletics Office folder. Jane must, at minimum, be able to see those events so she can assign requested locations to them.

Object Security Permission	Athletics Office (Mary's) Access	President's Office (Jane's) Access
Object Rights	View Only	View Only
Create Events?	Yes	No
New Event Rights	Edit, Delete, Copy	View Only

Default object security and assignment policies

You can set default object security permissions for event drafts, locations, resources, organizations, and reports for each security group. For locations and resources, you can also set default Events object security and assignment policy permissions. The default object security and assignment policy access you set determines each security group's access to ***new*** objects of that type.

For example, if you set the locations default object security of the Athletics security group to View Only and Assign/Request, and leave the default assignment policy access as Request (the system default), when a new location is created, members of that security group will be able to view it and request its assignment to events they create and/or edit.

Caution

It is very important that you determine the default object security you want for each security group for each object type—event drafts, locations, resources, and so on and, for locations and resources, their default Events object security and assignment policy access—and set defaults accordingly. Until you do, each group's default object security permission is set to the system default—Not Visible—which means that members of the security group *won't see any new objects of that type*.

Notification Policies

Description

Notification Policies allow you to specify which 25Live users need to be notified when a particular event scheduling activity occurs—the assignment of a particular location or resource, the designation of a particular requirement, the sponsorship of a particular organization, or the creation of an event of a particular type. They specify:

- Who should be notified. You can have one or more 25Live users receive a notification.
- The type of notification: Approval Required or Information Only.
- Whether all recipients need to approve or just one recipient (when notifications requiring approval are sent to more than one user).

When an event is saved, appropriate notifications are displayed in the 25Live Task List of the user whose action triggered the notification and in the 25Live Task List(s) of the notification recipient(s)—as is each recipient's response to the notification.

Note Notification policies are not enforced for event drafts.

Notification types

There are two types of notifications:

- **Approval Required**: The notification requires approval by the recipient(s). Each recipient has the option of approving or denying the notification request.
- **Information Only:** The notification is for information only; it requires no explicit action on the part of the recipient(s).

What triggers the sending of a notification

A notification (either Approval Required or Information Only) can be set up to be generated and sent to the Task List(s) of 25Live user(s) based on any of these event scheduling actions:

- Creation of an event of a particular event type
- Assignment of a particular location or resource to an event
- Association of a certain organization with an event
- Association of a certain requirement with an event

Notification examples

Here are some examples of how notifications can be used:

- **Event type:** The Dean of Students receives an Approval Required notification every time a student party is scheduled.
- **Location:** The Conference Center Coordinator receives an Approval Required notification every time the Banquet Hall is assigned to an event.
- **Resource:** The AV Director receives an Approval Required notification every time a video camera is assigned to an event.
- **Organization:** Campus Security receives an Information Only notification every time Sigma Tau sponsors an event.
- **Event requirement:** The College President receives an Information Only notification every time an alcohol permit is required for an event.

Key Concept

25Live doesn't enforce approvals and denials generated by notification recipients

25Live doesn't, for example, automatically remove the location assigned to an event if the location approval is denied by a notification recipient. If you elect to use notification policies, you should integrate them into your scheduling policies and practices. For example, you might require schedulers to assign a different location if the location they've assigned is denied by a notification recipient.

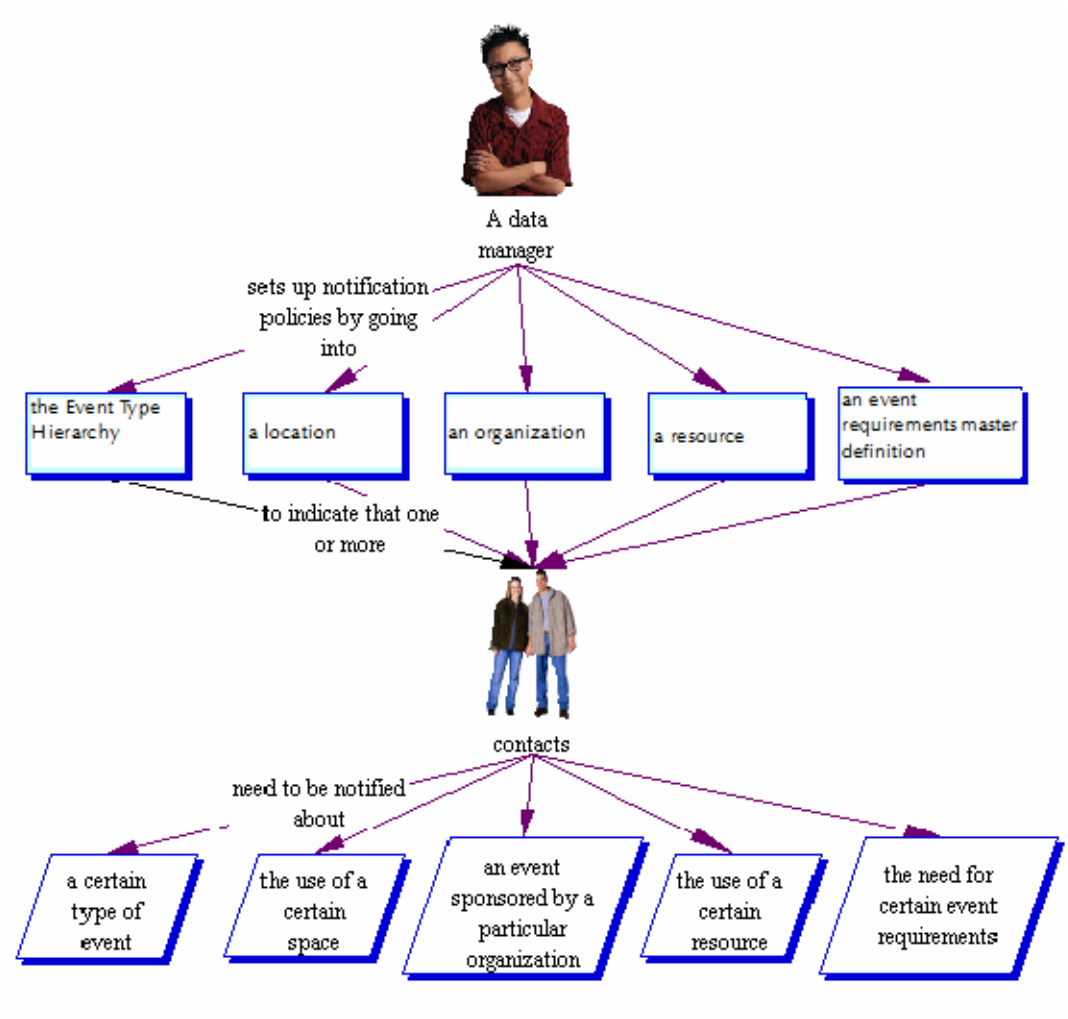
Approval by "at least one" vs approval by "all"

You can elect to require approval from at least one or approval from all notification recipients. This makes it possible to indicate that:

- If the main approver is out of the office, one of the backups can reply to the notifications.
- If two people have the same authority, either of them can reply to the notifications.
- Multiple people must reply to certain notifications.

Where notification policies are set up

Where you set up notification policies in the 25Live Administration Utility depends on what action you want to trigger the notification. Notifications are triggered automatically when any of the information illustrated below is saved with an event.



Events Security Administration

Events tab

The **Events** tab of the Administration Utility lets you perform these security administration tasks:

- Set object security access to specific events, folders, and cabinets for each of your 25Live security groups
- Set default object security access to event drafts for each of your 25Live security groups
- Define notification policies for event requirements and event types

Security

Functional security required to edit object security on cabinets, folders, and events and set default object security on event drafts

- Object Security, Assignment Policy, and Notification Policy**:** Event/Folder/Cabinet Object Security = Can view and edit object security
- Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change

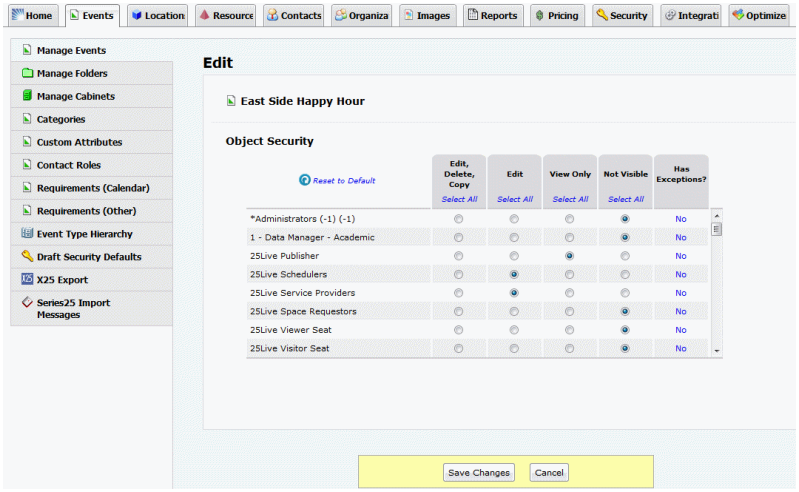
Functional security required to create and edit event requirement and event type notification policies

- Object Security, Assignment Policy, and Notification Policy: Event Requirement Notification Policy = Can view, edit, and create
- Cabinets and Folders: Event Type Hierarchy = Can view, edit, and change

Setting object security for events

Manage Events task tab

Use the **Manage Events** task tab to set object security access permissions to one or more events for each of your 25Live security groups.



Note For information on the object security needed to view the details of and possibly act on specific events, see "Appendix B - Event Details Information Access"

Setting object security for one or more events

1. With the Manage Events task tab selected, find the event(s) you want to set object security access permissions to by simple name search, by browsing your event structure, or by running one of your searches or your starred searches.
2. If you've browsed, highlight the event you want to edit, or hold down the Shift key and highlight each event to select multiple events. If you've searched, check each event you want to edit.

Caution

If you choose to edit multiple events, be aware that all *and only* the changes you make will be applied to all the events you select for edit. When in doubt, edit events one at a time.

3. Click Edit Security.

4 For each security group, select the object security access permission to the event(s).

If you set object security to...	Members of the security group...
Not Visible	Can't view the event(s).
View Only	Can view the event(s).
Edit	Can view and edit the event(s).
Edit, Delete, Copy	Can view, edit, delete, and copy the event(s).

5 To define an exception to the standard object security for the event(s) for a particular security group:

a Click "No" in the Has Exceptions? column for the security group.

b Click New Exception.

c Enter a name for the exception.

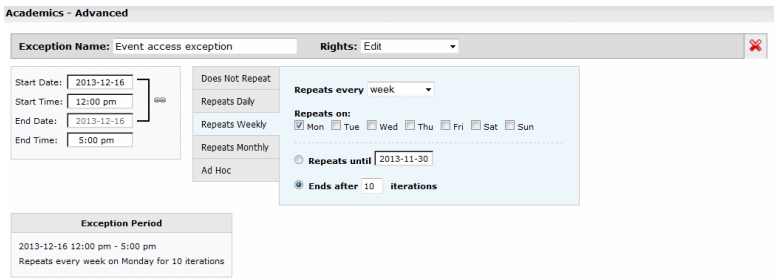
d Choose the object security access the group should have from the Rights drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

Object security exception example:



6 Click Save Changes.

Security

Effects of functional security

The Events functional security access you set for a security group must be at minimum “Can View” before the related object security is applied.

For information on modifying the functional security rights of security groups, see “Managing security groups”

Setting object security for folders

Manage Folders task tab

Use the **Manage Folders** task tab to specify object security access permissions to specific folders for each of your 25Live security groups.

Note The information presented here assumes you have already created folders as described in the *25Live Data Administration Guide*, accessible by clicking Help, and now want to edit some or all of the folders to change their default object security.

Key Concept

Default object security for new folders is the same as that of their cabinet

The default object security of a new folder is by default the same as the object security of its cabinet. To allow users in specific security groups different object security rights to a folder, you must set the appropriate object security on the folder for those security groups.

Setting object security for one or more folders

To set object security for a folder, you can do either of the following:

- Copy an existing folder as described in the *25Live Data Administration Guide* accessible by clicking Help, which also copies the security settings of that folder, then modify the security settings of the new folder as needed as described in steps **3 - 4** below.
- Set object security settings “from scratch” as described in steps **1 - 4** below.

1 Find the folder(s) you want to set object security access to by simple name search, by browsing your event structure, or by clicking "All Folders" to see a list of all the folders in your event structure.

2 Highlight the folder(s) and click Edit. To highlight multiple folders, hold down the Shift key and click each folder.

Caution

If you choose to edit multiple folders, be aware that all *and only* the changes you make will be applied to all the folders you select for edit. When in doubt, edit folders one at a time.

3 Set appropriate object security for the folder, its subfolders (if any), its events.

Note Depending on your cabinet and folder structure, you may not have to use the Security for Child Folders settings in Manage Folders, which are only relevant for folders that contain subfolders, which we do not recommend. If you don't have subfolders in your event structure, you can ignore these settings. If you do, use the Security for Child Folders settings only for folders that don't have subfolders.

To...	Do this...
Set security for the folder	1 Scroll down to the Object Security section, and click the "Edit" link. 2 Select the appropriate folder object security for each security group. 3 Define any exceptions to the standard object security for the folder for each security group by following step 5 in "Setting object security for one or more events"

To...	Do this...
Set security for the folder's subfolders **Note**: It is recommended that you avoid having subfolders of folders in your event structure.	**1** Scroll down to the Security for Child Folders section, and click the "Edit" link. **2** Expand each security area (Create Folders?, New Folder Rights, and New Folder: Create Folders?), and select the appropriate security setting for each security group. **3** For New Folder Rights, define any exceptions to the standard security for each security group by following step 5 in "Setting object security for one or more events"
Set security for the folder's events	**1** Scroll down to the Security for Child Events section, and click the "Edit" link. **2** Expand each security area (New Folder: Create Events?, Create Events?, New Event Rights), and select the appropriate security setting for each security group. **3** For New Event Rights, define any exceptions to the standard security for each security group by following step 5 in "Setting object security for one or more events"

4 Click Save Changes.

If you set this security area...	To...	Members of the security group...
Object Security	Not Visible	Can't see the folder(s) or create events in them.
	View Only	Can see the folder(s) and create events in them.
	Edit	Can see and edit the folder(s) and create events in them.
	Edit, Delete, Copy	Can see, edit, delete, and copy the folder(s) and create events in them.
Security for Child Folders: Create Folders?	No	Can't create folders in the folder(s).
	Yes	Can create folders in this folder(s).
Security for Child Folders: New Folder Rights	Not Visible	Can't see new folders in the folder(s).
	View Only	Can see new folders in the folder(s).
	Edit	Can see and edit new folders in the folder(s).
	Edit, Delete, Copy	Can see, edit, delete, and copy new folders in the folder(s).
Security for Child Folders: New Folder: Create Folders?	No	Can't create folders in new folders.
	Yes	Can create folders in new folders.
Security for Child Events: New Folder: Create Events?	No	Can't create events in new folders.
	Yes	Can create events in new folders.

If you set this security area...	To...	Members of the security group...
Security for Child Events: Create Events?	No	Can't create events in the folder(s).
	Yes	Can create events in the folder(s).
Security for Child Events: New Event Rights	Not Visible	Can't see new events in the folder(s).
	View Only	Can see new events in the folder(s).
	Edit	Can see and edit new events in the folder(s).
	Edit, Delete, Copy	Can see, edit, delete, and copy new events in the folder(s).

Security

Effects of functional security

The Folders functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Setting object security for cabinets

Manage Cabinets task tab

Use the **Manage Cabinets** task tab to set security access to specific cabinets for each of your 25Live security groups.

Note The information presented here assumes you have already created cabinets as described in the *25Live Data Administration Guide*, accessible by clicking Help, and now want to edit some or all of the cabinets to change their default object security.

Key Concept

Default object security for new cabinets is "Not Visible"

The default object security for new cabinets is set to "Not Visible" system-wide. To allow users in specific security groups to view and/or act on a specific cabinet, you must set the appropriate object security on the cabinet for those security groups.

Setting object security for one or more cabinets

1. Find the cabinet(s) you want to set object security access to by simple name search, by browsing your event structure, or by clicking "All Cabinets."
2. Highlight the cabinet(s) and click Edit. To highlight multiple cabinets, hold down the Shift key and click each cabinet.

Caution

If you choose to edit multiple cabinets, be aware that all *and only* the changes you make will be applied to all the cabinets you select for edit. When in doubt, edit cabinets one at a time.

3. If you selected one cabinet for edit, you have the option of loading the object security settings of another cabinet to the cabinet you're editing. To do so, choose a particular cabinet from the "Load Security Settings From:" drop-down list. This option is not available if you selected multiple cabinets for edit.
4. Set appropriate object security for the cabinet, its child folders, and/or its child events.

Note Depending on your cabinet and folder structure, you may not have to use the Security for Child Events settings which are only relevant to cabinets that directly contain events (that is, cabinets that don't have folders).

To...	Do this...
Set security for the cabinet	1 Scroll down to the Object Security section, and click the "Edit" link. 2 Select the appropriate cabinet object security for each security group. 3 Define any exceptions to the standard object security for the cabinet for each security group by following step 5 in "Setting object security for one or more events"

To...	Do this...
Set security for the cabinet's folders	**1** Scroll down to the Security for Child Folders section, and click the "Edit" link. **2** Expand each security area (Create Folders?, New Folder Rights, and New Folder: Create Folders?), and select the appropriate security setting for each security group. **3** For New Folder Rights, define any exceptions to the standard security for each security group by following step 5 on "Setting object security for one or more events"
Set security for the cabinet's child events **Note**: These settings are only applicable for cabinets that don't contain folders.	**1** Scroll down to the Security for Child Events section, and click the "Edit" link. **2** Expand each security area (New Folder: Create Events?, Create Events?, New Event Rights), and select the appropriate security setting for each security group. **3** For New Event Rights, define any exceptions to the standard security for each security group by following step 5 in "Setting object security for one or more events"

4 Click Save Changes.

If you set this security area...	To...	Members of the security group...
Object Security	Not Visible	Can't see the cabinet(s).
	View Only	Can see the cabinet(s).
	Edit	Can see and edit the cabinet(s).
	Edit, Delete, Copy	Can see, edit, delete, and copy the cabinet(s).
Security for Child Folders: Create Folders?	No	Can't create folders in the cabinet(s).
	Yes	Can create folders in the cabinet(s).
Security for Child Folders: New Folder Rights	Not Visible	Can't see new folders in the cabinet(s).
	View Only	Can see new folders in the cabinet(s).
	Edit	Can see and edit new folders in the cabinet(s).
	Edit, Delete, Copy	Can see, edit, delete, and copy new folders in the cabinet(s).
Security for Child Folders: New Folder: Create Folders?	No	Can't create folders in new folders.
	Yes	Can create folders in new folders.
Security for Child Events: New Folder: Create Events?	No	Can't create events in new folders.
	Yes	Can create events in new folders.
Security for Child Events: Create Events?	No	Can't create events in the cabinet(s).
	Yes	Can create events in the cabinet(s).

If you set this security area...	To...	Members of the security group...
Security for Child Events: New Event Rights	Not Visible	Can't see new events in the cabinet(s).
	View Only	Can see new events in the cabinet(s).
	Edit	Can see and edit new events in the cabinet(s).
	Edit, Delete, Copy	Can see, edit, delete, and copy new events in the cabinet(s).

Security

Effects of functional security

The Cabinets functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Defining the default object security of event draft

Key Concept

Default event draft object security defines the object security access permissions each security group has to ***newly created event drafts.***

If left unchanged for a security group, the system default of "Not Visible" applies. For example, if you leave the system default access of "Not Visible" for Event Drafts for a particular security group, members of that group won't see any new event drafts that are created.

See "Default object security and assignment policies" for more information.

Draft Security Defaults task tab

Use the **Set Draft Security Defaults** task tab to define the default event drafts object security for each of your 25Live security groups.

Setting event drafts object security defaults

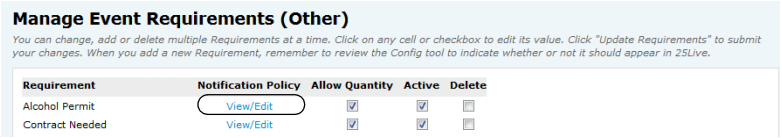
1. With the Draft Security Defaults task tab selected, select the default object security setting you want for event drafts for each security group.
2. Click Save Defaults.

Defining event requirement notification policies

You can use the 25Live Administration Utility to define a notification policy based on a particular event requirement. When a user creates an event with that requirement, the notification is automatically sent to the 25Live Task List of the user(s) specified in the notification policy. For example, you could define a notification policy that sends an Information Only notification to the Task List of the head of campus security every time an event is created with an alcohol permit requirement. For general information on notification policies, see "Notification Policies"

Defining an event requirement notification policy

1 With the Requirements (Calendar) or Requirements (Other) task tab selected, click the "View/Edit" link in the Notification Policy column of the requirement you want to define a notification policy for.



2 Choose whether the notification must be approved by at least one of the users associated with the notification or all users associated with the notification.

3 If you want to set a time limit within which the user(s) associated with the notification must act, check the Approval Required Within box, and set the number of days, hours, and/or minutes after the notification creation date that action must be taken.

4 Perform a simple full or partial name search for a user you want to associate with the notification policy, then click the Select button of that user. (You can also click Select All to select all returned users.)

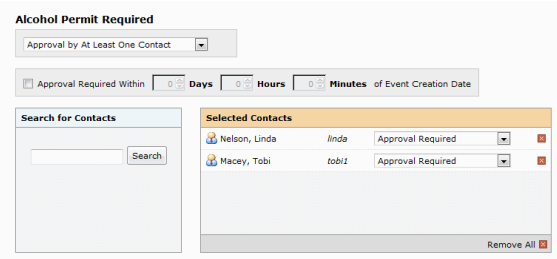
5 If you need to run another search to find other users you want to associate with the notification policy, click Search Again.

Note If you need to remove one or more users you've associated with the notification policy, click the Remove button of each, or click Remove All to remove all associated users.

6 For each associated user, choose the type of notification they should receive—Approval Required or Notification Only.

7 Click Save Changes.

Event requirement notification policy example:

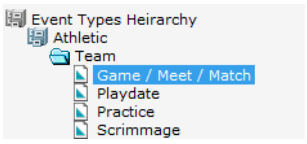


Defining event type notification policies

You can use the 25Live Administration Utility to define a notification policy based on a particular event type. When a user creates an event of that type, the notification is automatically sent to the 25Live Task List of the user(s) specified in the notification policy. For example, you could define a notification policy that sends an Approval Required notification to the Task List of the Dean of Students every time an event is created with a "Student Party" event type. For general information on notification policies, see "Notification Policies"

Defining an event type notification policy

1. With the Event Type Hierarchy task tab selected, expand the cabinet and folder section of your Event Type Hierarchy that includes the event type you want to define a notification policy for, and highlight the event type. In this example, we're defining a notification policy for the "Game/Meet/Match" event type.



2. Click Edit.
3. Scroll down to the Notification Policy section of the page and click its "Edit" link.
4. Choose whether the notification must be approved by at least one of the users associated with the notification or all users associated with the notification.

5 If you want to set a time limit within which the user(s) associated with the notification must act, check the Approval Required Within box, and set the number of days, hours, and/or minutes after the notification creation date that action must be taken.

6 Perform a simple full or partial name search for a user you want to associate with the notification policy, then select the user(s) in the search results. (You can also click Select All to select all returned users.)

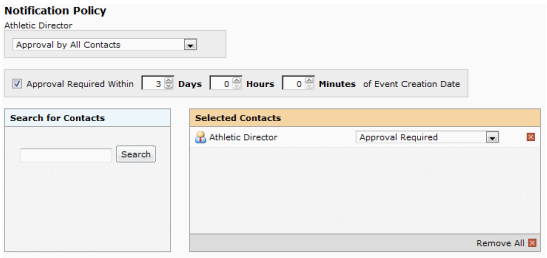
7 If you need to run another search to find other users you want to associate with the notification policy, click the Back arrow and repeat step **6**.

Note If you need to remove one or more users you've associated with the notification policy, click the Remove button (red X) of each, or click Remove All to remove all associated users.

8 For each associated user, choose the type of notification they should receive—Approval Required or Notification Only.

9 Click Save Changes.

Event type notification policy example:



Locations Security Administration

Locations tab

The **Locations** tab of the Administration Utility lets you perform these security administration tasks:

- Set the object security and assignment policy access permissions for specific locations for each of your 25Live security groups
- Define notification policies for specific locations for each of your 25Live security groups
- Set the default location object security and assignment policy for each of your 25Live security groups

Note The information presented here assumes you have already created locations as described in the *25Live Data Administration Guide*, accessible by clicking Help, and now want to edit them to define their object security, assignment policies, and possibly notification policies.

Security

Functional security required to edit the object security of specific locations and set default object security and assignment policies for locations

- Object Security, Assignment Policy, and Notification Policy: Location Object Security = Can view and edit object security
- Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change

Functional security required to create and edit location assignment policies

- Object Security, Assignment Policy, and Notification Policy: Location Assignment Policy = Can view, edit and create

Functional security required to create and edit location notification policies

- Object Security, Assignment Policy, and Notification Policy: Location Notification Policy = Can view, edit, and create

Defining the object security, assignment policies, and notification policies of locations

Manage Locations task tab

Use the **Manage Locations** task tab to define the object security, assignment policies, and notification policies of locations.

Defining location object security, assignment policies, and notification policies

1 With the Manage Locations task tab selected, click the EDIT icon.

2 Find the location(s) whose object security, assignment policy, and/or notification policy you want to define by simple name search, alphabetical index, grouping, or saved search.

Note Selecting "All Locations" is not recommended because of the large amount of data that could be returned.

3 Highlight the location(s) and click Edit. To highlight multiple locations, hold down the Shift key and click each location. Locations you have permission to edit have a "Yes" in the Can Edit? column of the location list.

Caution

If you choose to edit multiple locations, be aware that all *and only* the changes you make will be applied to all the locations you select for edit. When in doubt, edit locations one at a time.

4 Set object security access permissions to the location(s):

a If you selected one location, click the Object Security "EDIT" link.

If you selected multiple locations, check the Object Security box.

b Change the object access setting for each security group as needed. See "Object security access levels"

5 To define an exception to the standard object security for the location(s) for a particular security group:

a Click "No" in the Has Exceptions? column for the security group.

b Click New Exception.

c Enter a name for the exception.

d Choose the object security access the group should have from the Rights drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

6 Set assignment policy access permissions to the location(s):

a If you selected one location, click the Assignment Policy "EDIT" link.

If you selected multiple locations, check the Assignment Policy box.

b Change the assignment policy access setting for each security group as needed. See "Assignment policy access levels"

7 To define an exception to the standard assignment policy for a particular security group:

a Click "No" in the Has Exceptions column for the security group.

b Click New Exception.

c Enter a name for the exception.

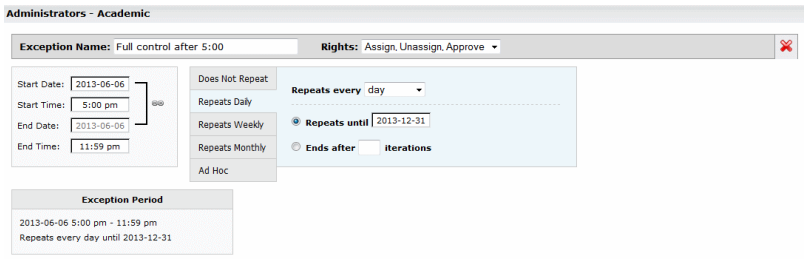
d Choose the assignment rights the group should have from the drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

Assignment policy exception example:



8 If you want to define a notification policy for the location(s), do the following:

a If you selected one location, click the Notification Policy "EDIT" link.

If you selected multiple locations, check the Notification Policy box.

b Choose whether the notification must be approved by at least one of the users associated with the notification or all users associated with the notification.

c If you want to set a time limit within which the user(s) associated with the notification must act, check the Approval Required Within box, and set the number of days, hours, and/or minutes after the notification creation date that action must be taken.

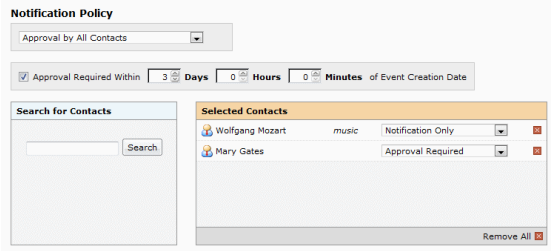
d Perform a simple full or partial name search for a user you want to associate with the notification policy, then select the user(s) in the search results. (You can also click the Select All arrow to select all returned users.)

e If you need to run another search to find other users you want to associate with the notification policy, click the Back arrow and repeat step **d**.

Note If you need to remove one or more users you've associated with the notification policy, click the Remove button (red X) of each, or click Remove All to remove all associated users.

f For each associated user, choose the type of notification they should receive—Approval Required or Notification Only.

Location notification policy example:



9 Click Save Changes.

Tip

You can use the notification policy of a location as a "template" to define the same notification policy for other locations. To do this:

a Find the location with the notification policy you want to use as a template.

b Select that location for edit along with the other locations you want to define a notification policy for.

c Check the Notification Policy box, then choose the location whose notification policy you wish to use as a template from the Use Template drop-down list.

d Click Save Changes to apply the notification policy "template" you chose to all selected locations.

Security

Effects of functional security

The Location Access functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Defining the default object security and assignment policies of locations

Key Concept

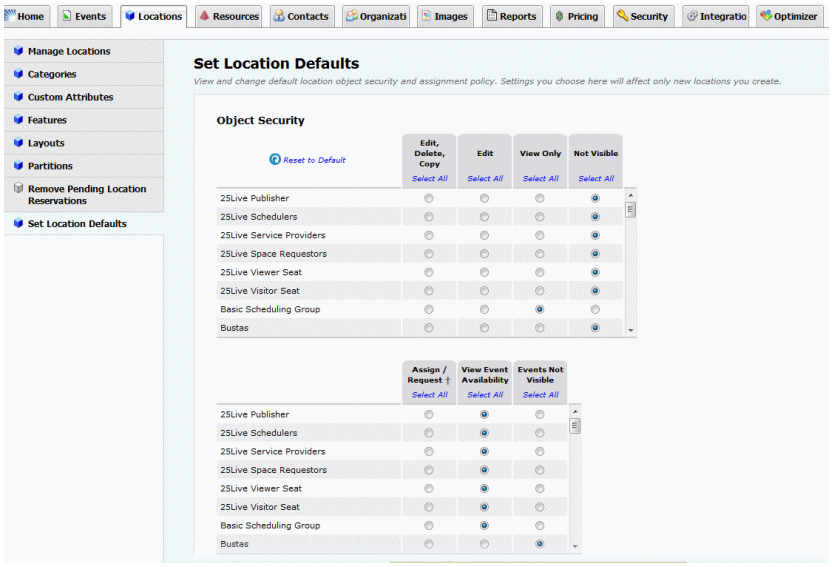
Default location object security and assignment policies define the object security access permissions and assignment policy permission each security group has to ***newly created locations***.

If left unchanged for a security group, the object security system defaults of "Not Visible" and "Events Not Visible" applies, meaning that members of the group won't see any new locations that are created nor any events they're assigned to. In this case, the system default assignment policy of "Request" doesn't apply, since a security group must have at least "View Only" and "Assign/Request" location object security to be able to request assignment of a location.

See "Default object security and assignment policies" for more information.

Set Location Defaults task tab

Use the **Set Location Defaults** task tab to define the default location object security and assignment policy access for each of your 25Live security groups.



Setting location object security and assignment policy defaults

1. With the Set Location Defaults task tab selected, choose the default object security settings you want for each security group.
2. Scroll down and choose the default assignment policy setting you want for each security group.
3. Click Save Location Defaults.

Resources Security Administration

Resources tab

The **Resources** tab of the Administration Utility lets you perform these security administration tasks:

- Set the object security and assignment policy access permissions for specific resources for each of your 25Live security groups
- Define notification policies for specific resources for each of your 25Live security groups
- Set the default resource object security and assignment policy for each of your 25Live security groups

Note The information presented here assumes you have already created resources as described in the *25Live Data Administration Guide*, accessible by clicking Help, and now want to edit them to define their object security, assignment policies, and possibly notification policies.

Security

Functional security required to edit the object security of specific resources and set default object security and assignment policies for resources

- Object Security, Assignment Policy, and Notification Policy: Resource Object Security = Can view and edit object security
- Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change

Functional security required to create and edit resource assignment policies

- Object Security, Assignment Policy, and Notification Policy: Resource Assignment Policy = Can view, edit and create

Functional security required to create and edit resource notification policies

- Object Security, Assignment Policy, and Notification Policy: Resource Notification Policy = Can view, edit, and create

Defining the object security, assignment policies, and notification policies of resources

Manage Resources task tab

Use the **Manage Resources** task tab to define the object security, assignment policies, and notification policies of resources.

Defining resource object security, assignment policies, and notification policies

1. With the Manage Resources task tab selected, click the EDIT icon.
2. Find the resource(s) whose object security, assignment policy, and/or notification policy you want to define by simple name search, alphabetical index, category, or saved search.

   Note Selecting "All Resources" is not recommended because of the large amount of data that could be returned.

3. Highlight the resource(s) and click Edit. To highlight multiple resources, hold down the Shift key and click each resource. Resources you have permission to edit have a "Yes" in the Can Edit? column of the resource list.

Caution

If you choose to edit multiple resources, be aware that all *and only* the changes you make will be applied to all the resources you select for edit. When in doubt, edit resources one at a time.

4. Set object security access permissions to the resource(s):
   - **a** If you selected one resource, click the Object Security "EDIT" link.

     If you selected multiple resources, check the Object Security box.
   - **b** Change the object access setting for each security group as needed. See "Object security access levels"
5. To define an exception to the standard object security for the resource(s) for a particular security group:
   - **a** Click "No" in the Has Exceptions? column for the security group.
   - **b** Click New Exception.
   - **c** Enter a name for the exception.
   - **d** Choose the object security access the group should have from the Rights drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

6 Set assignment policy access permissions to the resource(s):

a If you selected one resource, click the Assignment Policy "EDIT" link.

If you selected multiple resources, check the Assignment Policy box.

b Change the assignment policy access setting for each security group as needed. See "Assignment policy access levels"

7 To define an exception to the standard assignment policy for a particular security group:

a Click "No" in the Has Exceptions column for the security group.

b Click New Exception.

c Enter a name for the exception.

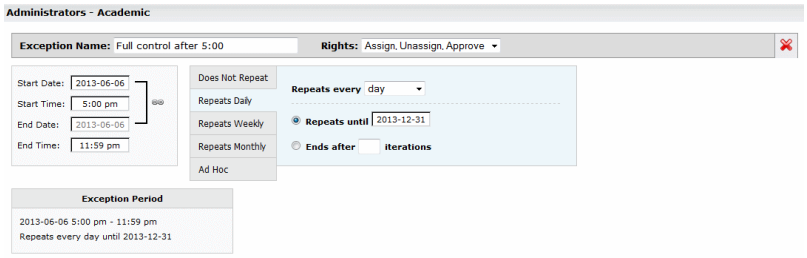
d Choose the assignment rights the group should have from the drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

Assignment policy exception example:



8 If you want to define a notification policy for the resource(s) you selected. do the following:

a If you selected one resource, click the Notification Policy "EDIT" link.

If you selected multiple resources, check the Notification Policy box.

b Choose whether the notification must be approved by at least one of the users associated with the notification or all users associated with the notification.

c If you want to set a time limit within which the user(s) associated with the notification must act, check the Approval Required Within box, and set the number of days, hours, and/or minutes after the notification creation date that action must be taken.

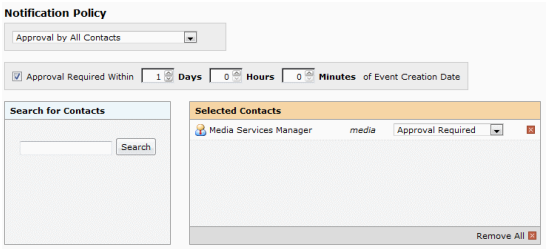
d Perform a simple full or partial name search for a user you want to associate with the notification policy, then select the user(s) in the search results. (You can also click the Select All arrow to select all returned users.)

e If you need to run another search to find other users you want to associate with the notification policy, click the Back arrow and repeat step **d**.

Note If you need to remove one or more users you've associated with the notification policy, click the Remove button (red X) of each, or click Remove All to remove all associated users.

f For each associated user, choose the type of notification they should receive—Approval Required or Notification Only.

Notification policy example:



9 Click Save Changes.

Tip

You can use the notification policy of a resource as a "template" to define the same notification policy for other resources. To do this:

- **a** Find the resource with the notification policy you want to use as a template.
- **b** Select that resource for edit along with the other resources you want to define a notification policy for.
- **c** Check the Notification Policy box, then choose the resource whose notification policy you wish to use as a template from the Use Template drop-down list.
- **d** Click Save Changes to apply the notification policy "template" you chose to all selected resources.

Security

Effects of functional security

The Resource Access functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Defining the default object security and assignment policies of resources

Key Concept

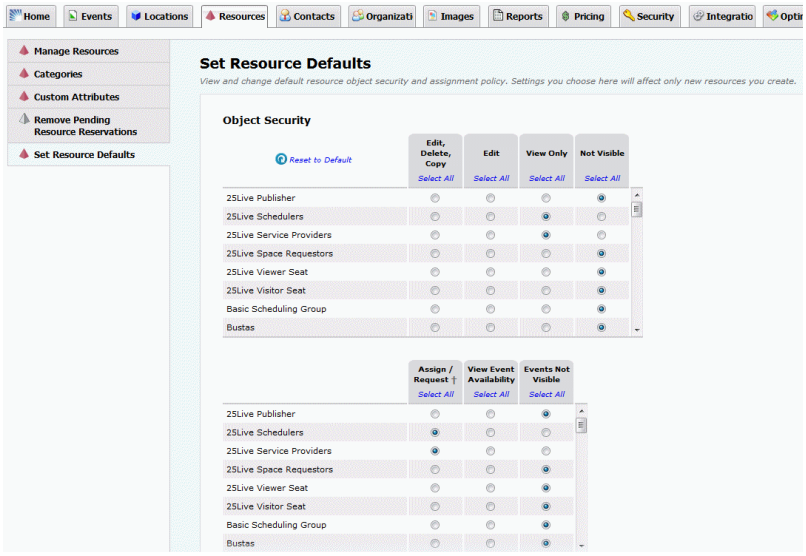
Default resource object security and assignment policies define the object security access permissions and assignment policy permission each security group has to ***newly created resources***.

If left unchanged for a security group, the object security system defaults of "Not Visible" and "Events Not Visible" applies, meaning that members of the group won't see any new resources that are created nor any events they're assigned to. In this case, the system default assignment policy of "Request" doesn't apply, since a security group must have at least "View Only" and "Assign/Request" resource object security to be able to request assignment of a resource.

See "Default object security and assignment policies" for more information.

Set Resource Defaults task tab

Use the **Set Resource Defaults** task tab to define the default resource object security and assignment policy access for each of your 25Live security groups.



Setting resource object security and assignment policy defaults

1. With the Set Resource Defaults task tab selected, choose the default object security settings you want for each security group.
2. Scroll down and choose the default assignment policy setting you want for each security group.
3. Click Save Resource Defaults.

Contacts Security Administration

Contacts tab

The **Contacts** tab of the Administration Utility lets you perform these security administration tasks:

- Manage (add, copy, edit, and delete) 25Live users
- View the 25Live users who are currently signed in

Security

Functional security required to create 25Live users, edit user information, activate/deactivate users, and delete users

- Contacts: Contact Access = Can view, edit, and create
- Contacts: Contact Delete = Can delete
- Security: Security = Can view user lists, change security group permissions, assign members to groups, make users active or inactive, create and delete security groups, and enable/disable object security

Functional security required to view the 25Live users who are currently signed in

- Contacts: Security = Can view user lists

Adding and managing 25Live users

Manage Contacts task tab

Use the **Manage Contacts** task tab to:

- Add 25Live users
- Copy 25Live users as the basis for creating new users
- Edit 25Live users one by one or multiple users simultaneously
- Delete 25Live users
- Activate and deactivate 25Live users

Adding a 25Live user

These instructions assume you have already created your 25Live security groups, as described beginning in "Adding security groups"

1. With the Manage Contacts task tab selected, click the ADD icon.
2. Enter the user's Last Name (required) and Work Email Address (required), and any other basic, email, address information, and/or comments you want for the user.
3. Enter the user's 25Live username and password. Passwords can only contain letters, numbers, and underscores.
4. Indicate whether the user is active (default) or inactive.
5. Choose the 25Live security group you want the user to be a member of.
6. If the user is associated with an organization or department:
   a. Click New Organization.
   b. Select the user's role in the organization.
   c. Find and select the organization. If the user is associated with other organizations, repeat these steps.
7. Check any custom attributes that pertain to this user and enter a value for each.
8. Click Add Contact.

Key Concept

The Public Search user

To provide the ability to create "public" searches that can be accessed and run by all 25Live Viewers and Users, you must create a generic "Public Search" user as described above and make sure that user is a member of a security group that has the functional security required to create robust searches—the -1 security group or a Functional Administration security group is recommended. For more information, see "Adding security groups". Once this user is entered in the 25Live Configuration Utility, any searches created by the user are automatically made "public" when saved. For information on entering the Public Search user in the Configuration Utility, see the *25Live Configuration Utility* document.

Copying a 25Live user

1. With the Manage Contacts task tab selected, click the COPY icon.
2. Find the user you want to copy by simple name search or alphabetical index, highlight the user, then click Copy. Users can be easily identified because they have a Username, Status, and Security Group.
3. Add or edit the information for the new user as needed, and enter their User Information.
4. Click Add Contact.

Editing one or more 25Live users

1. With the Manage Contacts task tab selected, click the EDIT icon.
2. Find the user(s) you want to edit by simple name search or alphabetical index.
3. Highlight the user(s) you want to edit and click Edit. To highlight multiple users, hold down the Shift key and click each user. Users can be easily identified because they have a Username, Status, and Security Group.

Caution

If you choose to edit multiple users, be aware that all *and only* the changes you make will be applied to all the users you select for edit. When in doubt, edit users one at a time.

4. If you highlighted one user, edit his/her information as needed. Click the "EDIT" link to expand sections that are closed. If you highlighted multiple users, check the box of each data section you want to edit, and change the information as needed.

Caution

Editing a user's work email address may break the connection between the user and your Active Directory. If you are unsure, check with your 25Live System Administrator before proceeding.

5. Click Save Changes.

Deleting a 25Live user

1. With the Manage Contacts task tab selected, click the DELETE icon.
2. Find the user you want to delete by simple name search or alphabetical index, highlight the user, then click Delete. Users can be easily identified because they have a Username, Status, and Security Group. You can only delete one user at a time.
3. Click Delete Contact to confirm.
4. To delete other users, click Delete Another Contact. To return to the Manage Contacts page, click Start Over.

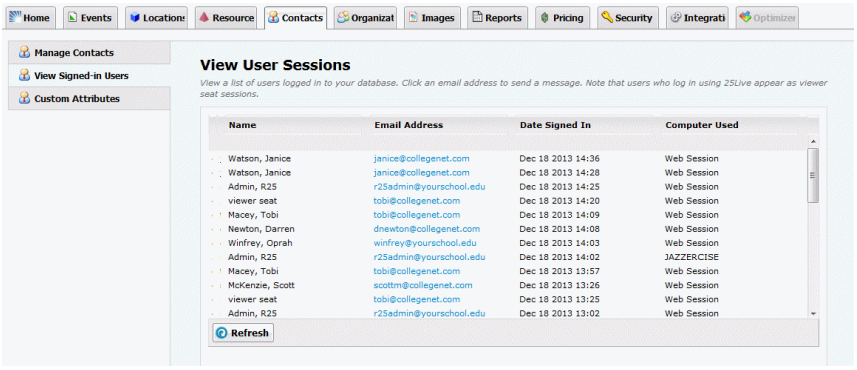
Activating or deactivating 25Live users

1. With the Manage Contacts task tab selected, click the EDIT icon.
2. Find the 25Live user(s) you want to activate or deactivate by simple name search or alphabetical index.
3. Highlight the user(s) and click Activate or Deactivate. To highlight multiple users, hold down the Shift key and click each user.

   25Live users can be easily identified because they have a value in the Status and Security Group columns of the list. Contacts who aren't 25Live users can't be activated or deactivated.
4. When the dialog appears, click OK.

Viewing signed-in users

Use the **View Signed-in Users task** tab to see a list of the users who are currently signed into 25Live, the 25Live Administration Utility, and/or the 25Live Configuration Utility. You can click the email link of one or more users to send them an email.



Organizations Security Administration

Organizations tab

The **Organizations** tab of the Administration Utility lets you perform these security administration tasks:

- Set the object security of specific organizations for each of your 25Live security groups
- Define notification policies for specific organizations for each of your 25Live security groups
- Set default organization object security for each of your 25Live security groups

Note The information presented here assumes you have already created organizations as described in the *25Live Data Administration Guide*, accessible by clicking Help, and now want to edit them to define their object security and possibly notification policies.

Security

Functional security required to edit the object security of specific organizations and set default object security for organizations

- Object Security, Assignment Policy, and Notification Policy: Organization Security = Can view and edit object security
- Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change

Functional security required to create and edit organization notification policies

- Object Security, Assignment Policy, and Notification Policy: Organization Notification Policy = Can view, edit, and create

Defining the object security and notification policies of organizations

Manage Organizations task tab

Use the **Manage Organizations** task tab to define the object security and notification policies of organizations.

Defining object security and notification policies for organizations

1 With the Manage Organizations task tab selected, click the EDIT icon.

2 Find the organization(s) whose object security and/or notification policy you want to define by simple name search, alphabetical index, type or category grouping, or saved search.

Note Selecting "All Organizations" is not recommended because of the large amount of data that could be returned.

3 Highlight the organization(s) and click Edit. To highlight multiple organizations, hold down the Shift key and click each organization.

Caution

If you choose to edit multiple organizations, be aware that all *and only* the changes you make will be applied to all the organizations you select for edit. When in doubt, edit organizations one at a time.

4 Set the object security setting to the organization(s) for each of your 25Live security groups.

a If you selected one organization, click the Object Security "EDIT" link.

If you selected multiple organizations, check the Object Security box.

b Change the object access setting for each security group as needed. See "Object security access levels"

5 To define an exception to the standard object security for the organization(s) for a particular security group:

a Click "No" in the Has Exceptions? column for the security group.

b Click New Exception.

c Enter a name for the exception.

d Choose the object security access the group should have from the Rights drop-down list.

e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

f If the exception repeats, define the repeating pattern or ad hoc dates.

g Click Done.

6 If you want to define a notification policy for the organization(s) you selected, do the following:

a If you selected one organization, click the Notification Policy "EDIT" link.

If you selected multiple organizations, check the Notification Policy box.

b Choose whether the notification must be approved by at least one of the users associated with the notification or all users associated with the notification.

c If you want to set a time limit within which the user(s) associated with the notification must act, check the Approval Required Within box, and set the number of days, hours, and/or minutes after the notification creation date that action must be taken.

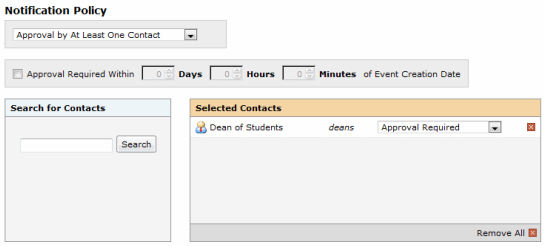
d Perform a simple full or partial name search for a user you want to associate with the notification policy, then select the user(s) in the search results. (You can also click the Select All arrow to select all returned users.)

e If you need to run another search to find other users you want to associate with the notification policy, click the Back arrow and repeat step **d**.

Note If you need to remove one or more users you've associated with the notification policy, click the Remove button (red X) of each, or click Remove All to remove all associated users.

f For each associated user, choose the type of notification they should receive—Approval Required or Notification Only.

Notification policy example:



7 Click Save Changes.

Tip

You can use the notification policy of an organization as a "template" to define the same notification policy for other organizations. To do this:

a Find the organization with the notification policy you want to use as a template.

b Select that organization for edit along with the other organizations you want to define a notification policy for.

c Check the Notification Policy box, then choose the organization whose notification policy you wish to use as a template from the Use Template drop-down list.

d Click Save Changes to apply the notification policy "template" you chose to all selected organizations.

Security

Effects of functional security

The Organization Access functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Defining the default object security of organizations

Key Concept

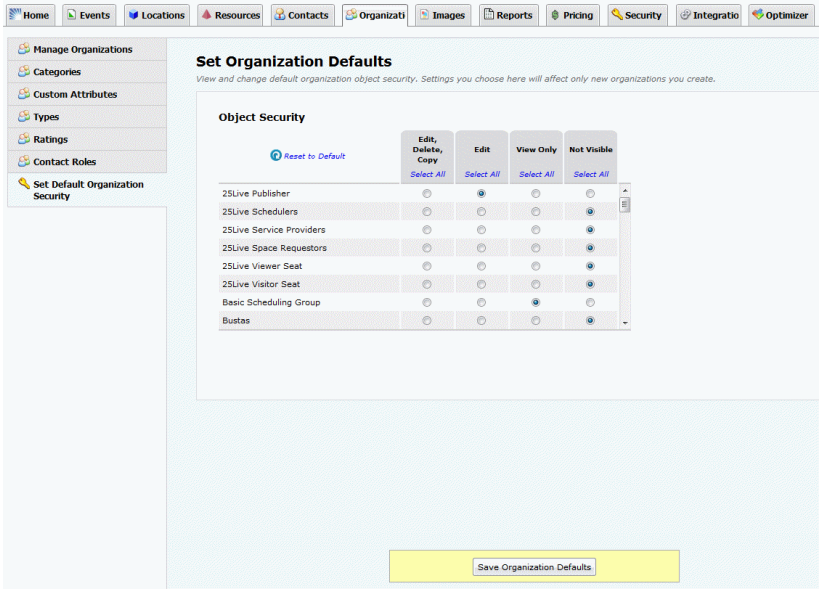
Default organization object security defines the object security access permission each security group has to ***newly created organizations***.

If left unchanged for a security group, the object security system default of "Not Visible" applies, meaning that members of the group won't see any new organizations that are created.

See "Default object security and assignment policies" for more information.

Set Default Organization Security task tab

Use the **Set Default Organization Security** task tab to define the default organization object security for each of your 25Live security groups.



Setting organization object security defaults

1. With the Set Default Organization Security task tab selected, select the default object security setting you want for each security group.
2. Click Save Organization Defaults.

Reports Security Administration

Reports tab

The **Reports** tab of the Administration Utility lets you perform these security administration tasks:

- Set the object security of specific reports for each of your 25Live security groups
- Set default report object security for each of your 25Live security groups

Security

Functional security required to edit the object security of specific reports and set default object security for reports

- Object Security, Assignment Policy, and Notification Policy: Report Object Security = Can view and edit object security
- Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change

Defining the object security of reports

Manage Reports task tab

Use the **Manage Reports** task tab to define the object security of reports for each of your 25Live security groups.

Defining object security for reports

1. With the Manage Reports task tab selected, click the EDIT icon.
2. Find the report(s) you want to set object security for by report grouping.
3. Highlight the report(s) and click Edit. To highlight multiple reports, hold down the Shift key and click each report.

Caution

If you choose to edit multiple reports, be aware that all *and only* the changes you make will be applied to all the reports you select for edit. When in doubt, edit reports one at a time.

4 Set object security access permissions to the report(s):

   a If you selected one report, scroll down and click the Object Security "EDIT" link.

   b Change the object access setting for each security group as needed. See "Object security access levels"

5 To define an exception to the standard object security for the report(s) for a particular security group:

   a Click "No" in the Has Exceptions? column for the security group.

   b Click New Exception.

   c Enter a name for the exception.

   d Choose the object security access the group should have from the Rights drop-down list.

   e Enter the start date/time and end time of the exception and, if it spans midnight, click the link icon and enter the end date.

   f If the exception repeats, define the repeating pattern or ad hoc dates.

   g Click Done.

6 Click Save Security Changes.

Security

Effects of functional security

The Report Access functional security access you set for a security group must be at minimum "Can View" before the related object security is applied.

For information on modifying the functional security rights of security groups, see "Managing security groups"

Defining the default object security of reports

Key Concept

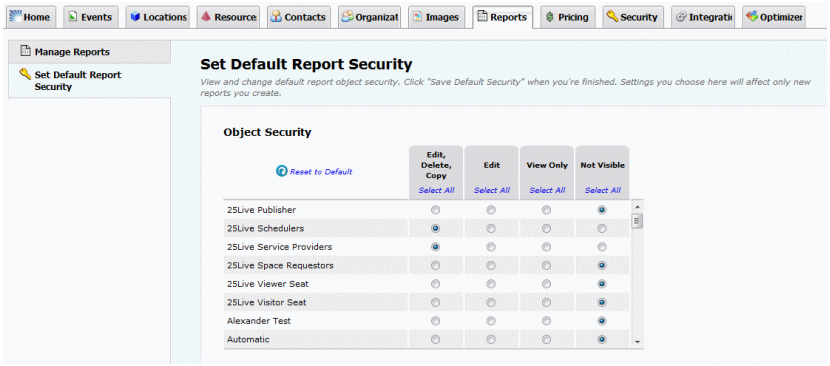
Default report object security defines the object security access permission each security group has to ***newly created custom reports***.

If left unchanged for a security group, the object security system default of "Not Visible" applies, meaning that members of the group won't see any new custom reports that are created.

See "Default object security and assignment policies" for more information.

Set Default Report Security task tab

Use the **Set Default Report Security** task tab to define the default report object security for each of your 25Live security groups.



Setting report object security defaults

1. With the Set Default Report Security task tab selected, select the default object security setting you want for each security group.
2. Click Save Default Security.

Security Administration

Security tab

The **Security** tab of the 25Live Administration Utility lets you perform these security administration tasks:

- Manage and add 25Live security groups and set the functional security rights of each
- View and "unlock" your own locked items and those of other users
- Enable and disable object security system-wide

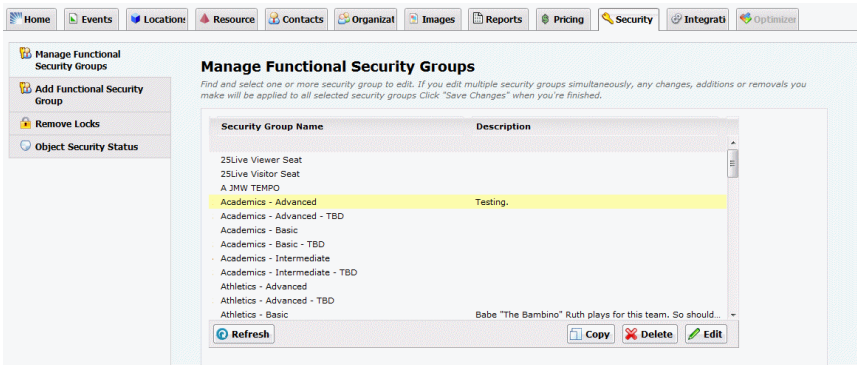
 **Security**	**Functional security required to create, edit, and delete security groups and enable/disable object security** · Contacts: Security Groups = Can view user lists, change security group permissions, assign members to groups, make users active or inactive, create and delete security groups, and enable/disable object security · Object Security, Assignment Policy, and Notification Policy: Default Object Security = Can view, edit, and change
	Functional security required to view and "unlock" your own locked items and those of other users · Locks and Overrides: Locks and Pending Reservations = Can view and remove anyone's locked items and pending reservations

Managing security groups

Manage Functional Security task tab

Use the **Manage Functional Security Groups** task tab to:

- Edit one or more security groups
- Copy security groups as the basis for creating new security groups
- Delete security groups



Editing one or more security groups

Note You can't edit the functional security rights of the System Administrators (-1) security group, but you can change the group members.

1 Highlight the security group(s) you want to edit, and click Edit. To highlight multiple security groups, hold down the Shift key and click each security group.

Caution

If you choose to edit multiple security groups, be aware that all *and only* the changes you make will be applied to all the security groups you select for edit. When in doubt, edit security groups one at a time.

2 If you highlighted one security group:

a Edit the security group name and/or description as needed.

b Edit the functional security rights of the group as needed by clicking the Rights "EDIT" link, expanding each of the rights areas you want to edit, and modifying the rights in each area as needed. See "Appendix A - Functional Security Settings" for descriptions of each functional security right.

Note "Revert to Saved" reloads the last saved copy of the security group's functional security settings.

c Edit the security group members as needed by clicking the Members "EDIT" link and following these instructions:

To...	Do this...
Move a member to another security group	Choose the group from the Change Group drop-down list.
Add new members	**1** Click Add a New Member. **2** Find a user you want to add by full or partial name. **3** If multiple users are returned, choose the user you want from the drop-down list. **4** Repeat steps 1 - 3 to add more members to the group.

If you highlighted more than one security group:

a Edit the description of all selected groups as needed by checking the Description box, then entering or modifying the description as needed.

b Edit the functional security rights of all selected groups as needed by checking the Rights box, expanding each of the rights areas you want to edit, and modifying the rights in each area as needed. See "Appendix A - Functional Security Settings" for descriptions of each functional security right.

3 Click Save Changes.

Copying a security group

Copying a security group copies its functional security, object security, and assignment policy rights.

1 Highlight the security group you want to copy, and click Copy.

2 Enter a name for the new security group, and enter or edit the description as needed.

3 To edit the functional rights of the new group, click the Rights "EDIT" link, then modify the rights as needed. See "Appendix A - Functional Security Settings" for descriptions of each functional security right.

4 Add members to the group.

   a Click Add a New Member.

   b Find a user you want to add by full or partial name.

   c If multiple users are returned, choose the user you want from the drop-down list.

   d Repeat steps **a** - **c** to add more members to the group.

5 Click Add Security Group.

Deleting a security group

1 Click the Security tab, then click "Manage Security Groups."

2 Highlight the security group you want to delete, and click Delete. You can only delete one security group at a time.

3 Click Delete Security Group to confirm.

4 Click Manage More Security Groups to return to the Manage Security Groups page.

Adding security groups

Add Functional Security Group task tab

Use the **Add Functional Security Group** task tab to add a new security group and set its functional security rights.

25Live security group templates

When creating a 25Live security group, you must copy one of the security group "templates" described in "Security group template descriptions" as the starting point for creating the security group.

Security group template descriptions

This table lists each of the security group templates available in the 25Live Administration Utility and the kind of user each is intended for.

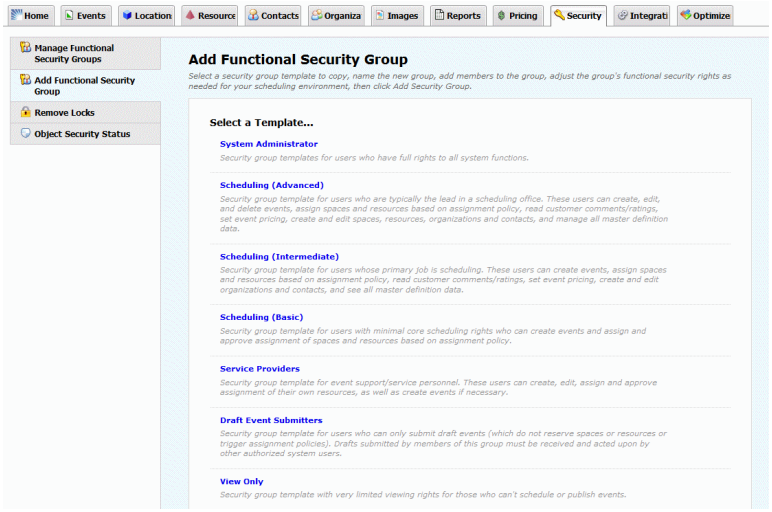
Use this template...	For users who must be able to do all or most of the following...
System Administrator	· Perform all system functions This is the security group template to use for those responsible for supporting and administering 25Live, including the Public Search User (see "The Public Search user").
Scheduling (Advanced)	· Create, edit, and delete events · Assign locations and resources to events based on assignment policy · Read organization comments/ratings · Set up event pricing · Create and edit locations, resources, organizations, and contacts · Create and edit all master list data This is the security group template to use for those who are leads in a scheduling office and/or functional administrators responsible for data management.
Scheduling (Intermediate)	· Create events · Assign locations and resources to events based on assignment policy · Read organization comments/ratings · Set up event pricing · Create and edit organizations and contacts · Create and edit all master list data This is the security group template to use for those whose primary job is scheduling.
Scheduling (Basic)	· Create events · Assign and approve assignment of locations and resources based on assignment policy This is the security group template to use for those with basic core scheduling rights.

Use this template...	For users who must be able to do all or most of the following...
Service Providers	· Create and edit their own resources · Assign and approve assignment of their own resources · Create events when necessary This is the security group template to use for support/ service personnel.
Draft Event Submitters	· Submit event drafts This is the security group template to use for those who can only submit event drafts. Event drafts don't reserve locations/resources or trigger assignment policies until saved as "real" events by an authorized scheduler.
View Only	· View events, locations, and resources This is the security group template to use for the Viewer Seat.

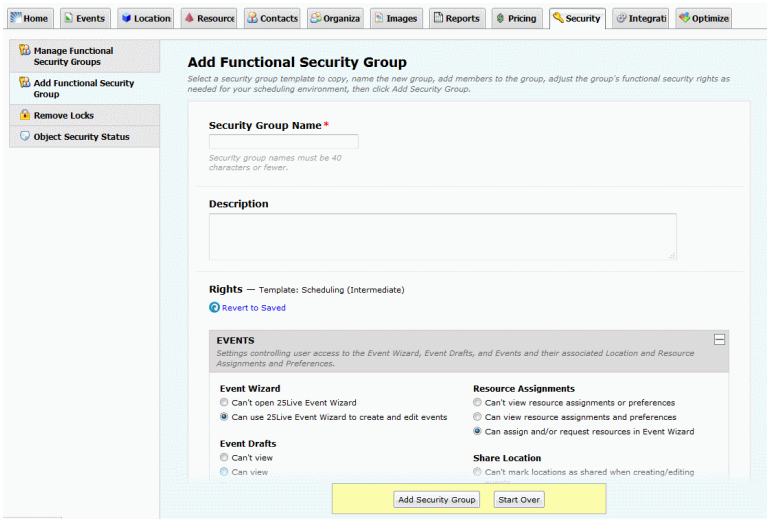
Adding a security group

The instructions below tell you how to add any 25Live security group, except the Viewer Seat group. For information on creating the 25Live Viewer Seat and its security group, see *25Live Viewer Seat Setup* available here: http://knowledge25.collegenet.com/display/CustomerResources/25Live+Documentation

1 Click the Add Functional Security Group task tab.



2 Click the security group template name that best describes the permissions of the security group you want to add. You must copy a security group template to create your new security group. See "Security group template descriptions"



3 Enter a name for the security group (required), and, optionally, a description.

4 In the Rights area of the page, modify the functional security rights of the new security group as needed. You must scroll down to see the entire rights list. The rights that have been selected by CollegeNET for the security group template you copied represent the recommended and most common selections for a security group of this type. See "Appendix A - Functional Security Settings" for information on all functional security settings.

5 Click Add Security Group.

Security

Functional security required to view, create, and edit events and run simple event searches

Below is a list of the minimal functional security required for a security group to be able to create and edit events, assign and/or request locations and resources, view event details, and run simple event searches. Functional security settings not listed can be set to the least privileged access level.

- Events: Event Wizard = Can use 25Live Event Wizard to create and edit events
- Events: Event Drafts = Can view, edit, create, and copy
- Events: Events = Can view
- Events: Location Assignments = Can assign and/or request locations in Event Wizard
- Events: Resource Assignments = Can assign and/or request resources in Event Wizard
- Events: Description and Confirmation Notes = Can view and edit
- Tasks, Reports, and Email: To Do Tasks = Can view, create, assign, complete and delete To Dos
- Cabinets and Folders: Cabinets = Can view
- Cabinets and Folders: Folders = Can view
- Searches and Master Definitions: Event Search = Can view, run, create and save event searches

Security

Functional security required for searching

The information below describes how functional security must be set up for a security group to be able to access and use 25Live searching capabilities. "<object>" indicates the type of object that can be searched for. For example, to be able to do a simple search for events, Events functional security "Events" must at minimum be set to "Can view" and Searches and Master Definitions functional security "Event Search" must be set to "Can view, run, create and save event searches."

As a non-signed in user, to be able to view and run public searches and define and run simple searches on the Search For <object> tab, functional security must be set to:

- <object> = Can view
- <object> Search = Can view, run, create, and save searches

As a signed-in user, to be able to view and run public searches and your saved searches, delete and rename your saved searches, and define, run, and save simple searches on the Search For <object> tab, functional security must be set to:

- <object> = Can view
- <object> Search = Can view, run, create, and save searches

As a signed-in user, to be able to view and run public searches and your saved searches, delete and rename your saved searches, define, run, and save simple searches on the Search For <object> tab, and define, run, edit, delete, copy, and save searches on the Advanced <object> Search tab, functional security must be set to:

- <object> = Can view
- <object> Search = Can view, run, create, and save searches
- object> Master Definitions = Can view all active items

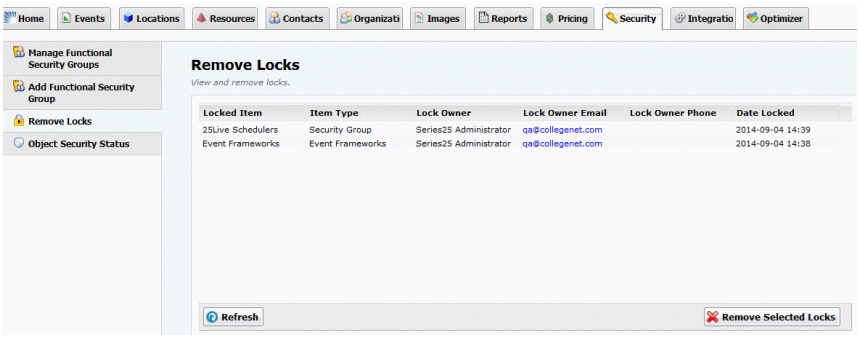
If a security group has the required access to the advanced event search, but has "Can't View" access to locations, resources, and/or organizations, members of the group are able to access the advanced event search, but can't edit location, resource, and/or organization search criteria (whichever they don't have at minimum "Can View" access to).

The master list search criteria available in an advanced search is controlled by a combination of functional security and the master definition settings in the 25Live Configuration Utility. For example, if a user has "Can view, edit, deactivate, create and delete" access to Event Master Definitions, but only "Can view abridged list of active items managed in the Config Utility" access to Location Master Definitions, their options for selecting locations by category, for example, would be controlled by the settings in the Configuration Utility. For information, see the *25Live Configuration Utility* document.

Removing locks

Remove Locks task tab

Use the **Remove Locks** task tab to view locked 25Live items and remove locks.



Removing locks

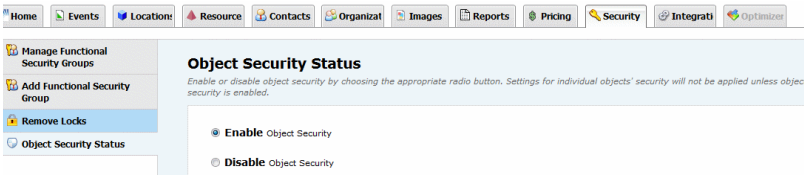
Highlight the locked items in the list and click Remove Selected Locks.

Enabling and disabling object security system-wide

Use the **Object Security Status** task tab to enable or disable object security system-wide.

Enabling or disabling object security

1 Select Enable or Disable.



2 Click Save Object Security Status.

Key Concept

Settings for individual object security are not applied until object security is enabled.

Appendix A - Functional Security Settings

Rights settings and definitions

This table summarizes how functional security access settings affect the ability of security groups to access and use functional areas of 25Live and the 25Live Administration Utility.

If this functional right...	Is set to...	Members of the security group...
Events: Event Wizard	Can't open 25Live Event Wizard	Can't open the 25Live Event Wizard.
	Can use 25Live Event Wizard to create and edit events	Can open and use the 25Live Event Wizard to create and edit events. **Note**: This security level is required regardless of whether you access the Event Wizard from 25Live or via a link from your published calendar environment as described in the 25Live Configuration Utility documentation.
Events: Event Drafts	Can't view	Can't view event drafts.
	Can view	Can view event drafts.
	Can view and edit	Can view and edit event drafts.
	Can view, edit, create, and copy	Can view, edit, create, and copy event drafts. **Note**: Events: Events must also be set to "Can view events" to be able to create event drafts.
Events: Events	Can't view	Can't view events.
	Can view	Can view events.
	Can view and edit	Can view events and edit events.
	Can view, edit, create, and copy	Can view, edit, create, and copy events.
Events: Event Delete	Can't delete	Can't delete events.
	Can delete	Can delete events.

If this functional right...	Is set to...	Members of the security group...
Events: Location Assignments	Can't view location assignments or preferences	Can't view the location assignments and preferences of events.
	Can view location assignments and preferences	Can view the location assignments and preferences of events.
	Can assign and/or request locations in Event Wizard	Can assign and/or request assignment of locations to events using the Event Wizard.
Events: Resource Assignments	Can't view resource assignments or preferences	Can't view the resource assignments and preferences of events.
	Can view resource assignments and preferences	Can view the resource assignments and preferences of events.
	Can assign and/or request resources in Event Wizard	Can assign and/or request assignment of resources to events using the Event Wizard.
Events: Share Location	Can't mark locations as shared when creating/ editing events	Can't indicate when creating or editing an event that the event's assigned location can be shared by other events.
	Can mark locations as shared when creating/editing events	Can indicate when creating or editing an event that the event's assigned location can be shared by other events.
Events: Description and Confirmation Notes	Can't view	Can't view event descriptions and confirmation notes.
	Can view	Can view event descriptions and confirmation notes.
	Can view and edit	Can view and edit event descriptions and confirmation notes. **Note**: To edit, the user must also have "Can View/Edit/ Delete" object security permission to the event.
Events: Internal Notes	Can't view	Can't view internal event notes.
	Can view	Can view internal event notes.
	Can view and edit	Can view and edit internal event notes. **Note**: To edit, the user must also have "Can View/Edit/ Delete" object security permission to the event.

If this functional right...	Is set to...	Members of the security group...
Events: Change State	View only	Can view the event state of events.
	Can view and change	Can view the event state of events, and change the event state of events that are not in a Denied or Cancelled state.
	Can view, change and uncancel	Can view the event state of events, and change the event state of events, including events in a Denied or Cancelled state.
Tasks, Reports, and Email: Task List	No access to task items	Can't view their 25Live Task List.
	Can view and act on task items	Can view and act on items in their 25Live Task List.
Tasks, Reports, and Email: Send Email	Can't send	Can't send email from within 25Live.
	Can send	Can send email from within 25Live.
Tasks, Reports, and Email: View Others' Tasks	Can't view	Can't view the tasks assigned to other 25Live users.
	Can view	Can view the tasks assigned to other 25Live users.
Tasks, Reports, and Email: To Do Tasks	Can't create To Dos	Can't create To Do task items.
	Can view, create, assign, complete and delete To Dos	Can create, assign, complete, and delete To Do task items.
Tasks, Reports, and Email: Report Access	No access to reports	Can't access reports.
	Can view and generate reports	Can view and generate reports.
	Can add, delete and modify custom reports	Can view and generate reports, and add, delete, and modify custom reports.
Searches and Master Definitions: Event	Can view abridged list of active items managed in the Config Utility	Can view the active event master definition items that have been selected in the 25Live Configuration Utility.
	Can view all active items	Can view all active event master definition items. **Note**: This is also the minimum required permission to access event Advanced Search functionality.
	Can view, edit, create, delete and deactivate all items	Can view all active and inactive items in event master definitions; edit, deactivate/activate, create, and delete items; and view, edit, and create event type notification policies.

If this functional right...	Is set to...	Members of the security group...
Searches and Master Definitions: Event Search	Cannot search for events or access event searches	Can't search for events or access event searches.
	Can view, run, create and save event searches	Can view, run, create, and save event searches.
Searches and Master Definitions: Location	Can view abridged list of active items managed in the Config Utility	Can view the active location master definition items that have been selected in the 25Live Configuration Utility.
	Can view all active items	Can view all active location master definition items. **Note**: This is also the minimum required permission to access location Advanced Search functionality.
	Can view, edit, create, delete and deactivate all items	Can view all active and inactive items in location master definitions, and edit, deactivate/activate, create, and delete items.
Searches and Master Definitions: Location Search	Cannot search for locations or access location searches	Can't search for locations or access location searches.
	Can view, run, create and save location searches	Can view, run, create, and save location searches.
Searches and Master Definitions: Resource	Can view abridged list of active items managed in the Config Utility	Can view the active resource master definition items that have been selected in the 25Live Configuration Utility.
	Can view all active items	Can view all active resource master definition items. **Note**: This is also the minimum required permission to access resource Advanced Search functionality.
	Can view, edit, create, delete and deactivate all items	Can view all active and inactive items in resource master definitions, and edit, deactivate/activate, create, and delete items.
Searches and Master Definitions: Resource Search	Cannot search for resources or access resource searches	Can't search for resources or access resource searches.
	Can view, run, create and save resource searches	Can view, run, create, and save resource searches.

If this functional right...	Is set to...	Members of the security group...
Searches and Master Definitions: Organization	Can view abridged list of active items managed in the Config Utility	Can view the active organization master definition items that have been selected in the 25Live Configuration Utility.
	Can view all active items	Can view all active organization master definition items. **Note**: This is also the minimum required permission to access organization Advanced Search functionality.
	Can view, edit, create, delete and deactivate all items	Can view all active and inactive items in organization master definitions, and edit, deactivate/activate, create, and delete items.
Searches and Master Definitions: Organization Search	Cannot search for organizations or access organization searches	Can't search for organizations or access organization searches.
	Can view, run, create and save organization searches	Can view, run, create, and save organization searches.
Searches and Master Definitions: Contact	Can view abridged list of items managed in the Config Utility	Can view the active items in the Contact Custom Attributes master definition that have been selected in the 25Live Configuration Utility.
	Can view all active items	Can view all active items in the Contact Custom Attributes master definition.
	Can view, edit, create, delete and deactivate all items	Can view all active and inactive items in the Contact Custom Attributes master definition, and edit, deactivate/activate, create, and delete items in the list.
Cabinets and Folders: Cabinets	Can't view	Can't view cabinets.
	Can view	Can view cabinets.
	Can view, edit and create	Can view, edit, and create cabinets.
Cabinets and Folders: Folders	Can't view	Can't view folders.
	Can view	Can view folders.
	Can view, edit and create	Can view, edit, and create folders.
Cabinets and Folders: Cabinet Delete	Can't delete	Can't delete cabinets.
	Can delete	Can delete cabinets.
Cabinets and Folders: Folder Delete	Can't delete	Can't delete folders.
	Can delete	Can delete folders.

If this functional right...	Is set to...	Members of the security group...
Cabinets and Folders: Event Type Hierarchy	Can't edit	Can't view or edit the Event Type Hierarchy.
	Can view, edit, deactivate, create and delete	Can view the Event Type Hierarchy, and create, edit, deactivate/activate, and delete cabinet types, folder types, and event types in it.
Locations: Location Access	Can't view, Locations tab doesn't appear in 25Live	Can't view locations.
	Can view, Locations tab appears in 25Live	Can view locations.
	Can view and edit, Locations tab appears in 25Live	Can view and edit locations.
	Can view, edit and create, Locations tab appears in 25Live	Can view, edit, create, and copy locations.
Locations: Location Delete	Can't delete	Can't delete locations.
	Can delete	Can delete locations.
Locations: Layouts and Images	Can't view	Can't view location layout information or images.
	Can view	Can view location layout information and images.
	Can view, edit and add images	Can view and edit location layout information, select photographs and diagrams of layouts, add new layout images to the selection list, and delete layout images.
Locations: Location Open/Close/ Blackout Hours	Can't view in the Admin Tool	Can't view location hours of availability (open/close times) and blackouts in the 25Live Administration Utility.
	Can view	Can view location hours of availability (open/close times) and blackouts in the 25Live Administration Utility.
	Can view, edit, and create	Can view, edit, and create location hours of availability (open/close times) and blackouts in the 25Live Administration Utility.

If this functional right...	Is set to...	Members of the security group...
Resources: Resource Access	Can't view, Resources tab doesn't appear in 25Live	Can't view resources.
	Can view, Resources tab appears in 25Live	Can view resources.
	Can view and edit, Resources tab appears in 25Live	Can view and edit resources.
	Can view, edit and create, Resources tab appears in 25Live	Can view, edit, create, and copy resources.
Resources: Resource Delete	Can't delete	Can't delete resources.
	Can delete	Can delete resources.
Organizations: Organization Access	Can't view, Organizations tab doesn't appear in 25Live	Can't view organizations.
	Can view, Organizations tab appears in 25Live	Can view organizations.
	Can view and edit, Organizations tab appears in 25Live	Can view and edit organizations.
	Can view, edit and create, Organizations tab appears in 25Live	Can view, edit, create, and copy organizations.
Organizations: Organization Delete	Can't delete	Can't delete organizations.
	Can delete	Can delete organizations.
Organizations: Organization Rating	Can't view	Can't view organization ratings.
	Can view	Can view organization ratings.
	Can view, edit, and create	Can view, edit, and create organization ratings.
Organizations: Comments	Can't view	Can't view organization comments.
	Can view	Can view organization comments.
	Can view, edit and create	Can view, edit, and create organization comments.

If this functional right...	Is set to...	Members of the security group...
Contacts: Contact Access	Can't view	Can't view contacts.
	Can view	Can view contacts.
	Can view and edit	Can view and edit contacts.
	Can view, edit and create	Can view, edit, and create contacts.
Contacts: Contact Delete	Can't delete	Can't delete contacts.
	Can delete	Can delete contacts.
Contacts: Security Groups	Can't view user lists	Can't view the security group list or user list.
	Can view user lists, change security group permissions, and assign members to groups	Can view the security group list and user list, change the permissions of security groups, and assign members to security groups.
	Can view user lists, change security group permissions, assign members to groups, make users active or inactive, create and delete security groups, and enable/disable object security	Can view the security group list and user list, change the permissions of security groups, assign members to security groups, make 25Live users active or inactive, create and delete security groups, and enable/disable object security system-wide.
Contacts: Change Password	Can't change their own password	Can't change their 25Live password.
	Can change their own password	Can change their 25Live password.
Object Security, Assignment Policy, and Notification Policy: Default Object Security	Can't view	Can't view default object security.
	Can view, edit, and change	Can view, edit, and change default object security. **Note**: In addition to this setting, the user must have permission to edit the object security of the object type (event draft, event, folder, cabinet, location, resource, organization, and/or report).
Object Security, Assignment Policy, and Notification Policy: Event/Folder/Cabinet Object Security	Can't view object security settings	Can't view the object security of events, folders, and cabinets.
	Can view and edit object security	Can view and edit the object security of events, folders, and cabinets.

If this functional right...	Is set to...	Members of the security group...
Object Security, Assignment Policy, and Notification Policy: Event Requirement Notification Policy	Can't view	Can't view event requirement notification policies.
	Can view, edit, and create	Can view, edit, and create event requirement notification policies.
Object Security, Assignment Policy, and Notification Policy: Location Object Security	Can't view object security settings	Can't view the object security of locations.
	Can view and edit object security	Can view and edit the object security of locations.
Object Security, Assignment Policy, and Notification Policy: Location Notification Policy	Can't view	Can't view location notification policies.
	Can view, edit, and create	Can view, edit, and create location notification policies.
Object Security, Assignment Policy, and Notification Policy: Location Assignment Policy	Can't view	Can't view location assignment policies.
	Can view, edit, and create	Can view, edit, and create location assignment policies.
Object Security, Assignment Policy, and Notification Policy: Resource Object Security	Can't view object security settings	Can't view the object security of resources.
	Can view and edit object security	Can view and edit the object security of resources.
Object Security, Assignment Policy, and Notification Policy: Resource Notification Policy	Can't view	Can't view resource notification policies.
	Can view, edit, and create	Can view, edit, and create resource notification policies.
Object Security, Assignment Policy, and Notification Policy: Resource Assignment Policy	Can't view	Can't view resource assignment policies.
	Can view, edit, and create	Can view, edit, and create resource assignment policies.
Object Security, Assignment Policy, and Notification Policy: Organization Security	Can't view object security settings	Can't view the object security of organizations.
	Can view and edit object security	Can view and edit the object security of organizations.

If this functional right...	Is set to...	Members of the security group...
Object Security, Assignment Policy, and Notification Policy: Organization Notification Policy	Can't view	Can't view organization notification policies.
	Can view, edit, and create	Can view, edit, and create organization notification policies.
Object Security, Assignment Policy, and Notification Policy: Report Object Security	Can't view object security settings	Can't view the object security of reports.
	Can view and edit object security	Can view and edit the object security of reports.
Locks and Overrides: Override Event/Folder/ Cabinet Security	Can't override	Can't override the functional and object security of events, folder, and cabinets.
	Can override	Can override the functional and object security of events, folders, and cabinets.
Locks and Overrides: Override Location Assignment Policy	Can't override	Can't override a location's assignment policy restrictions when assigning the location to an event.
	Can override	Can override a location's assignment policy restrictions when assigning the location to an event.
Locks and Overrides: Override Location Blackouts	Can't override	Can't override blackouts when assigning a location to an event.
	Can override	Can override blackouts when assigning a location to an event.
Locks and Overrides: Override Blocked By Relationships	Can't override	Can't override a Blocked By relationship when assigning a location to an event.
	Can override	Can override a Blocked By relationship when assigning a location to an event.
Locks and Overrides: Override Location Open Hours	Can't override	Can't override the hours of availability (open hours) of a location when assigning it to an event.
	Can override	Can override the hours of availability (open hours) of a location when assigning it to an event.
Locks and Overrides: Override Location Permissions	Can't override	Can't override the functional and object security of locations.
	Can override	Can override the functional and object security of locations.
Locks and Overrides: Override Resource Assignment Policy	Can't override	Can't override a resource's assignment policy restrictions when assigning the resource to an event.
	Can override	Can override a resource's assignment policy restrictions when assigning the resource to an event.

If this functional right...	Is set to...	Members of the security group...
Locks and Overrides: Override Resource Permissions	Can't override	Can't override the functional and object security of resources.
	Can override	Can override the functional and object security of resources..
Locks and Overrides: Override Organization Permissions	Can't override contact and organization security	Can't override the functional and object security of organizations..
	Can override contact and organization security	Can override the functional and object security of organizations.
Locks and Overrides: Override Permissions	Can't override report security	Can't override the functional and object security of reports.
	Can override report security	Can override the functional and object security of reports.
Locks and Overrides: Locks and Pending Reservations	Can't view locked items and pending reservations	Can't view locked items and pending location and resource reservations.
	Can view locked items and pending reservations	Can view locked items and pending location and resource reservations.
	Can view and remove their own locked items and pending reservations	Can view locked items, remove the lock on their own locked items, and remove their own pending location and resource reservations.
	Can view and remove anyone's locked items and pending reservations	Can view locked items, remove the lock on any 25Live user's locked items, and remove any 25Live user's pending location and resource reservations.
Integration: Schedule25 Optimizer	Can't view Schedule25	Can't view the Schedule25 Optimizer in the 25Live Administration Utility. Optimizer tab isn't available.
	Can view and prepare Schedule25 runs and view output results and reports	Can view and prepare Schedule25 Optimizer runs and view and act on output results.

If this functional right...	Is set to...	Members of the security group...
Integration: Schedule25 Optimizer Defaults	Can't view	Can't view the default Schedule25 Optimizer run settings.
	Can view	Can view the default Schedule25 Optimizer run settings.
	Can view, edit, and change	Can view, edit, and change the Schedule25 Optimizer run settings.
Integration: vCalendar Export	Can't view or run	Can't run the vCalendar export.
	Can use all features	Can run the vCalendar export.
Integration: vCalendar Import	Can't view or run	Can't run the vCalendar import.
	Can use all features	Can run the vCalendar import.
Integration: X25 Export	Can't view or run	Can't export Series25 information for analysis in X25.
	Can use all features	Can export Series25 information for analysis in X25.
Integration: 25Live Publisher	Can't view or run	Can't use the 25Live Publisher to publish events.
	Can use all features	Can use the 25Live Publisher to publish events.
Integration: E-Commerce	Can't view	Can't view event e-commerce transactions.
	Can view	Can view event e-commerce transactions.
	Can view, edit, and create	Can view, edit, and create event e-commerce transactions.
Pricing and Invoicing: Rate Groups	Can't view	Can't view the Rate Groups master definition.
	Can view, edit, deactivate, create and delete	Can view the Rate Groups master definition, and edit, deactivate/activate, create, and delete items in it.
Pricing and Invoicing: Event Details Pricing	Can't view	Can't view pricing information in event details.
	Can view, edit, and create	Can view, edit, and create pricing information for events.
Pricing and Invoicing: Organization Accounting Code	Can't view	Can't view organization accounting codes.
	Can view	Can view organization accounting codes.
	Can view, edit, and create	Can view, edit, and create organization accounting codes.
Pricing and Invoicing: Pricing Administration	Can't view	Can't view pricing administration functions in the 25Live Administration Utility. Pricing tab isn't available.
	Can view, edit, and change	Can view and use pricing administration functions.

Appendix B - Event Details Information Access

The role a user plays for an event (scheduler, requestor, or task recipient) and, for users not in one of the roles, the object security of their security group for the event determine the event information users can view and possibly act on, as shown in the table below. An X in a table cell indicates that the user by virtue of their role in the event or membership in a security group with the designated object security for the event can see the related event information in event details.

Event Information	**Scheduler**	**Requestor**	**Task Recipient**	**Object Security: Edit, Delete, Copy**	**Object Security: View Only**
Attendee List	X	X	X	X	
Audit Trail	X			X	
Cabinet the event is in	X			X	
Categories	X	X	X	X	X
Confirmation Notice Text	X	X	X	X	
Contact Roles (other than Requestor and Scheduler)	X	X	X	X	
Custom Attributes (full list)	X	X	X	X	
Custom Attributes (subset)					X
Description	X	X	X	X	X
eCommerce Form Information	X	X		X	
Headcount	X	X	X	X	X
Location Assignment(s)	X	X	X	X	X

Event Information	Scheduler	Requestor	Task Recipient	Object Security: Edit, Delete, Copy	Object Security: View Only
Location Instructions	X	X	X	X	
Location Layouts	X	X	X	X	
Name	X	X	X	X	X
Notes	X			X	
Occurrences	X	X	X	X	X
Organization (primary)	X	X	X	X	X
Organization(s) (secondary)	X	X	X	X	X
Reference Number	X	X	X	X	X
Related Events	X	X	X	X	X
Requestor	X	X	X	X	X
Reservation Comments	X	X	X	X	X
Resource Assignment(s)	X	X	X	X	
Resource Instructions	X	X	X	X	
Scheduler	X	X	X	X	
Setup/Takedown Time	X	X	X	X	X
State	X	X	X	X	X
Task Comments	X		X	X	
Task List	X	X	X	X	
Task Total	X	X	X	X	
Title	X	X	X	X	X

Event Information	Scheduler	Requestor	Task Recipient	Object Security: Edit, Delete, Copy	Object Security: View Only
Type	X	X	X	X	X
vCalendar Publish	X	X	X	X	X