Contents

Chapter 1 – Welcome to Academus ................................................................. 5
  Overview ............................................................................................................ 5
  What is the Academus Portal? ........................................................................... 5
  What is Academus Collaborative Groupware? .................................................... 5
  What is uPortal? .................................................................................................. 5
  Changes to this Guide ......................................................................................... 6

Chapter 2 – Preferences in the Portal ............................................................ 7
  Overview ............................................................................................................ 7
  User Preferences ............................................................................................... 7
  Setting up your personal tabs – Creating a new tab .......................................... 8
  Setting up your personal tabs – Modifying your created tab .............................. 9
  Aggregated Layouts – Creating Fragments ....................................................... 10

Chapter 3 – Templates and Layouts ............................................................... 15
  Overview ............................................................................................................ 15
  Layouts ............................................................................................................... 15
  Templates ........................................................................................................... 16
  Setting Up and Configuring Template Users ..................................................... 16
  Academus default template users ..................................................................... 17
  Managing Template Users ................................................................................ 18

Chapter 4 – Groups in the Portal ................................................................. 19
  Overview ............................................................................................................ 19
  Groups Manager Channel .................................................................................. 20
  Permissions Manager Channel .......................................................................... 22
  Using LDAP to setup your initial group membership ......................................... 23
  Group Selection Restrictor ................................................................................ 23

Chapter 5 – Channel Administration ......................................................... 28
  Overview ............................................................................................................ 28
  Channel Publishing Basics ............................................................................... 29
  Image Channel .................................................................................................. 29
  Inline Frame Channel ........................................................................................ 31
  RSS Channel ...................................................................................................... 32

Chapter 6 – Configuration Options .............................................................. 34
  Overview ............................................................................................................ 34
  Academus Theme and Skin Presentation .......................................................... 34
  Online Help Link ............................................................................................... 34
  Blogging Portlets .............................................................................................. 35
  Briefcase Portlet ............................................................................................... 35
  SSO Gateway Portlet ......................................................................................... 36
  Change Password Channel ............................................................................... 36
  Academus Web Content .................................................................................... 37
  PAGS .................................................................................................................. 37
  Authentication/Person Dirs .............................................................................. 37

Chapter 7 - Administration Channels ......................................................... 38
  User Administration Channel ......................................................................... 38
  Discussion Forums ............................................................................................ 39
  Group Chat Administration .............................................................................. 40
  Survey Author ................................................................................................... 41
  Campus Announcements ................................................................................... 42
  Campus News .................................................................................................... 43
<table>
<thead>
<tr>
<th>Portlet</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifieds</td>
<td>44</td>
</tr>
<tr>
<td>Blogging Portlet</td>
<td>45</td>
</tr>
<tr>
<td>Briefcase Portlet</td>
<td>47</td>
</tr>
<tr>
<td>Notification Portlet</td>
<td>49</td>
</tr>
</tbody>
</table>
Chapter 1 – Welcome to Academus

Overview
This Portal Manager Guide will walk you through many of the administrative features of the Academus application in order to get your Portal site up and running. It will focus on those tasks generally performed at the Portal Manager level such as group setup, template creation, portal personalization, and numerous tasks within the various administrative channels.

What is the Academus Portal?
Academus Portal delivers the framework, software, and services needed to establish an online campus and provide a single, user-friendly web-based interface. Academus is an easily integrated enterprise-portal solution built on uPortal. It includes ready-to-use portal channels, branding, installation, and more. Academus Portal simplifies the process of integrating applications and data sources and streamlines administrative tasks such as portal user membership. The Portal includes an integrated database to store portal data and features built-in, ready-to-use premium channels to help your institution create new user groups quickly. Academus Portal enables you to build a secure, scalable and manageable campus portal – a portal that gives users convenient, single-point access to multiple applications, rich content, and a vibrant online community.

What is Academus Collaborative Groupware?
Academus integrates the campus portal with robust collaboration functionality, extending the portal paradigm of personalization to the group collaboration experience. Academus Collaborative Groupware gives institutions the tools to create dynamic group environments or to power, deliver, and track online learning experiences when utilized as a course management solution. Academus is the first commercial course management system built as a native uPortal application. The complete groupware solution integrates calendar, roster, gradebook, a file sharing system, and more.

What is uPortal?
uPortal is the underlying architecture on which UNICON has built the Academus application. uPortal, from the Java Architectures Special Interest Group (JA-SIG), is an open-source enterprise portal collaboratively developed by higher-education, for higher-education. Currently, over 25 institutions and several commercial entities contribute to the uPortal project, and over 100 institutions have implemented uPortal on campus.
Utilizing Java, XML, JSP, and J2EE technologies, the uPortal framework enables easy standards-based integration with authentication and security applications, single sign-on, secure access and end-user customization. Academus enables institutions to leverage uPortal's open-source framework to maintain administrative control and flexibility with economy of effort and expense.

For more information on the uPortal application visit the following URL address: http://mis105.mis.udel.edu/ja-sig/uportal/index.html.

Changes to this Guide
Existing Academus Portal Managers familiar with version 1.5 of the Academus Portal and Academus Portal Manager Quick Start Guide will notice the following changes and additions to this document:

Chapter 2 – Preferences in the Portal
- Revised Workflows and User Interface when in Preferences or Customization Mode

Chapter 4 – Groups in the Portal
- Removed configuration detail on the LDAP Change Password Channel. This information is now available in LDAP Change Password Configuration Guide.

Chapter 5 – Channel Administration
- Increase in the number of channel types supported by the portal
- Correction to the information provided on Channel Title and Channel Name. Channel titles appear when a user is subscribing to a channel. Channel Names appear in the channel header within the portal layout.

Chapter 6 – Configuration Options
- New section which outlines many new portal tools and features, as well as a number of general configuration options to better customize the portal and its capabilities to your campus community. Topics covered include:
  - Theme and Skins
  - Online Help Links
  - Blogging Portlets
  - Briefcase Portlet
  - SSO Gateway Portlet
  - Change LDAP Password Channel
  - Academus Web Content Management
  - PAGS
  - Authentication/PersonDirs

Chapter 7 – Administration Channels
- New information on use of the Portlet Permissions Manager to set and manage privileges for the Blogging Portlet, the Briefcase Portlet and the Notification Portlet.
Chapter 2 – Preferences in the Portal

Overview
One of the major benefits of utilizing the Academus Portal is the amount of customization and personal flexibility the system gives its end users. Based on the needs of your institution, you may have several different “skins” (visual styles) that end users can pick from. Additionally, you may have a variety of channels that users can add to their layout based on some form of interest. Finally, your end-users may want to rearrange, add, or delete tabs, columns, and channels that have been “preset” for them. All of these options are possible through the “Customize” link within your Portal.

Note: Based on your deployment of the Academus application, your institution may have chosen to turn this level of flexibility off for its end-users. Additionally, the link to these changes may be called something other than “Customize”. Please see your Portal Administrator or UNICON deployment manager for specific details.

User Preferences
There are several options on the Customize your Portal page.

- **Change Content & Layout** - This section allows any user to rearrange tabs, channels, columns, etc. to meet their own conveniences.
- **Pick Colors** – This allows each individual user to select the skin that they prefer.
- **Manage Fragments** – Occasionally it may become necessary to “force” users to see specific tabs and channels, regardless of how they’ve personalized their own view. This section covers pushed and pulled fragments.
- **Change Languages** – uPortal option to support multiple languages. This feature is not available for most portal installations.

Customize Your Portal

```
Change Content & Layout | Pick Colors | Manage Fragments | Change Languages
```

Add a new tab

```
Message Center | Collaboration | Personal | Briefcase | Groupware
```

Setting up your personal tabs – Creating a new tab

An individual’s personal tabs are places where each user can set up and group channels for their own personal use. After initial login, the user is responsible for the layout and the content of their personal tabs. These tabs will not be moderated or administered by anyone else.

Before you can begin grouping and placing channels in a tab, you need to create the tab. To begin, you must start by going to the Customize section of UNICON Academus. Follow these instructions:

To create a new tab in your portal layout, follow these steps:

- If the Customize your Portal Mode is not on, click the Customize link at the top of the page. This will take you into the Customize your Portal view.

- Click the Add a New Tab link.

- To name the tab click the Rename Tab link. Enter the tab name then click the Rename button.

- These buttons move the current tab:
  - moves tab left
  - moves tab right

- To add a new column within this tab, click the Add a New Column link.

- To begin adding content (channels or portlets) to this tab, click the Add Content button (as shown in diagram).

- Click Save Settings to save your new tab and all changes and exit Customize mode.
Setting up your personal tabs – Modifying your created tab

After creating a new tab, the system will give you options on ways to modify it.

To add content to any tab, click the Add Content button as explained in the previous steps. Then follow these steps:

- Browse or search for the channel or portlet you would like to add then click on its name. This will show you more information about the channel or portlet.

- If you are satisfied with this channel or portlet, click the Subscribe to this channel link.

- The channel will be added to your tab in the top position of the first column. Use the arrow icons displayed within the representation of the channel to reposition the channel within the tab layout.

- Continue adding additional channels by repeating the process.

- When all desired channels have been added, click Save Settings to save all changes and exit Customize mode.
Aggregated Layouts – Creating Fragments

Aggregated layouts allow portal administrators to create tabs that cannot be moved or removed by users in the portal community. These tabs, known as fragments, contain channels, which also cannot be moved or removed by the end user. This allows portal administrators to “force” certain channels upon all users or a specific group of users.

There are two types of fragments:

- **Pushed Fragments** – This fragment is “pushed” out to specified groups or users. The end users do not have the ability to unsubscribe from this fragment, nor can they remove it from view.

- **Pulled Fragments** – This fragment is created by the admin, who then decides which groups or users are allowed to view it. End users have the choice whether to subscribe to this fragment or not; however, they will not be able to modify any of the channels contained within this fragment.

Creating Pushed Fragments

To create a pushed fragment, you will need to first decide the contents of the fragment as well as the users who will be forced to see this fragment in their tab layouts. Then, follow these steps:

- Click the **Customize** link at the top of the page. This will take you into the Customize your Portal view.

- Click the **Manage Fragments** link at the top of the page. This will take you to the **Fragment Manager**. Not all users will have access to the Fragments link.

- Click the **Create new fragment** link.
Select **Pushed** fragment.

Enter a **Fragment display name.** This is the name that will be displayed on the tab.

Enter a **Fragment functional name.** This is used behind the scenes. It’s best to keep it the same as the display name.

Enter a **Fragment description.** A best practice idea for this box is to be as descriptive as possible about the reasoning behind the creation of this pushed tab. That way, others will know the purpose for its creation.

Leave the Add a content container to the new fragment root box checked. This creates the first column on the tab for you. If you remove the check, you will have to manually add a column later.

Click **Submit properties.**

Now you must decide the contents of your pushed fragment. To do so, click the **Edit Content** link. Then follow the usual steps for adding columns and channels to a tab.

Select desired column layout.

Click the **Save** link in the instruction text of step 2 – “If satisfied with changed, click Save.”

Click the **Fragment Manager** link in the instruction text of Step 3 – “To return to the fragment managed, click Fragment Manager.”
Finally, you must publish the fragment to the users who you’ve decided should always see it. Using the steps above, get back to your Fragments Manager channel.

Click the Publish fragment link for the appropriate fragment.

Navigate through the group hierarchy or search for groups. Check the boxes for those who should receive this pushed fragment. Assigning a template user such as “Students” will ensure all students see the tab when logging into the portal.

Click the **Done with Selection** button when all desired groups and users have been selected.

Click the **Save Settings** links to save your new fragment, all channels associated to the fragment and the publishing parameters. If you do not, click **Save Settings** all new fragment information will be lost.

The fragment will automatically show up for all users who have been selected.
Creating Pulled Fragments

To create a pulled fragment, you will need to first decide the contents of the fragment as well as the users who will be allowed to subscribe to this fragment. Then, follow these steps:

- Click the Preferences link at the top of the page. This will take you into User Preferences Mode.

- Click the Fragments link at the top of the page. This will take you to the Fragment Manager.

- Click the Create new fragment link.

- Select Pulled fragment.

- Enter a Fragment display name. This is the name that will be displayed on the tab.

- Enter a Fragment functional name. This is used behind the scenes. It’s best to keep it the same as the display name.

- Enter a Fragment description. A best practice idea for this box is to be as descriptive as possible about the reasoning behind the creation of this pushed tab. That way, others will know the purpose for its creation.

- Leave the Add a content container to the new fragment root box checked. This creates the first column on the tab for you. If you remove the check, you will have to manually add a column later.

- Click Submit properties.
Now you must decide the contents of your pulled fragment. To do so, click the **Edit Content** link. Then follow the usual steps for adding columns and channels to a tab.

Select desired column layout.

Click the **Save** link in the instruction text of step 2 – “If satisfied with changed, click Save.”

Click the **Fragment Manager** link in the instruction text of Step 3 – “To return to the fragment managed, click Fragment Manager.”

Finally, you must publish the fragment to the users who will be able to subscribe to it. Using the steps above, get back to your Fragments Manager channel.

Click the **Publish fragment** link for the appropriate fragment.

Navigate through the group hierarchy or search for groups. Check the boxes for those who should be able to subscribe to this pulled fragment.

Click the **Done with Selection** button when all desired groups and users have been selected.

Click the **Save Settings** links to save your new fragment, all channels associated to the fragment and the publishing parameters. If you do not, click **Save Settings** all new fragment information will be lost.

In order to see this fragment, users will have to go to the Customize your Portal area and manually add it to their layouts.
Chapter 3 – Templates and Layouts

Overview
The layout of the Academus Portal is based on a combination of tabs, columns and channels controlled by the security model. The Portal takes multiple layouts and combines them to present an end user with a final composite view. Academus tracks individual changes that the end user makes to the composite view. This allows an end user to customize their different layouts, as long as customization is permitted under the parameters of the security model.

The users combined layout (see diagram) is a combination of tabs, columns, and channels. This layout is first determined at the administrator level using templates. Once an individual has logged into the system, they can alter this defined layout based on the groups in which they are enrolled, and the permissions those groups give them within certain channels.

Layouts
As discussed above and during the user preferences section, the end-user has ultimate control over the layout of their portal. Giving users the flexibility to tailor the content and location within their portal is one of the key reasons for a portal’s success on campus. There are, however, a few administrative restrictions that can be placed on end-users. For example, you may want to restrict the groups of people that have access to a certain channel. This can easily be accomplished through a publishing parameter (see Overview section of “Groups in the Portal”).

An individual’s layout can also be dictated at the tab level. For example, if your institution determines that there are a variety of channels that it wants to guarantee all members of the institution have and do not have the ability to delete; this can also be accomplished by locking down an entire tab. In order to do this, the tab should be created as a pushed fragment. (Refer to Chapter 2 for more specifics on Aggregated Layouts – Creating Fragments).

Finally, User Preferences can be turned off at the institution level so nobody on campus can alter their layouts. Currently, this is an “all or nothing” option. This can be accomplished through a configuration option in your Academus theme. Reference your Academus Visual Style Guide for specific instructions on removing the customize link.
Templates

Templates allow you to effectively tailor your portal for different constituent groups on campus. The System Administrator can setup a variety of template users in the Portal System. For example, staff, students, alumni, and faculty may all have different template users in the system. This allows an institution to setup the “skin”, number of tabs, channel locations, and group enrollment for an entire grouping of individuals. Once an individual logs into the portal for the first time, all of the attributes of the template user are copied over to that user. In addition, template users also control the default groups to which users are assigned upon their first portal login.

The administration of template users requires the participation of a portal administrator and possibly an LDAP administrator. In this document “LDAP” is used as a generic term for a user directory solution. Other products such as Microsoft Active Directory and Sun One Directory are interchangeable in this context. It is also important to note that template users are only relevant to institutions utilizing LDAP authentication. The portal database does not accommodate template users out of the box. Non-LDAP institutions can still create a default layout, but it is not possible to assign users to multiple template users without custom development.

Setting Up and Configuring Template Users

The following steps detail the creation and configuration of a template user.

- **Step 1: Create the template user**
  The template user can be created in either the portal database or in LDAP. The template user is created as a standard user, with a username that is descriptive of the user type that will follow the template user’s layout.
  
  To create a template user that will define the layout for all portal users who are students, add a user called “student” to the portal database or LDAP. Standard practice is to enter a first name of “Student” and a last name of “User”.

- **Step 2: Configure the template user’s layout**
  Template users control the default layouts for each user type.
  
  To configure the template user’s layout, log in to the portal as user “student”. Using the Customize link, set up the student user’s layout to include the desired tabs, channels, and skin. When you are finished, log out.

- **Step 3: Assign the template user to the appropriate group(s)**
  Template users control the default groups to which user groups are assigned. The Groups Manager channel is used to assign users to the appropriate default groups.
  
  To assign a group affiliation for the template user “student”, log in to the portal as an admin user and add the user “student” to the group Everyone -> Students. More information about groups and the group manager channel is provided in Chapter 4 of this guide.
Step 4: Configure Academus to utilize template users

Template users are simply portal users that have been set up for the purpose of managing user layouts. There is no database field or portal setting that designates a specific user as a template user. A user exists as a template user when there is a reference in LDAP to the template user name.

The first step to configure Academus to utilize template users is to designate the field within LDAP that holds or will hold the template user value. This field will vary based upon the LDAP schema utilized by your institution. An example of a standard schema within LDAP is the eduPerson schema. Within the eduPerson schema, the eduPersonPrimaryAffiliation field is typically used to store a value that can be used as the template user value such as “student”, “staff” or “faculty”.

In this example, the Academus portal administrator will set the following attribute in the PersonDirs.xml file:

```xml
<attribute>
  <name>eduPersonPrimaryAffiliation</name>
  <alias>uPortalTemplateUserName</alias>
</attribute>
```

The LDAP administrator will update LDAP to include the value of “student” in the eduPersonPrimaryAffiliation field for each portal user who is a student, if the field is not already populated with this value.

Step 5: Verify successful completion of the template user setup

To verify that the template user setup was successful, log in to the portal as an LDAP user who has a template user value (in this case, the value in “eduPersonPrimaryAffiliation”) of “student”, and who has never logged in before. If you are presented with the tab, channel, skin, and group settings that you configured for user “student”, you have successfully set up this template user.

Academus default template users

Academus does include in a set of default template user settings. During your deployment of Academus you are asked to define the default groups/tabs/channels for up to 5 template users. These are set up during your installation. If you elect to take the default template user setup, you will find the following template users in your portal:

- admin
- student
- faculty
- staff
- demo
- guest

These template users are set up by Unicon using the process defined in the steps above, and are available for you to use/update/manage as soon as your deployment is complete. Your Deployment Manager will provide you with passwords for these users.

The first four template users listed -- “admin”, “student”, “faculty”, and “staff” -- are easily recognizable as typical campus user types that might be required by an educational institution. In contrast, the uPortal framework, by default, requires the existence of the last two template users, namely “demo” and “guest”.

Template user “demo”

You may be wondering what happens if a portal user does not have an appropriate template user value in his/her eduPersonPrimaryAffiliation field. If the attribute is not populated, or contains a value that is
not the name of a valid template user, the user will receive the layout and group assignment of the
template user “demo”. Demo is the default user layout designated in the uPortal framework, however
this is a configurable setting. To change the default template user, identify the following line of code in
the “portal.properties” file, and replace “demo” with the desired template user name:

```
org.jasig.portal.services.Authentication.defaultTemplateUserName=demo
```

Once this value has been changed, the user template you designated will be the default layout provided
for portal users who have missing or invalid template assignments.

- **Template user “guest”**
  By default, the uPortal framework uses the template user “guest” to manage the pre-authenticated portal
  layout. This is the screen you will see when you access the main page of your portal where you are
  prompted to log in. In order to change the layout of the pre-authenticated portal page, you simply log in
  as “guest” and configure the layout and skin as desired. Note that after updating the guest layout, you
  must restart the portal in order to see your changes. This is true only for the template user guest and the
  layout of the pre-authenticated portal page.

**Managing Template Users**
It is important to understand the behavior between the portal and LDAP when managing template users.

- **Template user values are retrieved once per user**
  When a portal user logs in, the portal queries LDAP for the value in the user’s
  `eduPersonPrimaryAffiliation` field. This value is then saved in the portal database to designate whose
  layout the user should point to upon login. This value is saved once, and referenced upon each login.
  Hence, any change made in a user’s `eduPersonPrimaryAffiliation` value **WILL NOT** be recognized by the
  portal after the user’s first login.

- **Template user layout changes will be visible to users associated to the changed template**
  It is expected that template user layouts will need to change over time. When a template user layout has
  changed and the template user has logged out, users associated to the template user will see the
  changes upon their next log in. However, this applies only to those instances where the user has not
  made manual modifications to his/her layout.

- **Users break affiliation with template users if they make changes to their layout**
  Once a portal user logs in and makes a layout change, such as adding or moving a channel, the user will
  no longer follow the layout provided for the template user. After the layout is changed, any updates
  made to the template user layout will not be visible to the portal user who has modified his/her layout –
  unless these changes are made to a pushed fragment within the user’s layout.

  In the event you do not want your users to make any changes to their layouts, you can elect to lock down
  the preferences functionality within Academus. This can be accomplished through a configuration option
  in your Academus theme. Reference your Academus Visual Style Guide on specific instructions for how
  to shut off the Customize (or Preferences) option.

- **No automated way within portal functionality for resetting user layouts**
  uPortal 2.4 on which Academus 2.0 is built, does not provide a way via the user interface (UI) to reset
  user layouts. Information on how this can be accomplished via database scripts is provided in the
  **Academus 2.0 Custom Configuration Guide - User Layout - Access and Permissions**

  The aggregated layout push fragment features discussed in chapter 2 can be leveraged to push changes
to users and eliminate the need for user layout resets.
Chapter 4 – Groups in the Portal

Overview

The groups and permissions system within the Portal represents networks of groups whose members can have certain privileges, and who can inherit additional privileges from ancestor groups. The groups system allows for diverse ancestry of individuals within your institution, grouping of non-person objects such as channels, and application-specific groupings, such as Campus News Editors. The permissions system allows a channel to generate and check authorizations either directly assigned to a group or person, or inherited by that group or person from an ancestor in the group hierarchy.

Academus utilizes the group concept throughout numerous channels. Groups are first used to determine if access to a channel should be granted to a user. For example, an administrator channel like "Forums Admin" would only be available to certain groups such as Portal Administrators. The portal utilizes an individual's list of enrolled groups to determine this authority.

The image to the right is from the “Channel Admin” area of the portal. It displays the Publishing parameters of a channel. There are specific groups of individuals in the system that have access to this channel (the Survey Author channel). This flexibility allows the Portal Administrator to dictate the users in the system that can access certain channels.

Within the channels themselves, Academus also utilizes the group concept. For example, the Calendar Channel within the Portal allows a user to send an event to a user or a group. The Portal will determine the membership of that group and distribute the event to all of its members. There are a variety of channels that utilize this same type of behavior (e.g., Briefcase, Notifications, Discussion Forums, Survey, etc.).

The Academus Collaborative Groupware System also utilizes groups. The concepts of Topics, Offerings, and Roles are all considered groups. So, if an individual is enrolled in an Offering, they are also enrolled in a Portal group for that offering. This is explained in more detail in later sections.
Groups Manager Channel

The Groups Manager allows a user to browse or edit groups, their members, and their permissions. With this channel you can do the following activities:

- Add, edit, or delete groups
- Add, edit, or delete members of a group
- View the groups hierarchy in a drill down format
- Search for groups and/or members
- View available information about groups and members

The Groups Manager Channel has two primary screens. One shows a tree-structure representation of groups and their members, and operates in two modes, browse and select. In browse mode, you can expand and collapse groups to see their members, and click on any group to take you to its edit screen - this works similar to Windows Explorer. The edit screen shows a flat list of the selected group's immediate members, and has controls for renaming the group, adding and removing members, creating a new group as a member, and assigning permissions for the group. When adding members, you return to the tree screen in select mode, where you can build a list of selected groups and people to add. If the "Assign Permissions" button is chosen, the functionality of the Permissions Manager is invoked within the Groups Manager channel.

The Main Views of the Groups Manager Channel
Groups Manager

You will primarily use the Groups Manager channel to create new groups and add members to groups. The level of complexity of these groups is completely up to your institution. The more detailed that you are with the group structure, the more targeted the various messaging and controls within the Portal. Remember, that this also introduces a level of complexity and overhead into the system that your institution may not want or be equipped to handle.
Permissions Manager Channel

The Permissions Manager Channel is typically invoked from within the Groups Manager channel when setting specific permissions within a group. This is done by pressing the "Assign Permissions" button as shown in the diagram under the Groups Manager Channel. This will allow the Administrator to give other individuals within your institution specific privileges and administrative access to the group. For example, your Portal Administrator may want to setup the initial structure of the "Clubs" group. However, your Administrator may not want to be responsible for maintaining the memberships and subgroups that will be needed within this group. The Permissions Manager Channel allows him to assign others with these permissions. See the image below:

While the maintenance of permissions of users at the group level is one function of the Permissions Manager Channel, it can also be invoked as its own channel to set permissions for Groups, Channel Subscription, as well as Channel Publishing. The Permissions Manager workflow is actually a 5-step process:

1. Select Owners - First, you are asked to choose which type of permission you would like to set (Group, Channel Subscription, or Channel Publication)
2. Select Activities - Choose the specific permissions that you would like to alter for a group (if you have chosen the channel subscription or publication option in step 1, you will not need to select activities)
3. Select Targets - Choose the Group or Channel for which you would like to set permissions (if you have chosen Channel Publication you will not need to select targets). Note: The Permissions Manager view of groups within the Select Target screen is not hierarchical. This can be confusing if nested groups are named the same within the system. If this is a problem simply use the Assign Permissions button within the Groups Manager channel instead.
4. Select Principals - Choose the individuals or groups of individuals that you would like to give permissions to for a particular group, channel, or publication capability. Note: You do not need to be enrolled in a group to have permissions over that group.
5. Assign Permissions by Principal - Choose the specific permissions of the principals for the selected activities and targets.

The Channel Subscription and Publishing permissions can be set within the Channel Manager channel as well.
Using LDAP to setup your initial group membership

If your institution is utilizing any form of an LDAP system, you can automatically populate many of the groups in your system upon initial log-in. This will eliminate the need for much of the manual enrollment of users into groups via the Groups Manager channel. There are two methods for this group enrollment:

The Portal Administrator can utilize template users to determine group membership as described in Chapter 3. Based on the primary affiliation indicated within the LDAP system, the Portal will copy over the same groups as the template user – as well as the layout and channel structure.

The Portal Administrator can also utilize “Composite Groups” within the Portal. Composite groups allow the administrator to map a variety of different fields within the LDAP system to groups within the portal. This gives an institution a tremendous amount of flexibility in regards to initial group setup. A channel has been added to the solution for institutions managing users through LDAP or Active Directory. This channel pushed to students to give them the ability to change their LDAP or Active Directory password from within Academus.

Group Selection Restrictor

In Academus, the group hierarchy can be accessed from a variety of channels in the portal (e.g. Calendar, Forums, Campus Announcements, etc.). Academus can permit all individuals accessing these channels the capability of choosing any group in the system. For example, if an individual has access to the calendar channel, they can invite everyone on campus to a calendar event.

While this capability gives the system an extraordinary amount of flexibility, it could be undesirable. Either through malice or overzealousness, an individual could wreak havoc within the portal with these capabilities. To solve this potential concern, Academus includes Group Selection Restriction functionality. This feature allows institution to restrict some of the flexibility in the group selection process.

The Group Selection Restrictor affects the following channels:

- Calendar
- Notifications
- Discussion Forums Admin
- Survey Author
- User Administration
- Campus Announcements
- Group Chat Admin
- WebMail
- Topic Administration

There are two other channels that utilize their own utilities to access the group structure; Classifieds and Campus News. These two channels are not covered under the Group Selection Restrictor rules since they require specific permissions to even invoke the functionality where a group may be chosen.

By default, users can no longer select any group within the system to perform the various commands offered by the channels above. For example, a student user can no longer invite the “Everyone” group to an event they create in their calendar. Likewise, users who have permissions to distribute surveys will not be able to distribute a survey to the “Everyone” group (which consists of everyone in the system). Under the new rules, users cannot (by default) select groups above their current enrollment in the group hierarchy.

It may not always be in your best interest to restrict group selection from all users. For example, you may have a trusted user or two who need to send announcements to the “Everyone” group. In this instance, you need to override the Group Selection Restrictor for the individual user.
Granting Group Selection Privileges to a Single Individual for a Single Group

Follow these steps to override the Group Selection Restrictor for a specific user, thus allowing the user to select the “Everyone” group:

- You must be logged in as the super admin user or a user with privileges to access the Groups Manager channel.
- Locate the Groups Manager channel.
- Click the Everyone group.
- Click the lock icon to unlock the group.

Now that the group is in an unlocked state, its properties can be edited. We are interested in editing the permissions of this group, so click on the Assign Permissions button.

The next step is to locate the user that should be given the override. The easiest way is to use the search options that are located at the bottom of the Group Manager screen. Simply type all or part of a user’s name or their username.
• Check the box next to the user’s name and click the Select Marked button. Then click the Done with Selection button at the bottom of the window. This will take you to the permissions screen.

• On the permissions screen, locate the column that says “Select this group”. Then locate the row that has the user who should get the group selection override. Change their setting to GRANT. This will now allow them to select the “Everyone” group and any subgroup in the hierarchy.

• Click the Submit button when finished.
Granting Group Selection Privileges to a Group for Selection of Multiple Groups

Follow these steps to override the Group Selection Restrictor for multiple groups through a single process. In this example we will be granting the Faculty group privileges to select the Everyone, Staff, Student and Faculty groups.

- You must be logged in as an administrative user with access to the permission manager channel.
- Locate the Permission Manager channel.
- Check the box next to Group Manager.
- Click the Submit button to proceed to the next step.
- Now you will see the list of permissions assignable for a group.
- Check the box next to Select this group.
- Click the Submit button.
A list of all groups in the portal will be displayed. Select the group(s) for which selection privileges will be granted.

- Check the box next each desired group.
- Click the Submit.

The next step allows you to select the groups or individuals to whom the selection permissions are being granted.

For this scenario, check the box next to the Faculty group and click the Select Marked button. Then click the Done with Selection button at the bottom of the window. This will take you to the permissions screen.

- On the permissions screen, locate the column that says “Select this group”. Change the setting to GRANT for each group that the Faculty group is being granted permission to select.
- Click the Submit button when finished.
Chapter 5 – Channel Administration

Overview
Access to the Channel Administration area of the Portal is typically limited to Portal Administrators at your institution. The main purpose of utilizing the Channel Administration feature is for the creation, edit, or deletion of channels within your portal environment. There are ten different types of channels that can be published in the Portal. These channels range from very simple “image” channels, to highly complex “custom” channels and portlets that require extensive Java programming.

Channel Manager

<table>
<thead>
<tr>
<th>Workflow:</th>
<th>Channel Type</th>
<th>General Settings</th>
<th>Channel Controls</th>
<th>Categories</th>
<th>Groups</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Type:</td>
<td>Select the type of channel to add by clicking a selection icon in the option column</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Channel Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Custom</td>
<td>This channel type allows the publication of channels with no accompanying CPD (Channel Publishing Document). It is typically used to publish channels with only one corresponding channel definition.</td>
</tr>
<tr>
<td>☐</td>
<td>Applet</td>
<td>Displays a java applet</td>
</tr>
<tr>
<td>☐</td>
<td>Custom Channel</td>
<td>Custom Channel</td>
</tr>
<tr>
<td>☐</td>
<td>Image</td>
<td>Simple channel to display an image with optional caption and subcaption</td>
</tr>
<tr>
<td>☐</td>
<td>Inline Frame</td>
<td>The Inline Frame channel can be used to render an HTML page within a frame. This channel does not work correctly in browsers older than Internet Explorer 5 and Netscape 6.</td>
</tr>
<tr>
<td>☐</td>
<td>Portlet</td>
<td>Adapter for JSR-168 Portlets</td>
</tr>
<tr>
<td>☐</td>
<td>Remote Channel Proxy</td>
<td>Uses SOAP to communicate with and present to the user the contents of a channel living in a remote instance of UPortal</td>
</tr>
<tr>
<td>☐</td>
<td>RSS (Rich Site Summary)</td>
<td>RSS or Rich Site Summary, the most common channel format, is a channel which has its content defined through an XML document. Anyone may publish an RSS channel as long as the specification is adhered to and the file is stored on a publicly accessible web server. You will need to provide a URL for the RSS file.</td>
</tr>
<tr>
<td>☐</td>
<td>Simple XML Transformation</td>
<td>XSL renders XML to a particular style, is a channel which has its content defined through an XML document. Anyone may publish an XSL channel as long as the specification is adhered to and the file is stored on a publicly accessible web server. You will need to provide a URL or Path for the XML and XSL file.</td>
</tr>
<tr>
<td>☐</td>
<td>Web Proxy</td>
<td>Incorporate a dynamic HTML or XML application</td>
</tr>
</tbody>
</table>

As you can see in the image above, the Channel Manager follows a workflow process to guide you through several steps in publishing a new channel. The steps are:
- Channel Type
- General Settings
- Channel Controls
- Categories
- Groups
- Review
Channel Publishing Basics

UNICON provides extensive training classes on the creation of portal channels and portlets within the uPortal framework. Please talk to your UNICON Deployment Manager or Sales Consultant for more information on these classes. Some channels, however, can easily be created and integrated within your portal system with no training at all. These are the “Image”, “Inline Frame” and “RSS” Channel types. Instructions for creation of those channel types are included in the sections below.

A note of caution for administrators publishing any channel type.

Channel publishers must always include a default value for user modifiable parameters.

When creating a new channel, parameters with the ‘User Modifiable’ option should be used with great care due to a known issue in the uPortal framework. If the channel publisher sets the ‘User Can Modify’ flag to true, but does not enter a default value for the parameter then individuals with that channel in their portal layout will be unable to save layout changes.

This issue will also occur for a particular user if, when that user adds a channel to their layout that has a “user modifiable” parameter, and they remove the default value for the parameter and submit a blank response.

Image Channel

An Image Channel is a simple channel used to display an image with optional caption and sub-caption. This is one of the easiest channels to deploy on your campus.

After setting the channel type, the next step is to configure the general settings. This will require you to fill in the following pieces of information:

- Type in a **channel title**. This is the name users will see when they subscribe to a channel.
- Type in a **channel name**. This text appears as the header when the channel is rendered. Most often title and name are the same.
- Type in a **channel description**. This is used to provide additional information to a user about a channel.
- Set the **channel timeout**. This is the number of milliseconds a channel will attempt to render itself before the portal terminates that channel’s rendering.
- Click **Next** to advance to the next step. In this window, enter the following information:

<table>
<thead>
<tr>
<th>User can modify</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Type</td>
<td>Image</td>
<td></td>
</tr>
<tr>
<td>Channel Title</td>
<td>Image Example Title</td>
<td></td>
</tr>
<tr>
<td>Channel Name</td>
<td>Image Example Name</td>
<td></td>
</tr>
<tr>
<td>Channel Functional Name</td>
<td>Image Functional Name</td>
<td></td>
</tr>
<tr>
<td>Channel Description</td>
<td>Channel Description Text</td>
<td></td>
</tr>
<tr>
<td>Channel Timeout</td>
<td>90000 milliseconds</td>
<td></td>
</tr>
<tr>
<td>Channel Secure</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Image width (pixels)</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>Image height (pixels)</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Image URI</td>
<td><a href="http://www.unicon.net/images/home_feature_academann15.gif">http://www.unicon.net/images/home_feature_academann15.gif</a></td>
<td></td>
</tr>
<tr>
<td>Caption</td>
<td>The Hard Porter</td>
<td></td>
</tr>
<tr>
<td>Selected Categories</td>
<td>Portal Development</td>
<td></td>
</tr>
<tr>
<td>Selected Groups and/or People</td>
<td>Everyone</td>
<td></td>
</tr>
</tbody>
</table>
Enter Image URI. Uniform Resource Identifiers (URIs, aka URLs) are short strings that identify resources on the web: documents, images, downloadable files, services, electronic mailboxes, and other resources. They make resources available under a variety of naming schemes and access methods such as HTTP, FTP, and Internet mail addressable in the same simple way. Enter Image Dimensions (height and width)

Enter Size of an Image Border. The Border color is determined by the “Skin” your layout has set

URL if image is clicked. This will simply link your users out to a URL address if the image is clicked.

Click Next to advance to the Caption window, or Back to return to the previous screen. In the image caption window, enter a caption and/or sub-caption. Remember that the display of image captions is style sheet dependent and may not display on all devices.

Click Next to advance or Back to return to the previous screen. In the channel controls window, select the channel controls you wish to include in the custom channel. These controls (Editable, Has Help, and Has About) will not work with the simple channels we are discussing here so leave them unchecked. These only work with channels that have some code that can tell the program where the Help is stored.

Click Next to advance to the Categories window, or Back to return to the previous screen. The categories window allows you to browse and add the categories in which this channel will appear. Select a category from the list of channel categories. Select the checkbox next to the desired categories then click Select Marked. You can add multiple categories as appropriate. To remove a selected category, check the box next to the category in the lower portion of the channel and click the Deselect button.

Click Next to advance to the Groups window, or Back to return to the previous screen. From the groups window, browse and add the groups that have access to this channel. Clicking on a group name will bring up a list of sub-groups. You may also search for a group. Continue to select a group and click Go to access the groups you wish to give access to the channel to. Select the checkbox next to the desired group(s) then click Select Marked. You can add multiple groups as appropriate. To remove a selected group, check the box next to the group name in the lower portion of the channel and click the Deselect button.

Click Next to advance or Back to return to the previous screen. Once you have completed each of the steps above, you can review your selections for accuracy and make any last minute adjustments. Edits can be made by selecting workflow icons or items in the table. Once all data is confirmed to be accurate, click Finished. This will return you to the main window for the Channel Manager channel.
Inline Frame Channel

The inline frame channel is used to render an HTML page within a frame. This is an easy way to include general website information within your portal, or to create simple channels based on HTML. If you have no HTML skills within your institution, you can easily create a WORD or PowerPoint document, and simply save it as an HTML file. This can then be included within a Portal Channel. The Inline Frame Channel will also work for the inclusion of FLASH files.

After setting the channel type, the next step is to configure the general settings. This will require you to fill in the following pieces of information:

- **Type in a channel title.** This is the name users will see when they subscribe to a channel.
- **Type in a channel name.** This text appears as the header when the channel is rendered. Most often title and name are the same.
- **Type in a channel description.** This is used to provide additional information to a user about a channel.
- **Set the channel timeout.** This is the number of milliseconds a channel will attempt to render itself before the portal terminates that channel rendering.

Click Next to advance to the next step. In this window, enter the URL of the page you want to render in an inline frame. Be aware that inline frames are not supported in some browsers, in which case this channel will render a link to open the page in a new window. Enter the frame height. Note the default setting for frame height is 600 pixels.

Click Next to advance to the Channel Controls window, or Back to return to the previous screen. In the channel controls window, select the channel controls you wish to include in the custom channel. Again, these controls will not work for an Inline Frame Channel.

Click Next to advance to the Categories window, or Back to return to the previous screen. The categories window allows you to browse and add the categories in which this channel will appear. Select a category from the list of channel categories. Select the checkbox next to the desired categories then click Select Marked. You can add multiple categories as appropriate. To remove a selected category, check the box next to the category in the lower portion of the channel and click the Deselect button.
Click Next to advance or Back to return to the previous screen. From the groups window, browse and add the groups that have access to this channel. Clicking on a group name will bring up a list of sub-groups. You may also search for a group. Continue to select a group and click Go to access the groups you wish to give access to the channel to. Select the checkbox next to the desired group(s) then click Select Marked. You can add multiple groups as appropriate. To remove a selected group, check the box next to the group name in the lower portion of the channel and click the Deselect button.

**RSS Channel**

The RSS channel, or Rich Site Summary, is the most common channel. The RSS is a channel which has its content defined through an XML document. Anyone may publish an RSS channel as long as the specification is adhered to and the file is stored on a publicly accessible web server. Several types of RSS channels can be found on the Internet (e.g., Motley Fool, Dictionary.com, Yahoo News, etc.). You can create your own individual RSS channels as well.

After setting the channel type, the next step is to configure the general settings. This will require you to fill in the following pieces of information:

- **Type in a channel title.** This is the name users will see when they subscribe to a channel.
- **Type in a channel name.** This text appears as the header when the channel is rendered. Most often title and name are the same.
- **Type in a channel description.** This is used to provide additional information to a user about a channel.
- **Set the channel timeout.** This is the number of milliseconds a channel will attempt to render itself before the portal terminates that channels rendering.

Click Next to advance to the next step. In this window, enter the RSS URL, the RSS version for stylesheet selection, and the cache timeout (in seconds). URLs can optionally be specified relative to the classpath. For stylesheet selection, use 0.9 for original 0.9 rss files and 0.9x or 1.0x for rdf documents.
Click Next to advance to the Channel Controls window, or Back to return to the previous screen. In the channel controls window, select the channel controls you wish to include in the custom channel. Again, these controls will not work for an RSS Channel.

Select a category from the list of channel categories. Select the checkbox next to the desired categories then click Select Marked. You can add multiple categories as appropriate. To remove a selected category, check the box next to the category in the lower portion of the channel and click the Deselect button.

Click Next to advance or Back to return to the previous screen. From the groups window, browse and add the groups that have access to this channel. Clicking on a group name will bring up a list of sub-groups. You may also search for a group. Continue to select a group and click Go to access the groups you wish to give access to the channel to. Select the checkbox next to the desired group(s) then click Select Marked. You can add multiple groups as appropriate. To remove a selected group, check the box next to the group name in the lower portion of the channel and click the Deselect button.
Chapter 6 – Configuration Options

Overview

A great deal of the flexibility of Academus is enabled through configuration options for specific Academus channels, portlets, and themes. These options are controlled by configuration files which must be set up and managed by your portal system administrator. The key options and customizations are outlined in this section so that you will have the background information necessary to work with your system administrators to better fit the portal’s capabilities to the needs your campus.

Academus Theme and Skin Presentation

The Academus theme and skin control the overall look and feel of your institutions portal. As part of the deployment process, Unicon’s user experience team works with each of our clients to develop a custom skin which is branded for their institution. In addition to the custom color schemes, fonts and logo’s for your campus, other components of the presentation may be adjusted as well.

Customizable elements of your Academus Theme include:

- Selection of Left Hand or Horizontal Tab Structure
- Welcome message presentation
- Presentation of today’s date
- Footer contents – links to existing university info.
- Inclusion of a Left Hand Navigation Column
- Enable/Disable Quicklinks – set included channels and presentation location
- Enable/Disable Web Search - set desired websites for search and presentation location
- Enable/Disable Expanding Menus
- Enable/Disable Sub-navigation
- Enable/Disable Spell Check on all Text Areas
- Remove the Customize (Preferences) Link

More information on setup and configuration of Academus themes and skins is available in the Academus Visual Style Guide.

Online Help Link

Academus provides a placeholder within the portal for online help information specific to your institution. The online help link is located in the header bar of the between the Home and Sitemap links. The place holder page included with your base default deployment should be replaced with an informational page informing portal users about specific resources available to assist them on your campus. Information such as campus help desk phone numbers, email addresses and hours of operation is highly recommended.

More information on system administration steps for replacing the online help placeholder page is available in the Academus Online Help Customization Guide.
Blogging Portlets

The Blogging Portlet allows select individuals to author blogs that can be read and commented upon by the entire campus population. By default Academus is configured with a single instance of the Blog portlet. Portal managers can customize this instance using the Blog administration console to set the blog name and other properties. Permissions for this instance of the blog portlet are controlled through the portlet permission manager.

Multiple blog instances can be created. For example your campus might have a small number of independent blog channels (e.g. College of Engineering Blog, College of Pharmacy Blog, University President Blog). Privileges on each blog are controlled independently such that a user with permission to add blog entries to the Math Department Blog can be prohibited from adding entries to the University President blog.

To create a new blog instance
- Select a Name for the new blog
- Have your portal system administrator configure a new blog instance under the selected name
- Have your portal system administrator configure a permissions portlet entry for the new blog
- Have your portal system administrator publish a channel for the new blog instance
- Using the blog administration console within the new blog portlet – set up blog properties and categories
- Set permissions for the new blog establishing owners for blog properties, categories, and authoring privileges.
- Publish the new blog channel to the applicable group(s)

More information on system administration steps for setup and configuration of new Blog instances is available in the *Academus Blogger Multiple Instances Configuration Guide*.

Briefcase Portlet

Configuration options within the briefcase include
- Set maximum allowed file storage space by group
- Establish drives with access to Shared LDAP folders
- Establish drives with access to Shared Network folders
- Set maximum upload file size for each configured drive/node
- Set display icons for each drive/node
- Set view, edit and delete options by group

More information on system administration steps for setup and configuration of the Briefcase portal is available in the *Academus Briefcase Portlet Configuration Guide*.
SSO Gateway Portlet

This SSO Gateway portlet kit allows for streamlined integration with third-party applications. System administrators are able to quickly apply SSO to applications through Academus by editing a single configuration file.

To create a new SSO Gateway Portlet
- Identify the target application
- Have your portal system administrator create a SSO Gateway configuration file
- Have your portal system administrator publish a channel for the new SSO Gateway instance or add the SSO link to an existing SSO channel
- Publish the SSO Gateway channel instance to the applicable group(s)

Unicon already has SSO Gateway Portlets for easy integration with Outlook Web Access, LiveText, SAKAI 2.0 and the Academus Web Content Management system. Your system administrator can quickly leverage these existing integrations within your portal. More information on system administration steps for setup and configuration of single sign on integrations is available in the Academus SSO Gateway Configuration Guides.

Change Password Channel

The Change Password channel is for institutions managing users through LDAP or Active Directory. This channel can be pushed to students to give them the ability to change their LDAP or Active Directory password from within Academus.

The channel requires an administrator account on the LDAP or Active Directory server to perform the password changes. In addition, Active Directory requires an SSL connection to carry out a password change over the LDAP protocol.

Configuration options include:
- Support for LDAP or Active Directory
- Enabling Connection over SSL
- Request for current passwords before authorizing password change

More information on system administration steps for setup and configuration of the Change Password channel is available in the Academus LDAP Change Password Channel Configuration Guide.
Academus Web Content

Unicon now offers a Web Content Management (WCM) solution to compliment your portal and provide tools for your institution to manage their internet and intranet websites. A single sign on channel to the Academus Web Content Management solution is provided with your default installation. Your deployment team will assist with this configuration if you have purchase the Academus WCM.

Following your initial deployment your may choose to publish content from the web content management system for use in the portal (e.g. Weekly Bookstore Specials, Student Union Events and Promotions, etc) Academus provides special a Web Content Management portlet for displaying this information. These portlets have an advantage over inline frame or XML channels because they not only display the content – but also provide content managers the ability to link directly from the content channel in the portal to the web content management system to where they can update the content and publish their changes.

The process for creating a new Web Content Management channel for display of a particular piece of content will require support from your system administrator. A brief outline of the process is provided below:

1. Create a publication directory on the host server.
2. Update the Academus WCM to publish to that directory.
3. Publish the content which is to be displayed in the Academus portal the new directory.
4. Create a content portlet by setting up a content portlet XML configuration file.
5. Add your new WCM portlet to portlet.xml
6. Add your new WCM servlet and it's mapping to web.xml
7. Restart the Tomcat server
8. Publish the new WCM portlet in Academus via the Channel Manager, specifying the groups and individuals who will have access to this new content.

At this point individuals will be able to subscribe to the content channel or have it pushed to their layouts using fragments. Once the portlet is initially configured the Content Manager will be able to update the content of this portlet in the WCM and publish their changes directly to the portal – without additional system administrator support.

More information on the detailed system administration steps for setup and configuration of a new Web Content Channel is available in the Academus Web Content Management Channel Configuration Guide.

To learn more about purchasing the Academus Web Content Management solution, please contact your Unicon Account Manager.

PAGS

Additional information is available on the use of PAGs as the groups management strategy for your portal. Contact your Unicon Account Manager to receive additional documentation and mentoring on the use of PAGs for your institution.

Authentication/Person Dirs

Additional information is available on portal authentication mechanisms and the use of Person Dirs. Contact your Unicon Account Manager to receive additional documentation and mentoring on these topics.
Chapter 7 - Administration Channels

User Administration Channel

The User Administration channel allows you to add and edit users within the system. You can also set add or remove permissions for this channel to and from specific groups. The User Administration channel is only applicable in Academus implementations that do not use an extended authentication method, such as LDAP or Active Directory.

To search for any users who have already been added to the system, follow these steps:

1. Locate the User Administration channel and click the Search Users ink at the top of the channel.
2. You should now see the Search for User screen.
3. Enter as little or as much information as you know about the user in any or all of the four fields provided (User Name, First Name, Last Name, Email).
4. Click the Submit button.
5. The system will return all matches for your criteria. If no users are found, make your search less specific, click the Search button and try again until you get a satisfactory result.

To add a new user to the system, complete the following steps:

1. Locate the User Administration channel and click the Add User option at the top of the channel.
2. This will take you to the Add User screen where you must provide information about the new user.
3. Type a User Name in the first text field. The User Name must be unique to the system. If anyone else is already using the User Name you provide, you will have to choose another one.
4. Now select a Password. If you want the Password to be the same as the User Name, then select the Automatic Password radio button. Otherwise, select the Manually Entered radio button and type a Password in the text field provided.
5. Type the user's First Name in the next field.
6. Type the user's Last Name in the next field.
7. Type the user's Email Address in the next field.
8. Once you are satisfied with all of your selections, click the Next button to add this new user and be prompted to select groups with which to associate the new user.
9. Select the group(s) to which this new user will be assigned.
10. Click Submit Selections.
Discussion Forums

Discussion Forums Admin Channel makes it possible for an administrator to create forums for community discussion, or to delete forums that are no longer relevant. This channel also allows the administrator to restrict forum access to a certain users or groups, as well as set user and group permissions (i.e. viewing, adding and deleting messages, etc.) for each forum.

To create a new forum, add users and groups to the forum, and set permissions, follow these steps:

1. Locate the Discussion Forums Admin channel and click the Add Forum option.
2. You should now see the New Forum screen.
3. Choose a name for this forum by typing it in the Description field.
4. For the Newsgroup field, it is best to enter a single word in lower-case. This field is used to create a newsgroup on the community's news server. Newsgroups usually use a format similar to "university.academus.forums.homework" where "homework" might be the name of your discussion forum. By only entering one word into the Newsgroup field, it helps conform to the general standard.
5. If you click the OK button at this time, the forum will be created, but no one will be able to view it. This is because you haven't yet assigned users to this forum. So instead of clicking the OK button, simply click the Add user icon on the lower left side of the screen.
6. Click the Add User icon to add users to the forum.
   a. You will now see the Select Users and Groups screen. To add users and groups to this forum, follow these steps:
      b. Use the Browse tab to select group(s) from the group hierarchy, click the + icon next to a group name to expand the group list. (Figure 156)
      c. Place a checkmark next to each group for which the discussion forum will be enabled.
      d. To search for specific users, click the Search tab.
      e. Enter search criteria and click Search.
      f. Place a checkmark next to each user for whom the discussion forum will be enabled.
6. Once all desired users and/or groups have been selected, click the Submit Selections button at the bottom of the channel.
8. Now you need to assign privileges to these users and groups before they will be able to access the forum messages. There are four different permission settings, each of which should be granted or denied: (Archive Forums, View Posts, Add Posts, Delete Posts).

To find and delete any forum, follow these steps:

1. Locate the Discussion Forums Admin Channel.
2. Enter the name of a forum into the Find text box. Or, leave the box blank to see a list of all forums.
3. Click on the Find button.
4. You should now see a list of forums that match your search string. You can click on these forum names to edit their details, add or remove users and groups, or to alter the permissions for any groups or users.
5. If you would like to delete a forum, click on the Delete icon next to the forum name.
Group Chat Administration

The Chat Admin channel allows you to set up chat rooms for users within the community. You can create chat rooms for selected groups, and determine the permissions that each user or group has while in the chat room. In order for users to join a chat room, it must first be enabled from within the Chat Admin channel.

To create and enable a chat room, follow these steps:
1. Locate the Group Chat Admin channel.
2. In the Browse section, locate the group you wish to enable a chat session for. Clicking the + icon expands the group hierarchy to reveal sub-groups.
3. Check the radio button next to the desired group to enable a chat room or edit chat room privileges for that group.
4. Click the Submit Selections button at the bottom of the channel.
5. You will now see a new screen where you will be able to either enable or disable the chat room.
   Click the Disabled icon to enable the chat room.

After enabling a chat room for the first time, the default permissions must be determined. Follow these steps:
1. The Edit Default User Permissions screen appears, containing a list of permissions.
2. Check the box(es) to grant these permissions by default.
3. Uncheck any box(es) for to deny these permissions by default.
4. Click the Update button when finished.
Survey Author

There are two types of surveys: **Personal** and **Shared**. **Shared Surveys** can be edited by anyone has access to the Survey Author Channel. Likewise, its results will be visible to all users with access to the channel. **Personal Survey** can be edited only by the individual who created the survey, or by an individual granted super administrative privileges for the Survey Author Channel. In addition, only the author of a **Personal Survey** and the super administrator can view the results of the personal survey.

Surveys can be distributed to the portal user population in a number of ways.

- **Polls** are available to all users with poll channel access. All users can participate in the poll and see real time results of all poll responses made by other portal members.
- **Anonymous** response type surveys are targeted at specific groups or individuals. These surveys can be submitted multiple times per user. Each response submitted will be saved. The results screen will not show the specific answers from each user.
- **Named** response type surveys are targeted at specific groups or individuals. These can be submitted multiple times per user. However, only the most-recent responses will be saved. The results screen will show each user's specific answers.
- **Election** response type surveys are targeted at specific groups or individuals. These can only be submitted one time per user. Once a user submits a survey of this type, it will disappear from their Survey Channel.

For detailed instructions on the creation and distributions of surveys and polls, reference your Academus Portal User Guide.

Individuals with administrative privileges over the survey author channel will be able to access all personal and shared surveys regardless of the survey creator. This includes the ability to edit and delete another user’s personal surveys, close personal survey distributions, as well as review and delete personal survey results. Because of the capabilities granted with these privileges, the subset of individuals given the new permission should be closely controlled.

To create an administrator for the survey channel follow these steps:

1. Locate the **Permission Manager Channel**
2. You will see “Academus Survey Author” included in the list.
3. Click the checkbox next to Academus Survey Author then click **Submit**.
4. Use the tree to drill-down to the desired group or use the search option to locate a specific individual.
5. Once the individual or group to be selected is located, click the **Select Marked** button.
6. Repeat the process until all desired entities have been located.
7. The selected entities will now appear in the list at the bottom of the channel, click the **Done with Selection** button.
8. The Assign by Principal screen will appear with a section for each entity.
9. Select **Grant** from the dropdown list, to grant the user privileges to Edit and Delete All Surveys.

Note: Individuals granted this privilege must also be a member of a group that has been granted access to the Survey Author Channel.
Campus Announcements

The Campus Announcements channels allow users with administrative permissions to publish announcements that can be seen by the entire community or to target announcements at a particular group.

During the deployment of Academus, two groups are given administrative permissions to add announcers to this channel: Portal Administrators (group_id=14) and Channel Managers (group_id=128). You can remove the administrative permissions from these groups or you can add them to new groups or individuals by accessing Permissions Channel.

Campus Announcements has three level of permissions

- **User may assign announcers** – This privilege allows a user or group of users to access the Admin link within the channel. Access to this link allows the user to grant other groups and individuals the ability to add announcements.

- **User may add an announcement** – This privilege can be granted via the permissions channel or by selecting the Admin link within the Announcement Channel itself. Individuals with the Add Announcement privilege can create new announcements and distribute them to any group within the portal. The privilege also allows a user to edit and delete any announcements, which they have created.

- **User may edit all announcements** – This privilege provides an individual or group with administrative capabilities to edit and delete any announcement in the system, regardless of who originally created the announcement. Because of the capabilities granted with this privilege, the subset of individuals given the permission should be closely controlled. Individuals granted the Edit All permission must also be granted the Add an Announcement permission to access all announcement functionality.

To enable these permissions follow these steps:

1. Locate the Permission Manager Channel
2. You will see “Academus Campus Announcements” included in the list.
3. Click the checkbox next to Academus Campus Announcements then click Submit.
4. The three permissions supported for the channel are displayed.
5. Check the permission or permissions you wish to grant and click Submit.
6. Use the tree to drill-down to the desired group or use the search option to locate a specific individual.
7. Once the individual or group to be selected is located, click the Select Marked button.
8. Repeat the process until all desired entities have been located.
9. The selected entities will now appear in the list at the bottom of the channel. Click the Done with Selection button.
10. The Assign by Principal screen will appear with a section for each entity.
11. Select Grant from the dropdown list for each entity and permission then click the Submit button.
Campus News

The Campus News channel allows users to publish news articles under topics to which they’ve been granted access. The management of those topics is an administrative privilege that can be granted to specific groups and individuals.

During the deployment of Academus, two groups are given administrative permissions to add and edit topics within the Campus News channel: Portal Administrators (group_id=14) and Channel Managers (group_id=128). You can remove the administrative permissions from these groups or you can add them to new groups or individuals by accessing Permissions Channel.

Campus News has one administrative privilege:
  - User may view and edit news topics – Users with this privilege have the ability to create new news topics and assign individuals and groups rights to publish news articles for that topic. These users also have the ability to view and edit any news topic in the system.

To enable this permission follow these steps:

1. Locate the Permission Manager Channel
2. You will see “Academus Campus News” included in the list.
3. Click the checkbox next to Academus Campus News then click Submit.
4. Use the tree to drill-down to the desired group or use the search option to locate a specific individual.
5. Once the individual or group to be selected is located, click the Select Marked button.
6. Repeat the process until all desired entities have been located.
7. All selected entities will now appear in the list at the bottom of the channel.
8. Click the Done with Selection button.
9. The Assign by Principal screen will appear with a section for each entity.
10. Select Grant from the dropdown list for each entity, and then click the Submit button.
Classifieds

The Classified channel allows users to post classifieds. These classified are then route for approval based on the topic under which they were created. The management of classified topics is an administrative privilege that can be granted to specific groups and individuals. An additional permission has also been added which can be used to grant an administrative user the ability to delete any classified in the system, regardless of the original creator or approval status.

During the deployment of Academus, two groups are given administrative permissions to add and edit topics within the Classified channel: Portal Administrators (group_id=14) and Channel Managers (group_id=128). You can remove the administrative permission from these groups or you can add the permission to new groups or individuals by accessing Permissions Channel.

Classifieds has two administrative privileges:

- **User May Manage Classified Topics** – Users with this privilege have the ability to create new classified topics and assign individuals and groups rights to approve a classified for that topic. These users also have the ability to view and edit any classified topic in the system.

- **User May Delete Any Posted Classified** – Users with this privilege have the ability to delete any classified in the system, regardless of the initial creator. Because of the capability granted with this privilege, the subset of individuals given the new permission should be closely controlled.

To enable these permissions follow these steps:

1. Locate the Permission Manager Channel
2. You will see “Academus Classifieds” included in the list.
3. Click the checkbox next to Academus Classifieds then click Submit.
4. The two permissions supported for the channel are displayed.
5. Check the permission or permissions you wish to grant and click Submit.
6. Use the tree to drill-down to the desired group or use the search option to locate a specific individual.
7. Once the individual or group to be selected is located, click the Select Marked button.
8. Repeat the process until all desired entities have been located.
9. All selected entities will now appear in the list at the bottom of the channel.
10. Click the Done with Selection button.
11. The Assign by Principal screen will appear with a section for each entity.
12. Select Grant from the dropdown list for each entity and permission, and then click the Submit button.
Blogging Portlet

The Blogging Portlet allows select individuals to author blogs that can be read and commented upon by the entire campus population. The management of those blogs and authoring capabilities are administrative privileges that can be granted to specific groups and individuals. One campus might have a small number of independent blog channels (e.g. Math Department Blog, University President Blog). Privileges on each blog are controlled independently such that a user with permission to add blog entries to the Math Department Blog can be prohibited from adding entries to the University President blog.

Each Blog has four administrative privileges:

- **Edit Blog Properties** - Users with this privilege have the ability to set blog properties such as name, description, blog owners, business rules for emailing comments, etc.
- **Edit Blog Categories** – Users with this privilege have the ability to create, edit and delete blog categories and sub-categories.
- **Edit Blog Entries** - Users with this privilege have ability to post entries to the blog to be viewed by all blog subscribers.
- **Upload Files** – Users with this privilege have the ability to upload files to the blog which maybe be included in Blog Entries.

To establish permissions for a blog:

1. Navigate to the Portlet Permission Manager Channel.
2. Click the link for the Blog whose permissions will be created or updated.

Portlet Permission Manager

Permissions Management

Select the Portlet for which you want to manage permissions:

- Blog: Math Department
- Notification Portlet
- Briefcase Portlet

3. Click the **Add** button to select the users and groups to whom permissions will be granted.
4. You may select members and groups in one of two ways: you may search for specific members or groups, or browse through the directory of Campus Groups, your own Personal Groups, or individual Members.
5. To search for a specific member or group:
   a. Enter a whole or partial member or group name of the in the Search field.
   b. Click the **Go** button.
   c. From the list of search results, place a checkmark next to each member/group that you wish to add.
   d. Click the **Add to My Selection Basket** button.
6. To browse through the listings of Campus Groups or your Personal Groups:
   a. Click the Groups tab within the permission portlet
   b. Choose Campus or Personal Groups.
   c. Find the group you wish to add.
   d. Place a checkmark next to the group name.

7. Click the **Add to My Selection Basket** button.

8. When all desired groups and members have been selected, click the **Submit My Selections** button.

9. For each group or individual displayed in the permissions view, select the appropriate permission.
   a. **Grant** - Enables the group/user to perform the function
   b. **Deny** – Prohibits the group/user from performing the function
   c. **Defer** – Causes the group/users privileges to be inherited from those set for a parent group of which they are a member. If no privileges have been set for a parent group, defer will be treated as a permission of Deny.

10. When all permissions have been assigned, click **Save Changes**.

---

**Portlet Permission Manager**

Permissions / Blog: Math Department

<table>
<thead>
<tr>
<th>Name</th>
<th>edit_blog_categories</th>
<th>edit_blog_entries</th>
<th>file upload</th>
<th>edit_blog_properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone - Staff</td>
<td>Deny</td>
<td>Grant</td>
<td>Grant</td>
<td>Deny</td>
</tr>
<tr>
<td>User, Admin</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
</tr>
</tbody>
</table>

Display: All | Active Permissions | Inactive Permissions

Display 16 Per Page

Add Remove
Save Changes Cancel

1 - 2 of 2 Rows | Prev | Next | List
Briefcase Portlet

The Briefcase Portlet provides web enabled file storage for users. It can also provide a web based access point to Network Folders and Personal LDAP folders depending on the configuration of the institution. The portlet permission manager allows controls to be set on users briefcase use.

The briefcase has five administrative privileges:
- **View** - Users with this privilege have the ability to view files and folders accessible via the briefcase
- **Add** - Users with this privilege have the ability to add files and folders to the directories accessible via the briefcase
- **Delete Files** - Users with this privilege have the ability to delete files and folders in the directories accessible via the briefcase
- **Edit Files** - Users with this privilege have the ability to edit files and folders in the directories accessible via the briefcase
- **Share Folders** – User with this privilege have the ability to share briefcase folders with other users

To establish permissions for the briefcase portlet:
1. Navigate to the Portlet Permission Manager Channel.
2. Click the link for the Briefcase Portlet.
3. Click the Add button to select the users and groups to whom permissions will be granted.
4. You may select members and groups in one of two ways: you may search for specific members or groups, or browse through the directory of Campus Groups, your own Personal Groups, or individual Members.
5. To search for a specific member or group:
   a. Enter a whole or partial member or group name of the in the Search field.
   b. Click the Go button.
   c. From the list of search results, place a checkmark next to each member/group that you wish to add.
   d. Click the Add to My Selection Basket button.
6. To browse through the listings of Campus Groups or your Personal Groups:
   a. Click the Groups tab within the permission portlet.
   b. Choose Campus or Personal Groups.
   c. Find the group you wish to add.
   d. Place a checkmark next to the group name.
   e. Click the Add to My Selection Basket button.
7. When all desired groups and members have been selected, click the Submit My Selections button.
8. For each group or individual displayed in the permissions view, select the appropriate permission.
   a. Grant - Enables the group/user to perform the function
   b. Deny – Prohibits the group/user from performing the function
   c. Defer – Causes the group/users privileges to be inherited from those set for a parent group of which they are a member. If no privileges have been set for a parent group, defer will be treated as a permission of Deny.
9. When all permissions have been assigned, click Save Changes.

## Permissions / Briefcase Portlet

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>VIEW</th>
<th>ADD</th>
<th>DELETE</th>
<th>EDIT</th>
<th>SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Everyone</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
</tr>
<tr>
<td>✔️</td>
<td>Everyone - Staff</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
</tr>
<tr>
<td>✔️</td>
<td>Everyone - Students</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
<td>Grant</td>
</tr>
<tr>
<td></td>
<td>Student, Doug</td>
<td>Defer</td>
<td>Defer</td>
<td>Defer</td>
<td>Defer</td>
<td>Grant</td>
</tr>
</tbody>
</table>

Display: All | Active Permissions | Inactive Permissions

Add | Remove

Save Changes | Cancel
Notification Portlet

The Notification Portlet allows users to compose notifications online or import notifications from other systems. These messages are distributed to targeted individuals and groups.

The notification portlet has eight user permissions:
- **Attach** - Users with this privilege have the ability to attach files when composing a notification.
- **Delete** – Users with this privilege have the ability to delete messages to which they have access. For most users this will mean messages in their personal inboxes and save folders. For users also granted View All privileges, they will be enabled to delete any notification in the system.
- **Compose** - Users with this privilege have the ability to compose and send notifications.
- **Save** – Users with this privilege have the ability to Save notifications from their inboxes to a Save folder.
- **Import** – Users with this privilege have the ability to import a file of notifications and distribute their notifications.
- **Export** – Users with this privilege have the ability to export notifications, including the detailed report information on the read/unread status for each message recipient.
- **Detail Report** – Users with this privilege have the ability view a report for notifications they have send which detailed the read/unread status for each recipient.
- **View All** – User with this privilege have the ability to view all messages in the system. Combined with other privileges these users can view, delete, and/or export any notification.

To establish permissions for the notification portlet:
1. Navigate to the Portlet Permission Manager Channel.
2. Click the link for the Notification Portlet.
3. Click the Add button to select the users and groups to whom permissions will be granted.
4. You may select members and groups in one of two ways: you may search for specific members or groups, or browse through the directory of Campus Groups, your own Personal Groups, or individual Members.
5. To search for a specific member or group:
   a. Enter a whole or partial member or group name of the in the Search field.
   b. Click the Go button.
   c. From the list of search results, place a checkmark next to each member/group that you wish to add.
   d. Click the Add to My Selection Basket button.
6. To browse through the listings of Campus Groups or your Personal Groups:
   a. Click the Groups tab within the permission portlet.
   b. Choose Campus or Personal Groups.
   c. Find the group you wish to add.
   d. Place a checkmark next to the group name.
   e. Click the Add to My Selection Basket button.
7. When all desired groups and members have been selected, click the Submit My Selections button.
8. For each group or individual displayed in the permissions view, select the appropriate permission.
a. Grant - Enables the group/user to perform the function
b. Deny – Prohibits the group/user from performing the function
c. Defer – Causes the group/users privileges to be inherited from those set for a parent group of which they are a member. If no privileges have been set for a parent group, defer will be treated as a permission of Deny.

9. When all permissions have been assigned, click Save Changes.