

# INQUISIQ<sup>r3</sup>

Unleash the Power of e-Learning

## Master Administrator & Overview Manual

Version 1.4

November 2011 Edition

© 2002-2011 ICS Learning Group Inc.

# Table of Contents

---

OVERVIEW AND ORGANIZATION .....	3
SUMMARY OF MANUALS AND SUPPORT DOCUMENTATION .....	4
MASTER ADMINISTRATOR LOGIN .....	6
SETTING PERMISSIONS .....	6
GROUP PERMISSIONS .....	9
DISCONNECTING USER LOGINS .....	10
LOGGING IN AS ANOTHER USER .....	10

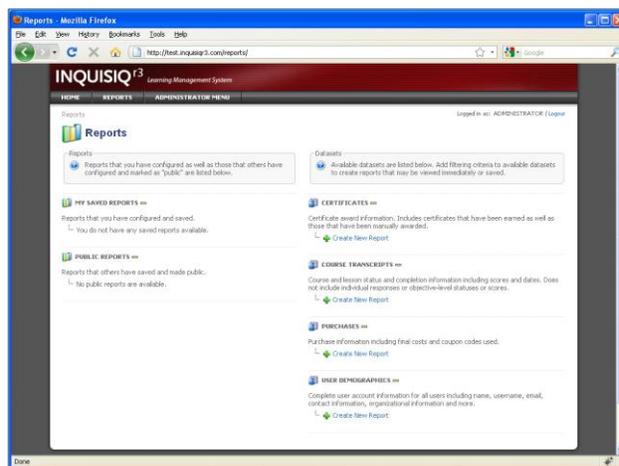
## Overview and Organization

The Inquisiq R3™ Learning Management System provides all the functionality that you expect while remaining easy to use and affordable. With years of experience and feedback from our clients, we have honed Inquisiq R3™ to a lean application with the user experience as a top priority. It has what you need to get the job done, without the rarely-used features that bloat most LMS systems making them needlessly complex and expensive. Visit our [Inquisiq R3™](http://next.inquisiq3.com) product site for more details and features.

Inquisiq R3™ has three primary areas:

1. **Learner Area**
2. **Reporting Area**
3. **Administrator Menu**

The **Learner Area** includes the screens that a typical learner would see if they were not given any administrator or reporting permissions. It will include the Home screen, Course Catalog, and My Account sections. For information regarding the Learner Area, such as basics of logging-in, browsing the site, and launching courseware, please refer to the **Inquisiq R3™ Learner's Manual**.



The **Reporting Area**, which requires special permissions to access, is where all reports are run, viewed, exported, and saved. For information on Reporting, please refer to the **Inquisiq R3™ Reporting Manual**.

The **Administrator Menu** includes all of the functionality surrounding the setup and configuration of your LMS. It is divided into four categories of functionality, each one requiring specific permissions to access for everyone except the Master Administrator. The Administrator menu categories are:

- **System settings** – includes all system wide settings ranging from basic account properties, E-commerce configuration, email notifications, user account data setup, and much more. For information on the system settings, please refer to the **Inquisiq R3™ Admin - Systems & Interface Manual**.
- **Interface Configuration** – includes configuration of the site branding properties such as the banner or masthead, footer information, and home screen. For information on the interface settings please refer to the **Inquisiq R3™ Admin - Systems & Interface Configuration Manual**.



- **User & Group Management** – provides access to all user and group management functions including creating, editing, and deleting user accounts and groups, course enrollments, and granting access to private catalogs. Importing of historical course data for users is also included in this section. For information on the functionality in the User and Group Management section, please refer to the **Inquisiq R3™ Admin - User & Groups Manual**.



- **Content setup and configuration** – includes loading SCORM content packages, creating and editing courses, lessons, sessions, course catalogs, coupon codes, and certificates. For more information on the content functions, please refer to the **Inquisiq R3™ Admin - Content Manual**.



## Summary of Manuals and Support Documentation

There are seven manuals that have been created for Inquisiq R3™ Users and Administrators. Each manual is listed below with a brief description of its purpose.

1. **R3 Learners Manual:** Provides an overview for a normal user/learner on how to login, browse the Course Catalog and navigate their My Account screen.
2. **R3 Master Administrator & Overview Manual:** Provides a broad overview of Inquisiq R3™ organization and includes details of the Master Administrator login and setting permissions.
3. **R3 Admin - System & Interface Configuration Manual:** Provides details of all functionality in the System and Interface Categories of the Administrator Menu.
4. **R3 Admin - Users & Groups Manual:** Provides details of all functionality in the User & Group Categories of the Administrator Menu. Includes all aspects of creating and modifying user accounts and groups including course enrollments.
5. **R3 Admin - Content Manual:** Provides details of all functionality in the Content Categories of the Administrator Menu. Includes uploading SCORM packages and all configuration options related to Courses, Lessons, Sessions, Catalogs, Certificates, and Coupon Codes.
6. **R3 Report Manual:** Provides details on how to create, run, and save reports.
7. **R3 API Manual:** Provides a reference manual of the functionality of the Inquisiq R3™ Application Programming Interface (API).
8. **R3 Control Panel Manual:** Provides an introduction and instructions on the Inquisiq R3™ Control Panel, which is only available for Installed solutions, and which allows the Master Administrator to create new 'instances' of the LMS, as well as access to a variety of configuration and reporting options.

9. **R3 Course History Import Manual:** Provides details for importing historical course data into user accounts via the Import Activity Data feature.

## Master Administrator Login

As part of your Inquisiq R3™ setup, a default or “Master Administrator” account is automatically created. This account has full administrator privileges to the system; however it is unique in the following important ways:

- It is not included in the list of user accounts
- It cannot be deleted
- It does not have access to the ‘Learner Area’
- It is the only user in the system that **is able to set permissions for other Users.**

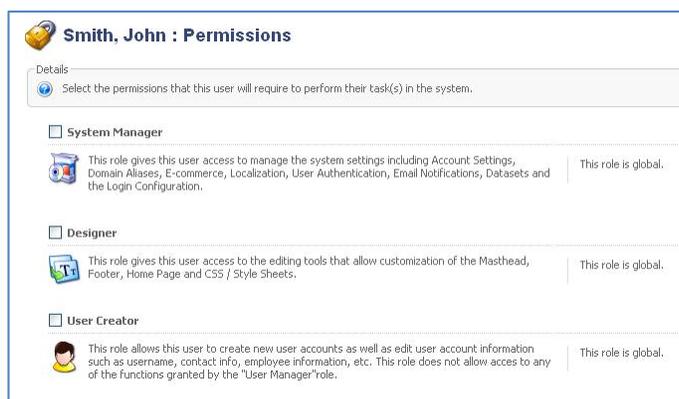
When you first access your Inquisiq R3™ account, you will need to login with this default Master Administrator login. Once you login under that account, you will see a simple ‘You Are Logged-In’ message on the Inquisiq R3™ Home Page. From here, click the **Administrator Menu** item at the top of the R3 interface.

Note that the username for the Master Administrator account is always ‘Administrator’ or ‘Admin’, (either will work). The password is what was entered during the creation of the LMS instance. An ‘LMS instance’ is a fully-functional R3 LMS site. Since the Inquisiq R3™ application can create/host multiple LMS sites, each one is generally referred to as an ‘instance’ and each one will have a separate Master Administrator account.

## Setting Permissions

One of the most important capabilities of the Master Administrator account is the unique ability to set permissions for other users. By default, when a new user account is created in Inquisiq R3™ (by any means) it will not have any special permissions and will be a normal Learner (and have access to only the Learner area). However, every user account can be assigned special permissions if you want to give them access to certain administrator or reporting functionality. For example, you may decide to give a user permission to change the interface settings and load content, but not create or delete user accounts. Alternatively, you could give someone the ability to run reports but not have any other administrator capabilities.

To change a user’s permissions, the Master Administrator would first login and go to the **Administrator Menu** screen. Then, click the **Users** icon under the **Users & Groups** category. This will then present you with a list of users in the system. If necessary, you can perform a search for the user account you are interested in changing. Once you have located the user in the list, click the **View** icon to access that user’s account information.



Click the Permissions icon in the tools section to access the permission panel for this user. Click the check box for any permission you would like to grant to the user. Make sure to click the Save Changes at the bottom of the screen to retain your changes.

The permissions that can be granted are listed below with a brief description of each. Note that some permissions are global (the permission allows access to all users in the system) and some permissions can be restricted based on group. For example, you can give someone the ability to run reports, but limit the users that will show up in their reports to specific groups. Also note that some permission choices may be disabled due to being inherited by a group membership (see Group Permissions below)

### Permissions:

- **System Manager** (global) -This role gives this user access to manage the system settings including Account Settings, Domain Aliases, E-commerce, Localization, User Authentication, Email Notifications, Datasets and Login Configuration.
- **Designer** (global) - This role gives this user access to the editing tools that allow customization of the Masthead, Footer, Home Page and CSS / Style Sheets.
- **User Creator** (global) - This role allows this user to create new user accounts as well as edit user account information such as username, contact info, employee information, etc. This role does not allow access to any of the functions granted by the "User Manager" role.
- **User Deleter** (can be restricted to specific groups) - This role allows this user to delete accounts. No other capabilities are granted.
- **User Editor** (can be restricted to specific groups) - This role allows the user to edit user account data such as username, contact info, employee information, etc. This role does not grant any other capabilities.
- **User Manager** (can be restricted to specific groups) - This role allows the user to perform user management functions such as assigning and revoking user and group enrollments, awarding and revoking certificates, and importing external training histories.
- **User Impersonator** - This role allows the user to impersonate (login as) other users as well as disconnect user sessions.

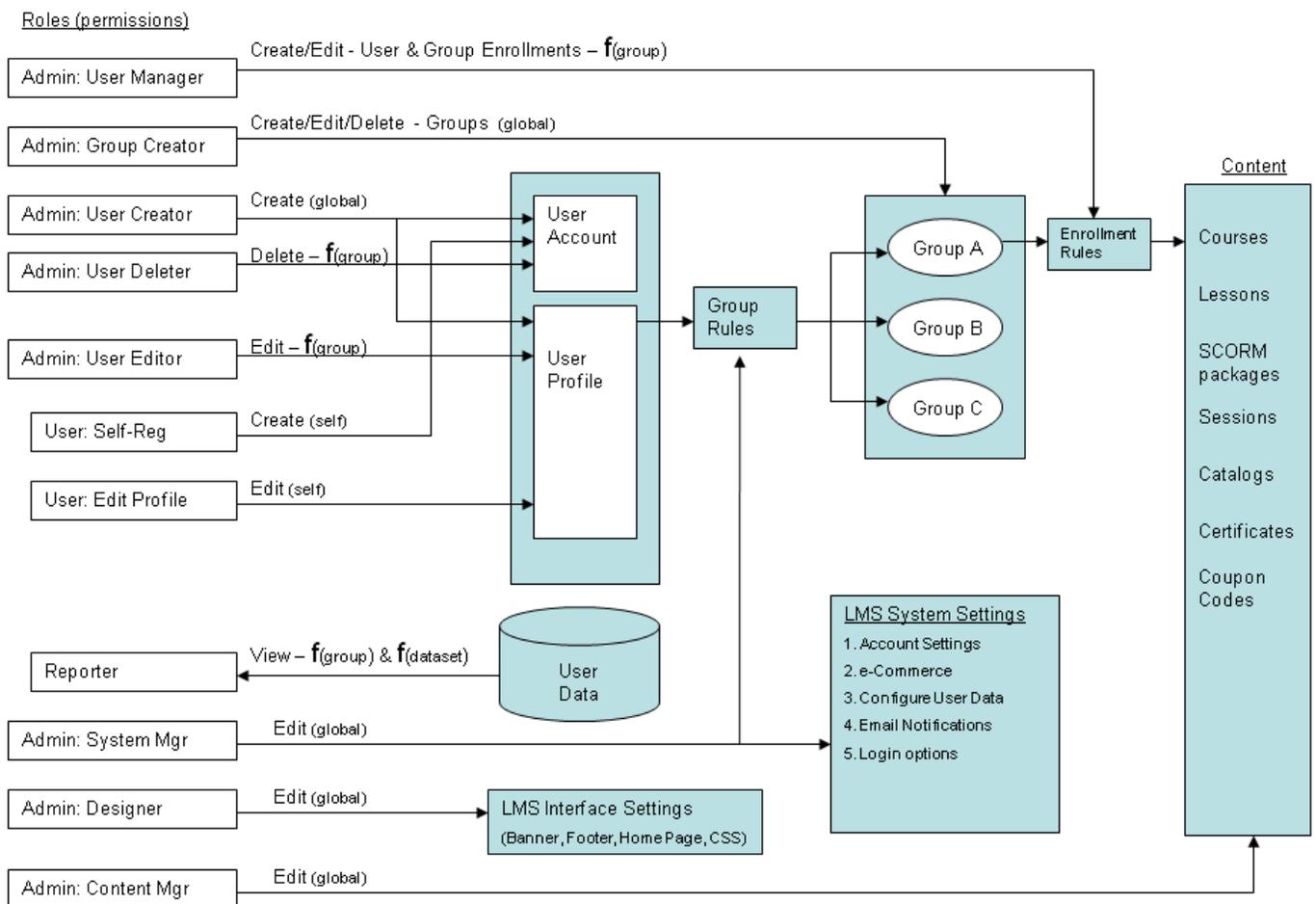
The screenshot shows a 'Group Creator' permission panel with three main sections:

- Group Creator:** Includes a description of the role and a checkbox for 'This role is global.' (checked).
- Content Manager:** Includes a description of the role and a checkbox for 'This role is global.' (checked).
- Reporter:** Includes a description of the role, a section for 'This user may access:' with radio buttons for 'any dataset.' (selected) and 'only the datasets selected below.' (unchecked), and a list of checkboxes for 'Certificates', 'Course Transcripts', 'Purchases', and 'User Demographics'. Below this is a 'Select: All | None' dropdown. To the right, there is a section for 'Within the selected datasets, this user may see:' with radio buttons for 'all users.' (selected), 'no users.' (unchecked), and 'only users within the groups selected below.' (unchecked). Below this is another 'Select: All | None' dropdown.

At the bottom of the panel are 'Save Changes' and 'Cancel' buttons.

- **Group Creator** (global) - This role allows the user to create, delete and manage the memberships of groups. This role does not grant any capability to create, edit, delete or manage users in any way other than joining and removing them from groups.
- **Content Manager** (global) - This role allows the user to manage content within the system. This user will have access to upload and delete SCORM packages, create and manage courses, lessons and sessions as well as certificates and coupon codes. This role grants no capability to assign, award or revoke any of these elements to users, nor does it grant any user editing or management capabilities.
- **Reporter** (can be restricted to specific groups and datasets) - This role allows the user to build, view, save and export reports.

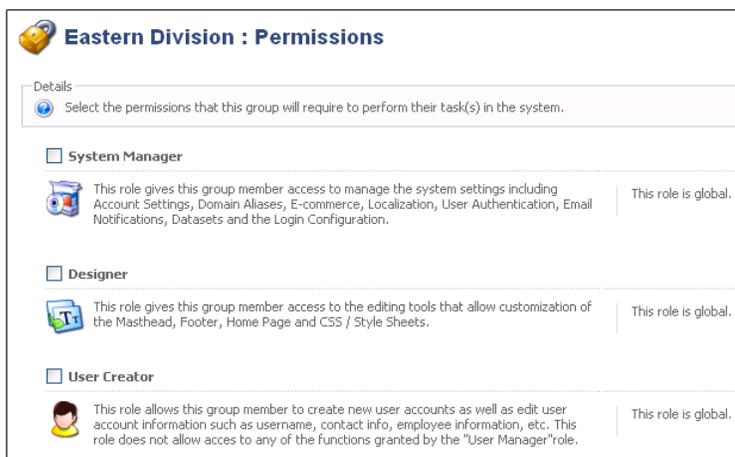
Below is an illustration that shows the functional areas of Inquisiq R3™ and the permissions control them.



## Group Permissions

In addition to user-level permissions, Inquisiq R3™ allows you to set permissions for an entire group of users in the same manner as you would set it for the individual user: to change a group's permissions, the Master Administrator would first login and go to the **Administrator Menu** screen. Then, click the Groups icon under the Users & Groups category. This will then present you with a list of groups in the system. If necessary, you can perform a search for the group you are interested in changing. Once you have located the group in the list, click the Modify icon to access that group's member list and group-level tools. Click the

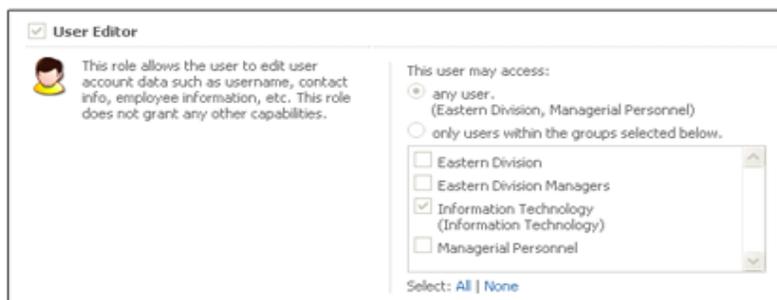
Permissions icon in the tools section to access the permission panel for this group. Click the check box for any permission you would like to grant to the group. Make sure to click the Save Changes at the bottom of the screen to retain your changes.



When a group is granted a permission, this group-level permission will also be viewable in the user-level permission page of every member of that group. In addition to the permission being checked there, it will be disabled (grayed out) and will indicate from which group membership the permission is inherited from.

The permission is disabled because of the way group and user-level permissions interact with each other. One cannot specify a user-level permission that is “less than” the group level for that same permission, only “greater than.” In

other words, user-level permissions are only additive – they can add additional permissions to the existing permissions inherited by group membership, but cannot take away any of the group inherited rights.



## Disconnecting User Logins

The Master Administrator and users with the User Manager or User Impersonator permission also have the ability to disconnect or terminate other user's logins. One time this function is particularly useful is if a user did not properly logout of the system and the login session is still active thereby potentially prohibiting them to log back in (depending on the how you have configured some of the system settings). The user session will time out but may take up to 20 minutes or longer depending on how the server is configured. If desired, the Master Administrator can login, go to the Administrator Menu > Users & Groups > **Users** and find the user on the list. You will notice that every user that has an active login session will have their Disconnect button highlighted (if it is grayed out then that user is not currently logged in). Click the Disconnect button to disconnect that user. As soon as you do this the user's login session is terminated and they will be automatically logged out of the system.

## Logging in as another User

The Master Administrator and users with the User Manager or User Impersonator permission have the ability to log in as another user. This may be helpful in some cases where the Master Administrator needs to see exactly what that user sees. To do to this, the Master Administrator would login and go to the Administrator Menu > Users & Groups > **Users**. This will present the list of users. Once you find the user that you want to login as, click the key login icon for that user.

<input type="checkbox"/>	Name ▲	Username	Email	Disconnect	Login	View
<input type="checkbox"/>	Smith, John	jsmith	jsmith@inquisiq.com			