Luminis Platform

Administration Guide

Release 5.3
March 2016

Notices

In preparing and providing this publication, Ellucian is not rendering legal, accounting, or other similar professional services. Ellucian makes no claims that an institution's use of this publication or the software for which it is provided will guarantee compliance with applicable federal or state laws, rules, or regulations. Each organization should seek legal, accounting, and other similar professional services from competent providers of the organization's own choosing.

Ellucian
4375 Fair Lakes Court
Fairfax, VA 22033
United States of America

Contents

Introduction

Administration involves information about the processes necessary to configure Luminis® Platform after you have completed the installation and integrated the system with Banner®.

Included are details about the general system architecture and technology, its use and value in the Luminis applications and tools, and instructions for customizing the system for your institution.

Luminis Platform is compatible with Google and Microsoft Office 365 calendar and e-mail systems, and Learning Management Systems such as Blackboard and Moodle. Instructions for integrating with those products are also included in this guide.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want submit a feature request or problem with the software, contact Ellucian Customer Support.

Luminis Platform Architecture and Component Overview

Details about the general system architecture and technology, and its use and value in the Luminis applications and tools.

If you have additional questions about Luminis® Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

This section describes the various servers and systems used in Luminis Platform. It also provides an overview of the architecture and various components in Luminis Platform.

Note: Luminis Platform does not provide any type of default denial of service protection services. It is expected that the application is protected by network software and services.

Luminis Platform architecture overview and technology

Luminis Platform is almost entirely services oriented. Web services and RESTful services are used throughout the product. Development efforts and the markup in the form of portlets is entirely Web-services based.

The system provides modularity and application isolation as a standard practice. Luminis Platform is no longer tightly integrated with infrastructure pieces such as the database, mail server, calendar server, or portal server software. This approach creates flexibility and modularity throughout the system providing flexible installation, simplified configuration, and logical system troubleshooting.

Luminis Platform leverages technology standards as much as possible. Standards around content, data services, security, and administration now represent and drive key parts of the solution.

Table 1: Example Luminis Platform architecture

Example	Description
JSR-286 portlet standards	Allows clients to build content according to standard specifications and consume conforming portlets.
Central Authentication Service (CAS)	An open and well-documented authentication system that acts as the basis for user authentication and an available method for external system integration.
Lightweight Content Management System	Based on Jackrabbit, which implements the Java Content Repository (JCR) API.
Tomcat Application Server	Used as the baseline application server.
SPRING	A lightweight container used to manage integration related to data objects, Java

Example	Description
	Message Service (JMS) connections, and directory access.
RESTful Services	Published using an Apache CxF and support the RESTful standard JSR-311.
Java Management Extensions (JMX) Beans	Implemented for instrumentation, system monitoring, and centralized configuration management.
Java API for XML Web Services (JAX-WS)	Allow the system to work with Web services security tools that may be in use in certain client networks.
Java Persistence Architecture API (JPA)	Provides abstraction from the database to support a number of prominent database applications.
Security Assertion Markup Language (SAML)	A method within the Luminis Platform security protocol stack that helps supports baseline integration with GoogleApps.

Luminis Platform is based on the Spring framework and Java. It uses the industry standard configuration mechanisms of XML files combined with the application user interface (UI) layer through the data representation layer. Spring MVC supports many of the UI elements through RESTful services with Bean-based models that support data access objects and various configuration options. The JMX container that is a standard part of Tomcat contains a configuration Mbean that is accessible from a JMX UI (jconsole) or from an API. This configuration Mbean retrieves values from the directory server in support of centralized storage of select property, configuration and settings values.

Data is stored in three locations in Luminis Platform:

- Database
- Directory server
- Disk storage

The tested and certified databases are outlined in the product material. The Luminis Platform architecture uses hibernate and the ORM (Object Relational Mapping) model to abstract the business logic and data management objects from the database. Although formal testing and certification is completed against a few select databases, this architecture theoretically allows for a broad selection of databases. The directory server is equally abstracted by an object layer and is a Spring configured data source. The overall long-term intent is to support any LDAP v3 compliant directory. Files are also stored on disk in the Luminis repository and are managed by the jackrabbit JCR-based content storage solution. This provides a simplistic but functional content system with check in and check out and ownership associations.

Luminis deployment inside Tomcat

Luminis Platform deploys within Tomcat using Spring to manage the deployment and dependency management.

Industry standard technologies used in Luminis Platform

Luminis Platform implements a number of industry standard technologies to help ensure the system is open and easy to implement and integrate across a variety of computing environments.

Object Relational Mapping

Object Relational Mapping (ORM, O/RM, and O/R mapping) in Luminis Platform is used as a technique for converting data between incompatible type systems in relational databases and the platform object model.

Hibernate is the current ORM of choice due to its position as an industry leader and because it is compatible with Liferay. Although Luminis is heavily dependent upon ORM for database abstraction, Luminis is isolated from Hibernate by the Spring Frameworks object management implementation.

Data Access Objects

The Data Access Objects (DAO) define the domain model for Luminis Platform and represent every table in the database in object form. A modification to an underlying table can cause failure of system startup because the objects have a direct relationship to the database schema.

Java Management Extensions

JMX provides a means for a console-based application to remotely access and control and application server over the network. Luminis Platform takes advantage of JMX technology to expose services and administrative functions.

Java Management eXtensions (JMX) is a standard protocol for managing and monitoring applications and services in Java. The Java Virtual Machine (JVM) provides a set of standard features for any application, and custom *mbeans* can also be created for managing application specific features.

In a basic JMX console operation, an administrator runs a JMX-enabled console, which attaches over the network to a server in a Luminis Platform deployment. From the console, the administrator can change configuration and monitor statistics of the running server without disturbing its operation. Multiple nodes may be monitored simultaneously.

Connections to the JMX port on Luminis servers are secured by default with a username and password supplied in the installation configuration properties file. Additional security may be added using a file-system configuration for additional users. JMX users can be given read-only permission, or permission to read and write using a JMX port.

Because JMX is a standard, any JMX-enabled management console can be used to connect to the JMX ports in the Luminis deployment. Some commercially available network management consoles are IBM's Tivoli or CA Unicenter. Other open source consoles are also available, such as jManage or MC4J. In general, examples in this guide will be shown using the console shipped with the Java JDK: JConsole.

Java Connector API

Java Connector API (JCA) is a solution for connecting application servers and Enterprise Information Systems (EIS) as part of Enterprise Application Integration solutions. While Java Database Connectivity (JDBC) is specifically used to connect Java EE applications to databases, JCA is a more generic architecture for connection to legacy systems, including databases.

Examples of EIS are enterprise resource planning, transaction processing systems, legacy database systems and so on.

Java Messaging System

A messaging system allows separate, uncoupled applications to reliably communicate asynchronously. The messaging system architecture generally replaces the client/server model with a peer-to-peer relationship between individual components, where each peer can send and receive messages to and from other peers.

Messaging systems provide a host of powerful advantages over other, more conventional distributed computing models. Primarily, they encourage loose coupling between message consumers and message producers. Other advantages of messaging systems include high scalability (commercial implementations boast the ability to support tens of thousands of clients and tens of thousands of operations per second), easy integration into heterogeneous networks, and reliability due to lack of a single point of failure.

There are two primary message system types:

Type	Description
Publish or Subscribe	Supports an event-driven model where information consumers and producers participate in the transmission of messages. Producers publish events, while consumers subscribe to and consume the events. Producers associate messages with a specific topic, and the messaging system routes messages to consumers based on the topics the consumers register interest in.
Point-to-Point	Messages are routed to an individual consumer, which maintains a queue of incoming messages. Messaging applications send messages to a specified queue, and clients retrieve messages from a queue.

The Java Message Service (JMS) API is a messaging standard that allows application components based on the Java 2 Platform, Enterprise Edition (J2EE) to create, send, receive, and read messages. It enables distributed communication that is loosely coupled, reliable, and asynchronous.

Spring framework

Luminis Platform uses the Spring Framework as a core solution in many product areas. The component areas of Spring provide a variety of solutions to technical issues and implementation choices resulting in a more uniform mechanism for managing configuration and deployment options.

Spring integration provides services for JMS, remoting, scheduling, email, lifecycle management, transaction management, event publication and subscription, and transaction management.

Asynchronous JavaScript and XML

Asynchronous JavaScript and XML (AJAX) combines coding with HTML, JavaScript, and XML, allowing interaction between the client and server to occur asynchronously.

The asynchronous element means that a user's interaction with the interface is not interrupted by page refreshes every time the server is called upon to do something.

Adobe FLEX

Adobe Flex is a free, open-source platform and component library for developing applications that can be deployed on Adobe Flash Player.

An Adobe Flash player is a powerful application platform. Flex, in comparison to the Flash IDE, is a more flexible development framework to build applications for the Flash and AIR runtime environment. Additionally, Flex opens up new design possibilities by enhancing standard Web browsers with the Adobe Flash technology on which Flex is built. Flex is specifically geared towards building robust, Rich Internet Application (RIA) solutions that deliver immersive experiences and behave with interactivity and user engagement similar to desktop applications.

Adobe Flex is used sparingly throughout Luminis Platform. It is used for select Admin portlets only.

Lightweight Directory Access Protocol

Luminis Platform makes use of a Lightweight Directory Access Protocol (LDAP) Directory server for the storage of some user information and for authentication.

In the default installation, the Luminis CAS server is configured to authenticate against an OpenDJ directory server. Luminis may also be configured to operate against other LDAP V3 compliant servers.

Relational database

Luminis Platform makes extensive use of a relational database (RDB) for the storage of data needed for system operation.

The database is accessed using an industry standard data access layer called Hibernate. Luminis may be run against different RDBs. For more information on supported RDBs and versions, refer to the *Luminis Platform Release Notes*.

On installation, Luminis creates many tables for storing system data related to users, groups, roles, and permissions, as well as application data for all the Luminis portlets. Liferay also creates a number of tables for storing portal-related data for layouts, portlet configuration, users, and all the Liferay-supplied applications. Luminis tables in the database will start with the prefix *LP_*. All other tables in the schema provided for Luminis operation will be Liferay-related tables.

Components of Luminis Platform Deployment

Depending on the deployment model, the following Luminis Platform components will be installed across one or more servers.

Database

The data storage requirements for Luminis Platform can be addressed by an enterprise database with schema storage providing approximately two Gigabytes or more storage space in the database.

The database installation should be provided by a database vendor and is beyond the scope of this document.

Directory

The default baseline directory server included in Luminis Platform is the Open Lightweight Directory Access Protocol (LDAP) server, which provides a lightweight LDAP V3 compliant data store for user records and credentials for authentication.

The Central Authentication Service (CAS) server and the portal server both read from this data store, and the administration server reads and writes to this data store.

CAS

Luminis Platform leverages the Jasig CAS solution to provide centralized Single Sign On (SSO) between the Luminis portal and the Luminis administrative servers.

CAS is also a central point of integration for Banner® when using the Banner Enterprise Identity Services (BEIS) solution. The CAS server is currently installed using version 3.5.2. For more information on Banner integration, refer to the *Luminis Platform Banner Integration Setup Guide*.

Administration server

When users log into Luminis Platform, membership in the Luminis Administrators Group will result in them being redirected to the administration server.

The administration server is a Tomcat server with the Liferay portal framework, Luminis application portlets, and administrative portlets. This server acts as the primary point of administration for the entire installation.

Portal server

When users log into Luminis Platform, they will be directed to a portal server (if not a member of the Luminis Administrators Group). This is the student facing server and will have limited administrative functions available.

The portal server is also a Tomcat server with the Liferay portal framework and the Luminis application portlets. This server acts as the primary point of contact with the end user population.

Outsourced e-mail and calendar

In the deployment models, the mail and calendar servers are deployed in the cloud to represent the trends in e-mail hosting.

This is not meant to preclude other possible on premise configurations for both e-mail and calendar.

Documents and Media Repository

By default, the Luminis Platform installer for 5.1 and beyond will configure Liferay's Document Library to point to a Jackrabbit repository configured to store documents in the Luminis database.

Luminis shares the CMS repository with Liferay for the **Documents and Media**, **Targeted Content**, **Luminis Announcements** portlets and others. Apache Jackrabbit is a fully conforming implementation of the Content Repository for Java Technology API (JCR).

Jackrabbit is used as a Content Management System (CMS) or Web Content Management (WCM) for Luminis Platform sites and users. It is intended to be as invisible as possible, but still provide ownership and content control for sites and courses.

When a file is uploaded, the system calls the jackrabbit to track and manage the file. Files uploaded with Luminis Platform version 5.1 and beyond will share the Liferay Jackrabbit repository.

You can find the Jackrabbit configuration files at the following location for the administration and portal servers respectively:

```
$CP_ROOT/products/liferay/liferay-admin/data/jackrabbit/repository.xml
$CP_ROOT/products/liferay/liferay-portal/data/jackrabbit/repository.xml
```

To change the Jackrabbit repository configuration to store documents to a shared file system, refer to the Jackrabbit documentation located at http://jackrabbit.apache.org/.

Liferay 6.1 offers several options for the Document Library repository for clustered deployments, including an advanced file system store, CMIS store, or Amazon or Documentum stores. To implement one of the other repository options please refer to the "Liferay Clustering" section in the *Liferay Portal 6.1 – User Guide* located at http://www.liferay.com/documentation.

Deployment Models

You can customize your deployment, combining or separating components on multiple servers, to fit the needs of your institution.

Single-box deployment

The simplest form of deployment is on a single box, where all components are installed onto a single computer with all references to services and server components residing on the same local machine.

All components in this model run under a single server and an operating system instance. The components install directly from the Luminis Platform installer with only the database component requiring a separate installation process. This model, while convenient to install and simple to configure, has very limited performance potential, unless configured with a large multi-core server system. Although this is the least powerful deployment model, it is the baseline development deployment. All components are configured under the same domain and differentiate themselves within the domain by means of alternate port usage.

Multi-box deployment

The multi-box installation is similar to the single-box installation, but the database and directory server are installed on external, dedicated machines.

This is a standard department-level deployment where the application is targeted at a small group of users without a high volume of concurrent use.

This configuration is supported by the Luminis Platform installer by reconfiguring the target nodes in the setup configuration. Each node can be configured individually to install the proper components for a given server. The figure above shows the directory manager as a separate component running the LDAP instance on the same server as the administration server instance to evenly divide the components between three boxes. This would require separate installation files for each server, one with portal and CAS configured, another with the admin server and LDAP configured, and a third containing the database. Once again the database installation is independent of and not included as part of the Luminis Platform installation.

This model's separation of server components provides more stability and scalability.

Cluster deployment

Cluster deployment allows you to separate and install system components to better manage failover and increase performance.

Cluster deployment utilizes a load balancer, which, like the database, is a component that is purchased, installed, and managed separately from the Luminis Platform. There are no recommendations about how to install and configure the load balancer. We assume that it will be done by a network administrator who understands your load balancer and how set it up for components based on your network topography.

Cluster deployments are intended for support of large user populations. Properly scaling the platform and servers to match the needs of the user site is an exercise that should be part of deployment planning.

How Liferay is used in Luminis Platform

Liferay is an enterprise portal, also known as an Enterprise Information Portal (EIP) or Corporate Portal, which is a framework for integrating information, people, and processes across organizational boundaries.

Liferay provides a secure, unified access point in the form of a Web-based user interface, and is designed to aggregate information through application-specific portlets.

Luminis Platform uses the Liferay portal as its underlying portal server framework. The Luminis Platform offering includes a set of tools, customizations, and content applied to the Liferay portal framework to create a specific portal environment that meets the unique needs of higher education institutions. Luminis customizes Liferay by adding, replacing, overriding, and extending functionality within the baseline portal framework in the following ways:

- The addition of higher education related content and applications
- Overall data and presentation layer integration with backend Enterprise Resource Planning (ERP) systems
- The ability to regularly update relationships and roles based on the changing status of a user in the institution. For example, content and portal view should dynamically change as students move from freshman through their senior year. This changing state of persona is unique to higher education and is not well addressed by corporate or public portals.
- The addition of sites and course constructs to meet the needs of providing content for academic courses. Content created for courses are like other sites, but have unique rules and relationships that do not exist by default in portal products. If a simple logo change is required, please keep the logo's height no more than 40px and width no longer than 300px. Good design practices are required.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Core System Set Up and Maintenance

Luminis® Platform system provides a number of administrative tools for managing, configuring, and monitoring a Luminis deployment.

Each installation contains an administrative server instance, where intensive operations are performed separate from the user portal.

Luminis Platform administrative overview

The administrative server is a full instance of the Luminis portal, but also contains special administrative portlets and JMX functions that are not available on the user portal.

All layouts and pages deployed to Luminis users are available to administrators, but normal users cannot access administrative functions.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Luminis Platform administrative interfaces

The key administrative interfaces are:

- Administrative portlets available to administrators, site owners, and other authorized portal users to manage system elements such as users, roles, and dynamic groups, as well as site related administration including the management of collaboration tools, members, approval processes, and content submission.
- Luminis Platform provides an industry-standard JMX interface, which may be accessed using any JMX-enabled management console. Luminis exposes through JMX the management of configuration values, monitoring and control of Luminis caches, and import of LDIS-compatible data files.
- Luminis Platform provides commands that are available through an administrative interfaces of the command line tools, which are used for administrative functions. The command line operations include system startup, shut down, and version identification.

Related Links

Administrative portlets on page 25

Access admin server

The Luminis Platform system employs an automatic redirect function for administrators accessing the Luminis system.

If a user is a member of a specified administrator-server dynamic group, then logging in to the portal will automatically redirect the user to the admin server. Conversely, if users who are not members of the administrative-server dynamic group attempt to log in to the admin server directly, they will automatically be redirected back to the main portal server.

Admin server access group

Those who need access to the admin server functionality, even if they have minimal delegated admin rights, must be a member of the dynamic group AdminServerAccessGroup.

Whenever administrators wish to delegate a particular user to have permission to perform administrative functions, they must either:

- Modify the dynamic group AdminServerAccessGroup to have an expression that will include the user in question.
- Add a role or other attribute to users so that they become members of the existing AdminServerAccessGroup by definition.

Administrative portlets

A number of portlets are deployed only to the Luminis Platform admin server specifically for administrative operations, though some may be used for both user and administrative functions.

These include:

- Luminis Announcements (User and Admin)
- Luminis Calendar Configuration
- Luminis Site Request Approval
- Luminis Group Manager
- Luminis External Services Configuration
- Luminis Mail Configuration
- Luminis Permission Grant Manager
- Luminis Role Management
- Luminis User Management
- Session Management Console
- Single Sign-on Configuration
- System Monitor
- System Question or Answer Password Recovery

Each of these will be described in detail in the sections that follow.

Note: Adobe Flash is a prerequisite for using the administrative portlet and only supported on 32-bit browsers.

Related Links

Luminis Platform administrative interfaces on page 24

Configuration management with JMX

How to manage JMX within Luminis Platform.

Related Links

Manage user roles through JMX on page 218

Monitor and control components from a JMX-capable console

An administrator can manage configuration values, monitor and control Luminis caches, and import LDIS-compatible user and course files in the Java Management Extensions (JMX) interface for configuration and management.

JMX enables monitoring and control of components from a remote JMX-capable console. In this document, the Sun Java JConsole is used for all examples. Other enterprise network management consoles such as IBM's Tivoli or CA Unicenter may also be used if they are JMX enabled or use an SNMP to JMX adapter. For more information about the JMX standard, see http://java.sun.com/javase/technologies/core/mntr-mgmt/javamanagement/.

Access JMX through a firewall

JMX RMI connector allows you to access JMX through a firewall.

If you use a standard connector, it will not allow you to access through a firewall, because it communicates to the jConsole a different, random port to find the information jConsole displays to you. Since this port is random, it is usually impractical to open up enough ports on your firewall to ensure that jConsole can receive the information. Hence, you would need to use the MX RMI connector.

The JMX RMI connector allows you to specify the ports that jConsole will use to get the information.

JMX RMI connector installation settings

When you run the installer, you can use properties in your `setup.properties` file to set the admin and portal servers.

By default, Luminis sets the ports to 9101 and 9201 for the portal servers and 9102 and 9202 for the admin server. These are the properties and their defaults:

```
admin.jmx.rmi.registry.port=9102
admin.jmx.rmi.server.port=9202
portal.jmx.rmi.registry.port=9101
portal.jmx.rmi.server.port=9201
```

You can set these properties depending on the type of installation. You then can open up these ports on your firewall and you will be able to access JMX from outside the firewall.

To access the external connector, you have to use a specially formatted RMI URL in jConsole. The URL is in the form:

- For admin server

  ```
  service:jmx:rmi://${admin.host}:${admin.jmx.rmi.server.port}/jndi/
  rmi://${admin.host}:${admin.jmx.rmi.registry.port}/server
  ```

- For portal servers

  ```
  service:jmx:rmi://${portal.virtual.host}:
  ${portal.jmx.rmi.server.port}/jndi/rmi://${portal.virtual.host}:
  ${portal.jmx.rmi.registry.port}/server
  ```

  The portal server URL will not send you to a specific node in your portal cluster. It will send you to whatever node your load balancer assigns you to. To access a specific portal node, you will have to be behind the firewall and access JMX on that node directly. For example, if your admin server is admin.luminis.edu and your portal virtual server is portal.luminis.edu. To access the admin server, you must use the following URL and enter the name and password in the appropriate fields:

  ```
  service:jmx:rmi://admin.luminis.edu:9202/jndi/rmi://
  admin.luminis.edu:9102/server
  ```

  To access JMX for your portal cluster, you must use the following URL:

  ```
  service:jmx:rmi://portal.luminis.edu:9201/jndi/rmi://
  ortal.luminis.edu:9101/server.
  ```

  You must enter your admin name and password in the appropriate fields.

Manage JMX-enabled Java in JConsole

JConsole is a Java-based standard console for managing JMX-enabled Java s.

About this task

JConsole is shipped with the Java JDK and may be found in the `bin` directory of the Java installation.

Procedure

1. Launch JConsole from the command line or from the Windows Explorer.
   - `jconsole` on Linux or Solaris
   - `jconsole.exe` on Windows
   - **Note:** JConsole is installed with the Java JDK when installing Luminis Platform. Otherwise, install JDK 6.0 or greater versions of Sun from http://java.sun.com/.

     Install JConsole on the computer where the administrator works to get the remote managing value.

2. After you start the JConsole, select the required server in the **Java Monitoring and Management Console - New Connection** page to connect using your login credentials. By default, the Luminis JMX port is configured with the username and password that was specified during installation for the administrator.

   All Luminis portal servers are configured to accept connections for JMX on port `9001`. The Luminis administration server is configured to use the port `9002`.

   Note: Review "Java Management Extentions" and perform suitable changes to the installation.

Results

Once logged in, you are presented with a summary screen. This summary presents graphs of some of the JVM parameters that can be monitored and managed in JConsole.

Related Links

Java Management Extensions on page 17

Monitor Luminis JVMs with jconsole on page 36

Luminis configuration management

The Luminis portal configuration values are accessed using a custom JMX mbean found on the **MBeans** tab of the JConsole.

Open the **Luminis** folder and then the **ConfigurationService** folder. Under the **ConfigurationService** folder you see two sub-headings:

Sub-heading	Description
Attributes	Read-only functions used to show configuration values and other information about the Luminis configuration sub-system, such as, the category names and the default write category.
Operations	Used to read, search for, and set the configuration values.

Configuration value categories

Configuration values in Luminis Platform are stored in categories.

The categories are:

- Default
- Install
- Site

The majority of administrative operations will be done on the site category, and this is the category that will be used if no category is specified. In general, an administrator should not change a value in the default or install categories unless directed to do so by a trained support engineer. However, it is valuable to know how categories operate to understand which values are being read and used by the Luminis system.

Categories are evaluated hierarchically. The configuration sub-system looks for a value in the site category first. If it is not found, it will look in the install category, followed by the default category. Categories exist primarily to aid in patching and migration, so the system can determine:

- Which values were set intentionally by an administrator
- Which were set during the installation process
- Which were set as defaults by product development

The category names are available from the `ConfigurationService` mbean, under **Attributes** > **CategoryNames**.

Similarly, you can also view the DefaultWriteCategory attribute.

Find and read configuration values

Configuration values may be read using one of the `ConfigurationService` mbean Operations.

About this task

To find the name of the configuration value:

Procedure

1. In the **Java Monitoring & Management Console**, **MBeans** tab, Operations, select **getString**.
2. Enter the name of the configuration key.

   If you do not know the exact configuration key name, the `getMatching` method is used to find all the configuration keys that matches a given string. For example, to find all keys that have password key, you must enter password in the **getMatching operation** field to list all the matching keys.

   Complex matching patterns such as, password*max can be used to find all keys that contain both password and max.

   Note: The `getString` operation evaluates the category hierarchy to determine which configuration value to show for a given key.

   - If you need to see what value is in a particular category, use the `getUnresolvedString` operation.
   - Configuration values may consist of literal strings as well as macros, which are specified using the following syntax:

     ```
     ${some.other.key}
     ```

   - The `getUnresolvedString` operation allows you to see the un-evaluated macro value, and must be done on a specific category.

> **Note:** When using macros, the macro referenced by a value must be valid, or the `getString` operation will return # no such key #, even though the key asked for exists technically.

For example, setting the key `my.test.string` to `my value is ${another.key}` will attempt to resolve `${another.value}` and insert it into the value for `my.test.string`. So if another.key=some other value, then `getString` on `my.test.string` will return my value is some other value.

- Using the `getUnresolvedString` operation will return my value is ${another.key}

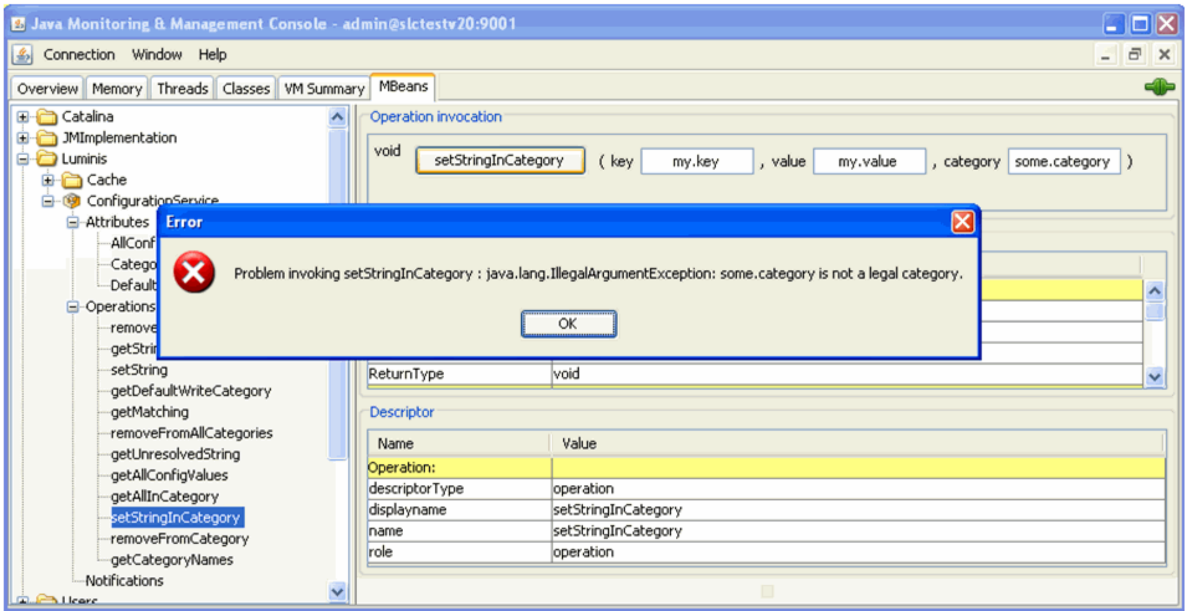
Set configuration values

Configuration values may be set in the default category (site) using the **setString** operation, or in a particular category using **setStringInCategory**.

To set a string in the default category (site), enter key and value in the **setString** fields.

Note: If you enter a non-existent category, an error will occur.

Figure 1: Non-existent Category Error



Java Monitoring & Management Console - admin@slctestv20:9001

void setStringInCategory (key my.key , value my.value , category some.category)

Error

Problem invoking setStringInCategory : java.lang.IllegalArgumentException: some.category is not a legal category.

OK

ReturnType	void

Name	Value
Operation:	
descriptorType	operation
displayname	setStringInCategory
name	setStringInCategory
role	operation

Remove configuration value

Configurations values may be removed by using the `remove` operation.

Procedure

1. To remove a value from a particular category, use **removeFromCategory**. You can also remove a value from all categories at once using **removeFromAllCategories**.
2. If you attempt to remove a non-existent value, the console will execute the command **successfully**, but give no indication that the value did not exist previously. Thus, in order to avoid an error by removing a value that does not exist, verify that the configuration value is removed using the `getString` operation.

Miscellaneous configuration operations

You can view all the configuration values at once, and see the category names and default write category.

The attributes available under the **ConfigurationService** > **Attributes** sub-headings are also available under the **Operations** sub-heading. This is an artifact of the way mbeans are specified. Additionally, you may view all the configuration values in a specific category using the operation **getAllInCategory**.

Import LDISP or IMS data with jconsole

Luminis Data Integration Suite Protocol (LDISP) format files can be imported into the Luminis system using the JConsole **IMSFileImporter** mbean.

It is executed using **importFile** found under the Luminis folder **IMSFileImporter** node under Operations.

Enter the full path name of a file located on a server that connects to the JConsole. Once the file is in place, you can simply select the **importFile** button to start the import. When the file has finished importing, the system will display the number of users imported.

Monitor import progress

The import process will send notifications while it is running. You must subscribe to the `IMSFileImporter` bean to receive the import notifications.

Procedure

1. Select **Notifications** from the IMSFileImporter node.
2. Click **Subscribe**.

   Once you click **Subscribe** button, you will see the **Notifications** change to show the number of notifications that have been received.

Results

You will receive notifications when the import process starts and each time a group of 10 records are imported until the import finishes. Notifications are displayed from the **Notifications** node.

Manage caches in Luminis

Caching in Luminis and Liferay, how caches may be monitored and reconfigured, and trade-offs to consider in cache configuration.

Data in the Luminis system is cached and reused to increase performance and reduce database transactions. While the system has been tuned by Ellucian® engineers to provide good performance in many situations, a customer's workload may perform better if the cache's configuration were modified.

Caching works in response to a user's request. It keeps frequently requested information in memory rather than requesting the data from the database or directory every time it is called for by code. The more data kept in memory the faster the performance will be. The trade-off between the performance that may be gained with larger caches is that the memory taken from the Java heap to store the cached data is affected. Memory used for caching will not be available for other purposes, which may impact overall system performance with more frequent garbage collection. Also, if the saved data is not re-used, then the caching process is wasted overhead. You should consider that when you decide whether to cache data and how large the cache should be. Luminis Platform provides a JMX Mbean for viewing the cache configuration and the statistics for each cache in the system.

Liferay also makes use of caching, and the configuration of both Luminis and Liferay caches has been combined into one file for common cache management. Both make use of EHCache, an industry-standard caching solution, as the cache implementation. Liferay may be configured to cache data at the value object level as well as the Hibernate database access level. The stock Luminis configuration has allocated space for the most frequently-used Liferay value-object entity and finder caches, but has disabled the Hibernate-level caching. Through performance testing, Ellucian has discovered that properly configured finder/entity caches obviate the need for lower-level (Hibernate) caching. Also, enabling Hibernate caching would require significant system re-configuration that is not recommended by Ellucian.

Clustering

Because the minimal installation requires both a portal and an admin server, Luminis caching is configured out-of-the-box to work in a clustered environment.

Luminis makes use of EHCache cluster invalidation to notify all nodes when a cache entry has changed. Depending on how the system was configured during installation, you can complete this invalidation through either UDP Multicast, or TCP point-to-point connections (see the *Luminis Platform Installation Guide* for the appropriate configuration values). Multicast is a more efficient algorithm to service large numbers of nodes, but may be unavailable in some network environments as frequently encountered using cloud-based hosting. EHCache cluster invalidation allows each node to re-load a cache entry with the latest data if you plan to reuse it.

Note: Some caches are configured to use cross-node invalidation, and many are configured to simply allow entry expiration to re-load changed values.

The caches configured for cluster-invalidation, such as the shared configuration cache, were selected for their need to more quickly reflect changes across the cluster. Administrators may decide to include more caches in the cluster-invalidation scheme to affect faster cross-node updates. However, each cache that generates invalidations adds to the network traffic and the time every node spends servicing invalidation requests which may not be applicable to their cached data. Administrators are advised to monitor performance carefully if additional caches are configured to be distributed in the cluster.

Another consideration when enabling cross-cluster invalidation is data coherence among related cached data. For example, if the User cache is enabled for cluster invalidation, and the Role cache is not, when an update on the administrator node occurs for a user (including the user's roles), the user data on other nodes will be invalidated but the role data will not. The role data will only be updated after the data in the Role cache times out. Therefore, there would be a window of time when the user data on the other node would not be in sync with the role data. Related data in separate caches should be enabled for cross-cluster invalidation together. It is important for the administrator configuring the caches to understand the relationship between different data sets before enabling cross-cluster invalidation.

Cache Configuration

Cache configuration for both Luminis and Liferay is done in the Spring configuration file:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/webapps/ROOT/META-INF/
luminis-cache-impl-applicationContext.xml
```

This file must be modified on each node in the system for the changes to take effect on that node. Caches of similar behavior are grouped so that changes may be made to all of the files at once rather than having to specify parameters for each cache individually. The top level cache configuration bean is as follows:

```
<bean id="cachingServiceImpl"…>
```

This configuration bean contains references to the configured cache groups, the default cache (to use if no explicit cache is allocated), and a list of disabled caches. The disabled cache list prevents the cache system from allocating a cache when requested because it has been determined that the cache has such a low utilization or hit rate that it is not efficient to even attempt caching for that item.

```
<property name="disabledCacheIds">
<list>
<value>com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay.
portal.model.impl.ResourceActionImpl</value>  <!-- low hit rate - don't
 use -->
…
```

Each cache group is configured as in the following example:

```
  <bean id="userRelatedCaches"
 class="com.sghe.luminis.cache.impl.CacheGroup">
    <property name="cacheIds">
      <list>
       <value>CompositePersonCache</value>
<value>com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay.
portal.model.impl.ContactImpl</value>
<value>com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay.
portal.model.impl.GroupImpl</value>
<value>com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay.
portal.model.impl.UserImpl</value>

 <value>com.liferay.portal.kernel.dao.orm.FinderCache.Users_Orgs</
value>

 <value>com.liferay.portal.kernel.dao.orm.FinderCache.Users_UserGroups</
value>
       <value>BRMFactsAttributeCache</value>
      </list>
    </property>
      <property name="template">
          <bean class="com.sghe.luminis.cache.impl.EHCacheCache">
              <property name="maxSize" value="5000" />
              <property name="expirationInSeconds" value="900" />
              <property name="ehcacheConfig" ref="ehcacheConfig" />
              <property name="distributed" value="false" />
              <property name="statisticsEnabled" value="true"/>
          </bean>
      </property>
  </bean>
```

The `template` property is used to define the cache that will be allocated for each of the caches defined in the `cacheIds` list.

Table 2: Template properties

Property	Definition
`maxSize`	Maximum number of objects that may be held in the cache. If you attempt to put more objects in the cache, the item used least recently will be evicted.
`expirationInSeconds`	Regardless of the number of objects in the cache, the value will expire after this length of time and require it to be reloaded from its respective data store.
`ehcacheConfig`	Reference to a separate base configuration for the EhCache implementation which is defined elsewhere in the file. It is not recommended that the EhCache configuration be changed.

Property	Definition
`distributed`	If true, new objects placed in the cache will cause invalidations for that object to be sent to other nodes in the cluster.
`statisticsEnabled`	If true, statistics showing the number of hits, misses, total size, and hit rate will be collected and made available for viewing via the JMX MBean described later in this document.

The most common changes for a cache are likely to be for the maximum size (allocate room for more entries) or the expiration time. If the distribution has not been enabled, a lower expiration time will allow quicker reload for items that may have been changed on another node. However, too-frequent reload for items that have not changed makes the cache less effective.

Liferay Cache Configuration Values

Values in the Liferay `portal-ext.properties` file that affect caching have been set by Ellucian so that caching works in conjunction with Luminis caching for a unified configuration and monitoring system.

The caching-related values in `portal-ext.properties` should not be changed.

Related Links

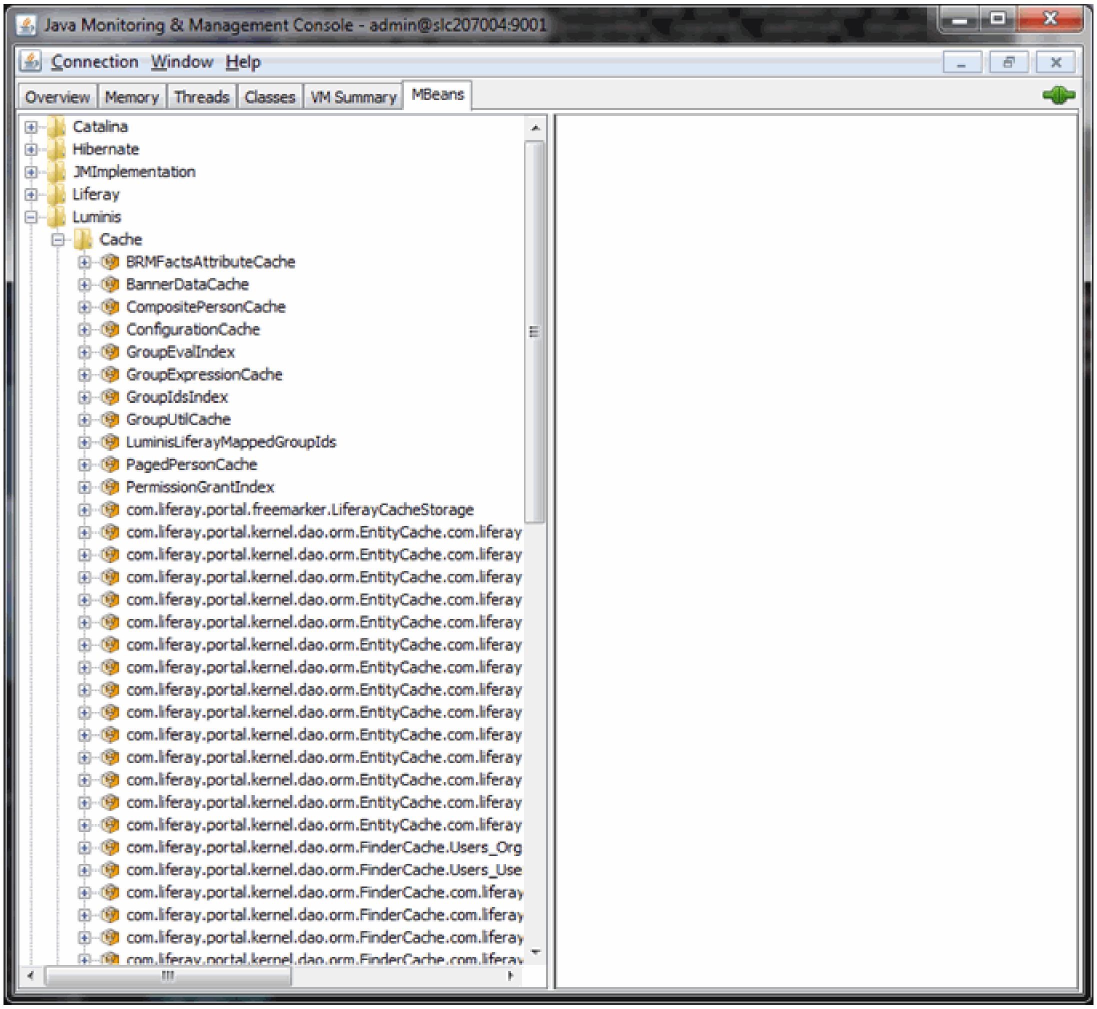
Database connection and caching properties on page 55

Monitoring Caches with JConsole

All Luminis and Liferay caches may be monitored using a Luminis MBean in a JMX management console, such as JConsole.

JConsole will be used in the following examples. Under the **MBeans** tab, opening the **Luminis** folder will show the `Cache` MBean. Under the `Cache` MBean there will be a list of all caches instantiated in the Luminis Platform and Liferay system.

The list of caches shown in a deployed system may vary because performance tuning is an ongoing process, and new caches may be defined or renamed as needed.



Catalina
Hibernate
JMImplementation
Liferay
Luminis
Cache
BRMFactsAttributeCache
BannerDataCache
CompositePersonCache
ConfigurationCache
GroupEvalIndex
GroupExpressionCache
GroupIdsIndex
GroupUtilCache
LuminisLiferayMappedGroupIds
PagedPersonCache
PermissionGrantIndex
com.liferay.portal.freemarker.LiferayCacheStorage
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.EntityCache.com.liferay
com.liferay.portal.kernel.dao.orm.FinderCache.Users_Org
com.liferay.portal.kernel.dao.orm.FinderCache.Users_Use
com.liferay.portal.kernel.dao.orm.FinderCache.com.liferay
com.liferay.portal.kernel.dao.orm.FinderCache.com.liferay
com.liferay.portal.kernel.dao.orm.FinderCache.com.liferay
com.liferay.portal.kernel.dao.orm.FinderCache.com.liferay

Expand an individual cache node to display the Attributes, Operations, and Notifications for the node. Use the attributes screen to view the current size, expiration time, and maximum size of the cache. Access the Operations screen to access each of the attributes individually or to see the cache statistics using the `getStatistics` operation. The statistics show the current size, hit count, miss count, eviction count, and calculates a hit ratio in percentage. For a cache to be truly useful, it must have a high hit ratio and be accessed frequently enough to have a significant impact.

Monitor Luminis JVMs with jconsole

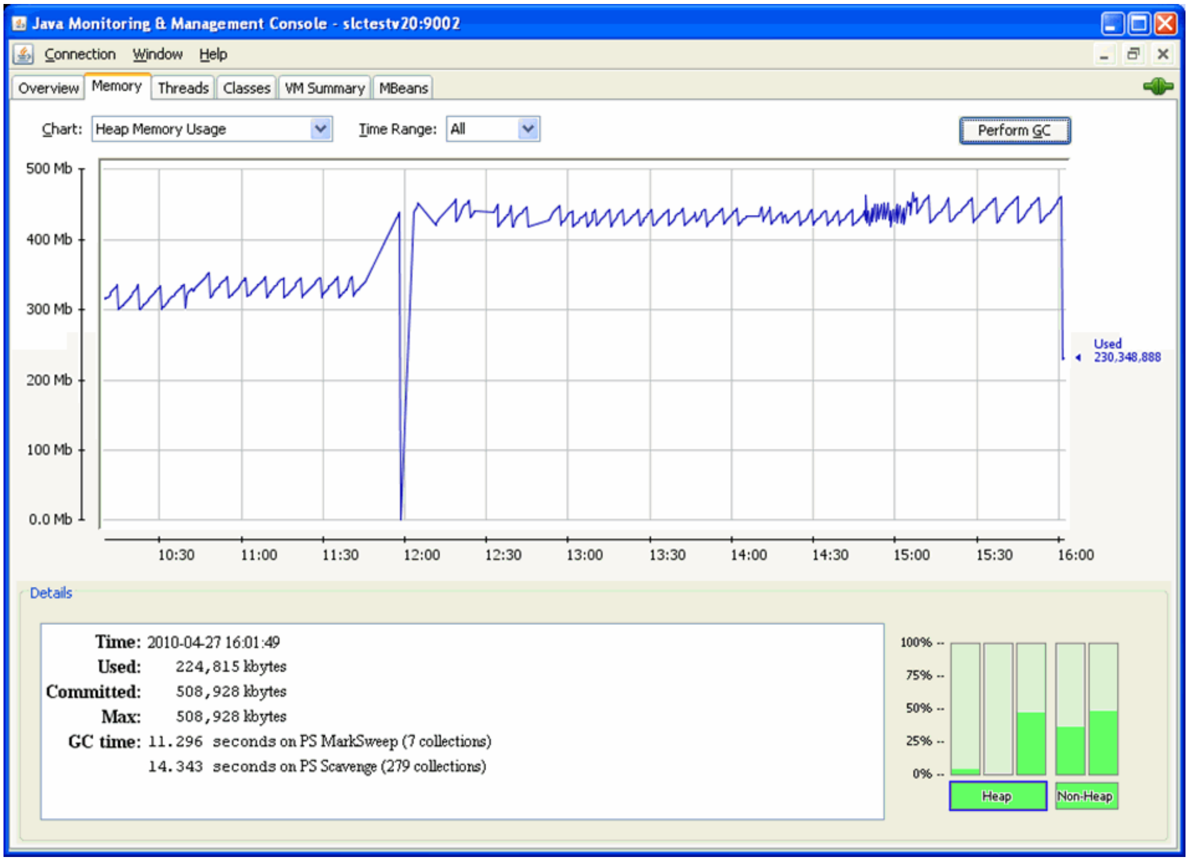
JConsole can be used to monitor the status of the Java Virtual Machines (JVMs) used by the Luminis Portal and Administrator servers.

The monitoring features are described in the following sections.

Heap Memory usage and garbage collection

JConsole provides a memory monitoring screen where the heap usage can be observed over time, and garbage collections are tracked.

It is important to monitor the system's heap memory, especially in periods of high usage.



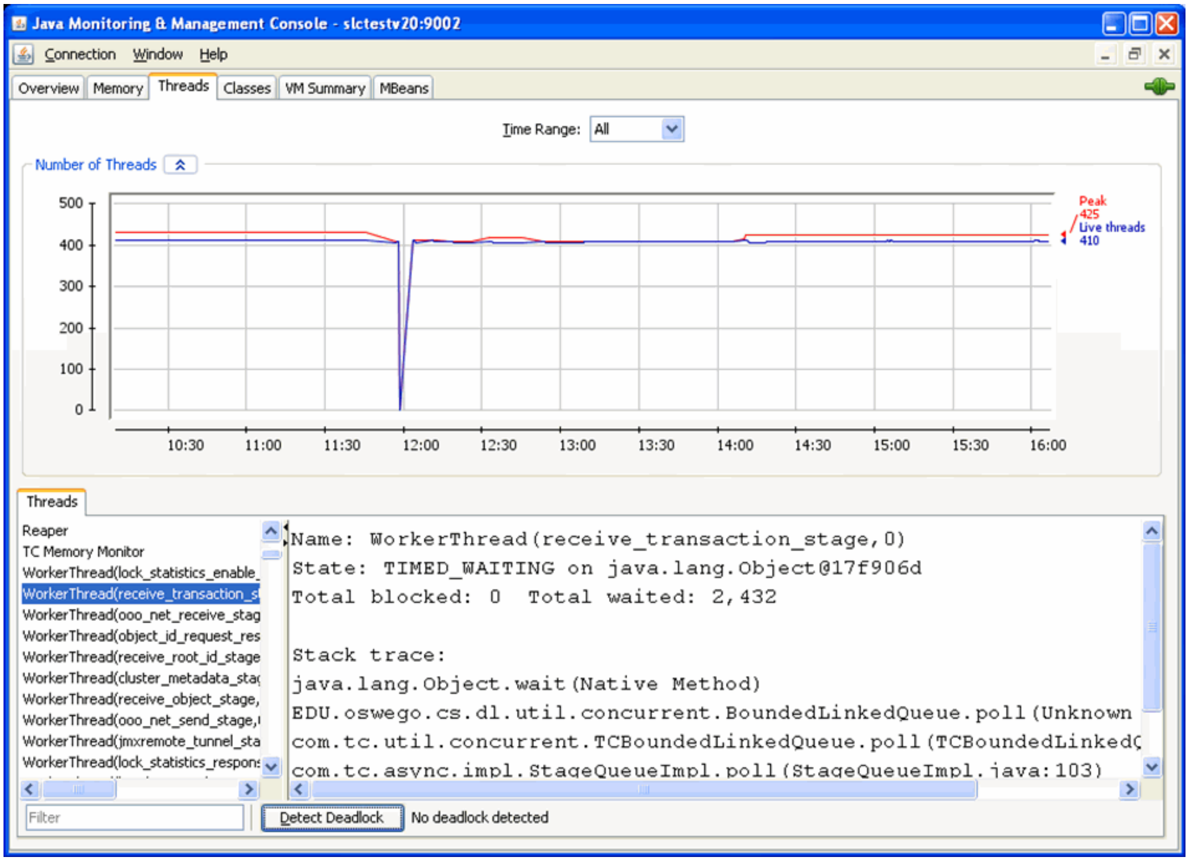
```
     Time: 2010-04-27 16:01:49
     Used:     224,815 kbytes
Committed:     508,928 kbytes
      Max:     508,928 kbytes
  GC time: 11.296  seconds on PS MarkSweep (7 collections)
           14.343  seconds on PS Scavenge (279 collections)
```

The Memory graph shows how much heap memory is being consumed. The data displayed in the Details area shows the maximum memory available, as well as the amount of time spent doing garbage collections. The time spent doing the collections and the number of collections indicates whether garbage collection is taking a significant portion of the system's processing time. If the line tends to increase over time and never drops, a memory leak is likely occurring. Click **Perform GC** to force a full garbage collection.

Threads

JConsole allows monitoring of the threads of execution being used by each server.

The number of threads used over time is displayed through a graph printed on the **Threads** tab, along with a list of each individual thread.



Time Range: All

```
Reaper
TC Memory Monitor
WorkerThread(lock_statistics_enable_
WorkerThread(receive_transaction_s
WorkerThread(ooo_net_receive_stag
WorkerThread(object_id_request_res
WorkerThread(receive_root_id_stage
WorkerThread(cluster_metadata_stag
WorkerThread(receive_object_stage,
WorkerThread(ooo_net_send_stage,(
WorkerThread(jmxremote_tunnel_sta
WorkerThread(lock_statistics_respons
```

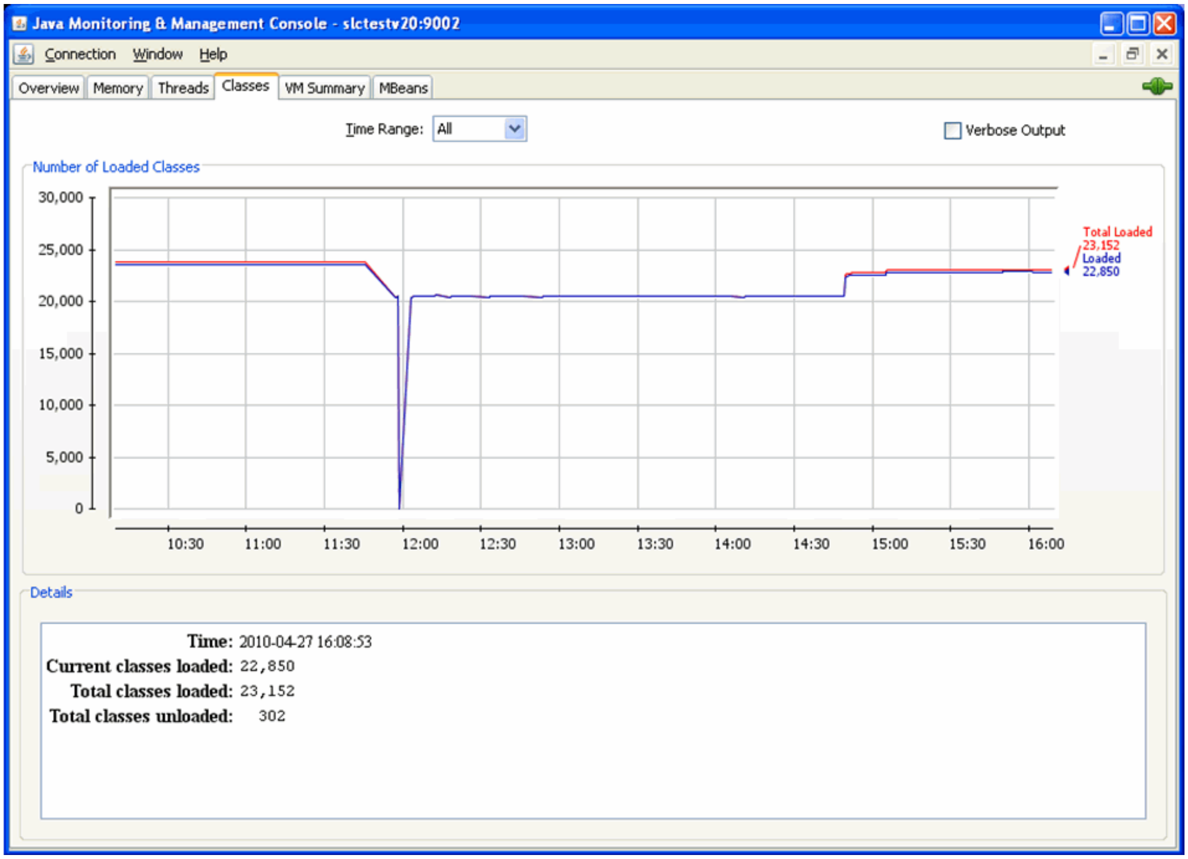
```
Name: WorkerThread(receive_transaction_stage,0)
State: TIMED_WAITING on java.lang.Object@17f906d
Total blocked: 0  Total waited: 2,432

Stack trace:
java.lang.Object.wait(Native Method)
EDU.oswego.cs.dl.util.concurrent.BoundedLinkedQueue.poll(Unknown
com.tc.util.concurrent.TCBoundedLinkedQueue.poll(TCBoundedLinkedQ
com.tc.async.impl.StageQueueImpl.poll(StageQueueImpl.java:103)
```

A problem is likely if the total number of threads continues to climb over time. If performance appears to degrade significantly, look for thread deadlocks. If a thread deadlock is detected, contact the Ellucian Support Center.

Classes

Use the **Classes** tab of JConsole to monitor the number of Java classes loaded into the system over time.

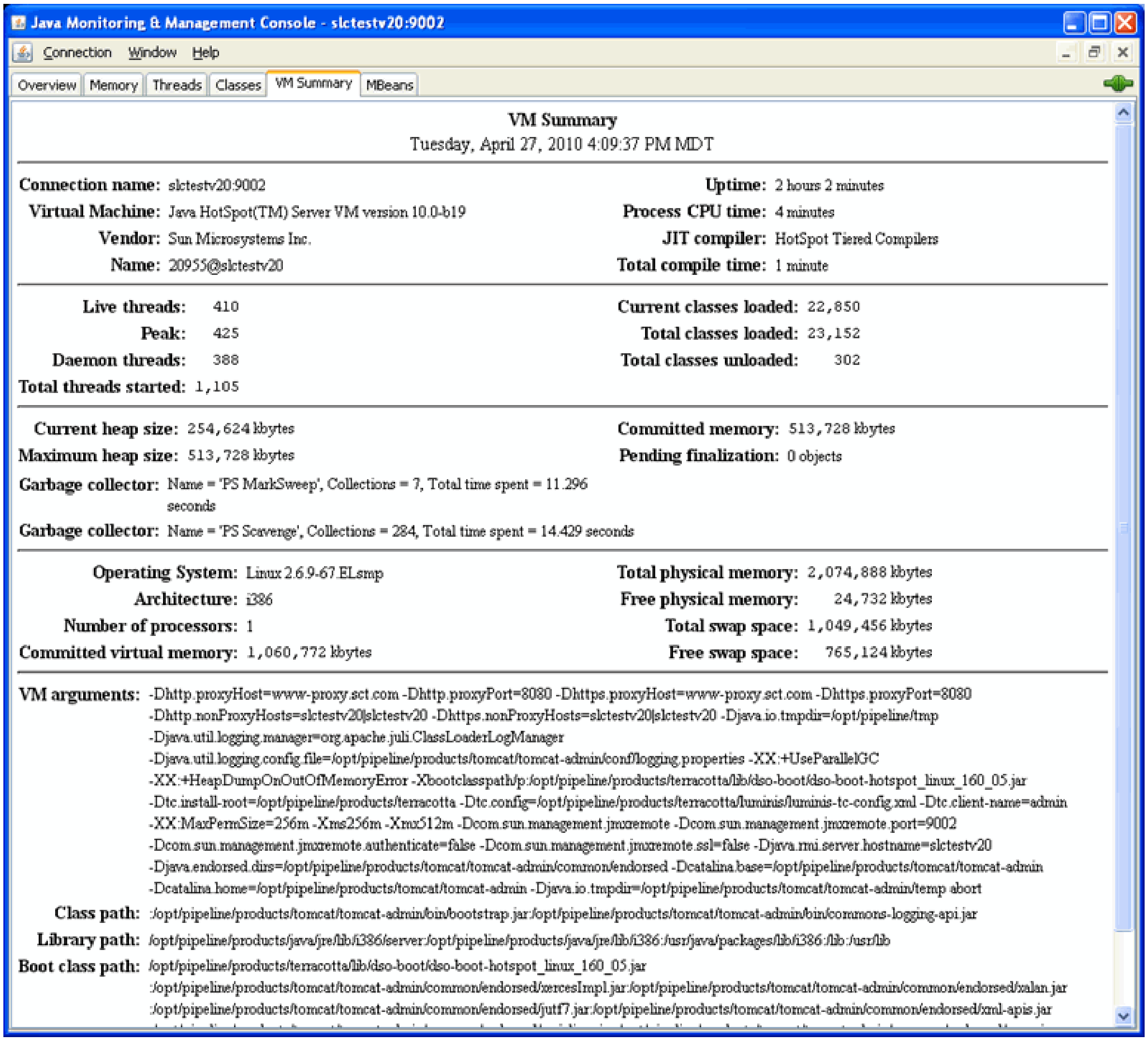
Figure 2: JConsole Java Class Monitoring Screen



```
            Time: 2010-04-27 16:08:53
Current classes loaded: 22,850
  Total classes loaded: 23,152
Total classes unloaded:   302
```

VM summary

The **VM Summary** tab lists statistics and information about the virtual machine in a single page, such as the version and the arguments supplied on the command line when the VM is started.


Java Monitoring & Management Console - slctestv20:9002
Connection Window Help
Overview Memory Threads Classes VM Summary MBeans

VM Summary
Tuesday, April 27, 2010 4:09:37 PM MDT

Connection name: slctestv20:9002
Virtual Machine: Java HotSpot(TM) Server VM version 10.0-b19
Vendor: Sun Microsystems Inc.
Name: 20955@slctestv20

Uptime: 2 hours 2 minutes
Process CPU time: 4 minutes
JIT compiler: HotSpot Tiered Compilers
Total compile time: 1 minute

Live threads: 410
Peak: 425
Daemon threads: 388
Total threads started: 1,105

Current classes loaded: 22,850
Total classes loaded: 23,152
Total classes unloaded: 302

Current heap size: 254,624 kbytes
Maximum heap size: 513,728 kbytes
Garbage collector: Name = 'PS MarkSweep', Collections = 7, Total time spent = 11.296 seconds
Garbage collector: Name = 'PS Scavenge', Collections = 284, Total time spent = 14.429 seconds

Committed memory: 513,728 kbytes
Pending finalization: 0 objects

Operating System: Linux 2.6.9-67.ELsmp
Architecture: i386
Number of processors: 1
Committed virtual memory: 1,060,772 kbytes

Total physical memory: 2,074,888 kbytes
Free physical memory: 24,732 kbytes
Total swap space: 1,049,456 kbytes
Free swap space: 765,124 kbytes

VM arguments: -Dhttp.proxyHost=www-proxy.sct.com -Dhttp.proxyPort=8080 -Dhttps.proxyHost=www-proxy.sct.com -Dhttps.proxyPort=8080 -Dhttp.nonProxyHosts=slctestv20|slctestv20 -Dhttps.nonProxyHosts=slctestv20|slctestv20 -Djava.io.tmpdir=/opt/pipeline/tmp -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.util.logging.config.file=/opt/pipeline/products/tomcat/tomcat-admin/conf/logging.properties -XX:+UseParallelGC -XX:+HeapDumpOnOutOfMemoryError -Xbootclasspath/p:/opt/pipeline/products/terracotta/lib/dso-boot/dso-boot-hotspot_linux_160_05.jar -Dtc.install-root=/opt/pipeline/products/terracotta -Dtc.config=/opt/pipeline/products/terracotta/luminis/luminis-tc-config.xml -Dtc.client-name=admin -XX:MaxPermSize=256m -Xms256m -Xmx512m -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=9002 -Dcom.sun.management.jmxremote.authenticate=false -Dcom.sun.management.jmxremote.ssl=false -Djava.rmi.server.hostname=slctestv20 -Djava.endorsed.dirs=/opt/pipeline/products/tomcat/tomcat-admin/common/endorsed -Dcatalina.base=/opt/pipeline/products/tomcat/tomcat-admin -Dcatalina.home=/opt/pipeline/products/tomcat/tomcat-admin -Djava.io.tmpdir=/opt/pipeline/products/tomcat/tomcat-admin/temp abort
Class path: :/opt/pipeline/products/tomcat/tomcat-admin/bin/bootstrap.jar:/opt/pipeline/products/tomcat/tomcat-admin/bin/commons-logging-api.jar
Library path: /opt/pipeline/products/java/jre/lib/i386/server:/opt/pipeline/products/java/jre/lib/i386:/usr/java/packages/lib/i386:/lib:/usr/lib
Boot class path: /opt/pipeline/products/terracotta/lib/dso-boot/dso-boot-hotspot_linux_160_05.jar :/opt/pipeline/products/tomcat/tomcat-admin/common/endorsed/xercesImpl.jar:/opt/pipeline/products/tomcat/tomcat-admin/common/endorsed/xalan.jar :/opt/pipeline/products/tomcat/tomcat-admin/common/endorsed/jutf7.jar:/opt/pipeline/products/tomcat/tomcat-admin/common/endorsed/xml-apis.jar

Monitor Luminis Platform with JConsole

You can use JConsole to monitor and manage applications running on a remote machine.

This requires additional configuration, especially if security is a concern or if the application is running behind a firewall. This section explains how to enable secure access to remote applications.

Consider these questions when you work with remote access to an application:

- Should access to the remote application be secured, or should access be granted to all local network users?
- Is the remote machine behind a firewall?

Step 1 Connect to remote applications

The first step to connect to a remote application is to configure the port that JConsole is going to use for connecting to Tomcat.

About this task

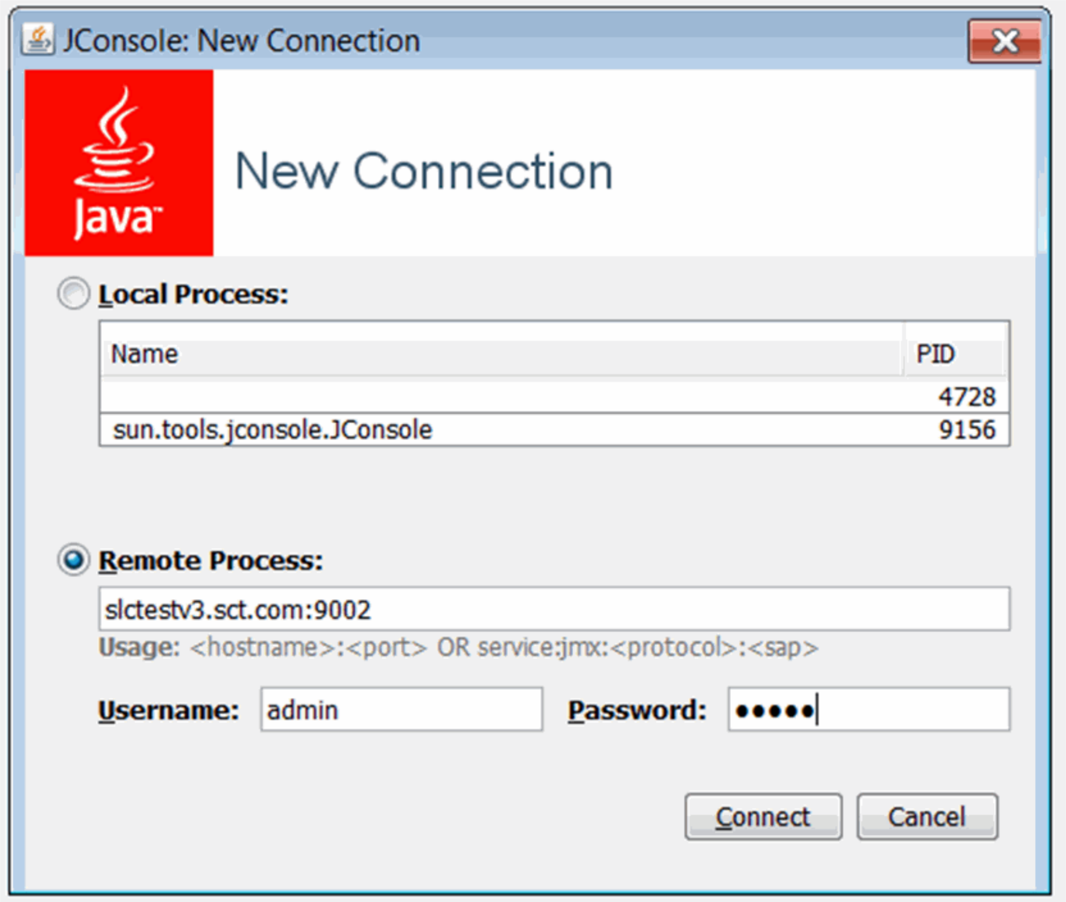
The simplest scenario is that the remote machine is not behind a firewall and is accessible to all network users.

Procedure

1. Add the following JVM option in the Tomcat startup script:

   ```
   -Dcom.sun.management.jmxremote.port=9002
   ```

2. Use the Remote Process connection, displayed in the example image below, to connect to the JVM running Tomcat. In this example, the hostname is connected to port `9002`.

   ○ Local Process:

Name	PID
	4728
sun.tools.jconsole.JConsole	9156

   ● Remote Process: slctestv3.sct.com:9002

   Usage: <hostname>:<port> OR service:jmx:<protocol>:<sap>

   Username: admin   Password: •••••

3. To locate the cause of potential connection problems, add a `logging.properties` file to JConsole that looks similar to:

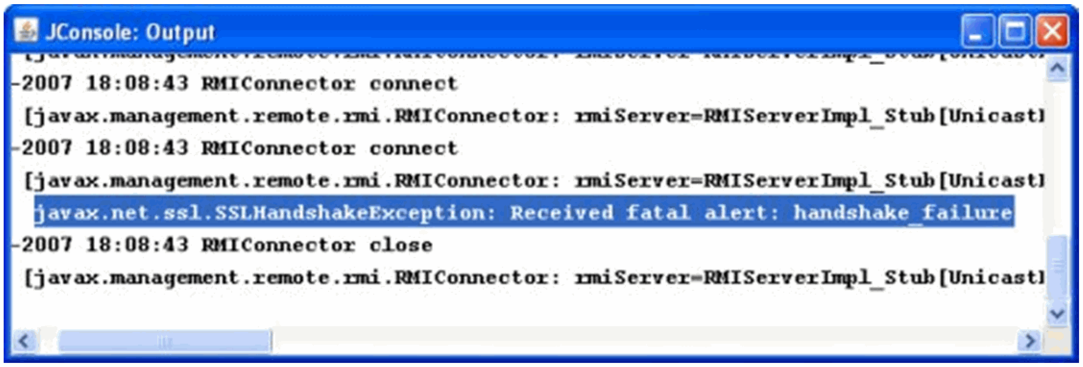
   ```
   handlers = java.util.logging.ConsoleHandler
   ```

```
.level = INFO
java.util.logging.ConsoleHandler.level = FINEST
java.util.logging.ConsoleHandler.formatter = \
java.util.logging.SimpleFormatter
// Use FINER or FINEST for javax.management.remote.level - FINEST is
// very verbose...
javax.management.level = FINEST
javax.management.remote.level = FINER
```

4. Start JConsole with this command to enable detailed logging of the `javax.management` classes:

   ```
   jconsole -J-Djava.util.logging.config.file=logging.properties
   ```

   When you connect to the remote JVM, a separate output window opens that contains the detailed logging. If you use JConsole with JDK 5, the log displays in a standard output. If you encounter a problem while connecting to Tomcat, you can use the log to diagnose the problem. For example, the logging shown in this image clearly indicates a problem in the SSL configuration:



```
-2007 18:08:43 RMIConnector connect
 [javax.management.remote.rmi.RMIConnector: rmiServer=RMIServerImpl_Stub[UnicastI
-2007 18:08:43 RMIConnector connect
 [javax.management.remote.rmi.RMIConnector: rmiServer=RMIServerImpl_Stub[UnicastI
  javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
-2007 18:08:43 RMIConnector close
 [javax.management.remote.rmi.RMIConnector: rmiServer=RMIServerImpl_Stub[UnicastI
```

5. If JConsole reports that the connection has been refused, it will not generate any additional logging because a connection to the MBeanServer has not yet been established. Most common reasons for refused connections are:

   - Wrong port number
   - Tomcast has not been started
   - The firewall is blocking the connection

   To solve this problem, you may want to configure more detailed logging in your `logging.properties` file to solve this problem. To rule out network-related issues, you could also first test the Tomcat configuration locally by using the Remote Processconnection to connect to a local process using `localhost:9002` as the connection string.

Step 2 Enable SSL

The next step in securing access to Tomcat with JConsole, is to add SSL.

About this task

This may not be necessary in certain circumstances. SSL may be required by the security policies in a production environment.

Enabling SSL allows you accomplish three goals:

- Encrypt the communication between JConsole and the MBeanServer
- Use client certificates for authentication
- Enable authentication for the RMI Registry

To generate a certificate that will be used by the Tomcat server to encrypt the communication:

Procedure

1. To create a self-signed certificate, use this keytool application within the JDK:

   ```
   keytool -genkey -alias jconsole -keystore TOMCAT_HOME/
   bin/.TomcatKeyStore
   ```

2. Use the `-genkey` or `-genkeypair` (JDK 6) command to generate a public and private key, and creates a certificate signed by the private key. The `-alias` option enables you to choose the alias used to store the certificate. The `-keystore` options allows you to create a keystore in the Tomcat bin directory instead of using the default keystore location.
3. Enter additional information, such as a password and name.

   The certificate is created.
4. Use the following `-list` command to list the created certificate in the keystore:

   ```
   keytool -list -keystore TOMCAT_HOME/bin/.TomcatKeyStore
   ```

   The output should look similar to:

   ```
   Keystore type: JKS

   Keystore provider: SUN

   Your keystore contains 1 entry

   jconsole, 21-apr-2007, PrivateKeyEntry,

   Certificate fingerprint (MD5):
   AF:3E:79:18:E7:4E:D1:42:A5:E2:7C:7F:1F:3D:5A:6D
   ```

   Note: JDK 5 uses the term `keyEntry` instead of `PrivateKeyEntry`.

5. When you use a self-signed certificate, you must export the certificate and import the certificate in the truststore used by JConsole. If you do not, JConsole cannot validate the certificate. Use the `-exportcommand` to export the certificate on the remote machine, as follows:

   ```
   keytool -export -alias jconsole -keystore TOMCAT_HOME/
   bin/.TomcatKeyStore -file jconsole.cert
   ```

A `jconsole.cert` file is created. You will copy this file to the machine used to run JConsole.

6. On this machine we import the certificate into a new truststore for JConsole using the `-import` command.

   ```
   keytool -import -alias Tomcat -keystore JAVA_HOME/
   bin/.jconsoleKeyStore -file jconsole.cert
   ```

   If we now use the `-list` command for this new truststore the output should look similar to:

   ```
   Keystore type: JKS

   Keystore provider: SUN

   Your keystore contains 1 entry

   Tomcat, 21-apr-2007, trustedCertEntry,

   Certificate fingerprint (MD5):
   AF:3E:79:18:E7:4E:D1:42:A5:E2:7C:7F:1F:3D:5A:6D
   ```

   You can now use a different alias for the truststore, and the entry is listed as a trustedCertEntry, which indicates that it does not contain the private key that is stored in the keystore on the remote machine.

   Note: It is only necessary to export and import self-signed certificates. Certificates signed by a certificate authority (CA) are already saved in the default truststore. The default truststore is located in the file cacerts in the `JRE_HOME/lib/security` directory.

7. After the keystore and truststore are created, enable SSL and configure the keystore options in the Tomcat startup script using these JVM options:

   - `-Dcom.sun.management.jmxremote.ssl=true`
   - `-Djavax.net.ssl.keyStore=TOMCAT_HOME/bin/.TomcatKeyStore`
   - `-Djavax.net.ssl.keyStorePassword=secret`

8. To restrict access to the keystore, use steps 1 and 2 for the password file.

9. When you start JConsole, add the location of the truststore containing the certificate used by Tomcat, as follows:

   ```
   jconsole -J-Djavax.net.ssl.trustStore=JAVA_HOME/bin/.jconsoleKeyStore
   -J-Djava.util.logging.config.file=logging.properties
   ```

   When you connect to Tomcat with JConsole, you see logging that indicates that you are using an SSL SocketFactory to make the connection.

Step 3 Enable SSL client authentication

After you enable SSL, the final step is to enable client authentication:

Procedure

1. Use this command to generate another certificate for the JConsole client:

```
keytool -genkey -alias jconsole_client -keystore JAVA_HOME/
bin/.jconsoleKeyStore
```

This command generates a public and private key and a self-signed certificate in the same keystore that you created as your truststore. The keystore information should appear similar to:

```
Keystore type: JKS

Keystore provider: SUN

Your keystore contains 2 entries

Tomcat, 21-apr-2007, trustedCertEntry,

Certificate fingerprint (MD5):
AF:3E:79:18:E7:4E:D1:42:A5:E2:7C:7F:1F:3D:5A:6D

jconsole_client, 21-apr-2007, PrivateKeyEntry,

Certificate fingerprint (MD5):
15:3F:7D:AD:A5:65:8C:E8:CB:D2:4D:39:4E:68:13:01
```

Note: You can create a separate keystore, if desired.

2. Export the certificate and copy it to the remote machine that is running Tomcat. For CA certificates, you can skip the export and import steps.

   ```
   keytool -export -alias jconsole_client -keystore JAVA_HOME/
   bin/.jconsoleKeyStore -file jconsole_client.cert
   ```

3. Import the certificate again on the remote machine.

   ```
   keytool -import -alias jconsole_client -keystore TOMCAT_HOME/
   bin/.TomcatKeyStore -file jconsole_client.cert
   ```

   The Tomcat keystore should appear similar to:

   ```
   Keystore type: JKS

   Keystore provider: SUN

   Your keystore contains 2 entries

   jconsole_client, 29-apr-2007, trustedCertEntry,

   Certificate fingerprint (MD5):
   15:3F:7D:AD:A5:65:8C:E8:CB:D2:4D:39:4E:68:13:01

   jconsole, 27-apr-2007, PrivateKeyEntry,

   Certificate fingerprint (MD5):
   AF:3E:79:18:E7:4E:D1:42:A5:E2:7C:7F:1F:3D:5A:6D
   ```

4. Add the following JVM option to the Tomcat startup script to enable SSL client authentication:

   - `-Dcom.sun.management.jmxremote.ssl.need.client.auth=true`
   - `-Djavax.net.ssl.trustStore=TOMCAT_HOME/bin/.TomcatKeyStore`

5. When you start JConsole, pass the location of the keystore and the keystore password.

   ```
   jconsole -J-Djavax.net.ssl.keyStore=JAVA_HOME/
   bin/.jconsoleKeyStore -J-Djavax.net.ssl.keyStorePassword=secret -
   ```

```
J-Djavax.net.ssl.trustStore=JAVA_HOME/bin/.jconsoleKeyStore -J-
Djava.util.logging.config.file=logging.properties
```

6. **Optional:** You can choose to use password authentication in combination with SSL client authentication. However, when you use SSL client authentication, you might not need the password authentication. The disadvantage of disabling password authentication is that access control can only be configured for password authentication, so you could not assign read-only access to users.

   To disable password authentication, set authentication to false in the Tomcat startup script.

   ```
   -Dcom.sun.management.jmxremote.authenticate=false
   ```

IMS Import properties

Properties related to the IMS import function, including a description of what each property controls and what the expected inputs are.

Property	Description
`ldisp.filtered.datasources`	Used to filter records in the `IMS-ES` XML import from being processed. Comma delimited list. Records with a `sourcedid.source` listed in this property will be ignored during the import process.
`data.integration.incoming.person.isRoleAppendEnabled`	If this property is true, upon a user update any new roles being assigned to the user will be appended to the user. If the property is false, upon a user update the user's list of roles will be replaced with the new list. The default value is false.
`data.integration.incoming.person.displayname.source`	Allows you to configure whether the display name that appears for users in the Luminis Platform is derived from the full name (fn) or nickname field specified in the `IMS-ES` XML import. The default value is fn.
`data.integration.incoming.person.email.address.source`	Allows you to configure whether a user's e-mail address is derived from an `LDISP IMS` XML import or event, and if so, which data element to use. The `data.integration.incoming.person.email.address.source` property accommodates one of three values: userid, email, or NONE. The default value is userid, which extracts an e-mail identifier (possibly without the domain) from the person/userid element with a `useridtype` attribute that has an EmailID value. The email value causes

Property	Description
	Luminis Platform to extract the e-mail address from the `person/email` element of the XML document. The NONE value specifies that the e-mail address should not be updated through an `LDISP IMS-ES` XML document. **Note:** If you set the `data.integration.incoming.person.email.address.source` property to email with provisioning enabled, you may receive duplicate e-mail address errors. For example, if provisioning is disabled, then *User_1*'s e-mail address of `mailto:john.doe@gmail.com` and `User_2`s e-`mail address of mailto:john.doe@yahoo.com` are unique enough not to cause any errors. However, when you provision with a provisioning domain of `luminis.edu`, the users' e-mail domains both change to `mailto:john.doe@luminis.edu`. This circumstance results in a duplicate e-mail address error and *User_1* and *User_2* are not provisioned.
`data.integration.incoming.synchronize.lp.with.ims.credential`	Controls whether the Luminis Platform login credential is automatically synchronized with that of an integrated student information system such as Banner. The default value is false.
`data.integration.incoming.synchronize.lp.credential.on.update`	Sets whether the log on credential is updated on person update operations. This property is only used if the `data.integration.incoming.synchronize.lp.with.ims.credential` is set to false. The default value is false.
`data.integration.incoming.synchronize.lp.credential.when.none`	Sets whether the login credential is updated on person update when the person record in Luminis has no credentials. The default value is true.
`data.integration.incoming.role.map`	Allows a mapping from ldisp roles to Luminis roles during user import. The format of this property should be: *ldispRole1:luminisRole1*, *ldispRole2:luminisRole2* The default value is empty.
`data.integration.incoming.community.admin.userid`	The Luminis user ID that will be used as the owner of a course site created for an imported course. Defaults to the default Luminis admin

Property	Description
	user are set in the `setup.properties` file during installation. This property value should not be modified.
`data.integration.incoming.delete_luminis_users`	If this property is set as true, the user will be deleted from the Luminis system. If this property is false, the user will be disabled in the Luminis system, not deleted. The default value is false.
`data.integration.incoming.use.secret.store`	The only supported value for this property in current releases of Luminis Platform is false.

Liferay configuration management with portal-ext.properties

The portal upon which Luminis is built has two mechanisms for controlling various aspects of the portal.

The first mechanism stores configuration properties in the database, and many of those are set using the **Control Panel** of the portal. The second configuration mechanism makes use of a file called `portal-ext.properties`. In a typical Luminis Platform installation, the file is located in these directories:

- Admin node: `$CP_ROOT/products/tomcat/tomcat-admin/webapps/ROOT/WEB-INF/classes`
- Portal node: `$CP_ROOT/products/tomcat/tomcat-portal/webapps/ROOT/WEB-INF/classes`

This chapter explains how to make changes to the file and why you should backup this file on a regular basis, list the properties Luminis has set within this file, and point you to documentation provided by Liferay about all of the available properties.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Update portal-ext.properties

You must have the correct system-level privileges to edit the `portal-ext.properties` file.

This is a text file and can be edited using any text editor. After making changes to the file, restart the node associated with the given file.

Back up portal-ext.properties

Ellucian recommends that you backup the `portal-ext.property` file before you make any changes to the file.

This backup should be stored in another location as this file could be overwritten by future Luminis Platform updates. If you keep a backup of your changes, you can reapply your changes to the file if the portal is updated.

Portal properties set by Luminis

The properties set by Luminis are used to define the look and feel, authentication properties, database connection and caching, resource repository paths, and other system level settings.

When Luminis Platform is installed, the `portal-ext.properties` file is already set with several properties. The tables in these sections describe the property name, the default value, and whether it is OK to change the property. Some properties may have additional notes associated with them.

Look and Feel properties

These values affect the look and feel of the portal.

Property name	Default value	OK to change
`breadcrumb.show.guest.group`	False	No. Luminis does not support Guest access to the portal.
`community.default.admin`	If you did not set the `luminis.admin.community` property during installation, then the default value set is as follows: Luminis Administrators Community	Yes. Set in the `portal-ext.properties` file of the admin node. Set this property to reflect the name of the site that Luminis Administrators see when they login to Luminis Platform. For more detail about this property and how it works with other properties, refer to the section "Customize the installation values" in the *Luminis Platform Installation Guide*.
`community.default.home`	If you did not set the `luminis.home.community` property during installation,	Yes.

Property name	Default value	OK to change
	then the default value set is as follows: Home Community	Set in the `portal-ext.properties` file of the portal node. Set this property to reflect the name of the site Luminis Portal users see when they login to Luminis. For more detail about this property and how it with other properties, refer to the section "Customize the installation values" in the *Luminis Platform Installation Guide*.

`community.default.home.url`	If you did not set the `luminis.admin.community.url` and `luminis.home.community.url` properties at installation time then the default value for the nodes are as follows:
	Admin Node:
	`/web/luminis-admin-group`
	Portal Node:
	`/web/home-community`
		Yes.
		For more detail about this property and how it works with other properties, refer to the "Customize the installation values" section in the *Luminis Platform Installation Guide*.

`company.default.web.id`	If you did not set the `school.web.id` property during installation, then the default value is as follows: `wasatch.edu`	Yes.
`default.regular.theme.id`	LP5ellucian_WAR_LP5ellucianthemes	Yes. Set this to the name of the theme you choose to create for your institution.
`default.user.private.layout.column-1` `default.user.private.layout.column-2`	No values set	Yes. Setting this property to empty causes the "My Private Pages" space to be created with a page with no portlets on the page. If you want portlets to appear by default, then set this property to

Property name	Default value	OK to change
		the portlet id values separated by commas.
`default.user.public.layout.column-1` `default.user.public.layout.column-2`	No values set	Yes. Setting this property to empty causes the "My Public Pages" space to be created with a page with no portlets on the page. If you want portlets to appear by default, then set this property to the portlet id values separated by commas.
`image.default.company.logo`	ellucian_university_logo.png	Yes. The image must be made available in the class path. If the logo has been changed using the **Control Panel**, then the Control Panel setting will override this item.
`layout.comments.enabled`	false	Yes. Comments can be added by users to pages. To allow comments to be added to pages set this to true.
`locales`	en_US,fr_FR,ar_SA,es_MX,pt_BR	Yes. The values Ellucian supports as localized languages include those listed with the default value. You can remove the languages that your institution does not need. The locales set with this property display in the **Languages** portlet.
`my.sites.max.elements`	20	Yes. This controls the maximum number of elements displayed in the **My Sites** navigation menu.
`theme.images.fast.load`	False	Yes.

Property name	Default value	OK to change
		To load the theme's merged image files more quickly, set this property to true.

Control Panel overrides

Several properties reflect features that Ellucian has disabled within the **Control Panel**.

Ellucian does not recommend that you change any of these properties.

Property name	Default values	OK to change
`users.form.update.main`	details, sites, personal-site	No. Modifies the available options in the right side panel when editing users from the Liferay Control Panel. Use the Luminis **User Management** portlet.
`users.form.update.identification`	No values set	No. Modifies the available options in the right side panel when editing users from the Liferay Control Panel. Use the Luminis **User Management** portlet.
`users.form.my.account.main`	details,sites,personal-site	No. Modifies the available options in the right side panel when editing users from the Liferay My Account Portlet. Use the Luminis **My Account** portlet.
`layout.form.update`	details,look-and-feel,layout,custom-fields,advanced,mobile-rule-groups	No. Modifies the available options in the right side panel when editing users from the Liferay Control Panel. Use the Luminis **User Management** portlet.
`layout.set.form.update`	look-and-feel,logo,advanced,mobile-rule-groups	No. Modifies the available options in the right side panel when editing layouts from the Liferay Control Panel.

Property name	Default values	OK to change
`sites.form.update.seo`	No values set	No. Modifies the available options in the right side panel when editing users from the Liferay Control Panel. Use the Luminis **Site** portlets should be used.
`company.settings.form.configuration`	general,authentication,users, mail-host-names	No. Modifies the available options in the right side panel when editing the company from the Liferay Control Panel.

`include-and-override`	Admin Node:
	`$CP_ROOT/products/liferay/liferay-admin/portal-setup-wizard.properties`
	Portal Node:
	`$CP_ROOT/products/liferay/liferay-portal/portal-setup-wizard.properties`
		No.
		This disables the Liferay Setup Wizard. This is done automatically when Luminis Platform is installed or patched.

`resource.action.config`	`resource-actions/default.xml,resource-actions/default-ext.xml`	No. Set for the default Liferay resource action overrides.

Authentication-related properties

The properties related to authentication.

Property name	Default value	OK to change
`auto.login.hooks`	In the `portal-ext.properties` file, the following items are separated by commas. com.sghe.luminis.liferay.security.auth.LuminisAuto Login com.liferay.portal.security.auth.NtlmAutoLogin	Yes with a note. The listed classes will run in order for all unauthenticated users until one of these returns a valid user id and password.

Property name	Default value	OK to change
	com.liferay.portal.security.auth.OpenIdAutoLogin com.liferay.portal.security.auth.OpenSSOAutoLogin com.liferay.portal.security.auth.RememberMeAutoLogin com.liferay.portal.security.auth.SiteMinderAutoLogin	
`cas.auth.enabled`	true	No. Luminis requires CAS to be enabled. Liferay supports and documents other CAS-related properties. Ellucian does not recommend setting any of those values in the `portal-ext.properties` file.
`ldap.password.policy.enabled`	true	No. Liferay provides a system for defining a user's password policy. Setting this property to false will use the Liferay password policy system instead of the LDAP policy.
`users.reminder.queries.enabled`	false	No. The Luminis **Q&A** portlet replaces this functionality.
`users.reminder.queries.custom.question.enabled`	false	No. The Luminis **Q&A** portlet replaces this functionality.
`terms.of.use.required`	false	No. Setting this true will not alter the functionality within Luminis Platform.

Database connection and caching properties

The properties related to database connection and caching properties.

Do not change any of these properties.

Property name	Default value	OK to change
`hibernate.cache.provider_class`	org.hibernate.cache.NoCacheProvider	No.
`hibernate.cache.region.factory _class`	org.hibernate.cache.impl.NoCachingRegionFactory	No.
`hibernate.cache.use_query_cache`	false	No.
`hibernate.cache.use_second_level_ cache`	false	No.
`hibernate.cache.use_minimal_puts`	true	No.
`hibernate.cache.use_structured_entries`	false	No.
`hibernate.dialect`	Based on the installation property value associated with `luminis.database.type`	No.
`jdbc.default.jndi.name`	`Jdbc/LuminisPooledDB`	No.
`value.object.finder.thread.local.cache.max.size`	0	No.
`value.object.entity.thread.local.cache.max.size`	0	No.

Related Links

Liferay Cache Configuration Values on page 35

Resource repository properties

Properties needed to store system and content-related resources associated with the portal.

Update these properties after Luminis Platform installation to ensure the resources are accessible by each node of your deployment. To set up a shared repository, see the section noted with each property in "Post-installation tasks" in *Luminis Platform Installation Guide*.

Property name	Default value	OK to change
`lucene.dir`	Fully-qualified path to where the Lucene index files are located.	Yes. To share the Lucene search index, follow the steps in the "Lucene setup in a Liferay cluster" section of the *Luminis Platform Installation Guide*.

`resource.repositories.root`	Fully-qualified path to where the Liferay resource repository is located for the node.
	Admin Node:
	`$CP_ROOT/products/liferay/liferay-admin`
	Portal Node:
	`$CP_ROOT/products/Liferay/liferay-portal`
		No.

`dl.store.impl`	This property determines the type of storage that is used by the Document Library. By default, Luminis is configured to use Jackrabbit. Default value: com.liferay.portlet.documentlibrary.store.JCRStore	Yes. To change the data store for Document Library, please refer to the Liferay Portal 6.1 user guide located at http://www.liferay.com. Additional information about the default Jackrabbit configuration is located in the "Documents and Media Repository" section of the *Luminis Platform Installation Guide*.
`jcr.initialize.on.startup`	true	Yes, if you choose not to initialize the repository with server startup.

System-level properties

The system-level properties.

Property name	Default value	OK to change
`application.startup.events`	In the `portal-ext.properties` file, these items are separated by commas.	Yes, with a note. Additional actions may be added, do not remove the actions listed.

Property name	Default value	OK to change
	com.sghe.luminis.liferay.integration.LuminisAddDefaultDataAction com.liferay.portal.events.AppStartupAction com.liferay.portal.events.ChannelHubAppStartupAction	
`auto.deploy.copy.commons.logging`	false	
`auto.deploy.copy.log4j`	false	
`direct.servlet.context.enabled`	false	
`log4j.configure.on.startup`	false	
`hot.deploy.listeners`	Value contains too many items to list.	No.
`plugin.notifications.enabled`	false	Not recommended.
`redirect.url.security.mode`	domain	Yes. Valid values are domain and ip. Consult the Liferay users guide at liferay.com before you change this property.
`redirect.url.domains.allowed`	Admin node: Value is the hostname of the admin node Portal node: Value is the virtual hostname of the portal node.	Yes, with a note. Other domains may be added. Do not remove the default hostname.
`users.screen.name.allow.numeric`	true	
`web.server.protocol`	https	

Documentation for other portal properties

The Liferay documentation site provides a properties reference guide.

About this task

You can access this reference online by using these steps:

Note: The links on the Liferay Web site are subject to change without notice.

Procedure

1. Access http://www.liferay.com.
2. Click **Documentation**.
3. In the Liferay **Portal** menu, click **Liferay 6.1**.
4. Either scroll through the numbered list, or complete a search for **Properties Reference**.

   As there are so many properties to control the behaviors of the portal, and various Liferay developed portlets, Ellucian cannot guarantee the behaviors associated with each property. When you test a particular property, Ellucian recommends you test the property within a development environment to understand what the property does before you deploy the property on a production environment. For those who are interested in discussing these properties, visit the Luminis Community on the Ellucian eCommunities Web site.

Backup and System Recovery

The Luminis Platform uses a directory server, a variety of configuration files, and an external database to manage, display, and store system and user information.

If information in these data stores or configuration files is corrupted, the operation of the system can be compromised, and in serious cases, rendered unusable. To prevent, or minimize, the effects of data corruption, you must back up your data and configuration files on a regular basis and be ready to restore them. The following sections provide information and procedures for backing up critical datastores.

Perform a complete backup of the system data

At a high level, perform a complete backup of the system data.

Procedure

1. Shut down all nodes in the Luminis system.
2. Back up all installed files and directories on each node of the Luminis system.
3. Back up the Lightweight Directory Access Protocol (LDAP) directory data.
4. Back up the database instance on the external database where Liferay and Luminis data is stored.
5. Restart the Luminis system.

Results

To create a complete and restorable backup copy of your system, make copies of all the data sources during the same backup session. Restoring back-up data created at different times would compromise the integrity of your system.

The following sections provide information about critical files and data stores in the Luminis system that you should consider as you back up the system.

System backup

After you shut down Luminis, you must successively back up the various file systems and data stores associated with the system.

These include:

- File system of each installed node
- Luminis Directory Server (OpenDJ) data
- External database

File system backup

Many commercial products are available for backing up and restoring file system data on computer servers.

We recommend you use a product able to take complete, incremental backups of the entire Luminis Platform file system.

You should save all files under `$CP_ROOT`.

If you do not use a commercial product, copy all the files from the Luminis root installation directory `($CP_ROOT)` to a separate drive on regular intervals.

Luminis directory server backup

Luminis ships the OpenDJ directory server for system configuration and user data.

To save all date for future restoration, make a complete copy of the directory structure where OpenDJ is installed (`$CP_ROOT/products/opendj`). You may also take either full or incremental backups of the OpenDJ data store to save space on the backup device.

Complete instructions and detailed information on backing up the OpenDJ server can be at this URL:

http://opendj.forgerock.org/opendj-server/doc/admin-guide/index/chap-monitoring.html

Note: The links on this Web site are subject to change without notice.

As a minimum requirement, you must open a terminal window and execute this command to back up all databases from the `$CP_ROOT/products/opendj/bin` directory:

```
 $ backup --backUpAll --compress --backupDirectory /tmp/backup
```

The previous command will take a backup of all data to the `/tmp/baOpenDJckup` directory.

To take an incremental backup, execute this command:

```
$ backup --backUpAll --incremental --compress --backupDirectory /tmp/
backup
```

Note: When you perform an incremental backup, it will save both time and space, incremental backups must be restored in the order they were taken.

If Luminis is installed using an external directory server instance, follow the instructions provided by the vendor for the particular directory server to back up the Luminis datastore.

External database backup

Create a backup of the entire database instance where any Luminis data is stored.

The backup and restore operations discussed in this guide do not address external databases. To back up the data stored in the external database, refer to the backup instructions provided with the database you chose to implement at your institution.

Restore system data

If you need to restore system data from a backup copy, make sure to restore all the system's data from the same backup session.

Note: Restoring data from backups that have been created at different times would compromise the integrity of your system.

Restore file systems

If you use a commercial backup product, then you must use the last good snapshot to restore the file system under `$CP_ROOT` on every node in the Luminis installation.

If you have not used a commercial product, then you must copy the data to `$CP_ROOT` from where you have saved it.

Restore directory server data

Restoration procedure depends on whether you saved the complete file system or backed up the OpenDJ datastore separately.

If saved the complete file system, using either a commercial product or your own copy procedure, then a separate Directory restoration process is not necessary. However, if you did a back up of the OpenDJ datastore separately, then you will need to restore the directory data as follows:

```
$ restore --listBackups --backupDirectory backup/userRoot
```

Note: After you stop the directory server, you must run this command from the $CP_ROOT/products/opendj/bin directory to restore data.

Restore external database

To restore data stored in the external database backup, refer to the instructions provided with the database you chose to implement at your institution.

Command line tools

Luminis Platform provides command line tools for administrative functions.

The administrative functions are described in the following sections.

Before using any of the commands, ensure that you source the .cprc file found under the $CP_ROOT.

```
cd $CP_ROOT
. ./.cprc
```

Luminis version information

Use the lpver command to print out the Luminis version information.

Startup and Shutdown of Luminis servers

Start up all Luminis components on a machine in proper order with the lpstart command.

Shut down all Luminis components on a machine with the lpstop command.

Use these commands to start up and shut down individual servers:

```
Start up LDAP server: 10-ldap start
Shut down LDAP server: 10-ldap stop
Start up CAS server: 20-cas-webserver start
Shut down CAS server: 20-cas-webserver stop
Start up Admin server: 25-admin-webserver start
Shut down Admin server: 25-admin-webserver stop
Start up Portal server: 30-portal-webserver start
Shut down Portal server: 30-portal-webserver stop
```

Startup timeout option

The admin and portal servers can take a long time to start up. You can use the -t option to change the default timeout if the server requires more than 15 minutes to start up.

For example, you must run this command to give each server up to 20 minutes to finish starting up:

```
lpstart -t 20
```

You must run this command to give the admin server 20 minutes to start up before timing out:

```
25-admin-server -t 20 start
```

By default, the startup script will timeout at 15 minutes if the server has not started.

Uninstall Luminis

Use this command to uninstall Luminis Platform:

```
uninstall
```

Alternatively, run this command to drop all database tables and uninstall Luminis Platform:

```
uninstall -d
```

Logs and reports

This section contains information about the logs and reports available in Luminis Platform.

System logs

System status logs are a valuable tool for troubleshooting.

There are two types of logs you should periodically review:

- Luminis logs
- Logs generated by the third party components

This section explains the logs, where they are located on your system, and how to adjust logging behavior.

Luminis root logs

Logs for installation, startup, and shutdown are found in this directory:

```
$CP_ROOT/logs
```

In the `$CP_ROOT/logs` directory you will find:

- `install.log`. Log created during the installation of Luminis components on this node.
- `startup.log`. Log created every time the command `lpstart` is run. It contains information on whether components on this node succeeded or failed to start.
- `shutdown.log`. Log created every time the command `lpstop` is run. It contains information on whether components on this node of the system succeeded or failed to stop.

Portal and admin server logs

Each portal and admin server deployment contains a logs directory as part of the Tomcat directory structure.

The admin server log is found under this path:

```
$CP_ROOT/products/tomcat/tomcat-admin/logs
```

The portal server logs are found in this directory:

```
$CP_ROOT/products/tomcat/tomcat-portal/logs
```

Each contains these log files:

- `luminis.log`. This log file contains general information from a running Luminis system. It is automatically versioned and rolled over when a specified size limit is reached. For more information about controlling maximum size and rollover behavior, see "Adjust Luminis loggin behavior."
- `luminis_access.<date>.log`. This log file contains entries for every access to the server. Versioning and rollover of this file is controlled by Tomcat, and the `<date>` field will change to reflect the date the log was started.
- `catalina.out`. This log file contains console output from Tomcat. This file is versioned and re-created every time the server is re-started.

Related Links

Adjust Luminis logging behavior on page 64

Adjust Luminis logging behavior

Using a logger hierarchy, it is possible to control which log statements are output, at arbitrarily fine granularity. This helps reduce the volume of logged output and minimizes the cost of logging.

The Luminis system uses the log4j logging package. One of the distinctive features of log4j is inheritance in loggers. The `log4j.xml` file that controls the content of the `luminis.log` for the admin server is found under this directory:

```
$CP_ROOT/products/tomcat/tomcat-admin/lib/classes
```

The `log4j.xml` file that controls content for the portal servers is found under this directory:

```
$CP_ROOT/products/tomcat/tomcat-portal/lib/classes
```

These files controls the level of detail written to the logs, the size of the logs, and the number of backup logs the system will create. The following sections explain how to control these options.

Note: This section does not go into detail about all of the logging behavior that can be controlled using log4j. You can obtain detailed information at the following Web site: http://jakarta.apache.org/log4j

Related Links

Portal and admin server logs on page 63

Set log detail

The level of detail in each log may be set with five options.

About this task

The printing detail determines the level of verbosity that goes into the log.

`FATAL` has the lowest priority and the lowest detail. The next level, `ERROR`, inherits the `FATAL` priority then adds additional detail. Priority increases at each level and inherits the priority of the lower level. `DEBUG` has the most priority and inherits the detail of the previous four levels.

Each level of priority increases the burden on system resources to produce the logs. You should use `DEBUG` sparingly, only when you must have all logging detail.

Table 3: Logging Levels

Log levels	Description
FATAL	This level designates very severe error events that will presumably lead the application to abort. Messages from these events are the

Log levels	Description
	most terse. FATAL is ideal for critical messages generated after an application quits abnormally.
ERROR	This level designates error events that might still allow the application to continue running. ERROR inherits the priority of FATAL. You might set the ERROR level to capture application error messages when the application can still hobble along.
WARN	This level designates potentially harmful situations. WARN inherits the priority of ERROR and FATAL. You might use WARN to log warning messages an application generates when it is able to run without problems.
INFO	This level designates informational messages that highlight the progress of the application at coarse-grained level. INFO inherits the priority of WARN, ERROR, and FATAL. You could use INFO for messages that are similar to the verbose mode of many applications.
DEBUG	This level designates fine-grained informational events that are most useful to debug an application. DEBUG inherits the priority of the previous four levels. Setting the level to DEBUG will place the greatest burden on system resources. You might use DEBUG to write debugging messages that should not be printed when the application is in production.

With a default installation, the `luminis.log` is set to the `WARN` logging level.

Use this procedure to change the logging level:

Procedure

1. Open the `log4j.xml` file located under the following path:

   ```
   $CP_ROOT/products/tomcat/tomcat-[admin|portal]/lib/classes
   ```

2. To set the verbosity, search for this parameter:

   ```
   <root>
   <priority value="INFO"/>
   <appender-ref ref="FILE"/>
   </root>
   ```

3. Change the **priority** value to the desired level such as, DEBUG, INFO, ERROR, and so on.
4. Save and close the file.

The logging level change will take effect approximately 60 seconds after you save the file.

Control Luminis log file size and backups

The `log4j.xml` file allows logging requests to be printed to multiple destinations.

In Log4j, an output destination is called an appender. By default, each Luminis Web server is configured with one appender that prints data to `luminis.log`.

Log4j monitors the size of the output file and creates backup copies of the file when the configured size limit is reached. The number of backup instances and size of the backup instances may be changed in the `log4j.xml` file. This will allow you to control the amount of disk space taken up by the logs.

You may adjust the size of the log file and the number of backups using these parameters in the `log4j.xml` file:

Locate the `<appender name="FILE" …>` tag and change:

```
<param name="MaxFileSize" value="10MB" />
<param name="MaxBackupIndex" value="5"/>
```

Once the maximum number of backups is reached, the oldest will be deleted, and the rest will have their index incremented. So on the file system, you see these file names:

```
luminis.log
luminis.log.1
luminis.log.2
luminis.log.3
luminis.log.4
luminis.log.5
```

Each file is 10.0 MB.

Access log management

Access logging is enabled by default in a Luminis installation.

If the data is not needed and additional performance is required, you can disable the log. To turn off access logging, edit this file:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/conf/server.xml
```

Comment out these lines:

```
<Valve className=”org.apache.catalina.valves.FastCommonAccessLogValve”
                 directory=”logs” prefix=”luminis_access.”
 suffix=”.log”
```

```
                 pattern=”common” resolveHosts=”false”/>
```

Surround the lines above with XML comments as follows:

```
<!--
        <Valve
 className=”org.apache.catalina.valves.FastCommonAccessLogValve”
                 directory=”logs” prefix=”luminis_access.”
 suffix=”.log”
                 pattern=”common” resolveHosts=”false”/>
-->
```

A server restart will be necessary for these changes to take effect.

The access log will be rolled over when the date on the computer changes. To control disk space usage, monitor this directory and delete logs that are no longer needed.

Here is an example of the output generated in the file:

```
149.24.205.104 - - [28/Apr/2010:16:30:22 -0600]
 “POST /web/luminis-admin-group/admins-welcome?
p_p_id=LuminisMonitor_WAR_luminis&p_p_lifecycle=0&p_p_state=maximi
zed&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2 HTTP/1.1” 200
 4041
127.0.0.1 - - [28/Apr/2010:16:30:23 -0600] “GET / HTTP/1.1” 302 -
127.0.0.1 - - [28/Apr/2010:16:30:24 -0600] “GET / HTTP/1.1” 302 -
149.24.205.104 - - [28/Apr/2010:16:30:24 -0600]
 “GET /web/luminis-admin-group/admins-welcome?
p_p_id=LuminisMonitor_WAR_luminis&p_p_lifecycle=0&p_p_state=normal
HTTP/1.1” 200 4808
```

Note: Each time a file is rolled over, a new file will be created. If access logging is enabled, you should monitor the logs directory and manage old logs to preserve file system space.

CAS logs

Logging in the CAS server installed with the Luminis deployment is controlled in a similar manner to that in the Luminis portal and admin servers.

The `log4j.xml` file is located in this directory:

```
$CP_ROOT/luminis/products/tomcat/cas-server/lib
```

The `cas.log` file for general logging located under this path:

```
$CP_ROOT/products/tomcat/cas-server/logs/cas.log
```

The size and number of backups of cas.log can be controlled by editing the fields in `log4j.xml` the same as the portal and admin servers.

OpenDJ logs

OpenDJ has three logs that should be monitored for size and errors.

```
$CP_ROOT/products/opends/logs/audit
$CP_ROOT/products/opends/logs/access
$CP_ROOT/products/opends/logs/errors
```

These logs may be configured and managed using the OpenDJ dsconfig utility. For more information on configuring and managing the logs, refer to the OpenDJ Wiki at this URL: https://wikis.forgerock.org/confluence/display/OPENDJ/OpenDJ+Documentation

Monitor system use

The total and peak number of users logged into the Luminis Platform system may be monitored from the **System Monitor** portlet.

The **System Monitor** portlet lists all nodes in the system by the host name where they are deployed and suffixed with `-admin` or `-portal` depending on whether they are an administration or a portal server. Peak session counts remain until the node is re-started. Counts are refreshed whenever the page is refreshed. The **Last Sample Time** field shows the last time a node updated its session count. Counts are periodically written to the database by each node, and all values read by the portlet.

Limit user sessions

Administrators should monitor system performance and set session limits appropriate to their particular installation.

It is desirable for an administrator to limit the number of active sessions on each portal node of the Luminis system. The number of users a portal can handle will depend on the hardware on which the system is installed as well as the average size and content of each user's layout.

Session limits may be set using the JMX interface and the Luminis Configuration Service MBean.

Limitations for simultaneous logins

Luminis Platform includes functionality that allows you to limit the number of simultaneous portal login attempts.

When a user logs in to the Luminis Platform portal, the system monitors the login attempts. If the login attempts reach a specified volume, users will be redirected to a page that states the server is currently busy. Monitoring simultaneous portal logins will prevent high volume of portal logins resulting in overwhelming servers and causing poor server performance.

There is a difference between the simultaneous portal login limit and the user session limit. The login limit monitors the overall number of logins. The user session limit is the number of logged in user sessions the portal server can support. The number of simultaneous login attempts the system can handle will depend on the hardware on which the portal is installed and the average size of the user's layout set.

By default, Luminis Platform is set up to limit the number of simultaneous login attempts. To change the default value, use the JMX interface and the Luminis Configuration Service MBean.

To disable the simultaneous portal login functionality, set this configuration property to false:

```
simultaneous.login.requests.enabled
```

To adjust the number of simultaneous portal logins, set this configuration property to an integer number:

```
maximum.simultaneous.login.requests
```

In some instances, you might not include certain URLs for simultaneous login monitoring. To exclude URLs from the simultaneous login monitoring process, a comma separated list of URLs must be added to this configuration property:

```
simultaneous.login.requests.exclude.urls
```

Warning! The JMX console does not check limits or properly formatted values. If non-integer value or an incorrect boolean value is entered, results will be unpredictable, including the potential inability to log in to the portal. Correct boolean values are true and false.

After connecting to the node to be managed, the configuration key for setting the session limit on a portal server is session.portal.maximum.concurrent.users. For an admin server, the value is session.admin.maximum.concurrent.users. The value should be set to an integer number, and the session limit will take effect immediately on the server to which the JMX console is connected.

Note: The session limits will propagate to other nodes once the configuration cache timeout is reached, set to 30 minutes by default. However, if you want to enforce session limits more quickly than a cache timeout, use the JMX console to set the value directly on each node.

Warning! JMX console does not check limits or properly formatted values. If a non-integer value is entered, results will be unpredictable, potentially including the inability to log in to the portal.

The Directory Server

Luminis Platform uses the OpenDJ software to house and manage LDAP-based data store that contains user data.

An overview of how Luminis Platform has implemented the Lightweight Directory Access Protocol (LDAP), information about browsing the LDAP directory, and suggestions for administering and backing up the OpenDJ Directory Service that manages the system's LDAP store.

Note: The Directory Server software is an open source site project. Initial development of OpenDJ was done by Sun Microsystems, but it is now available under the open source Common Development and Distribution License (CDDL). For more information on the OpenDJ software, refer to the following URL: http://opendj.forgerock.org. This URL contains links to several OpenDJ manuals. The links on this Web site are subject to change without notice.

LDAP overview

The Luminis system uses a Lightweight Directory Access Protocol (LDAP) server to store basic user information.

LDAP is an open Internet standard produced by the Internet Engineering Task Force (IETF) for accessing directories that store information about individuals, groups, files, and other relevant information on a network. The Luminis system uses an LDAP server to store basic user information.

LDAP makes it possible for almost any application running on virtually any computer platform to obtain directory information. Since LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

LDAP is an efficient approach to directory services for these reasons:

- Runs directly over Transmission Control Protocol (TCP), thus bypassing much of the upper-layer overhead of the Open Systems Interconnection (OSI) stack
- Simplifies the functionality provided by X.500, leaving out little-used features and redundant operations
- Uses simple string formats that are easy to process
- Inherits the same encoding rules used by X.500 to encode data for transport over the network

LDAP in the Luminis system

The Luminis systems use LDAP because it is well suited to the type of data that needs to be stored and retrieved.

A Lightweight Directory Access Protocol (LDAP) directory stores information in the form of entries. Each entry is a collection of attributes, and each attribute has a type and a value. An attribute's type is usually a string that is easy to remember, such as, `cn` to represent a common name. An attribute's value depends on the type. For example, an attribute for a user's e-mail address might contain the value mailto:admin@luminisplatform.edu.

The schema is a set of rules that define object classes and the attributes they contain, along with the type of data can be stored. Object classes act as templates for creating entries. Every item that is stored in an LDAP directory is an entry.

Containers are regular entries that create a branch point in the Directory Information Tree (DIT). Any entry can be used as a container, although organization unit (ou) objects are commonly used. The container does not maintain a list of entries; it only serves as a component of a Distinguished Name (DN) that specifies part of a path in a search base.

A Directory Server Entry (DSE) is a one-per-server entry that is created when the directory server is installed. The DSE contains server-wide configuration information including the version of the LDAP protocol, a list of server controls, and the suffixes.

Suffixes are naming contexts. Suffixes are listed in the DSE when it is created. An entry is associated with a suffix that is the root entry for the DIT. The last component of a DN is always a directory suffix, such as ou=people, o=cp.

In this entry, o=cp is the suffix, and ou=people,o=cp, is a subtree that provides a container in which to store other entries. The root and primary containers of the Luminis DIT are organized as follows:

- o=<cp>. This is the top node of the Luminis DIT. It is a variable that is set during installation.
- ou=People. This container includes the person entries (name, password, email, and so on).

View LDAP server data

To view LDAP server data, you can use any LDAP browser or standard LDAP URL search strings in any Web browser. You can also use a command line LDAP search utility provided with OpenDJ called ldapsearch.

This utility is located under the shared bin directory. A typical ldapsearch command looks similar to:

```
./ldapsearch -h localhost -p 389 -b “ou=people,o=cp” -D “cn=Directory
 Manager” -w password “objectclass=*”
```

When you run the ldapsearch command, you provide a number of arguments that define the LDAP directory to search and what you are searching for. For example, in the command above, the final portion of the ldapsearch command (objectclass=*) is the search filter that you use to narrow your result set.

Table 4: Example ldapsearch command arguments

-h	The hostname of the computer upon which the LDAP directory is installed (the Luminis server).
-p	The port on which the Directory Server is running.
-b	The base Distinguished Name (DN) for the search.
-D	The user object used to bind to the directory.
-w	The password for the user specified above (-D).

If you wanted to find the record for an individual whose username is johndoe, you would execute this ldapsearch command using a filter of uid=johndoe:

```
./ldapsearch -h localhost -p 389 -b “ou=people,o=cp” -D “cn=Directory
 Manager” -w password “uid=johndoe”
```

If you wanted to find the record for a user with an e-mail address of mailto:johndoe@school.edu , you would use this filter: `mail=mailto:johndoe@school.edu.`.

You may also use wildcards (represented by *) in these search filters. For example, a filter of mail=*smith* would return all users having the sequence smith in their e-mail addresses. If you want to limit the attributes for the objects returned in the search, you may specify a space-separated list of those attributes after the search filter. For example, this command would return the records for objectclass=* and would display only the givenname and surname (sn) attributes for these records.

```
./ldapsearch -h localhost -p 389 -b “ou=people,o=cp” -D “cn=Directory
 Manager” -w password “ objectclass=*” givenname sn
```

For more information on using the ldapsearch utility, refer to the OpenDJ documentation on forgerock.org.

Start and Stop the directory server

Although the Directory Server starts automatically when the Luminis system is started, you may have occasion to start and stop the Directory Server independent of the Luminis Platform.

For this you can use command line tools and the procedures listed below.

Stop the OpenDJ directory server

Use this procedure to stop the OpenDJ Directory Server:

Procedure

1. Log in to the Luminis server as the administrative user.
2. Open a console.
3. Change to one of these directories:
   - On Windows

     `$CP_ROOT/products/opends/bat`
   - On UNIX

     `$CP_ROOT/products/opends/bin`
4. Issue this command, depending on your operating system.
   - On Windows

     `stop-ds.bat`
   - On UNIX

     `stop-ds`

Results

Another way to stop the directory server is to execute this command:

```
10-ldap stop
```

The `10-ldap` script can be found inside the `<luminis install>/bin directory`. This command becomes available once you source the `$CP_ROOT/.cprc` file.

Start the OpenDJ directory server

Use this procedure to start the OpenDJ Directory Server:

Procedure

1. Log in to the Luminis server as an administrative user.
2. Open a console.
3. Change to one of these directories:
   - On Windows

     `$CP_ROOT/products/opends/bat`
   - On UNIX

     `$CP_ROOT/products/opends/bin`
4. Issue this command, depending on your operating system.
   - On Windows

     `start-ds.bat`
   - On UNIX

     `/start-ds`

   Another way to stop the directory server is to execute this command:

   `10-ldap start`

   This command becomes available once you source the `$CP_ROOT/.cprc` file.

Administer the directory server

The primary configuration file in OpenDJ can be used to administer or reset the behavior of the system: `config.ldif`.

This configuration file is located under this path:

```
../opends/config/config.ldif
```

You will need to restart the system before any changes to the configuration file take effect.

OpenDJ also comes with a command-line tool called `dsconfig`. This easy-to-use tool allows you to access the LDAP configuration while the server is online. The `dsconfig` tool allows you to make immediate changes to the directory server instance. You may find the tool in these directories:

- On Windows

```
../opends/bat/dsconfig.bat
```

- On UNIX

```
../opends/bin/dsconfig
```

If you execute the `dsconfig` command with no arguments, the tool will provide you with a menu of options. For more information on dsconfig, refer to *OpenDJ Administration Guide*.

The following sections outline some basic administrative routines that you could perform periodically.

Change admin password

OpenDJ comes with a command-line tool called `ldappasswordmodify`. This tool allows you to change user passwords.

You may find the tool in these directories:

- On Windows

```
../opends/bat/ ldappasswordmodify.bat
```

- On UNIX

```
../opends/bin/ ldappasswordmodify
```

Below is an example of how you would use the `ldappasswordmodify` tool to modify the admin password. With this example you can change the password from oldpassword to newpassword.

```
./ldappasswordmodify -h localhost -p 389 -D “cn=Directory Manager” -w
 oldpassword -c oldpassword -n newpassword
```

Table 5: Example ldappasswordmodify command arguments

-h	The hostname of the computer upon which the LDAP directory is installed (the Luminis server)
-p	The port on which the Directory Server is running
-D	The user object used to bind to the directory

-w	The password for the user specified above (-D)
-c	The current password
-n	The new password

For more information on changing passwords in OpenDJ, refer to the *OpenDJ Administration Guide*.

Monitor logs

To keep the Directory Server running smoothly and to ensure that the data it contains is protected, you will occasionally need to monitor the access, error, and audit logs associated with the Directory Server. This lists the logs located in the specified directories.

Name	Location
	`<luminis install>/products/opends…`
Access Log	`…/logs/access`
Error Log	`…/logs/errors`
Audit Log	`…/logs/audit`

LDAP directory backup

In addition to monitoring the logs, you will also need to periodically back up the data contained in the LDAP directory.

This is done by creating a Lightweight Directory Information Format (LDIF) file.

Determine the directory manager credentials

For some administrative tasks, you will need the Directory Manager Login credentials.

About this task

Use this procedure to get the Directory Manager Login credentials:

Procedure

1. Log in to the Luminis server as the administrative user.
2. Using an editor, open this file:

   ```
   $CP_ROOT/products/tomcat/tomcat-admin/shared/classes/
   bootstrap.properties
   ```
3. Inside the `bootstrap.properties` file, you will see these properties:

   ```
   ldap.directory.manager.dn
   ```

```
ldap.directory.manager.password
```

Results

The properties mentioned above indicate the current domain and password for the LDAP.

Optional configuration properties

You may need to add a number of properties to customize elements of the system for your organization or to facilitate integration with other external systems.

This table provides a comprehensive list of the site-specific properties that you may need to adjust to accommodate the Banner® Relationship Management (BRM) Prospective Student Portal (PSP), and includes a description of what each property does and the values it supports. For more information about configuring PSP to function within Luminis Platform, see the *Banner Relationship Management Luminis Platform 5 Prospective Student Portal Administration Guide*.

Table 6: PACWA Parameters

Property	Default Value	Description
`brm.pacwa.account_creation_enabled`	false	Set to true to enable the link to the un-invited scenario to appear in the prospect portal home page. Set to false to disable.
`brm.pacwa.accept_invite_enabled`	false	Set to true to enable the link to the invited scenario to appear in the prospect portal home page. Set to false to disable.
`brm.pacwa.cancel_url`	`Site/portalHome.jsp`	Redirect URL when an account creation process is canceled. If no value is supplied, the **Cancel** button is not available on the PACWA form(s).
`brm.pacwa.terms_of_use_url`	`Site/tos.html`	URL to open as a pop-up window to display terms of service. If no value is supplied, the **Terms of Use** check box is not displayed in the account creation form(s).
`brm.pacwa.portal_username_conflict_url`	`site/loginconflict1.html`	URL to open as a pop-up window when the user chooses a login identifier that is already associated with a Portal account. The login identifier in conflict is supplied as a

Property	Default Value	Description
		username query parameter appended to this URL.
brm.pacwa.account_ already_created_url	site/ loginconflict2.html	URL to open as a pop-up window when the system assigned login identifier is already associated with a Portal account when a prospect accepts an account creation invitation. The login identifier in conflict is supplied as a username query parameter appended to this URL.
brm.service_base_ url	No Default	Base URL for the Banner Relationship Management web service endpoint(s). The secure HTTP transport (https) port should be designated when configuring this parameter. Used by default for PACWA and other Banner Relationship Management prospect portal functionality.
brm.service_ username	No Default	Username to authenticate Banner Relationship Management web service operations. Used by default for PACWA and other Banner Relationship Management prospect portal functionality.
brm.service_ password	No Default	Password to authenticate Banner Relationship Management Web service operations. Used by default for PACWA and other Banner Relationship Management prospect portal functionality.
brm.service_timeout_ millis	20000	Time out in milliseconds for Banner Relationship Management Web service operations. If an operation takes longer than this time, it will be aborted and an error will be reported. The default is usually sufficient.

Property	Default Value	Description
`brm.pacwa.default_nation_code`	157 (United States)	Banner STVNATN validation for the Country value chosen as default in the account creation form.
`brm.pacwa.default_term_code`	Empty (1st term in list when sorted by validation code descending)	Banner STVTERM validation code for the Term Interest value chosen as default in the account creation form. Changes in this value require a restart of the Luminis Web server to become effective.
`brm.pacwa.default_state_code`	Empty (1st state in list when alpha sorted)	Banner STVSTAT validation code for the State value chosen as default in the account creation form.
`brm.pacwa.disabled_url`	/	Redirect URL used when account creation is disabled.
`brm.pacwa.webappName`	luminis-pacwa	Name of the Luminis PACWA web application.
`brm.prospect.immutable_group _id`	165	Luminis Group immutable id of the group where invited and unrestricted accounts are placed.
`brm.pacwa.portal_login_submit_url`	`https://%{cas.host}:%{cas.https.port}/%{cas.webapp.path}/login?service=https://%{portal.virtual.host}:%{portal.virtual.https.port}/c/portal/login`	URL for the Luminis portal login operation.
`brm.pacwa.portal_frame_url`	http://${cas.logout.redirect.url}	The URL behind the **Click here to log in** link on the PACWA page.
`brm.metadata_ version`	8	PACWA specific Banner version setting.
`brm.pacwa.field_used.birthdate`	false	Determines if the birth dates can be displayed in PACWA and the Prospect Portlet.
`brm.pacwa.field_used.gender`	false	Determines if the gender can be displayed in PACWA and the Prospect Portlet

Property	Default Value	Description
brm.pacwa.field_used.house_number	false	Determines if the house number can be displayed in PACWA and the Prospect Portlet
brm.pacwa.field_used.phone_country_code	false	Determines if the phone country code can be displayed in PACWA and the Prospect Portlet
brm.pacwa.field_used.street_line_4	false	Determines if the street line 4 can be displayed in PACWA and the Prospect Portlet
brm.pacwa.field_used.surname_prefix	false	Determines if the surname prefix can be displayed in PACWA and the Prospect Portlet

Change directory server admin password

When you change the Administrator's directory server password, you will need to make additional file modifications to Luminis Platform.

The following sections list the changes.

Change directory server password in CAS

To change the directory server password, you must modify one file for each CAS instance.

```
$CP_ROOT/products/tomcat/cas-server/webapps/cas-web/WEB-INF/
deployerConfigContext.xml
```

Note: The administrator may have changed the `cas-web.war` name during installation; use the value specified by the `cas.webapp.path` configuration value.

In this file, find the bean identified by contextSource:

```
<bean id=”contextSource”
 class=”org.jasig.cas.adaptors.ldap.util.AuthenticatedLdapContextSource”>
```

Within this block of XML code you'll see this:

```
<property name=”userDn” value=”cn=Directory Manager”/>
 <property name=”password” value=” OLD-PASSWORD “/>
```

Modify the password value OLD-PASSWORD so that it matches the new directory server admin password.

Change directory server password in the portal

For each portal, modify the `bootstrap.properties` file to change the directory server password.

This file will be found in one of two locations depending on the server node. For admin server instances, it will be under this path:

```
$CP_ROOT/products/tomcat/tomcat-admin/shared/classes/
bootstrap.properties
```

For portal instances it will be under this path:

```
$CP_ROOT/products/tomcat/tomcat-portal/shared/classes/
bootstrap.properties
```

Find the property named `ldap.directory.manager.password` and set it to the new directory server password.

Change database account password

If you change the password for Luminis Platform's database account, you must also modify the Luminis Platform system.

Listed below are the file changes you will need to make within the system.

Change database password in the installer

To perform installation functions on the product such as uninstall or patching, modify this file:

```
$CP_ROOT/install/resolved.properties
```

Find the property named `luminis.database.user.password` and set it to the new database password.

Change database password in CAS

For each CAS instance, modify this file to change the database password:

```
$CP_ROOT/products/tomcat/cas-server/webapps/cas-web/WEB-INF/classes
```

Inside this file you will need to find the bean identified by *dataSource*. Within that block of XML code you will see this:

```
p:password="OLD-PASSWORD"
p:username="DB-USER"
```

Modify the password to the new database password.

Change database password in the portal

For each portal instance, modify these four files to change the database password:

Admin portal instances

Modify these admin portal instances to change the database password.

```
$CP_ROOT/products/tomcat/tomcat-admin/shared/classes/
bootstrap.properties
$CP_ROOT/products/tomcat/tomcat-admin/conf/server.xml
$CP_ROOT/products/luminis-repository/admin/workspaces/luminisWorkSpace/
workspace.xml (patched system only)
$CP_ROOT/products/liferay/liferay-admin/data/jackrabbit/home/
workspaces/liferay/workspace.xml
```

User portal instances

Modify these user portal instances to change the database password.

```
$CP_ROOT/products/tomcat/tomcat-portal/shared/classes/
bootstrap.properties
$CP_ROOT/products/tomcat/tomcat-portal/conf/server.xml
$CP_ROOT/products/luminis-repository/portal/workspaces/
luminisWorkSpace/workspace.xml (patched system only)
$CP_ROOT/products/liferay/liferay-portal/data/jackrabbit/home/
workspaces/liferay/workspace.xml
```

Within each file, you will find references to the old database password. You will need to update these references to reflect the new database password.

File	Property	Change
`bootstrap.properties`	Find the property named `luminis.database.user.password`	Set it to the new database password

File	Property	Change
`server.xml`	Find the property inside the tag `<Resource name="jdbc/ LuminisPooledDB"` named password	Replace the old password in `password="OLD-PASSWORD"` with the new password.
`luminis-jcrRepository.xml`	Locate each instance of the following XML	Replace the old database password with the new password: *<param name=”password” value=”OLD-PASSWORD “/>*
`workspace.xml`	Locate each instance of the following XML	Replace the old database password with the new password: *<param name=”password” value=”OLD-PASSWORD “/>*

Luminis Database Connection Pooling

Luminis Platform makes use of the C3P0 connection pooling software to increase performance and reliability of the database connections.

About this task

While the default settings should be sufficient for most installations, you can modify the parameters to fit your institution's unique needs. The connection pool configuration is located in this file:

```
$CP_ROOT/products/tomcat/tomcat-[admin|porta]/conf/server.xml
```

In `server.xml`, the connection pool is defined within the `<Resource>` tag:

```
<Resource name="jdbc/LuminisPooledDB"
              auth="Container"
              description="Luminis database pooled connections"
              dataSourceName="LuminisPooled"
              driverClass="com.mysql.jdbc.Driver"
              user="[YOUR_DB_USER]"
              password="[YOUR_DB_PASSWORD]"
              jdbcUrl="jdbc:mysql://[servername]:[dbport]/[DBNAME]?
useUnicode=true&amp;characterEncoding=UTF-8"
              initialPoolSize="10"
              maxPoolSize="50"
              minPoolSize="10"
              acquireIncrement="5"
              factory="org.apache.naming.factory.BeanFactory"
              type="com.mchange.v2.c3p0.ComboPooledDataSource"
```

```
idleConnectionTestPeriod="60"
testConnectionOnCheckout="true"
unreturnedConnectionTimeout="3600"
numHelperThreads="10"
automaticTestTable="LP_C3P0_CONN_TEST"
/>
```

Table 7: Connection pool behavior values

Value	Description
`initialPoolSize`	The number of JDBC connections allocated on startup.
`maxPoolSize`	The maximum number of connections that may be allocated in the pool.
`minPoolSize`	The minimum number below which connections will not be closed.
`acquireIncrement`	The number of connections allocated at one time when the need for a new connection is determined.
`idleConnectionTestPeriod`	The number of seconds between times that connections will be tested and culled, if necessary.
`testConnectionOnCheckout`	Whether connections will be tested before being handed over to the caller.
`unreturnedConnectionTimeout`	The amount of time to wait before assuming a connection is hung and will not be returned.
`numHelperThreads`	The number of threads to allocate to asynchronous allocation, testing, and culling of connections.
`automaticTestTable`	The name of the table to be used in the database for testing connection operations.

Note: You must restart the Tomcat instance for changes to the `server.xml` file to take effect.

For a more complete description of the meaning of these and other C3P0 connection pooling parameters, click this link:

http://www.mchange.com/projects/c3p0/index.html#configuration_properties.

Note: The links on this Web site are subject to change without notice.

C3P0 pooling statistics may be monitored using the JMX protocol via JConsole or another JMX-compatible management console. To view the pooling statistics, complete these steps:

Procedure

1. Open JConsole and navigate to the **MBeans** tab.
2. Open the `com.mchange.v2.c3p0` folder.
   - Under the **Attributes** sub-category, you can view the current configuration of the pool
   - Under the **Operations** sub-category, you can view statistics of the connection pool, such as number of busy connections, idle connections, and so forth

Portal Content

Information about Web content and Luminis Portlets for Banner, including how to set up and deploy these portlets within Luminis Platform.

Content development and delivery

The system provides a number of tools to create, deploy and maintain content throughout the system.

Compliance with various portlet standards, such as JSR-286, is key to sophisticated content development. In addition to portlet support, the Luminis® Platform system offers alternative methods and tools to create, publish and maintain content throughout the system.

Some of the key content development features in Luminis Platform:

- Web content development portlets provide easy to use editing tools to quickly create rich Web content. These Web content portlets are available:

Portlet	Description
The Web Content Display application	Added to pages using the **Add** menu by both administrators and non-administrative users.
Administrators and Authorized Content Owners	Administrators and content owners create and publish content of all types using a rich text editor and simple workflow process. Advanced application source code can also be written and uploaded to the **Web Content Display** portlet. The Web Content Display application works alongside the layout management functions noted above allowing such content to be sent globally or personalized to various users. To manage content in the **Control Panel**, select the specific site from the drop down, then select **Web Content**.
Non-Administrative users	If you have configured permission, non-administrative users can create and publish content in the **Web Content Display** portlet. They can use this content personally or share it with other users using **My Public Pages**.Non-administrative users can manage their content in Web Content Display application from the **Control Panel** by selecting the specific site from the drop down for which to manage content, then selecting **Web Content**. However, the content is

Portlet	Description
	personal and kept separate from the admin content created using this tool.

- Add pages of different types. Provides greater access to Web content. For example, a URL page type, creates views to any content on the Web. When a user chooses to create a new page in the Luminis system, using the Manage Pages option, there are several page types which can be selected to control the content displayed on the page.

Page type	Description
Embedded	Shows an external Website or application as a page of a Liferay Website through an Iframe. Good for quick integration of external applications. The Iframe automatically resizes to avoid unnecessary scrolling.
Link to Page	An extension to the URL type. A link to other pages of the Liferay system.
Panel	A modification of the portlet page type. The user selects portlets from an available list. The selected portlets display as a menu. When a user clicks on a portlet in the menu, the portlet renders on the page. This allows the user to have access to many portlets, but you can only view one portlet at a time.
Portlet	Allows the user to place portlets on a page.
URL	A link to an external resource in the Web site menu. This page type does not show content. When you click a page, the corresponding URL opens in the window and replaces the page contents.

- Use inline frame portlets to pull in various content from external sites. Administrators use the iFrame portlet to organize content from external sites into a portlet that is placed on user layouts. Non-administrators syndicate content from external sites into a portlet that is placed on their personal pages in the portal. For example, an application for the iPhone works in Luminis Platform using the iFrame portlet.
- RSS portlet. Administrative and non-administrative tool to pull in and aggregate RSS feeds.
- Other Content Types. Tools for portal users such as bookmarks, dictionaries, currency converters, site maps, loan calculators and Google Maps.

  Note: Several portlets also support internal publication for RSS (not just consumption) and the Liferay framework supports creating a publishing mechanism for almost any portlet to be RSS enabled.

Options available for each page type

Once the page has been added to the system, the user can set various page options.

Field	Description
Name	The recognizable name in the system. This name identifies the page to the user in the User Interface.
HTML Title	The title used to display in the title bar of the browser.
Localized language	Set a translated page name and HTML title for each language in the list.
Type	Described in "Content development and delivery."
Hidden	Temporarily hides the page from others.
Friendly URL	Send this URL to other users for quick access to the page. This URL displays in the address bar of the browser.
Icon, User Icon, Target	Associate an icon with a page. The use of the icon is dependent on the theme.
Copy Page	Make a copy of an existing page. For example, if you create a portlet type page, you could select another portlet type page from the **Copy Page** menu. When you click **Save**, the new page is created and any content on that page is copied to the new page.

Specific page options

Once the page has been added to the system, the user can then set various page options.

Field	Description
URL	This is the URL of any page in the World Wide Web only available for the Embedded and URL page type.
Web Content ID	A reference to the Web Content created using the Liferay Web Content tools.
Link to Page	Creates a page which references to an existing page. The choices presented to the user are only for the time in which the new page is being created. For example, if a page is created in

Field	Description
	the Public Pages area for a user, then the list of choices are only pages in that space.

Create Web content

The **Web Content Display** portlet provides a rich text editing application for administrative users and non-administrative users to create new Web content within the portal.

About this task

Multiple instances of the portlet can be placed on the same page or added to different pages. Administrators can use this tool to create content and publish that content to users through the Shared Workspaces method. Non administrative users can add this portlet to any page within their personal pages to create robust content that is viewed and managed by them.

Note: As with all other end user areas, you may want to use a modified version of the instructions to support usability of this tool.

To add the **Web Content Display** portlet to your site:

Procedure

1. Log in to Luminis Platform as an administrator.
2. Select **Go to** > **Control Panel** > **Portal** > **Sites**.
3. Next to the home site, click **Actions** > **Manage Pages**.
4. In the home site page, click **View Pages**.

   A separate browser window appears with a view of a portal page. Here you build the content and layout for the page while viewing it as the end user would. An Administrator can see all the targeted pages under the home site in this view.
5. Select the page where you want to add the **Web Content Display** portlet.
6. Click **Add** to open the menu and add the portlets or applications to the page as needed.
7. Select the Content Management category or search Web Content Display.
8. Add the **Web Content Display** portlet to the page and move it to the page area you want to display the content.

   Note: You can add the portlet multiple times on one page or to a different page.
9. You can add new Web content or select existing Web content to be displayed within the portlet.

Add Web content via the Web Content Display portlet

Use the **Web Content Display** portlet to add content to a page.

Procedure

1. In the **Web Content Display** portlet, click

   📄

   .
2. Enter a valid name and the required content you want to display.
3. Set the permissions for the content.
4. Click **Publish** to immediately publish the content.
5. To save the content without displaying the content in the portlet or placing the content in a queue for approval, click **Save as Draft**.

Select Web content for display

If Web content has been previously created and approved, you can select content to display within the portlet.

About this task

This is useful for cases where you want the content to be displayed on multiple pages of the selected workspace.

Procedure

1. In the **Web Content Display** portlet, click

   ⚙

   .
2. Select a Web content item from the list of displayed Web Content items.
3. Click **Save**.
4. Close the **Web Content Display - Configuration** pop-up.

Set portlet title

Changing the portlet title allows users to focus on different content that has been created using the Web Content feature.

Procedure

1. Select the title of the portlet. For example, Web Content Display.
2. Change the title of the portlet.
3. Click outside the portlet title or click **Enter** to save the portlet title.

   Note: Changing the portlet title does not add this portlet to the **Add** menu. It only impacts this portlet instance displayed on the selected page.

Manage Web content using control panel

The **Web Content Display** portlet is one of several content development tools in Luminis Platform. It provides a rich text editing application to create new Web content within the portal.

Multiple instances of the portlet can be placed on the same page and added to different pages. Administrators can use the tool to create content and publish the content to users through the Shared Workspaces method. Non-administrative users can add the portlet to any page within their personal pages to create robust content that can be viewed and managed by the users.

The Web content section of the **Control Panel** can be used to manage all of the content associated with a specific workspace. Content can be created, edited, viewed, approved, and deleted using this interface. Additional groups can be given permissions to the content. In Luminis Platform, only those users, who have access to the Administrators node, will see this option in the **Control Panel**.

For more information about Web content management, refer to the "Web Content Management" section of the *Liferay Portal 6.1 User Guide* found on Liferay.com.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Select a site

Locate and open a site within Luminis Platform.

Procedure

1. Log in to Luminis Platform as an administrator.
2. Select **Go to** > **Control Panel**.
3. Select the required site from the drop-down menu.

Note: Web content is associated with sites. Web content created in one site cannot be shared with other sites.

Add Web content to a site

You can add Web content to your site page.

Procedure

1. Select the required site from the drop-down menu.
2. Click **Web Content**.
3. Click **Add**.
4. Enter a valid name and description.
5. Set the required permissions for the content.
6. Select the appropriate save option.
    - Click **Publish** to immediately publish the content.
    - Click **Save as Draft** to save the content but not display the content in the portlet. This action also places the content in a queue for approval.

Set Web content permissions

You can set permissions to view a Web content each time you create.

About this task

Field	Description
Delete Discussion	Allows users to delete comments on this content.
Update Discussion	Allows users to update comments on this content.

To set Web content permissions:

Procedure

1. Select the site from the drop-down menu.
2. Select **Web Content**.
3. Click **Actions** next to the Web Content for which you would like to manage permissions.
4. Select **Permissions** from the menu.
5. Select the appropriate check boxes to assign permissions to the appropriate roles.

Edit Web content for a site

You can edit site contents at any time.

Procedure

1. Select the site from the drop-down menu.
2. Select **Web Content**.
3. Click **Actions** next to the Web content that you want to edit.
4. Click **Edit**.
5. Make the required modifications and select the appropriate save option.
   - Click **Publish** to immediately publish the content.
   - Click **Save as Draft** to save the content but not display the content in the portlet. This action also places the content in a queue for approval.

Preview Web content

You can preview site content before you publish it for general view.

Procedure

1. Select the site from the drop-down menu.
2. Select **Web Content**.
3. Click **Actions** next to the Web content that you want to edit.
4. Click **View**.

Results

Depending on the browser preference setting, the content is displayed.

Approve Web content

You can approve site content that another user has written.

Procedure

1. Select the site from the drop-down menu.
2. Select **Web Content**.
3. Click **Actions** next to the Web content that you want to edit.
4. Click **Edit** and make the required modifications.
5. Click **Publish**.

Delete Web content

You can delete content no longer applicable for a site.

Procedure

1. Select the site from the drop-down menu.
2. Select **Web Content** tab.
3. Click **Actions** next to the Web content that you want to delete.
4. Click **Delete**. The system will prompt you to confirm the delete action.

Advanced features of Web content

Field	Description
Abstract	Create a brief summary of the Web content along with a small image
Categorization	Specify a type for content for Announcements, Blogs, General, and so forth. Apply categories and tags to the Web content so users can filter and search for content.
Custom Fields	Customize metadata about the Web content
Display Page	Determine where the Web contents are displayed when linked from other pages
Mail notifications for Web content	Set properties in the system to have e-mail notifications sent to users for approval, denials, and reviews. By default these features are disabled and must be enabled using properties in the `portal-ext.properties` file. Set these properties to true to enable the notification: • `journal.email.article.approval.denied.enabled=false` • `journal.email.article.approval.granted.enabled=false` • `journal.email.article.approval.requested.enabled=false` • `journal.email.article.review.enabled=false` Set these properties to set default templates associated with each notification:

Field	Description
	• `journal.email.article.approval.denied.subject=com/liferay/portlet/journal/dependencies/email_article_approval_denied_subject.tmpl` • `journal.email.article.approval.denied.body=com/liferay/portlet/journal/dependencies/email_article_approval_denied_body.tmpl` • `journal.email.article.approval.granted.subject=com/liferay/portlet/journal/dependencies/email_article_approval_granted_subject.tmpl` • `journal.email.article.approval.granted.body=com/liferay/portlet/journal/dependencies/email_article_approval_granted_body.tmpl` • `journal.email.article.approval.requested.subject=com/liferay/portlet/journal/dependencies/email_article_approval_requested_subject.tmpl` • `journal.email.article.approval.requested.body=com/liferay/portlet/journal/dependencies/email_article_approval_requested_body.tmpl` • `journal.email.article.review.subject=com/liferay/portlet/journal/dependencies/email_article_review_subject.tmpl` • `journal.email.article.review.body=com/liferay/portlet/journal/dependencies/email_article_review_body.tmpl`
Permissions	Determine the users who can access to the content
Related Assets	Connect any number of assets within a site or across the portal
Schedule	Set a range of dates during which the content will display or be removed from display.

Field	Description
	Set a review date for each piece of content. Luminis Platform uses a review date to send an e-mail message to Administrators to remind them to review a piece of content. The system needs to be configured to allow for review messages to be sent.

What is a portlet?

A portlet is a Web-based component managed by portlet containers that supply dynamic content.

Portals, such as Luminis Platform, support portlets as a pluggable user interface component (a presentation layer) for the backend information systems.

What is the JSR - 286 Standard?

The JSR - 286 standard is Java Portlet Specification (JSR-286), is a method to achieve interoperability among portlets and portals.

It is developed under the Java Site Process (JCP) and created in alignment with Web Services for Remote Portlets (WSRP) to improve the short comings of JSR-168 specification. Some of the features include:

- Inter-portlet Communication through events and public render parameters
- Serving dynamically generated resources directly through portlets
- Introduction of portlet filters and listeners
- Serving AJAX or JSON data directly through portlets

It is a method to achieve interoperability among portlets and portals. By adhering to the standards, it is easy to build portlets that can run in portals, irrespective of the vendors.

Previously, to develop and maintain a separate version of a portlet that complied with the vendor-specific portlet API for each and every vendor portal. The related tasks were time-consuming, aggravating, and cumbersome. Also, a major disadvantage to the end users, developers, and vendors, was that only a limited number of applications were available with few portals.

JSR-286 defines the Application Programming Interface (APIs) for portlets and by standardizing the rules for preferences, user data, portlet requests and responses, deployment, packaging, and security. In addition to JSR-286 support, Luminis Platform includes sophisticated personalization features to provide customized views of these varying types of content to different types of users.

Portlet lifecycle

A portlet is managed through a life cycle that defines certain questions.

- How is it loaded?

- How is it instantiated and initialized?
- How does it handle requests from clients?
- How is it taken out of service?

These methods are specified in the portlet interface:

- init(PortletConfig)
- processAction(ActionRequest, ActionResponse)
- render(RenderRequest, RenderResponse)
- destroy( )

The lifetime of a portlet is controlled by how long a portlet stays in the cache. When a portlet is removed from the cache, the portlet is effectively removed from memory and is no longer accessible. If a portlet is removed from the cache, and then requested again, the portlet will have its *init ( )* method called again and a new instance is created for the portlet.

Both the system administrator and programmer can control the lifetime of a portlet, by controlling how long a portlet resides in the cache. Cache is also used to control the refreshing of content.

A portlet interface also called portlet container defines two methods for handling requests, the processAction method and the render method.

A client request triggered by an action URL (related to the method processAction) translates into one action request and many render requests, (one per portlet in the portal page). While a client request triggered by a render URL (related to the render method) translates into many render requests (one per portlet in the portal page).

Typically, in response to an action request, a portlet updates the state based on the information sent in the action request parameters. Such request parameters are often contained in the URLs created by portlets, also called portlet URLs. Portlet URLs can either be action URLs or render URLs.

The destroy phase is dependent on the life time definition of the portlet.

Portlet phase

When a portlet is rendered, it undergoes different phases.

Phase	Description
End of Service	The portlet container is not required to keep a portlet loaded for a particular period of time. A portlet object may be kept active in a portlet container for a period of a millisecond, for the lifetime of the portlet container (which could be a number of days, months, or years), or any amount of time in between. When the portlet container determines that a portlet should be removed from service, it calls the destroy ( ) method of the portlet interface to allow the portlet to release any resources it is using and save any persistent state. For instance, the

Phase	Description
	portal will clean up any resources that it holds (including memory, file handles, and threads) in the implementation of the method destroy.
Initialization	The init ( ) method, after the portlet object is instantiated, the portlet container must initialize the portlet before invoking it to handle requests. Initialization is provided so that portlets can initialize the backend connections and perform the other one-time activity.
Loading and Instantiation	A portlet container is responsible for loading and instantiating the portlets. The loading and instantiation can occur when the portlet container starts the portlet application, or is delayed until the portlet container determines whether the portlet is needed to service a request.
Request Handling	After a portlet object is properly initialized, the portlet container may invoke the portlet to handle client requests.

Portlet modes

A portlet mode tells the portlet what task it should perform and what content it should generate. It indicates the function a portlet is performing.

The different modes for a portlet are:

- Look and feel
- Configuration
- Minimize
- Maximize
- Remove

Extend JSR-286 portlets

A JSR 286 portlet can be extended to add features and functionalities.

- Servlet lifecycle listeners
- Portlet filters for wrapping the request / response
- PortletURL listeners for manipulating the URL before it is written to the output stream
- Portlet-managed modes allowing the portlet to provide its own portlet modes

Related Links

Step 3 Compile the WAR file on page 101

Coordinate portlets

Inter-portlet communication is a communication between two portlets.

For example, a weather portlet displays the weather information of a city and a map portlet displays the location of the city. Since, both the portlets would use the same zip code for a user, there should be mechanism provided by the portal containers to allow portlets to share the zip code.

Previous to JSR 286, the support for inter portlet communication was rather minimal and information sharing between different portlets was accomplished primarily using application scoped session objects or vendor specific APIs. In JSR 168, maintaining the uniqueness of the session attribute over a complex application was a concern. It was regarded as one of the major short-comings for JSR 168.

JSR 286 has a well defined model to achieve inter-portlet communication. There are two primary ways by which inter-portlet communication can achieved:

- Public render parameters in order to share render state between portlets
- Portlet events that a portlet can receive and send

Deploy portlets

Luminis Platform supports the development of JSR 286 and JSR 168 portlets.

An example portlet helps you understand the specific Luminis Platform and, by extension, Liferay nuances that apply when developing portlets for your Luminis Platform environments. This section also includes information about customizing portlets and using groups.

Portlet deployment prerequisites

The developer must know how to develop JSR 286 or JSR 168 portlets.

For instructions for writing JSR 286 or JSR 168 portlets, refer to the appropriate JSRs.

Develop a portlet

Develop a portlet for Luminis Platform.

Step 1 Set up a development environment

When developing Luminis Platform portlets, your development environment should be separate from your production environment.

Luminis Platform, including the database, can run completely on one server if you choose to develop under MySQL.

After your database is configured and set up, installation takes about ten minutes. For detailed instructions, refer to the *Luminis Platform Installation Guide*.

Step 2 Modify your code

Portlets are deployed as WAR files.

This example the basic structure of the WAR file for a simple demonstration portlet:

```
META-INF/
META-INF/MANIFEST.MF
WEB-INF/
WEB-INF/classes
WEB-INF/classes/example
WEB-INF/classes/example/DemoPortlet.class
WEB-INF/portlet.xml
WEB-INF/web.xml
jsp/
jsp/index.jsp
```

This simple portlet has one class (`DemoPortlet.class`) and one JSP file (`index.jsp`).

Source code for the portlet

This is the source code for `DemoPortlet`:

```
// Demo Portlet
package examples;
import java.io.IOException;
import javax.portlet.*;
public class DemoPortlet  extends GenericPortlet
{
    private PortletContext portletContext;
    public void init (PortletConfig portletConfig) throws
 UnavailableException, PortletException
    {
        super.init(portletConfig);
        portletContext = portletConfig.getPortletContext();
    }
    protected void doView(RenderRequest request, RenderResponse
 response)
        throws PortletException, java.io.IOException
    {
        render(request, response, “/jsp/index.jsp”);
    }
    private void render(RenderRequest request, RenderResponse response,
 String page)
        throws PortletException, IOException
    {
        response.setContentType(“text/html”);
         PortletRequestDispatcher dispatcher =
             portletContext.getRequestDispatcher(page);
         dispatcher.include(request, response);
    }
}
```

This example portlet dispatches to the `index.jsp` file, where the interesting code is located.

Source code for index.jsp

This is the source code for the `index.jsp` file:

```
<%@page contentType=”text/html” pageEncoding=”UTF-8”%>
<!DOCTYPE HTML PUBLIC “-//W3C//DTD HTML 4.01 Transitional//EN”
   “http://www.w3.org/TR/html4/loose.dtd”>
<%
    String person = “”;
    if (request.isUserInRole(“The Chosen One”))
        person = “The Chosen One”;
    else if (request.isUserInRole(“Student”))
        person = “Student”;
    else if (request.isUserInRole(“Faculty”))
        person = “Faculty”;
%>
<html>
    <head>
        <meta http-equiv=”Content-Type” content=”text/html;
 charset=UTF-8”>
        <title>JSP Page</title>
    </head>
    <body>
        <h1>Hello <%= person %> World!</h1>
    </body>
</html>
```

Create the portlet.xml file

After you create the source files, you need to create the `portlet.xml` file.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<portlet-app xmlns=”http://java.sun.com/xml/ns/portlet/portlet-
app_1_0.xsd” version=”1.0”
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:schemaLocation=”http://java.sun.com/xml/ns/portlet/portlet-
app_1_0.xsd
http://java.sun.com/xml/ns/portlet/portlet-app_1_0.xsd”>
 <portlet>
  <portlet-name>DemoPortlet</portlet-name>
  <portlet-class>examples.DemoPortlet</portlet-class>
  <expiration-cache>0</expiration-cache>
  <supports>
   <mime-type>text/html</mime-type>
   <portlet-mode>VIEW</portlet-mode>
   <portlet-mode>EDIT</portlet-mode>
   <portlet-mode>HELP</portlet-mode>
  </supports>
  <portlet-info>
   <title>Demo Portlet</title>
   <keywords>Hello, world, demo</keywords>
  </portlet-info>
  <portlet-preferences>
   <preference>
    <name>name</name>
    <value>World</value>
   </preference>
  </portlet-preferences>
 </portlet>
</portlet-app>
```

Note: This example portlet does not support HELP or EDIT, but they are included for demonstration purposes.

Step 3 Compile the WAR file

Compile the WAR file in the standard JSR 286 or JSR 168 structure.

Related Links

Extend JSR-286 portlets on page 97

Step 4 Deploy in development environment

You can choose one of the following ways to deploy a portlet into Luminis Platform:

- Hot-deploy folder provided in the Luminis Platform install
- Liferay Web UI, if you are deploying to a Luminis Platform administration server cluster

Hot-deploy folder

Your Luminis Platform install includes a hot-deploy folder.

The name of the folder depends on the type of server:

- On an administration server: `$CP_ROOT/products/liferay/liferay-admin/deploy`
- On a portal server: `$CP_ROOT/products/liferay/liferay-portal/deploy`

  Note: `$CP_ROOT` is the location of your Luminis Platform install.

Copy the WAR file into the hot-deploy folder. Luminis Platform automatically deploys the portlet. Once the hot-deploy occurs, the list of applications in Luminis Platform shows the new portlet as a member of the Undefined category.

Step 5 Deploy on live cluster

After you finish developing your portlet, you can deploy the portlet on your live servers.

Portlets must be deployed on the live cluster using the hot-deploy folders. You must copy the WAR file to the hot-deploy folder of every node in your cluster.

Warning! Do not use a shared mount for all nodes. If you do, only the first node that detects the WAR file deploys the portlet.

Warning! The hot-deploy may encounter an issue if the server is currently servicing requests. It is recommended that you block access to each node and allow that node to finish processing its requests before deploying the portlet. Once Liferay deploys the portlet, you can open access to that node and proceed to the next node.

Keep in mind when you deploy a portlet to your live cluster:

- If your portlet requires a database connection, pool your connections to improve performance
- Use RESTful Web services, which can be tested
- Use AJAX liberally. The portlet should load fast and make AJAX requests to your RESTful services to finish rendering whatever information it needs to display to its users. This is especially important if the portlet makes heavy use of database calls or you expect the initial display of your portlet to take a long time.

Undeploy portlets

You may need to undeploy portlets.

To undeploy a portlet directly from the Admin and User Portal tier servers, execute the remove `(rm -rf)` command for this portlet file:

```
Admin - $CP_ROOT/products/tomcat/tomcat-admin/webapps
User - $CP_ROOT/products/tomcat/tomcat-portal/webapps
```

Customize portlets

Add metadata to your portlets so that Luminis or Liferay can put your portlets in different categories other than the Undefined category.

To choose a different category for your portlet, create a file called `liferay-display.xml` in the WEB-INF directory of your portlet. The following example shows the information needed to put your portlet into a different category.

```
<display>
        <category name=”Wasatch University”>
            <portlet id=”DemoPorlet”></portlet>
        </category>
</display>
```

This file places the previously imported `Demoportlet` into a category called Wasatch University.

To change the category after you deploy the portlet, create or edit your `liferay-display.xml` file, re-package your portlet, and redeploy it either through the built-in Liferay feature or through the hot-deploy folder.

Note: If the Banner portlets are not configured with the necessary permissions that allow users to add the portlets to their layouts, configure the portlet permissions.

Related Links

Users, Roles, Groups, and Permissions on page 208

Use dynamic groups within portlets

When dynamic groups are created in Luminis Platform, a corresponding Liferay role is also created that allows you to use those groups in your portlet.

For example:

The Student and Faculty groups are attached to the roles with the same name.

The `index.jsp` file in the WAR file uses `PortletRequest.isUserInRole` to customize the user interface to different target audiences. The user interface is different for each class of users.

Overview on Luminis Portlets for Banner

The basic model for Luminis Portlets for Banner® uses a Web service call into a servlet, running in the Luminis Channels Web application, running on a separate Web application server, or running as a Web application in the Internet Native Banner (INB) Application server.

The call into the servlet from the Luminis Server requires authentication into the Channels server, which is best accomplished using a SSO with the Luminis CAS server.

Note: In the current implementation, there is a userid and password configured in the portlet end and the same userid and password is configured in the channel application. The channel application allows the processing of the request from the portlet to go ahead only if the userid and password matches.

This authentication model requires BEIS to be installed in the Banner server and modification to be made to the deployment of the Luminis portlet for Banner Server. Additionally, both BEIS and the channel application should point to the same banner instance.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Banner portlet lifecycle

To surface content in the portlet by calling into Banner:

- The user authenticates into the portal
- The user places Banner portlet on Portal Page
- During portlet rendering the portlet class calls out to Banner
- XML content is generated by Banner in response to the request
- XML content is returned to the portlet class and is transformed using the preloaded XSLT style sheet
- The resulting XHTML generated from the transform is rendered in the portlet with deep links pointing directly to locations within SSB or INB

Use Luminis portlets for Banner

The Luminis portal page provides the focal entry for the Unified Digital Campus (UDC) and will give students, faculty and administrators easy access to information tailored to their roles on the campus. The portal page consists of portlets that provide quick, visual access to information, allow navigation to key Banner processes, and provide limited data entry.

Clients who have implemented both Luminis and at least one Self-Service product can use portlets to display Banner data in the Luminis portal.

Note: If the Banner portlets are not configured with the necessary permissions that allow users to add the portlets to their layouts, configure the portlet permissions.

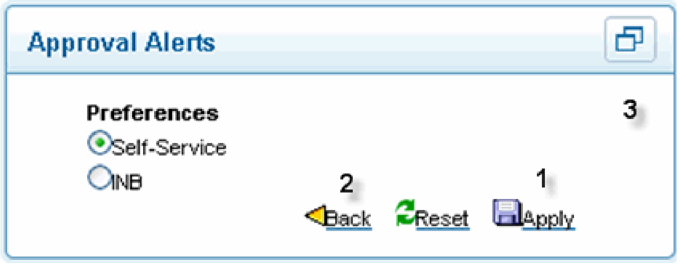
The Banner portlet descriptions are aimed at Luminis portlet users or subscribers.

Related Links

Users, Roles, Groups, and Permissions on page 208

Usage guidelines in Preferences page

If you want to save the changes in the **Preferences** page, click **Apply (1)** > **Back (2)** > 🗗 **(3)**.



Approval Alerts

Preferences

● Self-Service

○ INB

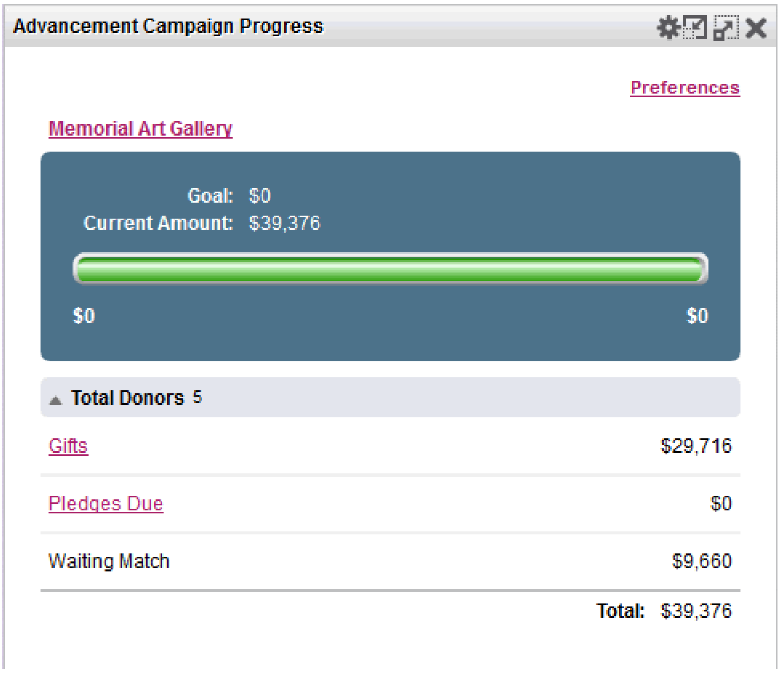
Advancement portlets

Banner® Advancement portlets available in Luminis Platform.

Advancement Campaign portlet

A visual overview of the progress of a campaign.

Users can select the campaign or campaigns they want to monitor. A progress bar shows progress toward the overall campaign goal. The sum of total receipts, outstanding pledge balance, and waiting matching gifts fills the progress bar proportionately. Displayed totals are derived directly from gift records within Advancement. The current status of the campaign is updated as gift entry occurs. The campaign total to-date refreshes as defined by portlet setup or when the portal page refreshes. Navigation options take the user directly to the **Campaign Gifts Form (AFAGIFT)** or the **Campaign Pledges Form (AFAPLDG)**. The campaign title links to the **Campaign Header Form (AFACAMP)**.



Advancement Campaign Progress

Preferences

Memorial Art Gallery

Goal: $0
Current Amount: $39,376

$0 $0

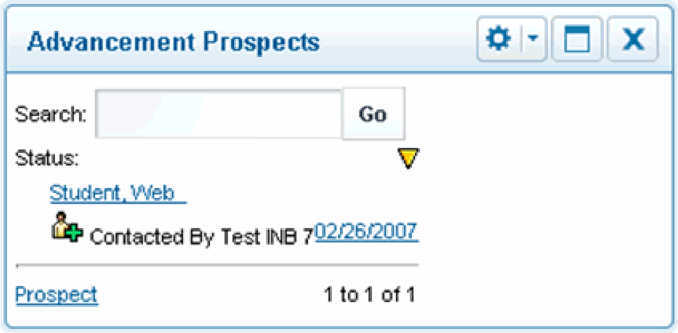
▲ Total Donors 5

Gifts	$29,716
Pledges Due	$0
Waiting Match	$9,660
Total:	$39,376

Advancement Prospects portlet

Fund-raising staff monitors the progress of assigned prospects at a glance.

Each user can view a complete list of assigned prospects or a subset of high priority assigned prospects. A user can also search for a specific prospect. All activity recorded for a prospect, including new gift and contact information, is immediately available.



Advancement Prospects

Search: Go

Status:

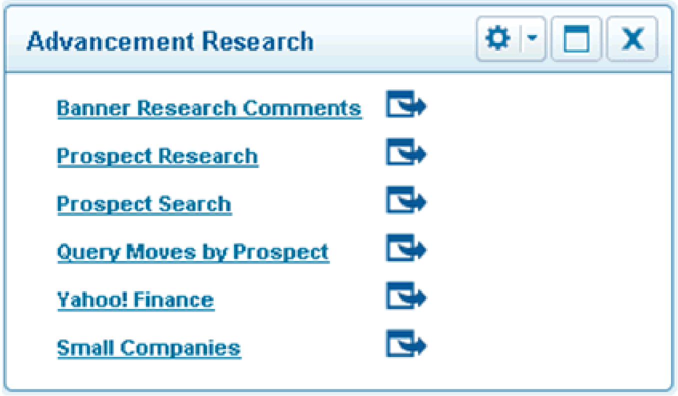
Student, Web

Contacted By Test INB 7 02/26/2007

Prospect 1 to 1 of 1

Advancement Research portlet

Advancement officers research potential and current prospects.



Advancement Research

Banner Research Comments

Prospect Research

Prospect Search

Query Moves by Prospect

Yahoo! Finance

Small Companies

Advancement Research portlet links:

- Banner Research Comments
- Prospect Research
- Prospect Search page
- Query Moves by Prospect
- Yahoo! Finance (http://finance.yahoo.com)
- Small Companies (http://www.wall-street.com)

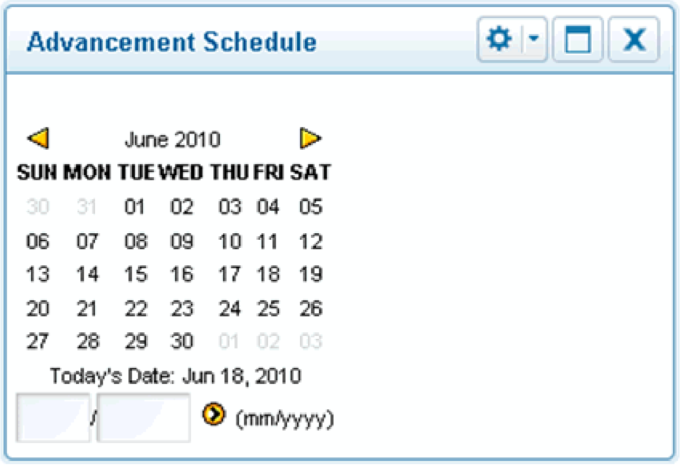
Note: This portlet has no user preferences.

Advancement Schedule portlet

An easy way for users to display details about planned prospect appointments and planned contacts.

A date is displayed as a hyperlink if one or more appointments are scheduled for user on that date. The date links to details regarding the scheduled appointment or contact on the **Planned Moves by Date** page within **Advancement Officer Self-Service**. To aid in planning, a user can navigate forward or backward by month or directly to a specific date. The display default always prompts with today's date and displays the current month.

- To navigate to the previous month, click the left arrow
- To navigate to the next month, click the right arrow
- To navigate to a specific month, enter the month and year in the fields at the bottom of the channel, then click the jump arrow



SUN	MON	TUE	WED	THU	FRI	SAT
30	31	01	02	03	04	05
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	01	02	03

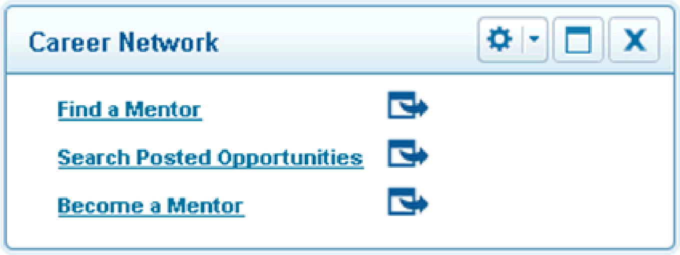
Today's Date: Jun 18, 2010

/ (mm/yyyy)

Note: This portlet has no user preferences.

Career Network portlet

Access the Self-Service menus to enable alumni and friends to search for mentors, post opportunities for employment, search for employment opportunities, and volunteer to become a mentor.

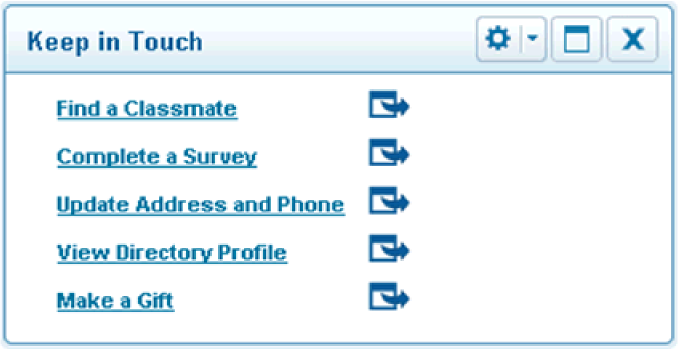


Note: This portlet has no user preferences.

Keep in Touch portlet

Access to Self-Service menus for alumni and friends to search for fellow classmates, complete a survey, update their address and phone numbers, view their directory profile, and make a gift.

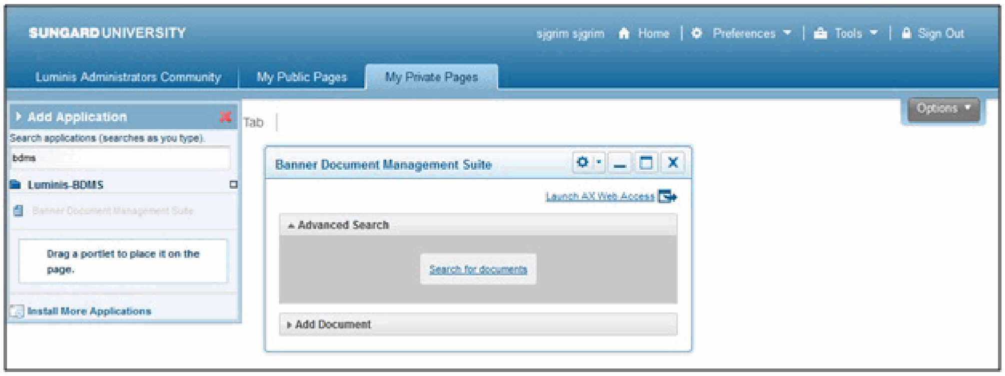
Other links can be added and or customized in this, as well as any other channel, by a Luminis user with Channel Administrator rights.



Note: This portlet has no user preferences.

Banner Document Management portlet

A tool to search for and add documents and images to your institution's database.



Search applications (searches as you type).

bdms

Drag a portlet to place it on the page.

If you have implemented both Luminis Platform and BDM, use the BDM portlet to display BDM data in the Luminis portal.

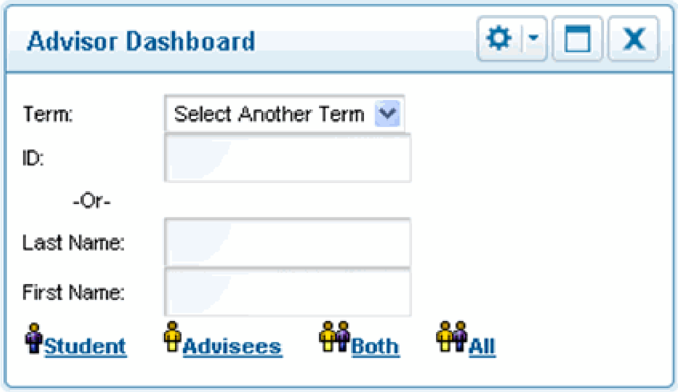
For instructions on installing the BDM portlet and using the portlet within Luminis Platform, see the *Luminis Platform Banner Document Management Portal Guide*.

Faculty and Advisor portlets

Banner® Faculty and Advisor portlets available in Luminis Platform.

Advisor Dashboard portlet

Search for an Advisee or a Student and display pertinent information to help you provide timely advice.



Advisor Dashboard

Term: Select Another Term

ID:

-Or-

Last Name:

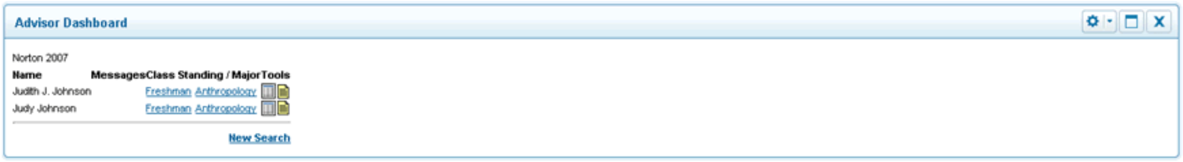
First Name:

You must select a term and enter either a student ID or all or the first part of the student's name, then click the appropriate search type.

Note: If you do not enter a student ID, you must enter something in at least one of the name fields.

- Click **Student** to tell the system to search only among your students for matching records
- Click **Advisees** to tell the system to search only among your advisees for matching records
- Click **Both** to tell the system to search among your students and advisees for matching records
- Click **All** to tell the system to search among all students and advisees for matching record

The system searches for records matching the search criteria and displays results (if any) in the portlet.



Advisor Dashboard

Norton 2007

Name	Messages	Class Standing / Major	Tools
Judith J. Johnson		Freshman Anthropology	
Judy Johnson		Freshman Anthropology	

The **Messages** column includes these links:

- A red flag indicates that a hold exists for the student and you can navigate to the **View Holds** page in Faculty and Advisor Self-Service, if hold information is available on that page
- Icons indicate each student's relationship (student, advisee, or both) to the user. The icons link to the **View Student Schedule** page in Faculty and Advisor Self-Service.

The Class Standing or Major column includes the following navigational links.

- The student's class standing link goes to the **Degree Evaluation** page in Faculty and Advisor Self-Service.
- The student's major link goes to the **General Student Information** page in Faculty and Advisor Self-Service.

The Tools column includes these navigational links:

- The transcript icon goes to the **Academic Transcript Options** page in Faculty and Advisor Self-Service
- The test scores icon goes to the **Test Scores** page in Faculty and Advisor Self- Service
- The e-mail icon launches your e-mail program with the student's e-mail address.

Note: This portlet has no user preferences.

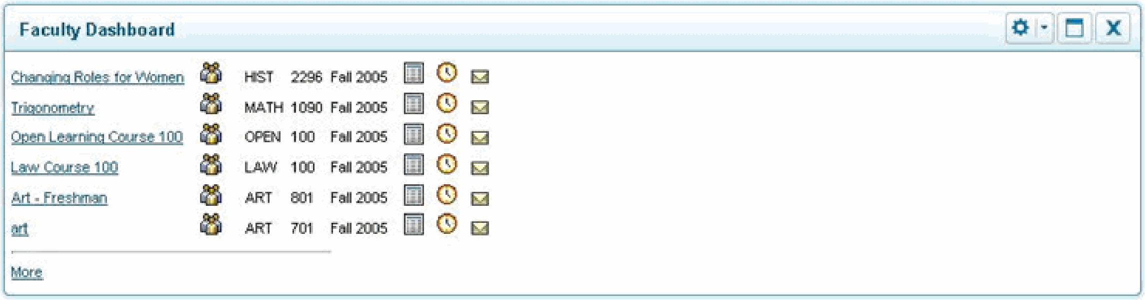
Faculty Dashboard portlet

Faculty members view active classes, e-mail class members, and access Faculty and Advisor Self-Service pages.

About this task

Navigational links:

- The class name link goes to the **Faculty Detail Schedule** page in Faculty and Advisor Self-Service
- The classlist icon goes to the **Summary Class List** page in Faculty and Advisor Self-Service
- The waitlist icon goes to the **Summary Wait List** page in Faculty and Advisor Self-Service. This icon displays only if a waitlist exists for the class.
- The syllabus icon goes to the **Syllabus Information** page in Faculty and Advisor Self-Service
- The clock icon goes to the **Office Hours** page in Faculty and Advisor Self- Service
- The e-mail icon launches a new e-mail in your e-mail program with the e-mail addresses of all students registered in the class and for whom an e-mail address has been entered on the E-mail Address Form (GOAEMAL)

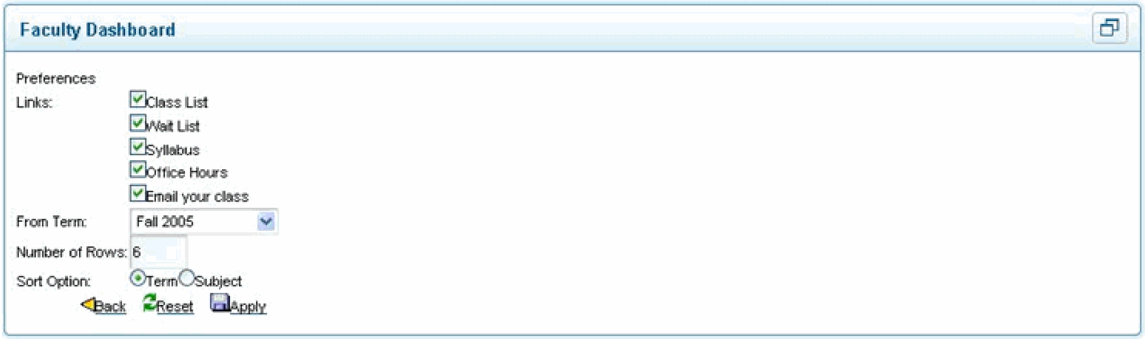


Changing Roles for Women		HIST	2296	Fall 2005			✉
Trigonometry		MATH	1090	Fall 2005			✉
Open Learning Course 100		OPEN	100	Fall 2005			✉
Law Course 100		LAW	100	Fall 2005			✉
Art - Freshman		ART	801	Fall 2005			✉
art		ART	701	Fall 2005			✉

To view a complete list of classes, if there are more records than are displayed in the channel, click the **More** link. The system displays the channel in focus mode with the complete list of classes.

To select which links display in the channel, click the **Preferences** menu item button in the channel. Select or clear the **Links** check boxes, as appropriate. Choices are:

- Class List
- Wait List
- Syllabus
- Office Hours
- Email Your Class



Faculty Dashboard

Preferences

Links:
☑Class List
☑Wait List
☑Syllabus
☑Office Hours
☑Email your class

From Term: Fall 2005

Number of Rows: 6

Sort Option: ●Term ○Subject

After making your choices, click **Apply**.

To change the default beginning term of the list of classes:

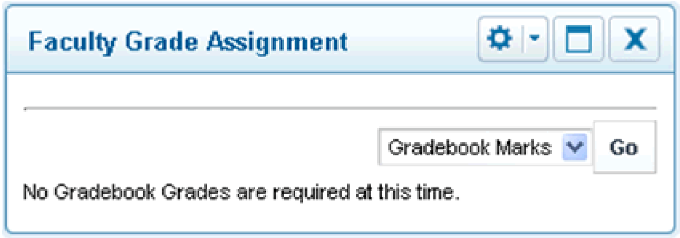
Procedure

1. In the **From Term** drop-down list, select the first term that you want to display.
2. To change the default number of records displayed in the portlet, enter the number of records that you want to display.
3. To change the default sort order, select one of the required radio buttons in the **Sort Option** field (**Term** or **Subject**), click **Apply.**
4. To return the display to the original defaults, click **Preferences**.
5. Click **Reset**, then click **Apply.**
6. After you make all your changes, click **Back** to return to the portlet.

Faculty Grade Assignment portlet

Faculty members view the grading status of classes and access grade pages in Faculty and Advisor Self-Service.

You can use the pull-down box to select the type of grades for which you want to see the status: midterm, final, or Electronic Gradebook.



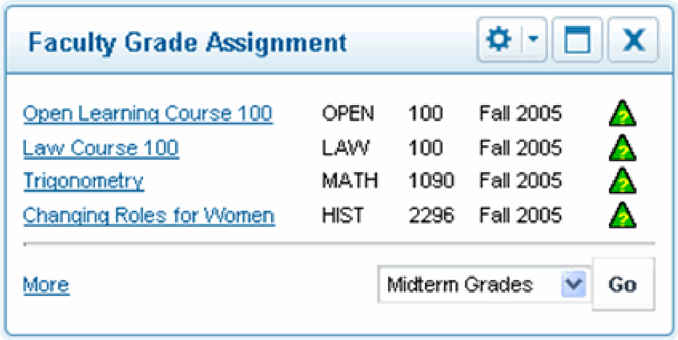
Faculty Grade Assignment

Gradebook Marks

No Gradebook Grades are required at this time.

The portlet includes these navigational links:

- The class name link goes to the **Class Schedule Listing** page in Faculty and Advisor Self-Service
- The icons in the last column indicate the class's grading status and, after you click, go to the page in Self-Service associated with the type of grade displayed in the pull-down box. The icons that can appear are the following:
  - The no enrollment icon indicates that no students have registered for the class. This icon is inactive.
  - The grades not started icon indicates that grade entry has not been started
  - The grades started icon indicates that grade entry has been started but not completed
  - The grades entered icon indicates that all grades have been entered but not rolled to academic history yet
  - The grades completed icon indicates that grades have been completed and rolled to academic history. No more action can be taken. This icon does not appear for midterm grades and gradebook, since these grades are not rolled to history.
  - The not gradable icon indicates that students have registered but the class is not gradable. This icon is inactive.



Open Learning Course 100	OPEN	100	Fall 2005	▲
Law Course 100	LAW	100	Fall 2005	▲
Trigonometry	MATH	1090	Fall 2005	▲
Changing Roles for Women	HIST	2296	Fall 2005	▲

When the icons are enabled, they go to the following pages:

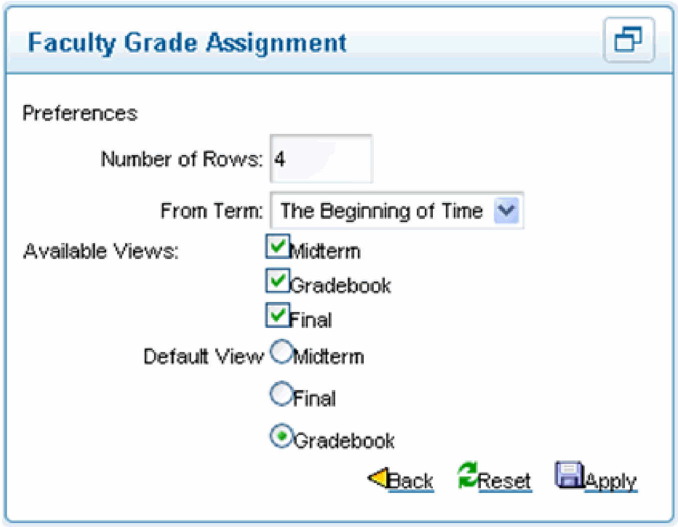
- If **Final Grades** is selected in the pull-down box, the icons go to the **Final Grades** page in Faculty and Advisor Self-Service
- If **Midterm Grades** is selected in the pull-down box, the icons go to the **Mid Term Grades** page in Faculty and Advisor Self-Service.
- If **Gradebook Marks** is selected in the pull-down box, the icons go to the **Electronic Gradebook by Component** page in Faculty and Advisor Self- Service.

To view a complete list of classes, if there are more records than are displayed in the channel, click the **More** link. The system displays the channel in focus mode with the complete list of classes.

Faculty Grade User Preferences

Change the default number of records, default beginning term of the list of classes, views displayed, and default view for the **Faculty Grade** portlet.

About this task



Faculty Grade Assignment

Preferences

Number of Rows: 4

From Term: The Beginning of Time

Available Views: ☑ Midterm ☑ Gradebook ☑ Final

Default View ○ Midterm ○ Final ● Gradebook

To adjust the user preferences:

Procedure

1. Click the **Preferences** menu of the portlet to navigate to the **Edit** page of the **Faculty Grade Assignment** portlet.
2. To change the default number of records displayed in the portlet, enter the number of records you want to be displayed in the **Number of Rows** field.
3. To change the default beginning term of the list of classes, select term you want to display first from the **From Term** drop-down list.
4. To select which views will be displayed, select the required check boxes in the **Available View** field.
5. To change the default view, select the required radio buttons in the **Default View** field.
6. Click **Apply**.
7. To return the display to the original defaults, click **Preferences** > **Reset** > **Apply**.
8. After you make all your changes, click **Back** to return to the portlet.

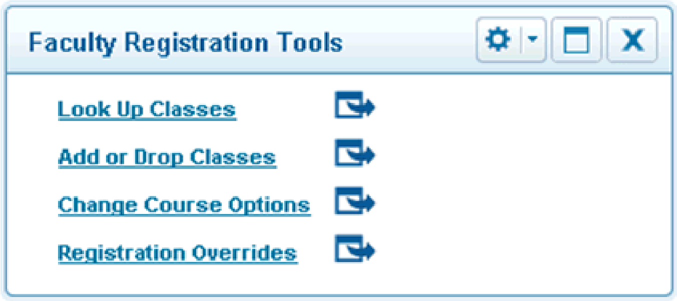
Faculty Registration Tools portlet

Access to registration-related information and activities.

Activities include these navigational links:

- **Look Up Classes** link goes to the **Look-Up Classes** page in Faculty and Advisor Self-Service
- **Add or Drop Classes** link goes to the **Add or Drop Classes** page in Faculty and Advisor Self-Service
- **Change Course Options** link goes to the **Change Class Options** page in Faculty and Advisor Self-Service
- **Registration Overrides** link goes to the **Registration Overrides** page in Faculty and Advisor Self-Service

  Note: When any of these links are accessed, the system always prompts for the term, CRN, student ID, and student PIN, as applicable for the task being performed, to ensure that any changes made are for the correct term, class, and student, as applicable. This portlet has no user preferences.



Faculty Registration Tools

Look Up Classes

Add or Drop Classes

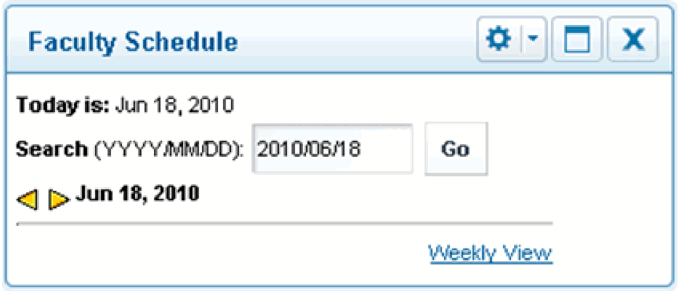
Change Course Options

Registration Overrides

Faculty Schedule portlet

Displays faculty class and office hour commitments in a daily or weekly format.

The default is the daily view. It shows commitments for the entire day. The weekly view can be accessed via a link in the portlet, shows all courses in the entire week, and is displayed with the portlet in focus mode. The system displays the current day (or week) by default, but you can select a different date in the **Search** field.



Faculty Schedule

Today is: Jun 18, 2010

Search (YYYY/MM/DD): 2010/06/18

Jun 18, 2010

To go to a specific date, enter the date, in YYYY/MM/DD format, in the **Search** field, then click **Go**.

The left and right arrows navigate to the previous and next day or week (depending on the current view).

The time conflict icon indicates that a class has a time conflict with another class.

The unassigned meeting times icon indicates a class with for which meeting times have not yet been assigned.

Faculty Schedule portlet includes the following navigational links:

- The course title link goes to the **Faculty Detail Schedule** page in Faculty and Advisor Self-Service.
- The clock icon goes to the **Office Hours** page in Faculty and Advisor Self-Service.

  Note: This portlet has no user preferences.

Finance portlets

Banner® Finance portlets available in Luminis® Platform.

Approval Alerts portlet

Notifies approvers that documents are waiting for approval.

More frequent and easier access to the **Approve Documents** pages means that purchase orders can be approved sooner, resulting in the earlier receipt of goods, and that vendors and suppliers can be paid on time.

The portlet includes navigational links that can be used to approve documents:

- The **Next Approver** link goes to either the User Approval Form (FOAUAPP) in Banner Finance or the **Approve Documents** page in Finance Self-Service, depending on the user preferences. The system displays the documents for which you are the next in line to approve.

  Note: Before displaying FOAUAPP, the system displays the Approvals Notification Form (FOIAINP). When you exit FOIAINP, FOAUAPP is displayed.

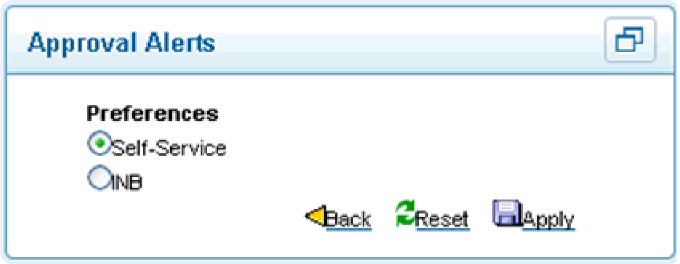
- The **All Documents** link goes to the **Approve Documents** page in Finance Self-Service. The system displays all documents for which you are an approver, regardless of where the documents are in the approval queue. This link is displayed only if the portlet is set up to go to Finance Self-Service; it is not displayed if the portlet is set up to go to Banner.

To change the system to which the links in the portlets, click **Preferences**. Select the radio button for the system you want to use, such as **Self-Service** or **INB** Banner form

Approval Alerts user preferences

Reset the alerts displayed in the **Personnel Action Notices** portlet.

About this task



Approval Alerts

Preferences

● Self-Service
○ INB

Return the display to the original default.

Procedure

1. Click the edit button in the portlet.
2. Click **Reset** > **Apply**.
3. Once you have made all your changes, click **Back** to return to the portlet.

Finance Alerts Grants portlet

Provides Principal Investigators (PIs) with information about grants that are due to end within the number of days specified in the user preferences.

The **Grant Code** link goes to the Grant Maintenance Form (FRAGRNT) in Banner Finance.

Note: Before displaying FRAGRNT, the system displays the Approvals Notification Form (FOIAINP). When you exit FOIAINP, FRAGRNT is displayed.

To change the default number of days for a grant to be displayed in the portlet, click **preferences** menu. In the **Number of Days** field, enter the number of days for which you want grant alerts to be displayed, then click **Apply**.

To return the display to the original defaults, click **Edit** > **Reset** > **Apply**.

Once you have made all your changes, click **Back** to return to the portlet.

Financial Advisor portlet

A bar graph to shows budget versus committed and actual expenses for up to five preferred fund or organization combinations or organization codes. An associated table shows details as well as the available balance, percentage spent, and percent budget remaining.

The bar graph allows you to track critical budgetary allocations in relation to the expenditures charged against that budget. Up-to-the-minute information supports proactive responses for budgetary transfers or follow-up on problematic activities. You can define which organization or combination of funds and organizations to track. These can be changed to other codes as needed.

The value in the **Legend** column goes to the **Budget Query FOAPAL** parameter page in Finance Self-Service and defaults the values for Fiscal Year, Chart of Accounts, Fund and Organization.

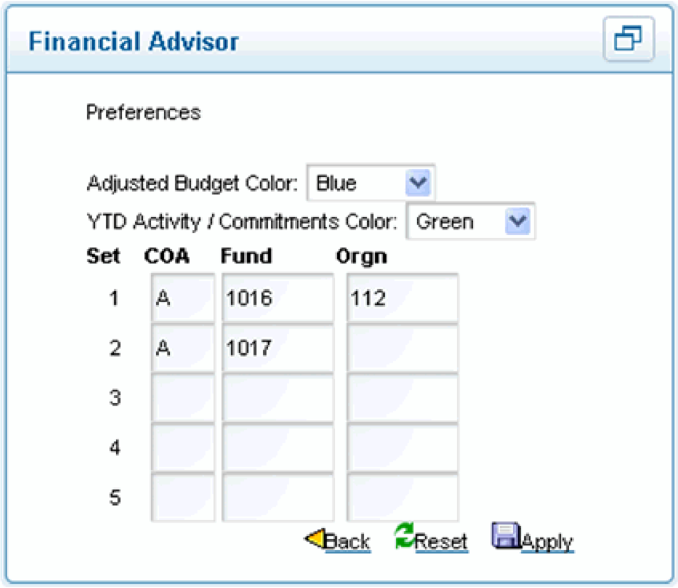
To monitor more than five fund/organization combinations or organization codes, subscribe to the portlet multiple times and set up different user preferences in each instance.

To change the color of the bars in the graph, click the **Preferences** menu. Select the color you want to use from the pull-down list in the **Color** field associated with the bar you want to change, then click **Apply**.

Financial Advisor portlet user preferences

Change the record type or status type displayed in the **Personnel Action Notices** portlet.

About this task



Financial Advisor

Preferences

Adjusted Budget Color: Blue

YTD Activity / Commitments Color: Green

Set	COA	Fund	Orgn
1	A	1016	112
2	A	1017	
3			
4			
5			

Procedure

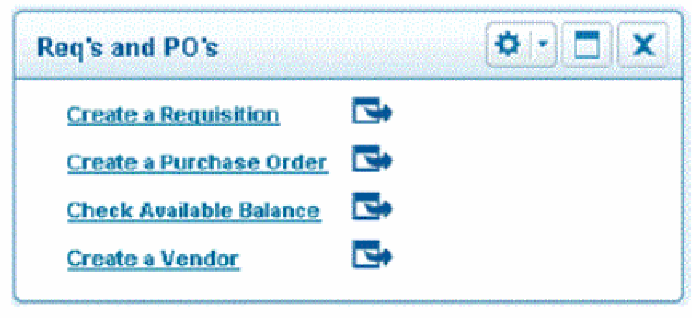
1. To add a fund or organization combination, enter:
   - Chart of accounts (COA) in the **COA** field
   - Fund code in the **Fund** field
   - Organization code in the **Orgn** field

   Note: You can enter up to five fund/organization combinations, one on each row.
2. After you enter the values, click **Apply.**
3. To return the display to the original defaults, click the portlet's edit button. Click **Reset** > **Apply**.

4. After you make all your changes, click **Back** to return to the portlet.

Req's and PO's portlet

Links to the Requisition, Purchase Order, and Budget Query pages in Finance Self-Service, and the Vendor Maintenance Form in Banner® Finance.



The Req's and PO's portlet includes the following navigational links:

- The **Create a Requisition link** goes to the **Requisition** page in Finance Self- Service.
- The **Create a Purchase Order** link goes to the **Purchase Order** page in Finance Self-Service.
- The **Check Available Balance** link goes to the **Budget Query** page in Finance Self- Service.
- The **Create a Vendor link** goes to the Vendor Maintenance Form (FTMVEND) in Banner Finance.

  Note: Before displaying FTMVEND, the system displays the Approvals Notification Form (FOIAINP). When you exit FOIAINP, FTMVEND is displayed.

  Note: This portlet has no user preferences.

Banner General portlets

Banner® General portlets available in Luminis Platform.

Note: The following portlets have no user preferences.

My Banner portlet

A link from the portal to your most-used Banner® forms and processes, based on your existing personal menu and preferences.

This portlet is available to anyone who has an Oracle login ID to Banner.

It displays links that match your personal menu in Banner, and includes the same menu choices that are displayed on the Banner main menu.

My Reports portlet

Displays your completed jobs for which Database was specified as the designated printer.

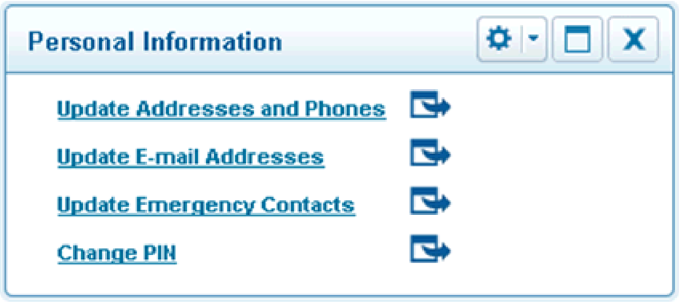
The Date/Time column displays the date and time that the report finished running. Information in this portlet is refreshed each time you leave the portal and then return it. This portlet is available to anyone who have an Oracle login ID to Banner.

The **filename** link goes to the Saved Output Review Form (GJIREVO) and displays the selected report's output.

To view a complete list of reports, if there are more reports than are displayed in the portal, click **More**. The system displays the portlet in focus mode with the complete list of reports.

Personal Information portlet

View and update your personal information.



Personal Information

Update Addresses and Phones

Update E-mail Addresses

Update Emergency Contacts

Change PIN

The portlet includes the following navigational links:

- The **Update Addresses and Phones** link goes to the **Update Addresses and Phones - Select Address** page in Web General.
- The **Update E-mail Addresses** link goes to the **Update E-mail Addresses - Select Address** page in Web General.
- The **Update Emergency Contacts** link goes to the **Update Emergency Contacts** page in Web General.
- The **Change PIN** link goes to the **Change PIN** page in Web General.

Your institution can add other links to these portlets.

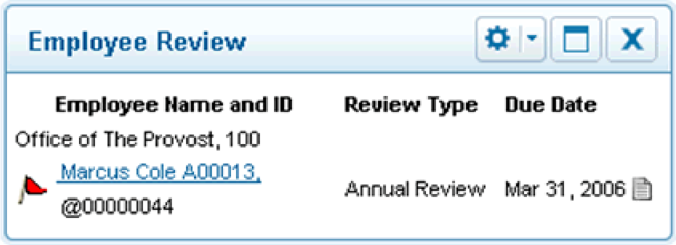
Human Resources portlets

Banner® Human Resources portlets available in Luminis Platform.

Employee Reviews portlet

A list of reviews that require action by the manager.

The display includes the name of the employee, type of review, and review due date.



Employee Review

Employee Name and ID	Review Type	Due Date
Office of The Provost, 100		
🚩 Marcus Cole A00013, @00000044	Annual Review	Mar 31, 2006

A red flag icon is displayed next to any record whose effective review date is 15 days or fewer away.

This portlet includes the employee name navigational link.

The **employee name** link and the text icon go to the **Employee Review Form (PEAREVW)** in Banner Human Resources, where you can update the record.

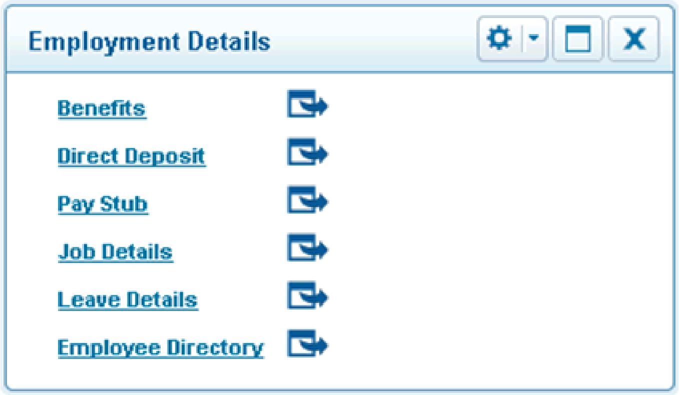
Note: This portlet has no user preferences.

Employment Details portlet

Access to important information about benefits and employment.

Navigational links:

- The **Benefits** link goes to the **Benefit Statement ID Criteria** page in Employee Self- Service.
- The **Direct Deposit** link goes to the **Direct Deposit Allocation** page in Employee Self-Service.
- The **Pay Stub** link goes to the **Pay Stub** page in Employee Self-Service.
- The **Job Details** link goes to the **Jobs Summary** page in Employee Self-Service.
- The **Leave Details** link goes to the **Leave Balances** page in Employee Self-Service.
- The **Employee Directory** link goes to the **Campus Directory** page in Employee Self-Service.



Employment Details

Benefits

Direct Deposit

Pay Stub

Job Details

Leave Details

Employee Directory

Note: This portlet has no user preferences.

Personnel Action Notices portlet

Summary data about personnel action notices that require attention.

Notices include:

- Employee name
- Type of transaction (for example, promotion)
- Effective date
- Action required

You can specify in the user preferences the types of transactions, statuses, and number of rows to be displayed in the portlet.

Note: The system can display up to 35 records. If, based on the transaction types you have selected to be displayed, the number of records is greater than 35, the system displays the message "The results of the search exceeded the portlet limits. Please limit your search criteria." If this happens, go to the user preferences and select fewer transaction types for display.

If no details need to be viewed, you can approve and acknowledge transactions directly in the portlet using the links in the Action column, if any are displayed. Click one of the links to update the record in Banner Human Resources.

A red flag icon is displayed for records whose effective date is within 15 days of the system date and for which action needs to be taken. Actions can include **FYI** and **Approve**.

A red flag icon is also displayed if the effective date is within 15 days of the system date and you need to apply the record to the database. The word "Apply" is also displayed in the Action column. You must go to the **Electronic Approval Summary Form (NOAAPSM)** or use the **EA Mass Apply Process (NOPEAMA)** to apply the record; it cannot be done from within the portlet.

Navigational links:

- The **Employee Name** link goes to the **EPAF Preview** page in Employee Self- Service.
- The **Create New PAF** link goes to the **New EPAF Person Selection** page in Employee Self-Service.
- If the **Display Alternate Log-on Verification Form** check box in the Electronic Approval window of the Position Control Installation Rules Form (NTRINST) has been checked, the **Verification** page in Employee Self-Service is displayed before the **New EPAF Person Selection** page. If this occurs, the user must enter the ID information and select **OK**, and then the system will display the **New EPAF Person Selection** page.
- The **Approver Summary Page** link goes to the **EPAF Approver Summary** page in Employee Self-Service.

To view a complete list of records, if there are more than what is displayed in the portlet, click **More**. The system displays the channel in focus mode with the complete list of records.

Personnel Action Notices portlet user preferences

Change the record type or status type displayed in the **Personnel Action Notices** portlet.

About this task

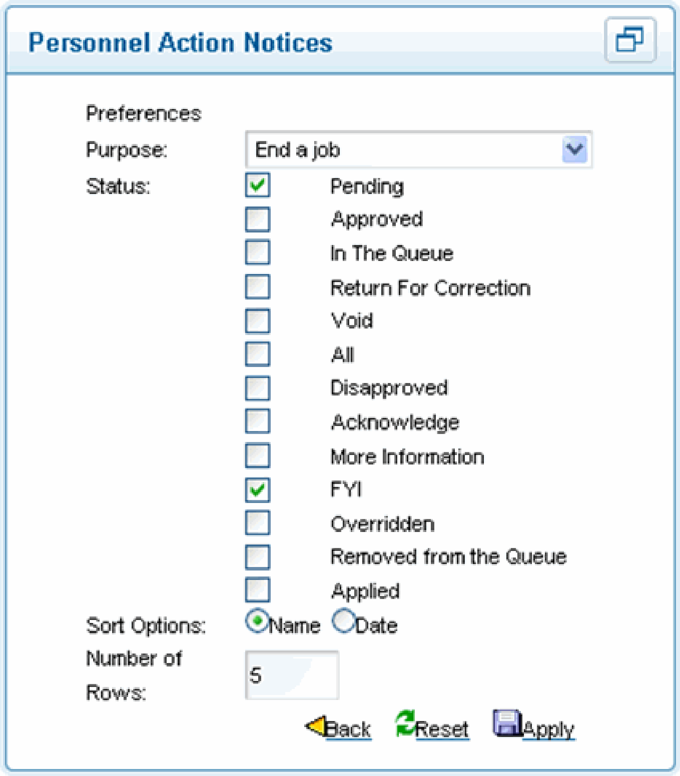
To change the record type displayed in the portlet:

Procedure

1. Click the edit button for the portlet.
2. Select the desired record type from the **Purpose** pull-down list.
3. Click **Apply**.

   To specify the status types you want displayed in the portlet:
4. Click the **Preferences** menu for the portlet.
5. Select or clear the Status check boxes, as appropriate. Status choices include:
   - Pending
   - Acknowledge
   - Approved
   - More Information
   - In the Queue
   - FYI
   - Return for Correction
   - Overridden
   - Void
   - Removed from the Queue
   - All
   - Disapproved
   - Applied

   Note: If **All** is selected, all records are displayed regardless of whether the other check boxes are checked.



Personnel Action Notices

Preferences

Purpose: End a job

Status:
☑ Pending
□ Approved
□ In The Queue
□ Return For Correction
□ Void
□ All
□ Disapproved
□ Acknowledge
□ More Information
☑ FYI
□ Overridden
□ Removed from the Queue
□ Applied

Sort Options: ● Name ○ Date

Number of Rows: 5

To change the default sort order:

6. Click the edit button for the portlet.
7. Select the applicable radio button in the **Sort Options** field (either **Name** or **Date**).
8. Click **Apply**.

To change the default number of records displayed in the portlet:

9. Click the edit button for the portlet.
10. In the **Number of Rows** field, enter the number of records you want displayed.
11. Click **Apply**.

To return the display to the original defaults:

12. Click the edit button for the portlet.
13. Click **Reset**.
14. Click **Apply**.

Results

Once you have made all your changes, click **Back** to return to the portlet.

Time Approval portlet

A list of the time transaction events that need to be approved.

A red flag icon is displayed next to any pay events that have reached the time entry cut-off date and when there are pending records within the queue.

Navigational links:

- The **pay period** link goes to the **Department Summary** page in Employee Self- Service so you can complete approvals.
- The **Update Approval Proxies** link goes to the **Proxy Set Up** page in Employee Self-Service so you can access your proxy list.
- The **Act As Superuser** link goes to the **Approver Selection** page in Employee Self- Service so you can act as a superuser for time transactions. This link is displayed only if you are defined as a time entry approvals superuser.

To view a complete list of records, if there are more than are displayed in the portlet, click **More**. The system displays the portlet in focus mode with the complete list of records.

Time Approval portlet user preferences

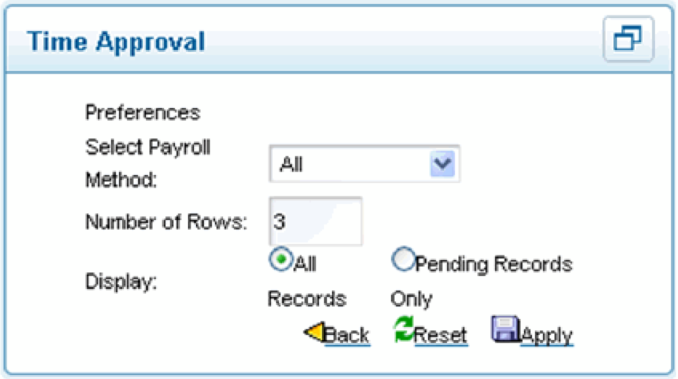
Change the default payroll method, number of rows displayed, or sort order in the **Time Approval** portlet.

About this task

To change the default payroll method for the portlet:

Procedure

1. Click **Preferences** menu for the portlet.
2. Select the desired payroll method from the **Select Payroll Method** pull-down list.
3. Click **Apply**.



Time Approval

Preferences

Select Payroll Method: All

Number of Rows: 3

Display: ● All Records ○ Pending Records Only

The payment options are:

- All

- Time Sheets
- Leave Report
- Leave Request

To change the default number of rows displayed in the portlet:

4. Click the edit button for the portlet.
5. In the **Number of Rows** field, enter the number of records you want displayed.
6. Click **Apply**.

   This preference is applied to both the department and the pay event listings.

   To change the default sort order:

7. Select the applicable radio button in the **Sort Option** field (**All Records** or **Pending Records Only**).
8. Click **Apply**.

   To return the display to the original defaults:

9. Click the edit button for the portlet.
10. Click **Reset**.
11. Click **Apply**.

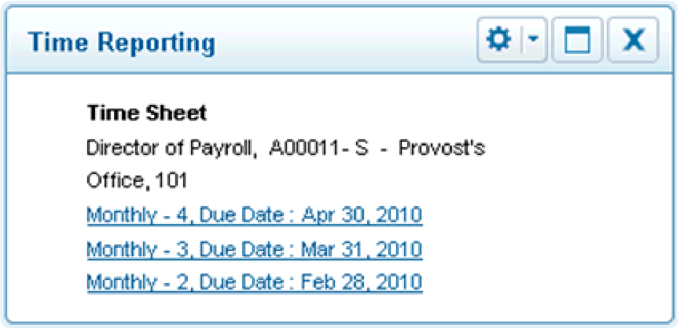
Results

Once you have made all your changes, click **Back** to return to the portlet.

Time Reporting portlet

Access to time sheets, leave reports, and advance leave requests.

There is a separate link for each time reporting period that is available for time entry by pay period and position.


Time Reporting

Time Sheet

Director of Payroll, A00011- S - Provost's Office, 101

Monthly - 4, Due Date : Apr 30, 2010

Monthly - 3, Due Date : Mar 31, 2010

Monthly - 2, Due Date : Feb 28, 2010

A red flag icon is displayed next to any time reporting record whose due date is a specified number days or fewer away. This number is specified by your institution.

Navigational links:

- The **time report** link goes to the **Time and Leave Reporting** page in Employee Self-Service so you can enter your time.
- The **Clock In and Out** icon goes to the appropriate, current timesheet in Employee Self-Service so you can clock in for the beginning of your shift or clock out for the end of your shift.

To view a complete list of records, if there are more time reports than are displayed in the portlet, click **More**. The system displays the portlet in focus mode with the complete list of time reports.

Time Reporting portlet user preferences

Change the default number of records displayed or default sort order for the **Time Reporting** portlet.

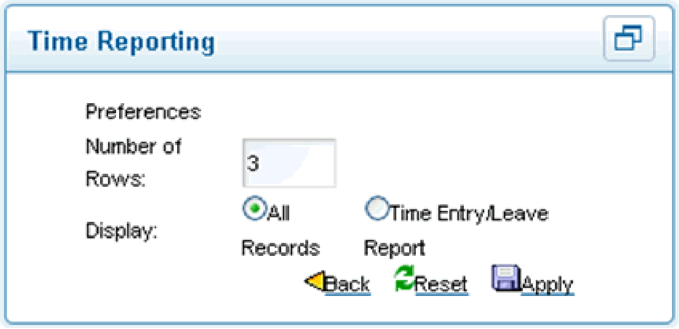
About this task

To change the default number of records displayed in the portlet:

Procedure

1. Click **Preferences** menu of the portlet.
2. In the **Number of Rows** field, enter the number of records you want displayed.
3. Click **Apply**.

   This preference is applied to both the department and the pay event listings.

   Time Reporting

   Preferences

   Number of Rows: 3

   Display: ● All Records ○ Time Entry/Leave Report

   To change the default sort order:
4. Select the applicable radio button in the **Display** field (either **All Records** or **Time Entry Only**).
5. Click **Apply**.

   To return the display to the original defaults:
6. Click the edit button for the portlet.
7. Click **Reset**.
8. Click **Apply**.

Results

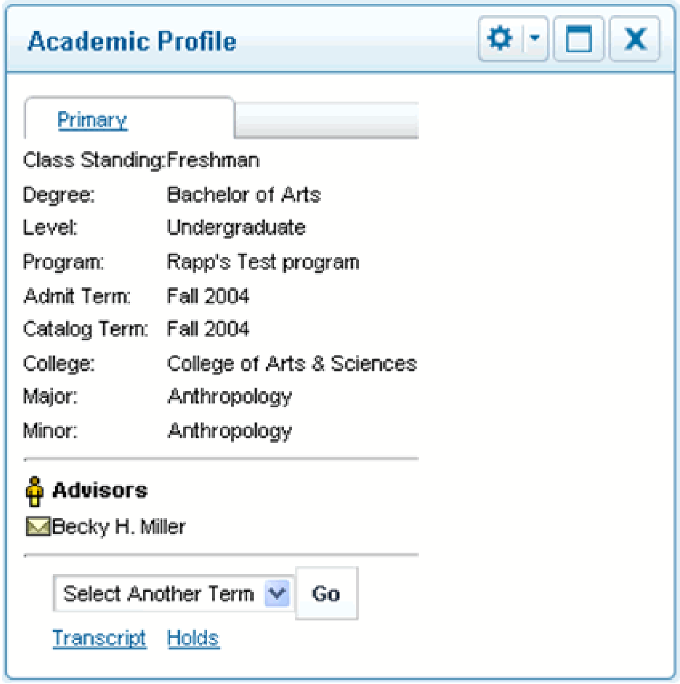
After you make your changes, click **Back** to return to the portlet.

Student portlets

Banner® Student portlets available in Luminis® Platform.

Academic Profile portlet

View curriculum and advisor information for a specified term.



Class Standing:	Freshman
Degree:	Bachelor of Arts
Level:	Undergraduate
Program:	Rapp's Test program
Admit Term:	Fall 2004
Catalog Term:	Fall 2004
College:	College of Arts & Sciences
Major:	Anthropology
Minor:	Anthropology

Becky H. Miller

To change the term displayed, select the desired term from the pull-down list, and click **Go**.

Navigational links:

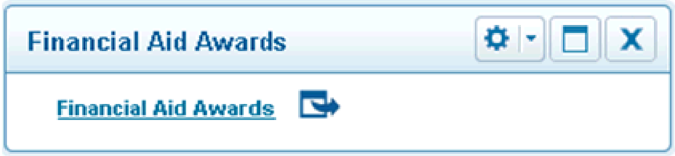
- The e-mail icon next to an advisor's name launches your e-mail program with the advisor's e-mail address.
- The **Transcript** icon and link go to the **Academic Transcript Options** page in Student Self-Service.
- The **Holds** icon and link go to the **View Holds** page in Student Self-Service.

Note: This portlet has no user preferences.

Financial Aid Awards portlet

Contains the **Financial Aid Awards** navigational link.

The **Financial Aid Awards** link goes to the **Accept or Decline or Reduce Awards** page in Student Self-Service.



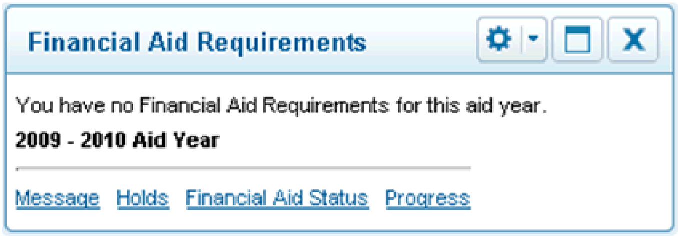
Financial Aid Awards

Financial Aid Awards

Note: This portlet has no user preferences.

Financial Aid Requirements portlet

View the status of requirements from the Financial Aid Office.



Financial Aid Requirements

You have no Financial Aid Requirements for this aid year.

2009 - 2010 Aid Year

Message Holds Financial Aid Status Progress

The Status column indicates whether a requirement has been met.

- A green check icon is displayed for requirements that have been met
- A red flag icon is displayed for requirements that have not been met

To change the aid year displayed, select the desired term from the pull-down list, and click **Go**.

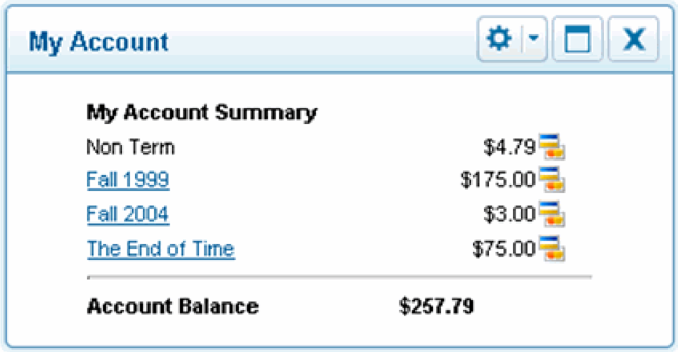
Navigational links:

- **Message** link goes to the **Requirement Messages** page in Student Self-Service.
- **Holds** link goes to the **Financial Aid Holds** page in Student Self-Service.
- **Financial Aid Status** link goes to the **Financial Aid Status for Award Year** page in Student Self-Service. If you have not previously specified an aid year, the system displays the **Aid Year** page first.
- **Progress** link goes to the **Academic Progress** page in Student Self-Service.
- **Transcript** link goes to the **Academic Transcript Options** page in Student Self- Service.

Note: This portlet has no user preferences.

My Account portlet

Displays account balances for term-related charges and non term-related charges.



My Account

My Account Summary

Non Term	$4.79
Fall 1999	$175.00
Fall 2004	$3.00
The End of Time	$75.00
Account Balance	**$257.79**

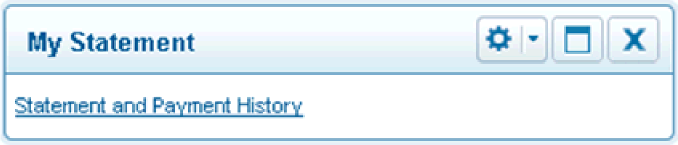
Navigational links:

- For a term-related item, the term link goes to the **Account Summary by Term** page in Student Self-Service.
- For a term-related balance, the credit card icon goes to the **Credit Card Payment** page in Student Self-Service. This link is displayed only for outstanding balances.

  Note: This portlet has no user preferences.

My Statement portlet

Displays summary information for the student's most recent statement, including bill date, amount due, due date, and term (if the statement is a schedule/bill format). The current account balance is also displayed.



My Statement

Statement and Payment History

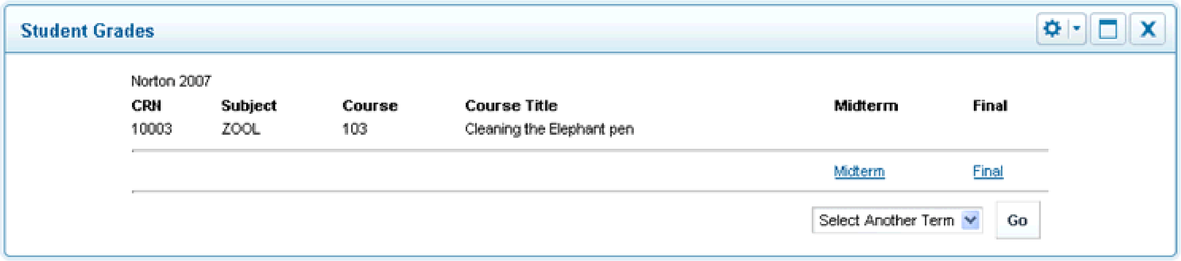
Navigational links:

- The credit card icon goes to the **Credit Card Payment** page in Student Self- Service. This link is displayed when either the Amount Due or Account Balance is a positive amount.
- The **Statement and Payment History** link accesses the **Statement and Payment History** page in Student Self-Service. This page enables users to view available statements, payment history, and unbilled activity for an account.

  Note: This portlet has no user preferences.

Student Grades portlet

View midterm and final grades for a student.



Norton 2007

CRN	Subject	Course	Course Title	Midterm	Final
10003	ZOOL	103	Cleaning the Elephant pen		
				Midterm	Final

To change the term displayed, select the desired term from the pull-down list and click **Go**.

To view a complete list of classes, if there are more records than are displayed in the channel, click the **More** link. The system displays the channel in focus mode with the complete list of classes.

If there is a hold on a student's grades, the portlet displays a message stating that grades are not available due to the hold.

Navigational links:

- The Course Reference Number (CRN), if displayed as a hyperlink, indicates that gradebook detail exists for the course and goes to the **Component Grade Detail** page in Student Self-Service. A check mark next to a linked CRN indicates that grades are assigned to components in the gradebook details.
- The **Midterm** link goes to the **Midterm Grades** page in Student Self-Service.
- The **Final** link goes to the **Final Grades** page in Student Self-Service.

Student Grades portlet user preferences

Change the default term or number of records displayed in the **Student Grades** portlet.

About this task

To change the default term displayed in the portlet:

Procedure

1. Click edit button for the portlet.
2. In the **Default Term** field, select the term you want displayed.
3. Click **Apply**.

   To change the default number of records displayed in the channel:
4. Click **Preferences** menu in the portlet.
5. In the **Number of Courses** field, enter the number of records you want displayed.
6. Click **Apply**.

   To return the display to the original defaults:

7. Click the edit button for the portlet.
8. Click **Reset**.
9. Click **Apply**.

Results

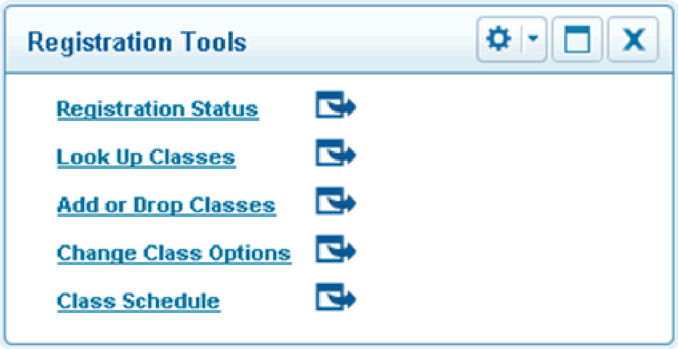
Once you have made all your changes, click **Back** to return to the portlet.

Student Registration Tools portlet

Access to registration-related information and activities.

Navigational links:

- Registration Status
- Look Up Classes
- Add or Drop Classes
- Change Course Options
- Class Schedule


Registration Tools

Registration Status

Look Up Classes

Add or Drop Classes

Change Class Options

Class Schedule

Note: When any of these links are accessed, the system always prompts for the term to ensure that any changes made are for the correct term. This portlet has no user preferences.

Student Work-Study Balance portlet

View the balance of your remaining work-study. The effective date of the balance data is also displayed.

Other information that might be displayed in the portlet, depending on your institution's setup are:

- Total Authorized Available
- Total Work Study Earned
- Remaining Work Study Balance
- Remaining Percentage of Work
- Total Hours Remaining to Work

To change the aid year displayed, select the desired year from the pull-down list and click **Go**.

Navigational links:

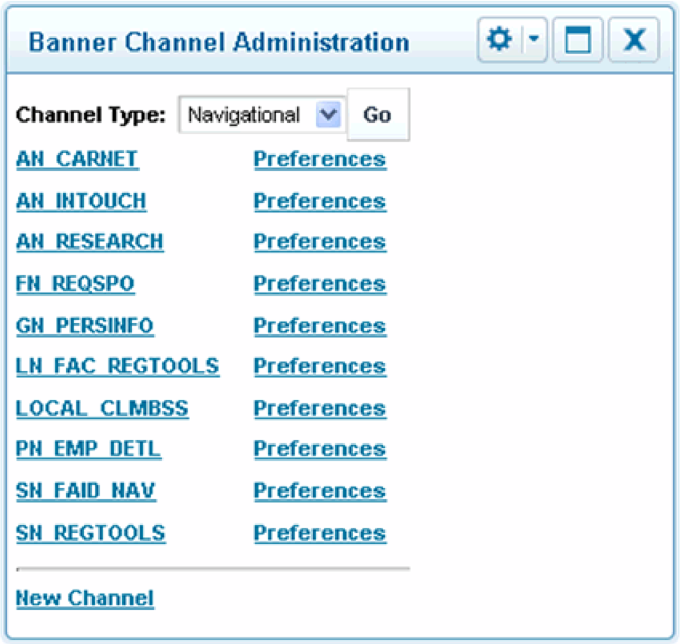
- The **Award Package** link goes to the **Award Package for Aid Year** page in Student Self-Service.
- The **Directory** link redisplays the channel with the telephone number(s) of your assigned supervisor(s).

Note: This portlet has no user preferences.

Banner Channel Administration portlet for Common

Perform administrative tasks on Luminis® portlets for Banner®.

To access the portlet, you must have the appropriate role assigned to your user ID.



Banner Channel Administration

Channel Type: Navigational

AN_CARNET	Preferences
AN_INTOUCH	Preferences
AN_RESEARCH	Preferences
FN_REQSPO	Preferences
GN_PERSINFO	Preferences
LN_FAC_REGTOOLS	Preferences
LOCAL_CLMBSS	Preferences
PN_EMP_DETL	Preferences
SN_FAID_NAV	Preferences
SN_REGTOOLS	Preferences

New Channel

By default, the portlet displays the list of navigational channels available at your institution. To view the list of informational channels, select **Informational** from the **Channel Type** pull-down list, then click **Go**.

Navigational links:

- The channel name link in the left column (for example, **GN_PERSINFO**) goes to the **Customize a Channel** page in Web Tailor.
- The **Preferences** link in the right column goes to the **Preferences** page in Web Tailor.
- The **New Channel** link goes to the **Channel Maintenance** page in Web Tailor.

Note: This portlet has no user preferences.

Luminis Announcements

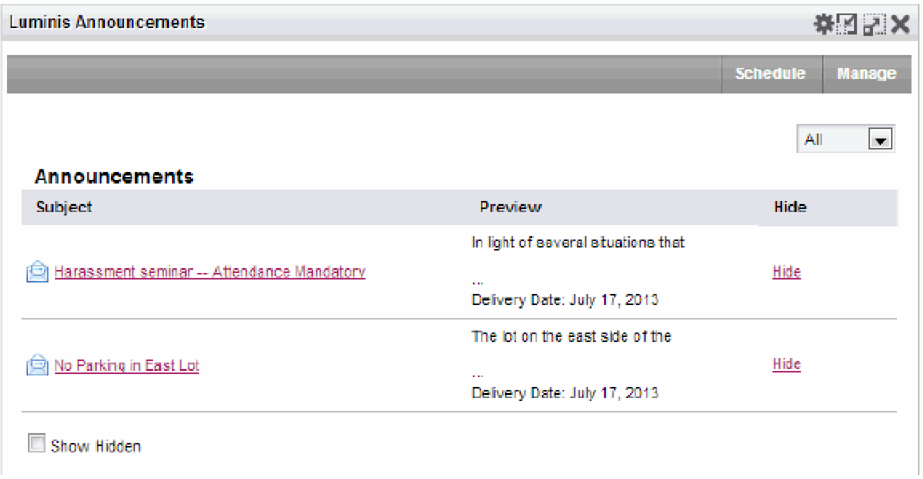
A Luminis® announcement, also known as a personal or targeted announcement, is an announcement sent to a group of users, members of a site or course, or the entire campus. It is a one way, group to group communication.

Examples where targeted announcements are required:

- Upcoming professional development and training announcements
- Changes to college, division or university policies and procedures
- Messages to students in a specific major
- Class cancellations sent by an authorized individual within the college
- Upcoming college, division or university events and activities

A notification announcement is a specific type of Luminis targeted announcement that originates in the Banner system as a Smart or Notify event. Examples of Smart events may include add hold, grades posted, or grades changed. Examples of Notify events may include admission application received or section canceled. These notifications are passed from the Banner system to the Luminis system through the configured JMS message broker, and the Luminis system delivers the notifications to the user through the **Announcements** portlet, e-mail, or the Ellucian GO mobile app.

When Luminis Platform is installed, the **Announcement** portlet will be placed on the default layout of each person who logs into the Luminis system.



Announcements

Subject	Preview	Hide
Harassment seminar -- Attendance Mandatory	In light of several situations that ... Delivery Date: July 17, 2013	Hide
No Parking in East Lot	The lot on the east side of the ... Delivery Date: July 17, 2013	Hide

□ Show Hidden

In the **Luminis Announcements** portlet, action bar menu, users can access the **Manage** and **Schedule** menus. These menus provide users access to additional functionality of the announcements system, including scheduling announcements and managing announcements they have scheduled.

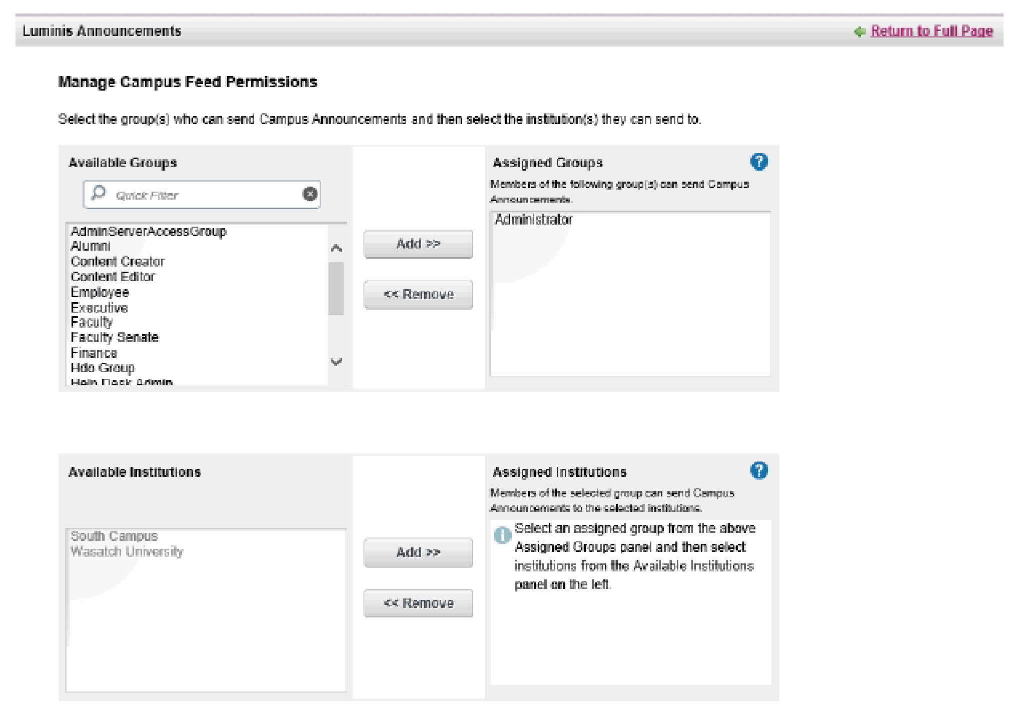
First time setup

When the Luminis system is installed, the administrator should delegate who can schedule campus announcements and who can schedule targeted announcements. They should also configure the default delivery method(s) for any notification announcements.

Initially, administrators can schedule targeted and campus announcements. Site leaders and course instructors can send targeted announcements to members belonging to sites or courses for which they are leader.

Manage Campus Feed Permissions

To setup other users to send campus announcements, the administrator must select **Campus Feed Permissions** from the **Manage** menu.



Luminis Announcements

Manage Campus Feed Permissions

Select the group(s) who can send Campus Announcements and then select the institution(s) they can send to.

Available Groups

AdminServerAccessGroup
Alumni
Content Creator
Content Editor
Employee
Executive
Faculty
Faculty Senate
Finance
Hdo Group
Help Desk Admin

Assigned Groups

Members of the following group(s) can send Campus Announcements.

Administrator

Available Institutions

South Campus
Wasatch University

Assigned Institutions

Members of the selected group can send Campus Announcements to the selected institutions.

Select an assigned group from the above Assigned Groups panel and then select institutions from the Available Institutions panel on the left.

For information about setting the campus feed permissions, see the *Multi-Entity Processing Implementation Guide*.

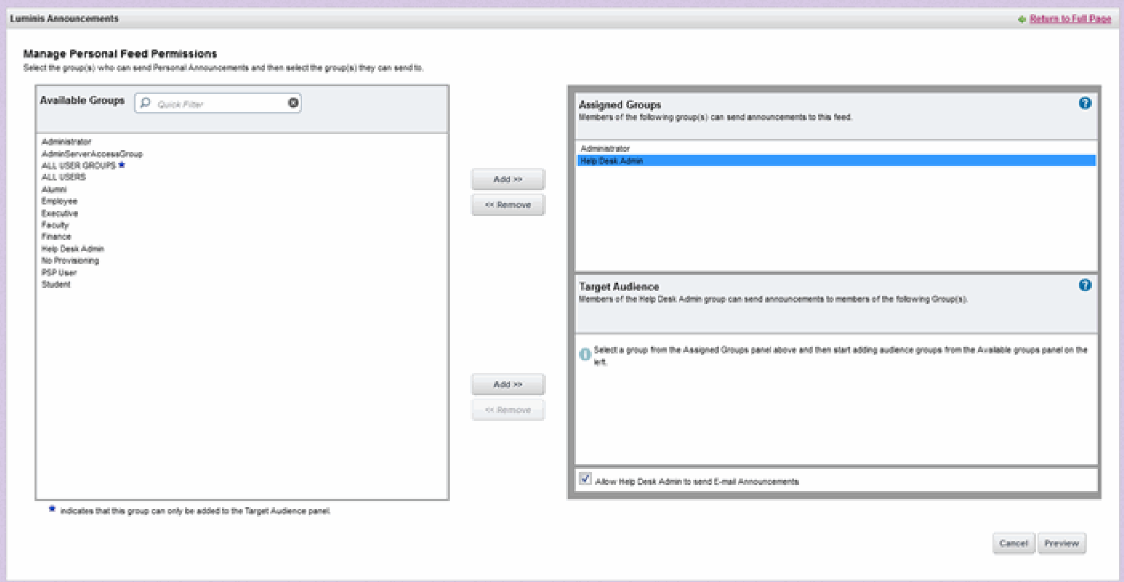
Warning! When assigning authorization for managing Campus and Personal (Targeted) Announcements, it is strongly recommended that the Administrator permission NOT be removed. Rare exceptions to this can occur if other administrative permissions have been previously created.

Manage Personal Feed Permissions

Initially, members of the Administrators group and site leaders -- including course instructors -- can send announcements targeted to the personal feed.

About this task

In the **Manage Personal Feed** page displayed below, you can grant permissions for members of other groups to send personal announcements to selected groups.



Manage Personal Feed Permissions

Select the group(s) who can send Personal Announcements and then select the group(s) they can send to.

Available Groups:

Administrator
AdminServerAccessGroup
ALL USER GROUPS ★
ALL USERS
Alumni
Employee
Executive
Faculty
Finance
Help Desk Admin
No Provisioning
PSP User
Student

★ indicates that this group can only be added to the Target Audience panel.

Assigned Groups

Members of the following group(s) can send announcements to this feed.

Administrator
Help Desk Admin

Target Audience

Members of the Help Desk Admin group can send announcements to members of the following Group(s).

Select a group from the Assigned Groups panel above and then start adding audience groups from the Available groups panel on the left.

☑ Allow Help Desk Admin to send E-mail Announcements

In the list of Available Groups, there is a predefined shortcut called ALL USER GROUPS. This shortcut allows the targeting of all groups of type USER. The ALL USER GROUPS shortcut and any groups that were created in the Luminis Group Manager that are not of type USER cannot be assigned permissions to send announcements. They can only be targeted for announcements. Thus, you can only add these groups to the Target Audience, not to the Assigned Groups. These groups are indicated by a star in the Available Groups list.

Warning! When assigning authorization for managing Campus and Personal (Targeted) Announcements, it is strongly recommended that the Administrator permission NOT be removed. Rare exceptions to this can occur if other administrative permissions have been previously created.

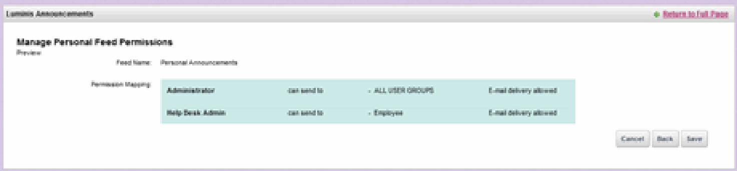
For example, to allow members of the Help Desk Admin group to send announcements to faculty and to all students:

Procedure

1. Select the Help Desk Admin group in the Available Groups box, and click **Add** on the top of the page to add it to the Assigned Groups.
2. When the Help Desk Admin group selected is in the Assigned Groups, add Faculty and Student groups to the Target Audience with the **Add** button at the bottom of the page.

3. If you want to send announcements by e-mail, check the **Allow Help Desk Admin to send E-mail Announcements** check box.
4. If you want to disable the option for site leaders to send personal announcements to members of their sites, select SITE LEADERS in the Assigned Groups box and click **Remove** on the top of the page.
5. If you want to grant site leaders the ability to send personal announcements to be delivered via e-mail, select SITE LEADERS in the Assigned Groups box and click the **Allow SITE LEADERS to send e-mail announcements** check box.
6. Click **Preview** to review and save your changes.

   The preview page will show you all the permissions granted for the announcements Personal Feed including any unsaved changes.



Manage Personal Feed Permissions

Preview

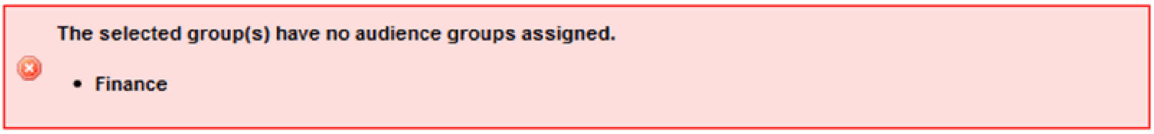
Feed Name: Personal Announcements

Permission Mapping:

Administrator	can send to	- ALL USER GROUPS	E-mail delivery allowed
Help Desk Admin	can send to	- Employee	E-mail delivery allowed

7. Click **Save** to save all changes to the server.

   If on the previous page there are groups in the Assigned Groups box, but none in the Target Audience panel, you will see an error on the preview page.



The selected group(s) have no audience groups assigned.

- Finance

8. Click **Back** to return to the previous page to correct the error.

   Note: If you are upgrading from a prior version of Luminis 5.0.X, any users who were granted permissions to send targeted announcements will now be allowed to target ALL USER GROUPS, including Administrators.

Manage Notifications

Change the notification delivery method and length of display time in the the **Manage Notifications** page.

The default method for delivery of notifications is initially only to deliver to the **Luminis Announcements** portlet, and to display the message in the portlet for 7 days.

If you select more than one delivery method, the message is delivered to the user in multiple ways. For example, when you select both **Publish notifications to e-mail** and **Publish notifications to announcements** portlet, the message is delivered to the user in the portlet and as an e-mail.

Publish notifications to mobile devices setup

To change mobile delivery settings, select the **Publish notifications to mobile devices using Ellucian GO** option in the **Manage Notifications** page.

In addition to the **Luminis Announcement** portlet and e-mail notification delivery, you can send notifications to mobile devices with the Ellucian GO application.

The values to send notifications through Ellucian GO come from the Ellucian Mobile server when the server plugin for the notification center is created. Contact the Ellucian Mobile server administrator for these values.

Examples of Ellucian GO notification values:

- URL to the Ellucian GO notification API:

  ```
  http://<your.server>/banner-mobileserver/api/notification/notifications
  ```
- Ellucian Application Name:

  ```
  Luminis 5.2.2
  ```
- Ellucian GO notification API key:

  ```
    a932731a-39ed-9a5c-gggd-4800cb71ff93
  ```

For more information see "Set up the Notifications" in the *Ellucian Mobile Implementation Guide*.

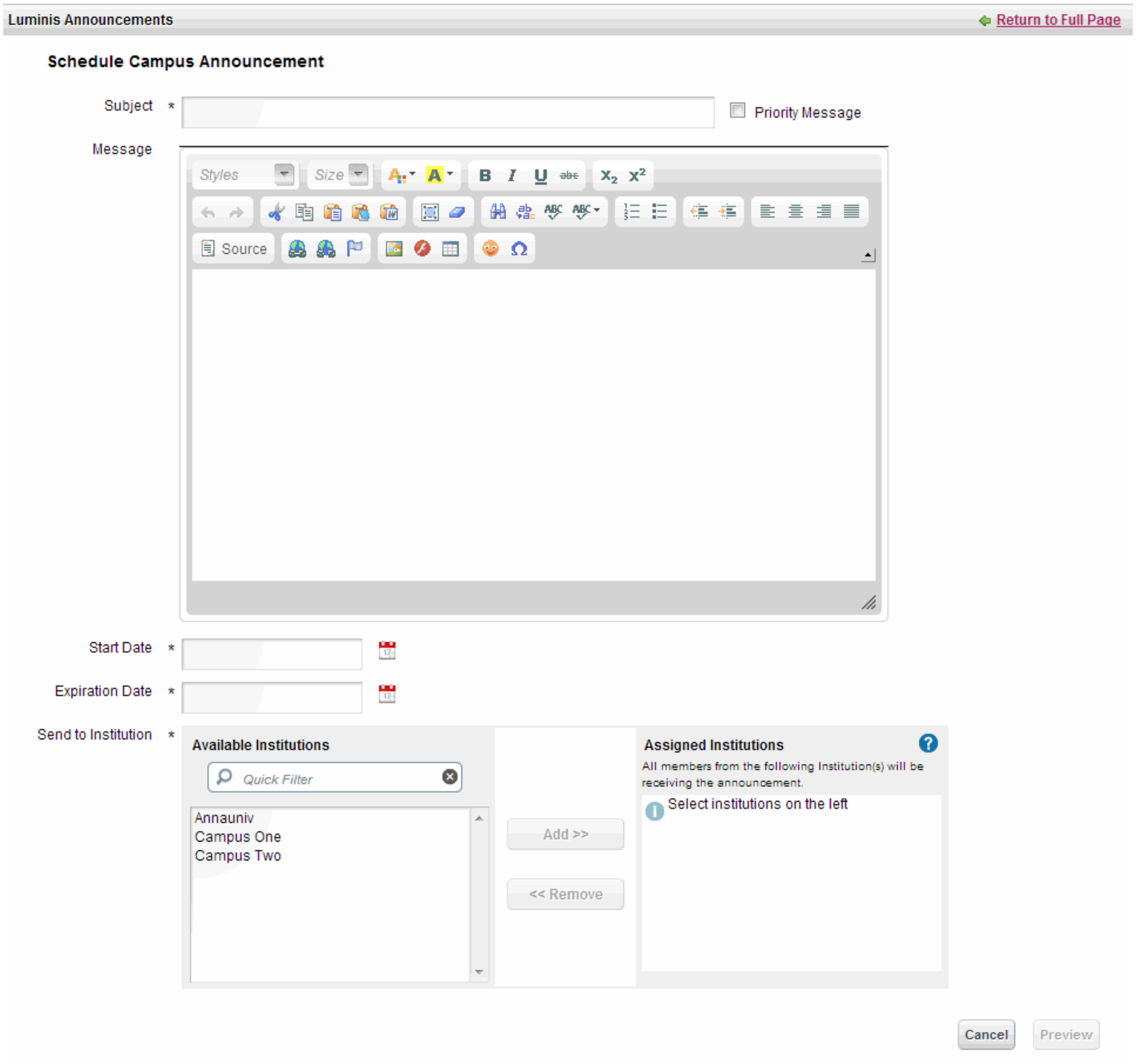
Schedule a campus announcement

Schedule an announcement to send to the entire campus.

Procedure

1. Select **Campus Announcement** from the **Schedule** menu.

   You see the **Schedule Campus Announcement** page.



Luminis Announcements

Return to Full Page

Schedule Campus Announcement

Subject *

□ Priority Message

Message

Start Date *

Expiration Date *

Send to Institution *

Available Institutions

Quick Filter

Annauniv
Campus One
Campus Two

Assigned Institutions

All members from the following Institution(s) will be receiving the announcement.

Select institutions on the left

2. Enter the required fields.

Field	Description
Subject	This field is required and accepts plain text.
Message	This field is an HTML text field. It will be displayed as HTML formatted text in the announcement portlet.
Start Date	The date and time that the announcement will first be displayed to users in their announcement portlet.

Field	Description
Expiration Date	The date and time the announcement will no longer be displayed in the user's announcement portlet.
Priority Message	If this is checked, this message will display at the top of the list in the announcements portlet.
Send to Institution	Select one or more institutions from the **Available Institutions** drop-down menu to send the announcement to only the selected institutions. **Note:** This option does not appear unless you import additional institutions into the system via multi-entity processing.

Note: Both the **Start Date** and the **Expiration Date** are relative to the browser time, not to the server time. All date or times in the announcement portlet are relative to the user.

3. Click **Schedule**, to schedule the announcement to be displayed on the Start date.

Schedule a targeted announcement

Schedule an announcement ahead of time to send to multiple groups and students at the same time.

Procedure

1. Select **Targeted Announcement** from the **Schedule** menu to schedule the announcement to be displayed on the Start date.
2. Enter the required fields.

Field	Description
Additional delivery option	Check the **E-mail** check box to send the announcement as an e-mail. If you do not want replies sent to the default name or e-mail address, type the preferred name in the **Reply To Name** field and the preferred e-mail address in the **Reply To Address** field.
Subject	This field only accepts plain text.
Message	This field is an HTML text field. It will be displayed as HTML formatted text in the announcement portlet.

Field	Description
Start Date	This is the date and time that the announcement will first be displayed to users in their announcement portlet.
Expiration Date	This is the date and time the announcement will no longer be displayed in the user's announcement portlet.
Priority Message	If this check box is checked, this message will display at the top of the list in the announcements portlet.
Target this message to	This radio button group defines the type of target audience for this message. For example: a faculty member can target announcements to members of courses he is instructing and can also target the Student group. When he creates a targeted announcement, he would select between the two options: **Members of Luminis Groups** and **Members of Luminis Sites**. The target audience is groups by default. **Note:** This radio button is only visible for users who have permission granted to target announcements to both groups and sites (or courses).
Send to Group	Select one or more groups of users from the **Available Groups** drop-down menu to send the announcement to only the selected groups.
Send to Site	Select one or more sites or courses from the **Available Sites** drop-down menu to send the announcement to only the selected sites.

Note: Both the **Start Date** and the **Expiration Date** are relative to the browser time, not to the server time. All date or times in the announcement portlet are relative to the user.

Results

The **Schedule Targeted Announcement** page is similar to the **Schedule Campus Announcements** page with the exception of the targeting criteria. The "Additional delivery option" e-mail is only available when scheduling targeted announcements. The announcement displays in the **Luminis Announcements** portlet for the selected groups on the given date and time. An announcement can target a:

- group
- list of groups

- site
- list of sites
- course
- list of courses

The target audience cannot be a mixture of groups and sites.

Note: You must be a member of any of the selected groups in order to receive the announcement.

Related Links

Targeted content permissions on page 298

View campus or personal announcements

Campus announcements are targeted to the entire campus. Personal announcements are targeted to a group or site in which you are a member.

About this task

When viewing announcements, all announcements are displayed by default. You can select a category from the drop-down to filter the portlet to display only the announcements from the selected category. Currently, Campus, Personal, and Notification are the only categories supported.

Procedure

1. In the preview page, click the subject of a given message.

   The portlet displays the details about the announcement such as the sender and the delivery date.
2. Click **Done** to return to the main portlet.

Results

A maximum of ten messages are displayed at a time. If more than ten messages are available, you can use the controls available at the bottom of the page.

Manage announcements

Administrators can track all campus announcements and targeted announcements which target a group or list of groups regardless of whether they created the announcement.

About this task

Administrators are the only users who can track notification announcements. Site leaders are the only users who can track targeted announcements which target a site or course, and only if they are the leaders of the specific site targeted. Non-administrator users can track the announcements either they or a member of his group has scheduled. For example, if John Smith is in the HelpDeskAdmin group and schedules an announcement targeting Employees, other members of the HelpDeskAdmin group can also track that announcement.

Procedure

1. In the **Announcements** portlet, click **Manage** and select **Announcements** from the drop-down menu.
2. Click the **Subject** line to view the details of an announcement.
3. Use the category drop-down list to filter the portlet to display only the announcements in a certain category.
4. Type into the filter box to filter the list so that only announcements that have the text somewhere in their subjects will be displayed.
5. To clear the filter, click ☒.

Results

Similar to the main announcement page, only ten messages are displayed at a time. If there are more then ten messages, controls for paging display so you can scroll through the pages.

You can sort by these fields: **Sent By**, **Subject**, **Feed**, **Delivery Date**, and **Expiration Date**. Controls to sort the fields in ascending or descending order appear when the mouse hovers over those fields.

Table 8: Announcement status options

Announcement Status	Description
Active	Messages currently on display to users
Pending	Messages scheduled to display on a future date
Expired	Messages that were displayed in the past and are no longer on display.
Archived	Messages stored in an archive and no longer display to the users.

Edit and reschedule announcements

Edit and reschedule campus or targeted announcements (except for notification announcements) either before or after the initial announcement is posted. You cannot edit notification announcements in Luminis Platform.

About this task

When you edit an active announcement, the original announcement automatically expires and a new announcement posts to the intended audience.

Procedure

1. In the **Luminis Announcements** portlet, click **Manage**, and select **Announcements** from the drop-down menu.
2. Click the Edit/Reschedule icon ✎ next to the announcement you want to update.
3. Update the announcement as needed.
4. Click **Next**.
5. Depending on the status of the original announcement, you may see a check box called **Saving as a new Active announcement on the Preview page. Select to immediately Expire the original announcement also**.
   - If the original announcement was pending, but not yet posted to target users, the check box does not display. The new announcement replaces the original announcement.
   - If the original announcement is active or expired (no longer pending), the check box displays. When you mark the check box and save the announcement, the new announcement is saved as a copy of the original.
   - If the original announcement is active and target users can view the announcement, the check box displays. When you mark the check box, the original announcement immediately expires and saves the new announcement. The target users can only view the new announcement. If you uncheck the check box, the target user can view both the original and the new announcement.
6. Click **Edit** to return to the **Edit/Reschedule Campus Announcement** page and make additional changes.
7. Click **Schedule** to post the announcement.

Archive and delete

You can archive and delete messages from the **Manage Announcements** page.

- Click ☒ next to the announcement to either archive or delete the announcement. Only announcements that have been archived first will be deleted. Once an announcement is archived, it will no longer display in the list of announcements unless the **Show Archived** check box is selected.

  If you archive an announcement scheduled for e-mail delivery, Luminis Platform automatically checks whether e-mail delivery has begun to process for that announcement. If the e-mail delivery is in process, a message displays.

  The announcement with e-mail delivery was archived successfully. However, the e-mail sender task will continue to process and send the e-mails.
- In the **Manage Archive** page, click ☒ to display the choices whether to archive or cancel. Archiving will remove the announcement from the list. Canceling will cancel the action.
- When you select the **Show Archived** check box, it will display all announcements, including those that have been archived.
- Click ☒ next to the archived message to permanently delete the message.

- Click **Delete** to remove the message.

  When you delete a pending e-mail announcement, the e-mail sender task for the announcement is deleted and delivery is canceled. Deletion does not affect e-mails that were successfully delivered.

Hide and unhide messages

Send announcements to either the entire campus at once, or to a targeted group of individuals.

About this task

These announcements are displayed in the **Luminis Announcements** portlet on the user's home page and remain available for as long as the institution deems necessary. If users do not wish to view an announcement, they can hide it. For example, the user may hide announcements that they have already read in order to reduce the visual clutter on their home page. They can also redisplay announcements they previously hid.

To display or hide an announcement in the **Luminis Announcements** portlet:

Procedure

1. Log in to Luminis Platform as a user.
2. In the **Luminis Announcements** portlet, mark the **Show Hidden** check box.
   - If hidden, click **Unhide** to view the message.
   - If you want to hide the message, click **Hide**.

   The portlet automatically refreshes to show the updated settings.

Targeted announcements via e-mail

You can configure Luminis Platform to send targeted announcements through e-mail.

Related Links

Schedule a targeted announcement on page 140

Set the default From e-mail address

If you mark the **Additional Delivery Email** check box, when you create a new targeted announcement, a default **From** e-mail address is automatically added to each targeted announcement.

About this task

To change the value for the default **From** email address:

Procedure

1. Log in to Luminis Platform as an administrator.
2. Click **Go to**, and then select **Control Panel**.
3. Under the **Portal** category, click **Portal Settings**.
4. In the **Configuration** menu, click **Email Notifications**.
5. Click the **Sender** tab and enter your changes in the **Name** and **Address** fields.
6. Click **Save**.

Configure the SMTP server

Set up your server to process e-mail exchange and delivery with various IPs.

Procedure

1. Log in to Luminis Platform as an administrator.
2. Click **Go to**, and then select **Control Panel**.
3. Under the **Server** category, select **Server Administration**.
4. On the **Server Administration** page, click the **Mail** link.
5. In their respective fields, enter the values for the **Outgoing SMTP Server** and **Outgoing Port**.
6. Click **Save**.

Configure settings for e-mail delivery

Set the batch size and sleep time between Luminis Platform e-mail tasks.

Procedure

1. Log in to Luminis Platform as an administrator.
2. Click **Go to**, and then select **Control Panel**.
3. Under the Portal category, click **Luminis Email Monitor**.
4. Click the **Configuration** tab.
5. Edit the fields.

Table 9: Targeted announcement e-mail configuration properties

Property	Description
Batch Size	The number of e-mails sent at one time. If the batch size is set to 100 and you want to send an e-mail to 1000 addresses, Luminis Platform will send 10 batches with 100 e-mail addresses included in each batch. The batch

Property	Description
	size must be at least 10 and can be no more than 200. The default is 100.
Sleep Time	The length of time in between how often Luminis Platform checks e-mail tasks. A minimum of 5 seconds to a maximum of 3600 seconds (60 minutes) can be set. The default is 15 seconds.

Manage targeted announcement e-mail tasks

When you schedule a targeted announcement to deliver via e-mail, Luminis Platform creates an e-mail sender task that handles the delivery of the e-mails off-line. The **Luminis Email Monitor** displays tasks related to targeted announcements e-mail delivery and tasks related to Smart and Notify event notifications delivered to e-mail and to Ellucian GO.

About this task

To view the targeted announcement e-mail tasks:

Procedure

1. Log in to Luminis Platform as an administrator.
2. Click **Go to**, and then select **Control Panel**.
3. Under the Portal category, click **Luminis Email Monitor**.

Results

Click the refresh button to reload the page and view the latest list of task data.

An `EmailSenderService` service thread processes these tasks from the queue and updates their statuses as they are processed. The announcement **Start Date** determines when the e-mail task is ready to send the announcement to the target groups. All `EmailSenderService` service thread activity is logged to the `email_sender.log` on the Luminis Platform Administration server.

Table 10: Targeted announcement e-mail task statuses

Status	Definition
New	Newly-created and waiting for the sender task service to begin processing.

Status	Definition
Scheduled	Scheduled to deliver the e-mails at a future date or time.
Submitted	Picked up by the `EmailSenderService` service thread and execution has started.
Processing	The execution process is determining the list of e-mail addresses for the submitted announcement.
Sending	The execution process is currently sending e-mails through the configured SMTP server in batches.
Complete	Task execution is complete. All batches of e-mails have been sent to the SMTP server.
Canceled	Task has been canceled. The processing or sending of e-mail batches to the SMTP server has halted.
Blocked	The `EmailSenderService` thread has been blocked. For more details about the reason the thread was blocked, refer to the `email_sender.log` server log on the admin node.

Interactions between an e-mail sender task and the corresponding targeted announcement:

- When you reschedule a targeted announcement that has not yet been delivered, the **Next Attempt** time is updated for the corresponding scheduled e-mail sender task.
- When you reschedule a targeted announcement that has been delivered, Luminis Platform creates a new e-mail sender task in the **Luminis Email Monitor** portlet.
- When you cancel an e-mail sender task, the original targeted announcement remains in the **Luminis Announcements** portlet.
- When you delete a targeted announcement that has not yet been delivered, Luminis Platform deletes the corresponding e-mail sender task.
- When you delete a targeted announcement that is currently processing or delivering e-mail, Luminis Platform cancels the corresponding e-mail sender task.
- When you archive a targeted announcement, the action has no impact on the corresponding e-mail sender task.

Related Links

Targeted content permissions on page 298

Purge completed e-mail sender tasks

Click the **Purge Completed Tasks** button to remove completed and canceled sender tasks from the task list.

You cannot undo this action.

Cancel an e-mail sender task

If the cancel ⊗ button displays next to a task in Cancel column, you can stop the task.

If the status of the task is sending, the task is stopped after the current batch is done.

Smart events and Notify events

Administrators can create their own templates or customize the default templates included during Luminis Platform installation. You can deliver events through the Luminis **Targeted Announcement** portlet, e-mail, or mobile notification.

Luminis Platform 5 consumes two types of message events from Banner: Notify events and Smart events. Both use a template in the Luminis system to format the end-user message and insert the information provided in the event or about the target recipient into that message.

Smart and Notify events are handled similarly by the Luminis Platform system. Smart events contain data elements you must insert into the template, and the template generates links to access the Banner system directly from the final formatted message. Notify events contain the actual message from the Banner system to insert into the template for the end user, and do not contain any links back to Banner.

Event XML format

Luminis Smart events and Notify events conform to an XML schema as specified in the *Banner Integration for eLearning Administration Guide 8.0, Appendix E*.

Events contain the event type of either User or Course, the recipient(s), the method of delivery, the name of the template to use for formatting the end-user message, and parameters to be substituted into the target message.

See the "Notify Events and Smarts Events" section of the *Banner Integration for eLearning Administration Guide* for full documentation about the events generated by Banner, the event triggers, and event content.

Configure the JMS connection

Luminis Platform uses the same configuration as Banner synchronization events to receive Smart events and Notify events via JMS.

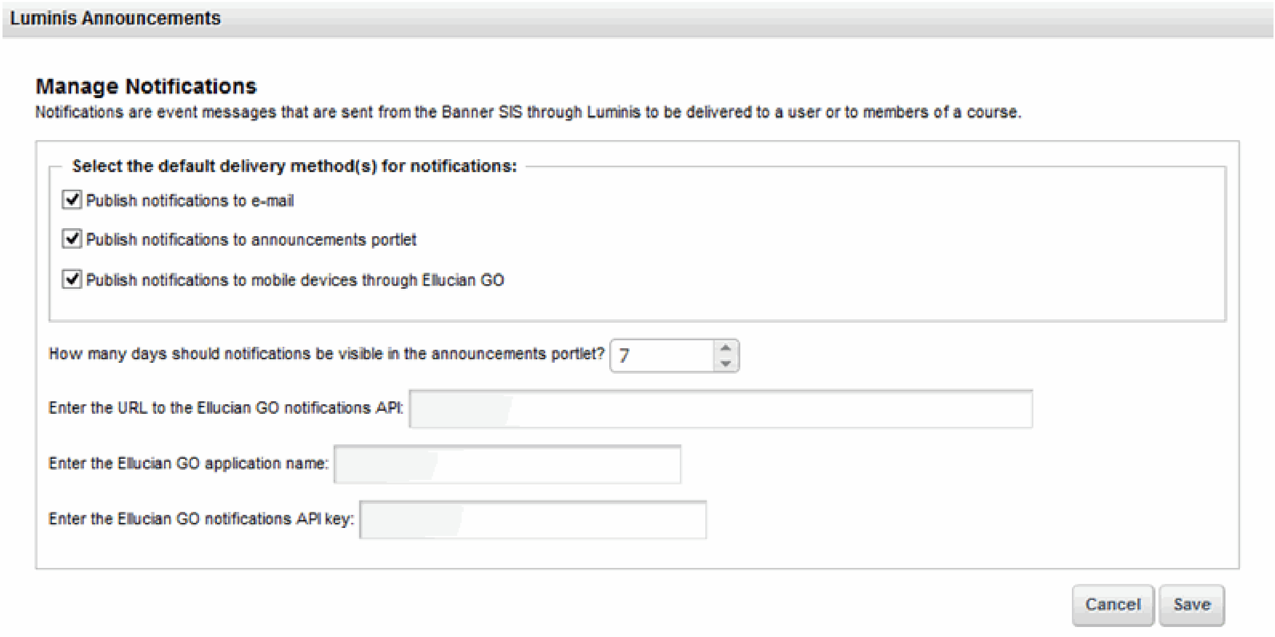
This configuration is described in the "Data-Level Integration and Provisioning" chapter of the *Luminis Platform Banner Integration Setup Guide.* The JMS message topic that handles Smart and Notify events is named `com_sct_ldi_sis_EntityEvents`, the same name used in Luminis Platform 4 events.

Configure delivery

To deliver messages by mobile notification, specify Default delivery in Banner then configure the mobile notification method of delivery as one of the delivery methods in the **Luminis Announcements** portlet.

The delivery method for the event is specified in the XML message received from Banner, either Default, Email, or TargetedAnnouncement. If the method is Default, Luminis Platform determines the delivery method according to configuration specified in the Manage announcements section of the **Luminis Announcements** portlet.

Figure 3: Set the default delivery method for announcement notifications



Luminis Announcements

Manage Notifications

Notifications are event messages that are sent from the Banner SIS through Luminis to be delivered to a user or to members of a course.

Select the default delivery method(s) for notifications:

☑ Publish notifications to e-mail

☑ Publish notifications to announcements portlet

☑ Publish notifications to mobile devices through Ellucian GO

How many days should notifications be visible in the announcements portlet? 7

Enter the URL to the Ellucian GO notifications API:

Enter the Ellucian GO application name:

Enter the Ellucian GO notifications API key:

If you chose the Default delivery method, you can select multiple delivery options. The Smart or Notify event is sent through all options that you select and configure.

- Configure the **Publish notifications to e-mail** option in targeted announcements via e-mail.
- If you select **Publish notifications to announcements portlet**, you can also enter the number of days you want the announcement to actively display to the users.

- To configure the fields related to **Publish notifications to mobile devices through Ellucian GO**, see the Ellucian Go documentation about configuring Ellucian Go mobile notifications.

Related Links

Manage announcements on page 142

Configure Banner system links

The end-user messages delivered from Smart events contain links for a user to access the Banner system directly. For these links to work, you must configure Luminis Platform for Banner integration as specified in the *Luminis Platform Banner Integration Setup Guide*.

Note: The links in messages received via e-mail or mobile notification require the user to log in to Luminis Platform before they can access the target data of that link.

Templates for notification events

Templates to format notification events are located in the admin server's Luminis `webapp` directory under `$CP_ROOT/products/tomcat/tomcat-admin/webapps/luminis/templates`.

Template names are specified in the XML event in the *<templateName>* element. You can prefix Banner XML event template names with the string `BSTUDENT:` which differentiated Banner templates from Plus templates in previous versions. In Luminis Platform 5, this prefix is removed and ignored when it matches a template file.

Templates are processed by the Apache Velocity Engine, and you can use all of the constructs, syntax, and programming used in Velocity. The objects available for Velocity processing in Luminis Platform depend on the EntityType of the XML event received. Velocity is highly flexible and programmable, and the output of the template may contain an HTML format that displays in the **Targeted Announcement** portlet message or e-mail message. You do not need in-depth knowledge of Velocity to create or modify the templates. See http://velocity.apache.org for more information about Velocity.

Warning! When you edit the template files with Unicode characters, ensure the file is stored as a UTF-8 encoded file.

Subject lines for notification event templates

Each template contains a tag to use as the subject in a targeted announcement e-mail, or as the subject line in an announcement targeted to the portlet.

The subject is specified between the XML tags *<subject>* and *</subject>*. You can enter text or references to configuration, event, user-specific, or course-specific information for the subject line.

For example:

```
<subject>${Event.SCTHoldDescription} Was Placed</subject>
```

After Velocity processing, the subject line should not contain any HTML tags or formatting. The subject line should only contain text.

The *.vtpl file you edit for the Smart and Notify events must be a valid formatted Velocity template. Velocity syntax uses "$", "#", "##", "!", "{}", and so forth in the template syntax. To include these symbols as literal characters for events posted to the **Targeted Announcement** portlet, you must specifically configure them.

Configuration values in a template

You can access any value that exists in the Luminis configuration service from the Velocity template and insert the value into the end-user message.

Configure Luminis Platform via JMX. Use the following format to access configuration values in the template:

```
${Configuration.getString('<luminis.config.value>')}
```

<*luminis.config.value*> is the name of the configuration value you wish to insert in the end-user notification. If the Luminis configuration value name is not enclosed in single quotes, Velocity attempts to interpret any `'.'` in the name as an operator. For example, this feature is useful to generate links with URLs that refer to the Luminis virtual host name.

User data in a template

An event that specifies a User as the EntityID target can substitute user-specific information in the template used for that event.

To insert information about a user into the template, use the form `${User.<dataelement>}` where <*dataelement*> may be:

- `PersonId`
- `DisplayName`
- `HomeInstitution`
- `FirstName`
- `LastName`
- `UdcIdentifier`
- `DateOfBirth`
- `EmailAddress`
- `LoginId`

Course data in a template

An event that specifies a course as the target EntityID can include course-specific information in the template used for that event.

To insert the course information, use the form `${Course.<dataelement>}` where *<dataelement>* may be any these:

- `CourseName`
- `CourseDesc`
- `CourseAndSectionId`
- `EndDate`
- `StartDate`
- `OrgUnit`

Event parameters in a template

You can insert parameters into the template for messages for Smart events generated by Banner.

The parameters contained in each specific event type are defined by the Banner system in the form of `SCT.XXX.YYY`, such as `SCT.Subject.Code`. You can access these parameters in a template using the form `${Event.SCTXXXYYY}`, such as `${Event.SCTSubjectCode}`.

Note: Each "`.`" is removed from the raw XML parameters due to Velocity processing constraints.

The parameters supplied depend on the event generated by Banner. The events defined as Smart events are Add Hold, Grades Posted, and Grade Changed. The parameters defined for each of these events are:

Table 11: Directory logs(continued)

Name	Location
Add Hold	`SCTHoldDescription`, `SCTActivityDate`
Grades Posted	`SCTSubjectCode`, `SCTCourseNumber`, `SCTSectionTitle`, `SCTTermDescription`
Grade Changed	`SCTSubjectCode`, `SCTCourseNumber`, `SCTSectionTitle`, `SCTTermDescription`

Notify events only contain one data parameter, which is the **MESSAGE** field. The content of the message is generated on the Banner system, and should be inserted into the template used to process that message.

For details describing all events and their triggers in Banner, see the *Banner Integration for eLearning Administration Guide*.

Support for multiple languages

You can use the Java file-name locale rules to create templates for a specific language.

For example, translate the default English template `mytemplate.vtpl` into French and name it `mytemplate_fr_FR.vtpl`. The file used to generate the target message is selected based on either the preferred language of the target user for User Smart and Notify events or the default language of the server in the case of Course Smart and Notify events. There is no current option to specify a preferred language for a specific course.

If you use a Left-To-Right language and want the Smart or Notify event results in the Luminis Announcements portlet to contain bidirectional text, edit the Velocity template so that the text and punctuation displays correctly. For example, if you want the `Event.SCTSectionTitle` variable to resolve to an English section title, format the `ic_grade_roll_ar_SA.vtpl` template text to display the bidirectional text and punctuation. You can use bidi_control characters, the HTML `<bdo>` tag, or remove the punctuation options, such as "()". For more information on bidirectional text and bidi-control characters, see http://en.wikipedia.org/wiki/Bi-directional_text.

Working with Layouts, Pages, and Content

Institutions can create user layouts and pushed pages to cater information and services to a widely diverse and dynamic audience.

Using the layout management capabilities outlined here, you can create default user layouts and views based on user data, roles, and other attributes. You can create pushed pages with pre-populated content to audiences of all types. The pages can be modified, for example, a user can delete content from pages, subscribe, and add new content and reposition page elements.

Using the Shared Workspace method, you can create pages and content within views that are shared by select user groups such as students and faculty. Using the Customization method, you can push out modifiable content to users.

Warning! Do not change the name of the Home Site, Luminis Administrators Site, or Guest Site at this time.

Navigation within Luminis Platform

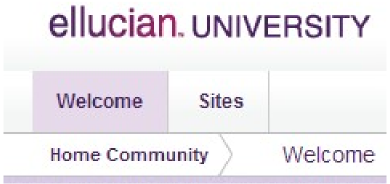
Before understanding how to create new content and present that content to portal users, it is important to first understand the basic navigation of the system from an administrative and user view.

Luminis® Platform ships with a default theme. The theme essentially encompasses the navigation construct, colors, logos, portlet borders and alignment. For those with the skill set and interest, the default Luminis Platform theme can be modified and changed per deployment. The information below relates to the default theme.

Navigation in Luminis Platform is performed mainly through pages set under pages. Pages with content can be added and pushed to users under these pages using the publishing methods outlined below. Pages can be locked down or made modifiable by users. Users can add their own pages to their personal portal areas and populate with content as they see fit. Pages added by users are seen in their view only but can be shared with other users through friendly URLs and **My Public Pages**.

As you navigate between pages you can view the sub-pages. However, the portal content below the pages does not change until you actually select the page. This provides two-tiered navigation allowing users to quickly scroll through their layout until their page decision is explicitly made.

Figure 4: Navigation for Admin and Non-admin Users: Pages



You can set up shared workspaces through the system for like users and user groups (for example, students, faculty, employees, and so on). The Home Community can be thought of as the place to deliver institution controlled pages and content to key audiences. All non-Admin users belong to a shared workspace called Home Community and will see the **Home Community** page. The pages and content within the Home Community (such as, **Welcome** and **Sites** pages in this example) are personalized to the user based on their dynamic group affiliation. Changes to these pages automatically reflect across the user group.

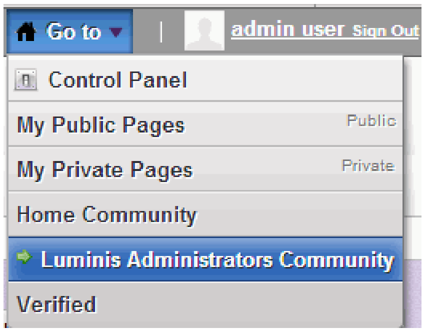
Note: System administrators belong to a comparable shared workspace called Luminis Administrators Community and will see the **Luminis Administrators Community** pages.

Add, Manage, and Go to navigation tools

The navigation menu items throughout the site provide portal users with access to various system functions such as adding applications and portlets to pages, changing the layout template for pages, managing pages, and accessing the **My Account** and **Control Panel** areas.

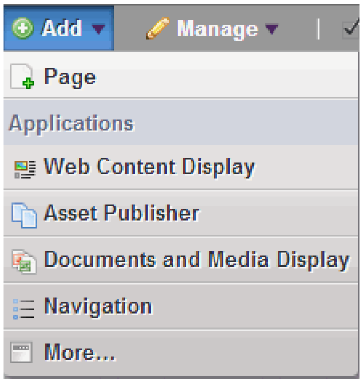
The **Go to** menu provides access to the **Control Panel** and to a user's public and private pages.

Navigation option	Description
Control Panel	Used in the addition to the administrative portlets and tools to maintain and administer various system functions.
My Public Pages	Represents personal user area in which only the user can add and modify content. However, other system users can view the content when the user explicitly shares friendly URLs.
My Private Pages	Represents personal user area in which only the user can add, modify, and view the content.



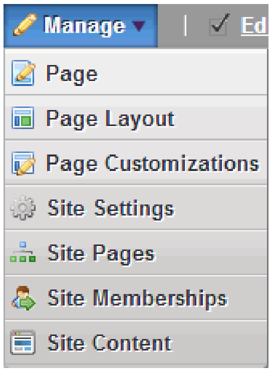
The **Add** menu provides access to page specific functions, such as adding new applications to the selected page, and publishing a mixed group of various kinds of assets such as images, documents, and blogs.

Figure 5: Add menu



The **Manage** menu provides access to additional page-specific functions, such as changing the layout of the selected page, creating new pages, and changing page titles.

Figure 6: Manage Menu



Overview of Creating and Publishing Pages and Content to Users

The Luminis Platform system includes personalization capabilities allowing pages, content, themes, and other system elements to be delivered to specific types of users and groups of users.

There are two primary methods of creating and publishing pages and content to users. First is the method of creating and publishing to shared workspaces. The **Home Site** and **Administrators Site** are shared workspace between like-users. The pages under these parent sites or pages are entirely role-based allowing you to create unique shared workspaces for almost any type of user. For example, Administrators, Students, Faculty and Employees. Changes to shared workspace pages and content reflect across all users of that workspace allowing centralized layout administration for select user groups.

The second method uses a process called Page Customizations. Page customizations allow administrators to create and deliver pages or sections of pages to users that are customizable. For more information about this option, see the documentation in Liferay.com.

Note: The links on the Liferay Web site are subject to change without notice.

The main differences between building pages using the Shared Workspace method and the Customization method are listed below.

Shared Workspace method	Customization method
Pages and content delivered using the Shared Workspace method show up under the **Home Site** or **Administrators Site** page.	Pages and content delivered using the Customizations method show up under the **Home Site** or **Administrators Site**.
Pages delivered using the Shared Workspace method typically are locked down and controlled by the institution. This method provides a dedicated area for institutional driven content. The Shared Workspace method can be used for important content that must be viewed by various user groups and typically must be controlled by the institution. Academic, curriculum, regulatory, and important institution content for example. Modifications to Shared Workspace pages and content reflect across all users in that shared workspace.	Pages delivered using the Customization method can be modified by users. This method allows institutional driven content to be pushed and viewed by users temporarily. Customization content is not locked down and can be removed by the end users after original push.
If you want to publish content locked down and not modifiable by users, use the Shared Workspace method. As noted, the pages and content published using this method are typically locked down and cannot be changed unless you are the administrator or owner of that respective site.	If you want to publish content not permanently controlled by the institution and is modifiable by users, use the Customization method. As noted, pages and content published using Customization are published to user's personal spaces where they can be changed and modified by the user as they see fit.

Publishing methods

There are two primary methods to choose from when delivering content to system users.

- Shared Workspace method allows you to build and deliver new pages with content to any size group of like-users.
- Customization method allows you to deliver modifiable pages to users throughout the site.

  Note: The term *Sites* describes the area of the control panel used in this method. Do not confuse it with the portal's collaboration environment, which is termed *Luminis Platform Sites*.

Building pages and content using the Shared Workspace method

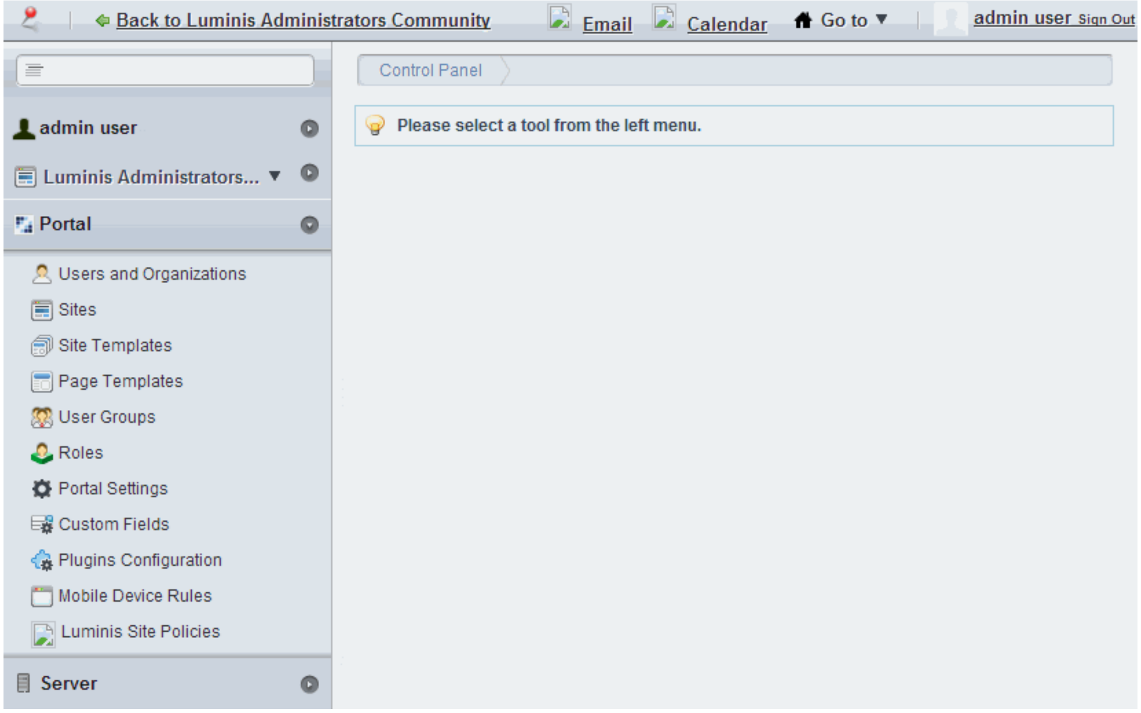
The following examples walk through the process of creating a new page in the system, using both methods, and populating that page with content, then delivering it to all system users or a defined subset. These are simple examples that you can expand upon.

Create a page using a Shared Workspace method

Create and deliver content to users within their shared workspace.

Procedure

1. Log in to Luminis Platform as an administrator.
2. Click **Go to**, then select **Control Panel** from the drop-down list.



Please select a tool from the left menu.

3. Click **Sites** in the menu under the Portal category.

   Default sites listed:

Table 12: Example Luminis Platform architecture

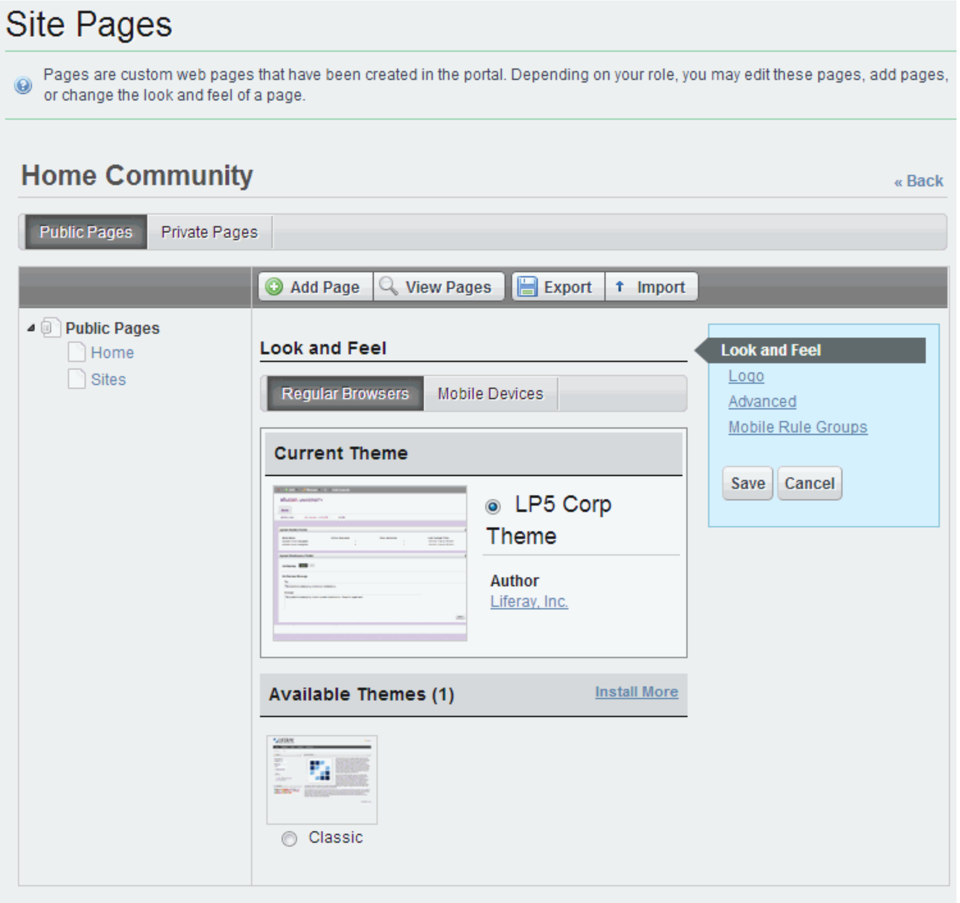
Site	Description
Guest	Default system layout site in support of guest views

Site	Description
Home Community	The start of the general layout site for all system users. You will often use this site as the starting point when creating pages and content and personalizing pages and content to users.
Luminis Administrators Site	Sample layout site for administrators.

4. Click **Actions** and then select **Manage Pages** from the drop-down menu.

   The system displays a Home Site title with two sub-pages, Home and Sites, listed on the left.

   Note: The two sub-pages provide a set of starting pages for the system and can be removed or changed as necessary. You can edit these pages under the user's Home Site directly in the Control Panel area of the system or you can create, modify and deploy your own .lar files for your specific deployment.



Pages are custom web pages that have been created in the portal. Depending on your role, you may edit these pages, add pages, or change the look and feel of a page.

5. To create a new page, click the **Public Pages** link, then click **Add Page**.
6. Enter the required name in the **Name** field.

7. Under Type drop-down box, select **Portlet**.

   When creating pages in the Luminis Platform system, you can select from multiple page types.

   - Portlet
   - Panel
   - Embedded
   - URL
   - Link to Page

8. Click **Add Page**.

   You will see the new page created under the Home Site title.

Related Links

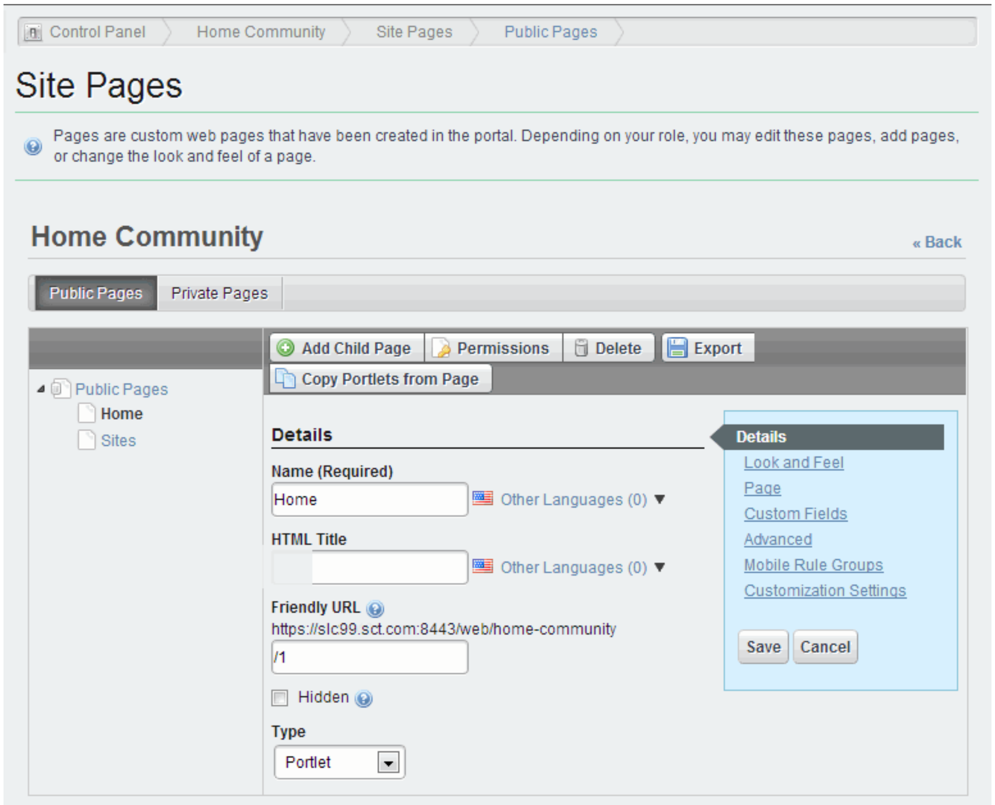
Content development and delivery on page 85

Assign permissions in a Shared Workspace method

Assign permissions for users to access the shared workspace.

Procedure

1. Create a page in a Shared Workspace method.
2. Navigate to **Control Panel** > **Sites** and click **Actions** > **Manage Pages** for the site you want to edit.
3. Click the page you want to edit.



Site Pages

Pages are custom web pages that have been created in the portal. Depending on your role, you may edit these pages, add pages, or change the look and feel of a page.

Home Community

Details

Name (Required)
Home

HTML Title

Friendly URL
https://slc99.sct.com:8443/web/home-community
/1

☐ Hidden

Type
Portlet

4. Click **Permissions**.
5. In the **Permissions** pop-up window, mark the check box to select the type of users who will have access to this page.
   - To make the page available for access by all system users, deselect all the check boxes except the default Owner permissions and the **View** check box for the User role. The User role includes all system users.
   - To make the page available for access only by a specific subset of system users, such as student content, faculty content or executive pages, deselect all the check boxes except the default Owner permissions and the **View** check box on the targeted <*user role*>. For example, to create and deliver a page for students, check the **View** box for the Student role. To create and deliver a page to faculty, check the **View** permission box for the Faculty role. This can be done with any role in the **Control Panel**. (A role in the **Control Panel** is actually a Luminis Dynamic Group).
6. Click **Save** and close the pop-up window.

   Note: For performance reasons, user pages are cached for some configured time (currently set at 15 minutes). Page changes will not display for users that have logged in and the 15 minute page expiration has not occurred. Cache expiration is a performance and tuning parameter that will be optimized. If the portlet access permission does not work, it is due to caching issue and it requires the system to be restarted before the Plugin Configuration settings will take effect.

Related Links

Manage dynamic groups on page 197

Add portlets in a Shared Workspace method

Add portlets to the shared workspace.

Procedure

1. Create a page in a Shared Workspace method.
2. Assign Permissions to a Home Site page.
3. Click the **Public Pages** link, then click **View Pages**.

   A separate browser window appears with a view of a portal page. An Administrator can see all the targeted pages under the Home Site in this view.
4. Select the page you created.
5. After you select the page you want to modify, click **Add** to open the menu and add the portlets or applications to the page as needed.
6. To change the layout of a page, click **Manage**, then **Page Layout**.
7. Select one of the Layout types then click **Save**.

   Note: You can use the drag-and-drop option to position portlets as desired.

Set up site workspace for administrators

This is an example of how an administrator might set up a site workspace. You should customize these steps to fit your institution's needs.

About this task

Procedure

1. Log in to Luminis Platform as an administrator.
2. In the Luminis Platform home page, to add applications to the page, select **Manage** > **Site Pages**.
3. Click **Add page** in the **Public Pages** menu.
4. Click the page link on the **Details** page to view the details for the page.
5. In the **Type** field, select a page type. In this example, we will use the Panel type page.
6. Mark the check boxes next to the applications you want available in the panel.
7. Click **Save**.

Note: The portlet page type presents a blank page that you can populate with applications. The Panel page type represents a dashboard-like page that has a configurable menu on the left side of the page. You can configure all the applications that appear in the menu. You can use the panel menu to switch back and forth between applications interacting with one application at a time.

8. Click **Cancel** to return to the Home page.
9. Select the new page that you created.
10. If you created a Portlet-type page, then in the Luminis Platform home page click **Manage** > **Page Layout**.
11. Select the desired Layout type then click **Save.**
12. In the Luminis Platform home page, click to open the **Add** menu and add the portlets or applications to the page as needed.
13. When you finish adding all portlets, review the page and content.

Customize Luminis Platform

The Luminis® system allows for changes to logos and stylesheets.

Luminis Themes: Customizing Look and Feel

Use Luminis themes to customize the look and feel of your portal.

Luminis Platform 5 uses an underlying portal framework from Liferay that provides a mechanism for developers to use themes to customize the look and feel of the user interface. Multiple themes can be added to the portal for users to choose from.

A theme can control the whole look and feel of the pages generated by Liferay. The portal-side of the page can be completely customized. Even the appearance of the portlets that come with Liferay can be customized using CSS, images, JavaScript, and special templates.

Customization Guidelines

Although the Luminis system allows for easy access to logo and stylesheet changes, ensure that you follow standard design principles.

Example customizations:

- Transparent backgrounds for all images
- Preferred use of .png files

The styles discussed in this chapter are examples that display some of the possibilities within Luminis Platform. There are many other style options you might implement.

Note: The user elements within Luminis Platform are created with HTML, JavaScript and Velocity templates. Creating a custom theme requires some level of skill set in each of these technologies. Though Velocity is part of the skill set, it is recommended that you do not change the Velocity templates.

In addition, as the product grows the style names may change. Most modern browsers support rich browser debugging tools. These tools are highly recommended as part of Web development activities. For example, Firebug is a debugging tool that works with the Firefox browser. The Chrome browser also has developer tools that can be useful. It is best practice for theme developers to use Firebug or developer tools as a tool to determine style names. Using Firebug, right click on the element in question and choose **Inspect Element**. Firebug will take you directly to the relevant area in the HTML code of the element. You can download Firebug at http://getfirebug.com/.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Luminis Platform theme development

Luminis Platform comes with a responsive theme that is based on the Inspinia theme produced by Themeray (www.themeray.com). You can create custom themes for your institution based on the Ellucian theme.

You may have different themes for different users, sites, and departments. The theme uses images, JavaScript, and Velocity templates to control the look and feel of the pages generated by the portal.

Create a custom Luminis Platform theme

You can use Liferay's IDE (Eclipse plug in) with the appropriate Liferay Plugins SDK to create and build your custom themes.

The source code for the default Ellucian Luminis theme is provided to you. Any custom theme for Luminis Platform must begin with the Ellucian theme or many of the user application may cease to function.

Related Links

Create and deploy a theme and theme WAR file

Download and install Liferay IDE and Plugins SDK

The Liferay IDE is an Eclipse plugin that allows for theme and portlet development.

You can download Eclipse from http://eclipse.org/downloads/. After installing Eclipse, you can install the Liferay IDE plugin directly into your Eclipse from the Install New Software wizard, which can be accessed from the Help menu. You can use this URL to install the IDE http://releases.liferay.com/tools/ide/latest/stable.

After installing the Liferay IDE into your Eclipse, you will need to download and set up Liferay's Plugins SDK. A version of the SDK can be downloaded from SourceForge by going to http://sourceforge.net/projects/lportal/files/Liferay%20Portal/. Navigate to the latest 6.2.X GA release and look through the list of files to find "liferay-plugins-sdk-6.2…" and download that file.

For further instructions about installing and configuring Liferay IDE and setting up the Plugins SDK, see https://dev.liferay.com/develop/tutorials/-/knowledge_base/6-2/plugins-sdk.

Create a Liferay Plugin project from the Ellucian default theme

Within the Liferay IDE, create a new Liferay Plugin Project for the custom theme.

In the new project wizard, complete the following steps:

1. Give your project a name.
2. Select **Ant** for the build type.
3. Select your plugins SDK.
4. Select the appropriate Liferay Runtime.

5. Select **Theme** for the plugin type.
6. On the next page select **_styled** for the theme parent.
7. Select **Velocity** for the theme framework.
8. Click **Finish** to create the project.

After creating the theme project, make a backup copy of the following files – they will be needed in a later step:

- `<project root>/docroot/WEB-INF/liferay-look-and-feel.xml`
- `<project root>/docroot/WEB-INF/liferay-plugin-package.properties`

There are a few validators that need to be disabled on the theme project for all the elements of the theme to build cleanly. In the IDE, right click on the project name and select **Properties**, then do the following:

1. Select **Builders** from the left panel.
2. Disable the JavaScript validation.
3. Select **Validation** from the left panel.
4. Enable project specific settings.
5. Disable the Facelet HTML Validation.
6. Disable the HTML Syntax Validation.
7. Click **OK** to save your project changes

The source files for the default Ellucian theme are included with the Luminis installation in `$CP_ROOT/luminis/install/LP5-ellucian-theme-src.zip`. Copy this file to your theme plugin project location (the default location for this is *`<your Liferay SDK folder>`*`/themes/`*`<project name>`*). Unzip the source files into the project directory (overwrite existing files).

Edit the file *`<project root>`*`/docroot/WEB-INF/liferay-look-and-feel.xml` and change the theme id and name attributes of the `<theme>` tag. Use the backup copy of this file we created in an earlier step as reference for the correct value for your theme project.

Edit the file *`<project root>`*`/docroot/WEB-INF/liferay-plugin-package.properties` and change the name properties. Use the backup copy of this file we created in an earlier step as a reference for the correct value for your theme project.

You now have a copy of the default Ellucian theme as your project starting point. You should now deploy and test your theme before you start making customizations. To build and deploy your theme to the Liferay instance set up in your IDE, select **Liferay** > **SDK** > **deploy**. This will build and deploy your theme to the embedded Liferay instance. Or, if you want to deploy the theme to Luminis for testing, you can follow the instruction in Build the WAR file and deploy the new theme on page 168

Note: If you are building your theme from behind a proxy there are a couple of additional steps to get the project to build cleanly. Add a system environment variable called *GRADLE_OPTS* to define your proxy for gradle. (example: `GRADLE_OPTS= "-Dhttp.proxyHost=<your proxy> -Dhttp.proxyPort=<your port> -Dhttps.proxyHost=<your proxy> -Dhttps.proxyPort=<your port>"`. You will also need to edit build-common-plugin.xml and build-common-ivy.xml located in your plugins SDK folder to add appropriate proxy settings (example: `<setproxy proxyhost="your proxy" proxyport="your port"/>`).

Update and customize the theme

There are many different ways in which you can customize the look-and-feel of the Luminis for your users including modifying and adding new color schemes, customizing images, modifying CSS styles and creating customized layouts.

For documentation and tutorials on Liferay theme development, see dev.liferay.com/develop/tutorials/-/knowledge_base/6-2/themes-and-layout-templates.

The Ellucian default theme is a responsive theme built on top of Themeray's Inspinia theme. This theme includes Bootstrap 3 CSS styles, Font Awesome 4.3.0 Icons, and several jQuery plugins, and UI Elements that you can take advantage of within your custom theme. More information about the Inspinia theme can be found at www.themeray.com.

Build the WAR file and deploy the new theme

After making your customizations to the theme in the theme plugin project, build the WAR file and deploy it to the Luminis Platform admin and portal nodes.

Before you begin

When deploying your new theme, confirm that the write permissions are set. Otherwise, the theme will not deploy.

Procedure

1. Copy the WAR file from your Liferay Plugins SDK dist folder to the Liferay hot deploy directory on the Luminis server at: `$CP_ROOT/products/liferay/liferay-admin/deploy` and `$CP_ROOT/products/liferay/liferay-portal/deploy`
2. Monitor the Luminis log files to ensure the theme WAR file is deployed correctly into the Luminis servers.

Apply the Luminis Platform theme

After you deploy the new theme, you can change a site's appearance.

Procedure

1. Log in to Luminis Platform as an administrator.

2. Navigate to the Control Panel.
3. In the Control Panel, click **Sites**
4. From the **Actions** pop-up menu, select **Site Administration** for the desired site.
5. On the site's management page, select either the **Public Pages** tab or the **Private Pages** tab.
6. On the right navigation menu, click **Look and Feel**.

   You see the currently assigned and other available themes. The new theme that was deployed should display in the Available Themes section.
7. From the Available Themes section, select the theme you want to use.
8. Click **Save** to apply the selected theme to the pages.

   The new theme is set and the changes are saved.

Results

The system will apply the default color scheme when you save your theme selection. After saving your theme selection, you can select a different color scheme and then click **Save** again to apply.

Customize logos

Upload a custom logo to customize the logos within the Luminis application and site-specific pages.

Modify a logo for Luminis Platform

Modify a logo for the Luminis system.

Procedure

1. Log in to the Luminis system as an administrator.
2. Navigate to the Control Panel.
3. Click **Portal Settings** in the Portal section of the Control Panel.
4. Click **Display Settings**.
5. Use the provided interface to upload the desired logo image.
6. **Optional:** To prevent the modification of the logo within individual sites, deselect the **Allow site administrators to user their own logo?** check box.
7. Click **Save** to commit the changes to the portal settings.

Modify a logo for a site

Modify the logo for a specific site's pages.

Procedure

1. Log in to the Luminis system as an administrator.
2. Navigate to the Control Panel.
3. Click **Sites** in the Sites section of the Control Panel.
4. Locate the desired site by either using the **Search** box, or navigating through the list of sites.
5. Click **Actions** then **Site Administration** for the specific site.
6. Select either the **Public Pages** tab or the **Private Pages** tab.
7. Select **Logo**.
8. Use the provided interface to upload the desired logo image.
9. Click **Save** to commit the changes for the site pages.

Customize CAS theme

Customize the CAS theme for Luminis Platform.

In the `/$CP_ROOT/products/tomcat/cas-server/webapps/cas-web` you will find a number of directories. During customization, most of these files should remain untouched:

- images
- javascript
- js
- META-INF
- themes
- WEB-INF

In order to customize the CAS login page, it is recommended that you make all modifications in the `Themes` directory:

- `themes/default`

  In the `themes/default` directory, you will find the main stylesheet . Note the reset styles. They affect browser compatibility so you will need to touch those styles as well.

  Note: If you change these files, they may be over-written during a product patch.

- `images`

  The images for logos, footers, and other graphics are located in this directory. The simplest way to customize a theme is to rename your custom image to the appropriate counterpart.

An alternative to editing these files is to create a new theme under the theme directory as described in the "Custom-themed login pages" section in the *Luminis Platform Multi-Entity Processing Implementation Guide*. Then, the CAS services may be edited to use those themes instead of the default theme. The new theme will not be modified by a product patch.

Aside from the images and styles, you may want to add components to the Login and Logout pages and other JSP pages. These pages are found in the following location:

```
/$CP_ROOT/products/tomcat/cas-server/webapps/cas-web/WEB-INF/view/jsp/
default/ui
```

The `casLoginView.jsp` is the main JSP for the login page, and the `casLogoutView.jsp` is for the page you are directed to when the user logs off.

CAS is set up for i18n. All of the locale messages such as the welcome message, failed login, and form validation can be found in the following file:

```
cas-web/WEB-INF/classes/messages.properties
```

After the modifications are complete, back up the files to an external directory. If you do not, later patches will replace these files and you will need to reset previous modifications.

Note: For instructions on how to customize the login/logout pages when using Ellucian Identity Service (EIS) with WSO2, refer to the appropriate EIS product documents or go to www.wso2.com.

Customize non-portlet, non-themed pages

Customize end-user content that is not included within the Liferay portal theme context.

Luminis Platform features display end-user content that is not included within the Liferay portal theme context. These pages come with logos and color formatting from Ellucian that your institution may choose to re-brand to match your theme. This section describes what files to modify to affect these changes.

Pages affected by this formatting are:

- Forced change password on first login
- Forced MyQA (question-answer) password recovery setup
- GCF login error page

To make changes to these pages, you should be familiar with HTML, CSS, and Web page design. The header and footer .css file used by all of these pages may be found here:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/webapps/luminis/css/
common/header_footer.css
```

There is also an RTL (right-to-left) version of this file used by languages requiring RTL, such as Arabic:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/webapps/luminis/css/
common/header_footer_rtl.css
```

Any changes should be made to both versions of the file.

The *logo* class definition specifies the header image. By default, the definition is `/luminis/images/header/ellucian_university_logo_drk.png`. You can substitute this with an image file. The path referred to for the default image is found on the file system under the directory:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/webapps/luminis/images/
header
```

The image used for the header logo should be placed in that directory and the path and file name in the .css file changed to match.

You can change the colors and layout in the .css file. The changes will take effect after you restart the server.

Note: You should save any changes made to `header_footer.css` before you apply a Luminis Platform system patch. If Ellucian changed the default files, the updates will display in the new patch file and overwrite any customizations.

Hide personal user sites

You can disable the option to provide a personal site unique to each user.

A unique aspect of the portal is the option to allow each user to have a unique personal site. Each user can also be the administrator of their own site. These sites are fully customizable by the user. However, the site only allows that user to be a member of their site. The user can create public pages to share with other authenticated users within the system, or private pages where they can create content and access applications for their own use.

If you want to disable the public pages, or the private pages, or both, set the appropriate properties in the `portal-ext.properties` for each node:

- `layout.user.public.layouts.enabled=false`
- `layout.user.private.layouts.enabled=false`

  When these items are set to *false*, the **My Public Pages** and the **My Private Pages** options will not display in the **Go to** menu.

  To allow your users to use private or public pages, set the appropriate properties to *true*.

The `portal-ext.properties` file can be found in these directories:

- Admin Node

  ```
  $CP_ROOT/products/tomcat/tomcat-admin/webapps/ROOT/WEB-INF/classes
  ```
- Portal Node

  ```
  $CP_ROOT/products/tomcat/tomcat-portal/webapps/ROOT/WEB-INF/classes
  ```

After updating these files, restart Luminis Platform to apply the changes.

For more information about the `portal-ext.properties` file, see Liferay configuration management with portal-ext.properties on page 48.

Security

Luminis® Platform offers a robust and flexible security model protecting system areas spanning user authentication, authorization, federation, portlet security, content security, external authentication services, and Enterprise Identity Management (EIM).

Highlights:

- Protected out-of-the-box with the Centralized Authentication Service (CAS) security system
- CAS 3.5.2 used for baseline authentication against default OpenDJ. The CAS server may be configured to authenticate against a different directory other than the default OpenDJ Directory Server shipped with Luminis Platform.
- Supports integration with external CAS servers, version 3.2 or higher
- Supports External Authentication Services (EAS) integration against a school's existing Lightweight Directory Access Protocol (LDAP) version 3.0 compliant campus directory server for either authentication only or for both authentication and data management

  Note: This requires additional provisioning or integration prerequisites that must be taken into consideration. The login IDs from the external authentication server must match those in Luminis Platform, and users must exist in Luminis Platform before they can use the system, even if they could authenticate against the external directory. For more information, refer to the *Luminis Platform Installation Guide*.
- SPRING security architecture to protect URLs and objects throughout the system
- Personalization framework supports the distribution of content and information to dynamic groups of end users, and also supports the delegation of fine grained security operations

Each security check request must pass through a CAS validation filter to ensure the user is authenticated upon completion, a Security Context is created to identify the user to the Security Evaluation Engine. When the call attempts to access protected code, the call is intercepted and handed to the Security Evaluation Engine to check the user against the necessary permissions.

Access to the protected code is allowed or denied for the following three elements:

- The permission associated with the protected code, which is statically set by the developers of Luminis Platform
- The dynamic group membership of the person attempting to access the protected code, which is managed by the Luminis administrator
- The assignments of permissions to dynamic groups, which is managed by the Luminis administrator

Dynamic group membership associations are created using the **Luminis Dynamic Group Manager** portlet. Permissions may be associated with dynamic groups using the **Luminis Permission Management** portlet. A Luminis administrator must understand how to use both of these portlets in order to manage system security and delegate administrative authority.

Liferay security with Luminis

Luminis Platform customizes Liferay by adding, replacing, overriding, and extending functionality within the baseline portal framework in several areas. Security represents one of those extended areas.

Luminis Platform uses Liferay portal as its portal server framework. Part of the Luminis Platform offering includes a set of tools, customizations and content applied to the Liferay portal framework to create a higher education specific portal environment that meets the unique needs of institutions of higher learning.

The Liferay portal has its own security model based on Liferay roles. These roles, however, have been linked by custom code in the Luminis deployment to Luminis dynamic groups, and should not be confused with a role attribute assigned to a user in the **Luminis User Manager**. Users are not assigned roles directly in Liferay; Liferay roles are associated by virtue of their membership in a Luminis dynamic group. This allows flexible assignment and management of Liferay permissions due to the flexibility and power of Luminis dynamic groups.

Liferay role names are the same as the associated Luminis dynamic group name, with the addition of a suffix of the form such as, `-LP-<number>`, where *<number>* is the dynamic group ID in Luminis.

Note: Roles created by Luminis dynamic groups have a description of Mapped Luminis Dynamic Group.

When a Luminis dynamic group is created, an event causes the creation of a role in Liferay. Hence, no action is necessary from the administrator to enable Luminis dynamic groups for Liferay. A default set of dynamic groups (and thus, Liferay roles) are available for use on initial installation.

Permissions in Liferay are assigned using Liferay's management tools. Portlets, layouts, and themes are available to users based on the Liferay role (and hence, the Luminis dynamic group) that have the permission to view, edit, or manage the portlet, layout, or theme.

Enable and Manage Password Security

Luminis Platform provides the ability to perform single sign-on (SSO) to several external applications. To support the SSO operations, the Luminis system requires a secure way to store user credentials for those applications. This method is called Password Management.

You will use the **Single sign-on Configuration** portlet located on the Administration Server to perform Password Management.

When an external system is saved, Luminis Platform enables password management to store the external system's credentials. A message displays to notify the administrator that Password Management System is enabled. For example, the following credentials are stored in the `LP_SECRET_ENTRY` table, also known as the secret store, in the Luminis Platform database:

- Google:

  Google administrator account credentials

- Office 365:
  - Impersonating User
  - Microsoft Admin User

When Password Management is enabled, Luminis securely stores your users' credentials. This makes it important to enforce a policy to periodically change the key in which these credentials are encrypted.

When a configuration is modified, those credentials will be updated in the database. When a configuration is deleted, the stored credentials will be deleted from the `LP_SECRET_ENTRY` table.

Enable password security

When Luminis is installed, password management is disabled. This means by default, Luminis does not store your credentials to sign into external applications.

About this task

To enable single sign-on (SSO) to external applications:

Procedure

1. Access the **Single Sign-on Configuration** portlet.
2. Click **Configure**.
3. Click **Enable** to enable Password Management and SSO for external applications.

Results

After you enable password management, a message informs you a system key is used to manage passwords. Every credential being managed will be encrypted using the key.

Disable password security

After you enable password management, there may come a time when you want to disable this feature.

About this task

To disable single sign-on (SSO) to external applications:

Procedure

1. Access the **Single Sign-on Configuration** portlet.
2. Click **Configure**.
3. Click **Disable** to disable Password Management and SSO for external applications.

Change password management system key

When Password Management is enabled, it is recommended that you periodically change the system key that manages the passwords.

About this task

To change the key:

Procedure

1. Access the **Single Sign-on Configuration** portlet.
2. Click **Configure**.

   A message informs you a system key is being used to manage passwords.
3. Click **Change Key**.

   The system will:

   - Generate a new system key
   - Decrypt credentials with the old system key
   - Encrypt the credentials with the newly generated key

     Changing the system key does not affect user access to external applications. The amount of time it takes for the process to complete varies, depending on how many external user passwords are being managed.

Enable Password Security Policies

Password creation, management, and recovery are critical components for maintaining the security and privacy of your Luminis users. The system offers features that allow you to manage passwords effectively.

These features impose policies that constrain what type of passwords can be created. Policies that impose when a password must be changed, and how a user is locked out after unsuccessfully attempting to login, are configured at the Luminis Platform directory server. Luminis Platform does not enforce password policies that are handled by the directory service.

Luminis Platform will install a Central Authentication Service (CAS) and OpenDJ as the directory service for CAS. Password management is not handled by Luminis Platform if a directory service is external to the Luminis Platform, or the CAS server uses an external authentication source; passwords are maintained by those external services.

Character constraints on passwords

To prevent unauthorized users from guessing passwords, you can configure your system so passwords contain unique formats.

The easiest way to prevent passwords from being guessed is to prevent users from creating passwords that are common enough to be found in dictionaries or other compendiums. Administrators can specify a set of rules to which users must comply when they create their passwords.

The system allows administrators to impose these requirements:

- Must contain a certain number of characters
- Must contain at least one letter of the alphabet
- Must contain at least one numeric
- Must contain at least one character out of a list of special characters

If a password fails to meet all of the constraints established by the administrator, the user is notified the password does not meet the specified criteria.

These password policies are enforced any time a user is created either through the **Luminis User Management** portlet or through a XML import. These constraints are not enforced by the directory service.

Implement password security policies

To address the security measures outlined in "Character constraints on passwords", configurable properties are contained in the system's configuration directory.

Default settings:

```
security.ias.password.must_change_on_first_login=false
security.ias.password.min_length=5
security.ias.password.max_length=20
security.ias.password.require_alpha=true
security.ias.password.require_digit=true
security.ias.password.require_special_char=
```

Use the ConfigurationService JMX mbean to change the properties.

Manage which users may change their password

Through the Luminis **My Account** portlet, users have the option to change their password and their account's timeout limits. You can determine which users may change their own passwords

About this task

This is useful when the CAS server is configured to authenticate against an external source, rather than the Luminis directory. In the scenario where the CAS server is configured to authenticate against an external source, users should not be able to change their own password in Luminis Platform since there should be a separate enterprise facility for managing passwords. For instructions on changing the password or timeout limits, see "Manage user sessions."

If you configure Luminis Platform to allow some users to authenticate against an external directory and deny the option to others (as may be the case when using Prospective Student Portal), then create a dynamic group within the Luminis Platform to define which users do not authenticate against an external source.

To allow only one segment of the user population to set their password:

Procedure

1. Navigate to the **Permission Grant Manager** portlet.
2. Modify the permission assignment under User Management for **Set User Password**. The **Allowed For** should be SELF, and the **Granted To** group should be just those users who authenticate against the Luminis directory server.

   This permission also determines if the password fields are active in the Luminis **My Account** portlet.

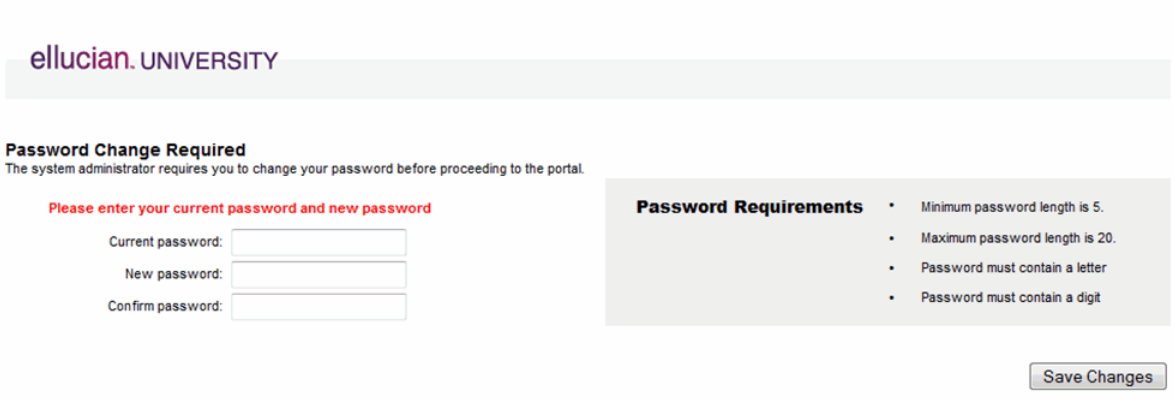
Related Links

Manage user sessions on page 201

Require users to change password on first login

The system administrator can configure Luminis Platform to require users to change their password when they log in for the first time.

You must log in as a system administrator, and set the configuration value for `security.ias.password.must_change_on_first_login` to true. When this value is set, new users are presented with the following page after they enter their initial credentials at the CAS login page:



Password Change Required

The system administrator requires you to change your password before proceeding to the portal.

Please enter your current password and new password

Current password:

New password:

Confirm password:

Password Requirements

- Minimum password length is 5.
- Maximum password length is 20.
- Password must contain a letter
- Password must contain a digit

The user must enter their old password, as well as a new password that conforms to the constraints listed on the right side of the page. After the user successfully changes their password, a link displays to allowing the user to continue to the portal.

Note: Users must have permission to manage their own password before this configuration value is set. If they do not have permission, the users will not be able to access the system.

The language presented on the forced change password page will be the default platform language as specified in the `system-ext.properties` file.

Related Links

Manage which users may change their password on page 177

Synchronize credentials with Banner or Plus

In some instances, you may want to synchronize the password that users supply to access the Luminis system with their Banner® or Plus PIN.

If you elect to synchronize these credentials, you can update user passwords directly from your Banner or Plus system. To synchronize Luminis system credentials with Banner or Plus, you must disable your users' ability to change their passwords through the Luminis system, then add a parameter to the configuration directory that synchronizes passwords.

Encryption is applied to the Banner PIN information that is shared with Luminis Platform to provide new levels of security across the institution. In support of this hash function, Luminis Platform has been modified to accept and process the encrypted PIN information.

Synchronize passwords

To synchronize passwords:

Procedure

1. If you have not already done so, log in to the server as the administrative user.
2. Set this configuration value using the `setString` operation in the JConsole:

   ```
   data.integration.incoming.synchronize.lp.with.ims.credential
   ```

   The default value for this configuration property is false. To enable the password sync, change the value to true as follows:

   ```
   data.integration.incoming.synchronize.lp.with.ims.credential=true
   ```

Results

The Banner or Plus PIN and Luminis Platform passwords are synchronized.

Related Links

Set configuration values on page 30

Set up password recovery

You can provide automatic password recovery using the Question/Answer (Q/A) Password Recovery feature.

If a user sets up Q/A Password Recovery, they can easily recover their password by answering the defined questions. The administration portlet allows you to configure this feature.

Configure password recovery feature - Administrator

When Luminis is installed, Q/A Password Recovery is not enabled or configured.

About this task

An Administrator can enable and configure the Q/A Password Recovery feature.

Procedure

1. Access the **System Question/Answer Password Recovery** portlet found in the Administration category.
2. Click **Configure**.
3. Enter questions for a user to answer for password recovery.

   If your institution supports more than one language, you can set up questions for multiple languages. When configuring this functionality for more than one language, please keep the following in mind:

   - You must enter questions in the default language (English in this example) to enable Q/A Password Recovery
   - If you choose to enter questions for additional languages, you must enter the same number of questions for each language
   - There is no limit to the number of questions you can add

   a) Click **Add**.

   b) Enter a question in the **Questions** field.

   c) If you want to allow a user to edit a question, select the **Editable** check box.

   d) Click **OK**.

   e) Repeat the three above steps to add additional questions.

   You can edit or delete a question by clicking the buttons associated with the question.

   - ✎
   - ☒

   Note: Editing or deleting a question after users have configured their Q/A Password Recovery will require them to re-enter their password recovery upon next login.

f) Enter a value in the **Minimum length of user defined questions** field to require a minimum length on the user-defined questions.

If you allow users to create their own questions, it is recommended you specify a minimum length for user defined questions. A longer length requirement forces the user to define a true question, instead of a shortcut they may forget such as Q1.

g) Enter a value in the **Number of questions user needs** field to specify how many questions the user must answer to properly configure the password recovery. This number must be less than or equal to the number of questions the administrator has entered in the system.

4. Click **Next: Configure Answers** to access the window where you define aspects of the password recovery answers.

Table 13: Configure Answer options

Configuration option	Description
Answers are case sensitive	Check this check box to require users to answer the questions using the exact case they supplied for the answer when they set up their password recovery. Choosing this option provides a higher level of security, but can make it more difficult for users to provide a correct answer.
Allow white space to count in the answer length	Check this check box to specify spaces can count as part of the answer length. For example, if the answer must be five characters in length, then 1 345 will work as an answer. If white space is not allowed, the 1 345 answer would result in an error. If you do not check this box, they would have to enter 12345 for a 5 character length answer.
Disallow duplicate answers	Check this check box to require users to choose a unique answer for every question.
User must answer random questions	Check this check box to require users to answer a random selection of the questions when recovering their password. This options is only enforced if a user has more questions configured than they need to answer or recover their password.
Minimum Answer Length	Enter a number to enforce a minimum length on all answers. A longer-length requirement forces the user to specify a true answer and not something short such as 1 which they may forget later.

Configuration option	Description
Number of questions user must answer	Enter a number of questions a user needs to answer correctly to successfully recover their password.
Number of recovery attempts a user can make	Enter a number of attempts a user can make to answer any one question. When this number is exceeded, the system locks the user out of password recovery.
At which point, the system will:	Specify what action the system will take when a user is locked out: • **Lock out QA for the allotted time and specify Hours** disables the password recovery for the number of hours indicated. During this time, password recovery is disabled unless the user successfully logs in. • **Lock out QA until the user logs in** locks out the user until the user successfully logs in.

5. Click **Next: Configure Post-Recovery.**

   a) Specify what the system will do when the user successfully answers the recovery questions:

   - **Force user to change password** displays the user's password, then when the user successfully logs in, they are required to change the password before continuing to the landing page.
   - **Display password to user** displays the user's password so they can use it to login.

6. Click **Next: Configure Override Group**.

   Specify certain groups of users that would not be required to set up password recovery.

   a) From the **Available Groups** list, select a group that you want to assign the password recovery override.

   b) Click the arrow to move the select group to the **Selected Groups** list.

   Members of any of the selected groups will not be required to set up their password recovery, even if the system is configured that way.

7. Click **Next: Configure Effective Date**.

   a) Check the **Enable Q/A** check box to enable password recovery.

   b) Check the **Force Q/A setup on the date given below** check box and select a date and time to specify a date by which users are required to set up Q/A Password Recovery.

   If this is enabled, users in the override groups are not forced to set up questions and answers for password recovery.

8. Click **OK** to save all Q/A Password Recovery settings.

Setup Q/A Password Recovery - User

After the Q/A Password Recovery feature is configured and enabled by the System Administrator, users can go into their account management and set up their personal Q/A Password Recovery.

About this task

Procedure

1. Locate the **Luminis My Account** portlet.
2. Click **My Account**.
3. Click the **Change password recovery answers** link to set up the QA/password recovery answers.
4. On the **Secret Questions and Answers Setup** page, enter your **Login Password**, and a question and corresponding answer in the indicated fields.
5. Click **Submit Setup**.

Recover a password

If you are logging in to the system and do not remember your password, you can recover your password.

Procedure

1. Click **Forgot password?** on the login page.
2. Enter your **User Name**.
3. Click **Submit**.
4. Enter **Answers** to the questions.

   Correctly answering the indicated number of questions will successfully recover your password.
5. Click **Submit Answers**.
6. Click **Login**.

   If the system is configured to force you to reset your password after password recovery, you will be prompted to do so.

   a) Enter the new password in the **Enter new password** and **Verify new password** fields.

   b) Click **Change Password**.

Results

You successfully recovered your password.

Assign access rights for operations

The Luminis Platform permission grant manager is used to assign access rights for operations by users to applications in the Luminis Platform system.

For some applications these rights are fine grained; others comprise the basic CRUD (Create, Read, Update, and Delete) operations that can be performed on that application data.

Use the permission grant manager whenever a particular group of users should or should not be allowed to perform some operation in the Luminis Platform system, which is secured using the permission grant manager. In general, the users of the permission grant manager application will be administrative users. For this reason, on an initial install, bootstrap data is loaded, which grants access to the Permission Grant Manager operations to the bootstrap Administrators dynamic user group.

Note: If the portlet access permission does not work, it is due to a caching issue and it requires that you restart the system before the Plugin Configuration settings will take effect.

Permission grant management prerequisites

Before assigning permission grants to a dynamic user group, the user group must be defined in the group management application.

These user groups serve to define the group of users that are being granted the permission and sometimes to define a group of context objects for the permission. There are two built-in special user groups that can always be used in the permission grant manager and do not need to be predefined:

- SELF
- ALL

Since permission grants control who is allowed to carry out operations in the system, the user should ensure they are aware of the impact of their changes before they add or remove any permission grants in the permission grant manager. For example, there are currently no checks made to prevent a user from removing access to the permission grant manager itself. If all grants to the permission grant manager are removed or if there are no members of the associated dynamic user groups, then the permission grant manager will become unusable. Direct database editing or a database restore from database backup may then be required to recover from this scenario.

General permission grant manager operation

The Luminis Platform system uses a domain object security model based on the dynamic group functionality provided by the platform. Each permission grant definition in the system is made of at most three pieces.

Table 14: Permission Grant definition components

Column	Description
Permission	The name of the permission being granted.
Allowed For	The group of context values associated with the permission (possibly null).
Granted To	The dynamic user group to which the permission is granted.

In Luminis Platform, system permission grants must be explicitly granted to a user group. The system does not support deny semantics as all permissions are denied implicitly by default. To deny a particular user the ability to perform an operation, ensure they are not a member of any dynamic user group that is granted that permission. No explicit permission hierarchy is supported.

These simplifications avoid the necessity of priority rules, hierarchy management, and the associated complexities. It is also believed that the flexibility of the dynamic group definitions make this type of functionality unnecessary.

Set Internet Explorer browser settings

If you are using an Internet Explorer browser window, you must configure the browser settings to honor the permissions you assign with the **Permission Grant Manager**. To configure the browser settings:

Procedure

1. Open a browser window and click **Tools** in the browser menu.
2. In the drop-down menu, click **Internet Options**.
3. In the **General** tab, locate the Browsing history section and click **Settings**.
4. In the Temporary Internet Files section, mark the radio button next to **Every time I visit the webpage**, and click **OK**.
5. Click **OK** to exit the **Internet Options** window.

Add new permission grant

To add a new permission grant, select **New** on the lower-right corner of the window. A new empty line is inserted in the table.

You may select each field in the table:

- The desired permission to assign
- A context for that permission (if any)
- The target Dynamic Group that will receive this permission

Note: If a particular permission does not allow a context, it will not be available for selection in the **Allowed For** column.

When you have selected the values for the fields of the grant, click **Save** to store the grant in the database.

Edit existing grant

To edit an existing permission, select the line with the pointer.

When you double-click the field you want to edit, a drop-down selection box will appear, from which you can select a new entry. Once you are satisfied with your edits, click **Save** to store the edited permission grant. If during the editing process you decide to go back to the original value of the grant, click **Reset**.

Delete grant

To delete a permission grant, highlight the grant with the cursor and then click **Delete**.

When prompted, confirm you want to delete the grant.

Filter displayed grants

To filter a large list of grants, navigate to the filter window in the upper-right corner of the **Permission Grant Manager** window.

First, select the column on which to filter - **Permission**, **Allowed For**, or **Granted-to** - from the drop-down list, which is next to the text entry box. Then, enter the first letters of the permission, context, or granted-to items you would like to see. The entries are dynamically filtered to display only the entries beginning with the text entered in the filter box.

Permission grant manager categories

Below is a detailed description of each permission defined in each category along with any additional information relevant to management of permissions for the corresponding category.

Announcements

Assign announcements permissions in the **Luminis Announcements** portlet.

Category service

There is one permission available for controlling access to the Luminis Site Categories, Delete Category. Assigning this permission allows the recipient to delete categories within the Luminis Site Categories.

Configuration management

There are three permissions associated with Configuration Management. These permissions apply to the applications using the configuration Web service, which includes the administrator **Session Management** portlet.

Permission	Description
Administer Config	Includes both read and write permissions.
Write Config	Required to write values.
Read Config	Required to view configuration values which are available in that portlet (user timeout, and so on).

Group management

There is a single permission defined under Group Management, which is the Administer Group. A member of a group that has this permission may do all functions in the **Luminis Group Manager** portlet.

Institution management

Table 15: Institution management category permissions

Permission	Granted To	Description
Administer Institutions	Administrator	Overall permission to administer institutions. This

Permission	Granted To	Description
	Any User	should only be granted to Administrators.
Create Institutions	Any User	Permission to create institutions.
Update Institutions	Any User	Permission to update institutions.
Delete Institutions	Any User	Permission to delete institutions.

Integration

The permission Integration Administration allows a member of the dynamic group with this permission to do all functions in the **Luminis External Services Configuration** portlet. The Integration security simply enforces the Administrator right at the service for Create, Update, and Delete. Authenticated users have read access to their external data.

Permission Grant management

The permission Administer Permissions allows a member of the dynamic group with this permission to perform all functions in the **Permission Grant Manager** portlet.

Note: Special care must be taken when you remove this permission. If no one is left with permission to administer permissions, it will not be possible to add it back without directly modifying the database. For any help, contact the Ellucian Support Center.

Role management

Permissions to configure for access to the Role management categories.

Table 16: Role Management category permissions

Permission	Description	Allowed For	Granted To
Administer Role	Overall permission to administer roles. This should only be granted to Administrators.	All Users, Self, Administrators	Administrator
Create Role	Permission to create roles. Can be granted to any user.	All Users, Self, Administrators	Any User

Permission	Description	Allowed For	Granted To
Delete Role	Permission to delete roles. Can be granted to any user.	All Users, Self, Administrators	Any User
Read Role	Permission to read any role. Can be granted to any user.	All Users, Self, Administrators	Any User
Read Role Permission	Permission to read role permission grants. Can be granted to any user.	All Users, Self, Administrators	Any User
Update Role	Permission to update role. Can be granted to any user.	All Users, Self, Administrators	Any User

Warning! Do not modify the Allowed For and the Granted To default settings in the **Luminis Permission Grant Manager** portlet.

User management

The User Management category contains a number of roles to fine-grain the operations that a delegated administrator can take with users in the **User Management** portlet.

Warning! Granting the Set User Roles permission will allow the setting of any user roles. This could result in unintentional allowance or removal of user access to specific features. For example, a student user might accidentally be assigned the Administrator role.

Table 17: User management category permissions

Permission	Description	Allowed For	Granted To
Administer User	Overall permission to administer users. Should only be given to Administrators.	All Users, Self	Administrator
Create User	Permission to create users. Can be granted to any user.	All Users, Self	Any User
Delete User	Permission to delete users. Can be granted to any user.	All Users, Self	Any User
Read User	Permission to read users. Can be granted to any user.	All Users, Self	Any User

Permission	Description	Allowed For	Granted To
Read User Permission	Permission to read user grants. Can be granted to any user.	All Users, Self	Any User
Read User Protected Data	Permission to read all user fields without granting read permission on them individually.	All Users, Self	Any User
Set Account Status	Permission to change or update the user's account status. Can be granted to any user.	All Users, Self	Any User
Set Display Name	Permission to add or update the user's display name. Can be granted to any user.	All Users, Self	Any User
Set Email Address	Permission to change or update the users email id. Can be granted to any user.	All Users, Self	Any User
Set First Name	Permission to change or update the users first name. Can be granted to any user.	All Users, Self	Any User
Set Last Name	Permission to change or update the user's last name. Can be granted to any user.	All Users, Self	Any User
Set Login Id	Permission to change or update the users login id. Can be granted to any user.	All Users, Self	Any User
Set Session Timeout	Permission to change or update the users session timeout. Can be granted to any user.	All Users, Self	Any User
Set User Majors	Permission to change or update majors for the user. Can be granted to any user.	All Users, Self	Any User
Set User Password	Permission to change or update the user's	All Users, Self	Any User

Permission	Description	Allowed For	Granted To
	password. Can be granted to any user.		
Set User Roles	Permission to change or update roles for the user. Can be granted to any user.	All Users, Self	Any User
Update User	Permission to update user. Can be granted to any user.	All Users, Self	Any User

Warning! Do not modify the Allowed For and the Granted To default settings in the **Luminis Permission Grant Manager** portlet.

Related Links

Assign access rights for operations on page 184
Admin server access group on page 25

Site management

Permissions to configure for access to the Site management categories.

The Site category enables the restriction of functions in many site-related portlets both in the admin and portal servers.

Table 18: Site Management category permissions

Permission	Description	Allowed For	Granted To
Delete Site	The administrator is the only person who has permission to delete the site.	-	Administrator
Save Site Applications	• Only the site owner has permission to save applications to the site. • Only an administrator has permission to save applications to the site.	Site Site	Site Owners Administrator
Save Admin Site Applications	Only the administrator has permission to save	-	Administrator

Permission	Description	Allowed For	Granted To
	applications for the entire product.		
Save Site Policy	Only the administrator has permission to change the site policy.	-	Administrator
Update Site	Only the administrator has permission to update sites.	-	Administrator
Delete Site Message	Only the owner or administrator has permission to delete the site welcome and guest message.	- Site - Site	- Site Owners - Administrator
Update Site Message Status	Only the site owner or administrator has permission to change the status of welcome/ guest messages.	- Site - Site	- Site Owners - Administrator

Warning! Do not modify the Allowed For and the Granted To default settings in the **Luminis Permission Grant Manager** portlet.

Targeted Content

Permissions that control access to the Targeted Content categories.

Note: To give users access to the Targeted Content categories, you must also grant users the Edit Block or Manage Block permission.

Table 19: Targeted Content permissions

Permission	Description
Create block	Permission to create blocks. Grant this permission to enable and display the add block icon. ⊕ After a new block is created, the copy icon and display block list icons appear. ⊞ ▤
Create category	Permission to create categories. Grant this permission to enable and display the create category icon on the block category header.
Delete block	Permission to delete blocks in the targeted content block list. Grant this permission to

Permission	Description
	enable and display the delete block icon on the targeted content blocks header.✖ The display block list icon on the content management header is also enabled.
Delete category	Permission to delete categories. Grant this permission to enable and display the delete category icon on the block category header.⊖
Edit block	Permission to edit blocks in the targeted content block list. Grant this permission to enable the view targeted content block list icon. ▤
Edit category	Permission to edit categories. Grant this permission to enable and display the edit category icon in the block category header.✎
Manage block	Permission to edit, delete, and set the display of the blocks. All action icons are displayed. Similar to Edit block, but includes the Set display block permission.
Manage category	Permission to create, edit, and delete categories.
Set block admin	Permission to set block administrators. Grant this permission to display the available groups in the block administrator list. The groups in the list are determined by the permission’s allowed for value. To access the block list, you must also grant users the Create, Edit, or Manage Block permissions.
Set display block	Permission to select blocks for display. The targeted content portlet must be set to configure for the group you want to grant the permission to. Grant this permission to allow the user to select different blocks to display. The blocks available for selection are determined by the permission allowed for value.
Set section target audience	Permission to set the target audience for a block section. Grant this permission to display the available groups in the target audience list. The groups in the list are determined by the permission allowed for value.

Permission	Description
	To access the block list, you must also grant users the Create, Edit, or Manage Block permissions.

Note: To allow access to the icons to view and create blocks and the link to select a display block, users who are granted Targeted Content permissions must configure permissions on the individual portlet.

Table 20: Targeted Content Groups

Permission	Description
TC BLOCK CREATOR	Default group for users who have created targeted content blocks.
TC BLOCK ADMIN	Default group for users who have been selected as block administrators.
ALL TC BLOCKS	Default group that includes all targeted content blocks.
TC BLOCKS TARGETED TO THEM	Default group for users that have content targeted to them.

Related Links

Schedule a targeted announcement on page 140
Targeted content permissions on page 298
Targeted Content permissions practical example on page 298

Luminis Dynamic Groups

Dynamic groups are used in a number of capacities in Luminis Platform, including fine-grained permission delegation, targeting of announcements and content, and distributing pages to targeted user sets.

A dynamic group is a collection of objects that become a member of the group by virtue of a set of attributes of those objects. Most commonly, dynamic groups consist of a set of users, but other group types also exist for application-specific purposes. In this section, we primarily discuss the user-based dynamic groups, though the same principles and actions apply to other group types as well.

Dynamic groups are commonly created to target an announcement at a certain set of users. For example, create a dynamic group of users in the **Luminis Group Manager**. To send an announcement to the group, use the **Luminis Announcements** portlet to create and schedule the announcement; however, you must select from a pre-existing dynamic group to whom you wish to send the announcement.

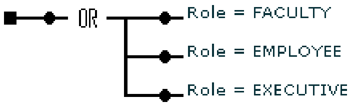
A group is dynamic because membership is continually re-evaluated based on the user's current set of attributes. You do not need to edit the membership of a group for a user to become a part of it. If they gain an attribute that makes them a member of the group, they will be considered a member the next time an application needs to decide if they are a member. Similarly, if they lose an attribute at any point, they will no longer be a member of the group.

Each dynamic group is defined by a Boolean expression that contains attributes, other dynamic groups, and operators on those attributes and dynamic groups. Each expression can be arbitrarily complex, allowing grouping of users in a wide variety of ways, either as narrow or broad as per the administrator's decision.

For example, to send an announcement to all users who have a role, such as Faculty, Employee, or Executive. The boolean expression for this would be:

```
 TargetGroup = Role = FACULTY OR Role = EMPLOYEE OR Role = EXECUTIVE
```

Figure 7: Boolean Expression in Luminis Group Manager



Group operators

Attributes may be combined using the Boolean operators, such as *And*, *Or*, and *Not*.

And and *Or* may have an arbitrary number of operands associated with them. *Not* only applies to a single attribute. An administrator should be familiar with Boolean logic so the groups formed contain the expected membership.

Attribute operators

Each attribute added to the group expression may have an operator, including equals (=), equals(ignore case), contains, contains(ignore case), endsWith, endsWith(ignore case), exists, matches, startsWith, and startsWith(ignore case).

Operators are as follows:

- *Equals (=)*. Must be an exact match with the attribute string
- *Equals ignore case (=(ignore case))*. Must be an exact match, but upper and lower case is ignored in making the comparison
- *Contains*. The given string must be contained somewhere in the actual attribute
- *Contains(ignore case)*. The given string must be contained somewhere in the attribute, but case is ignored in making the comparison
- *endsWith*. The attribute must end with the given string
- *endsWith (ignore case)*. The attribute must end with the given string, but case is ignored in making the comparison

- *exists*. The given attribute must contain a value
- *matches*. This operator takes a regular expression string and determines if the attribute matches the regular expression. The regular expression may be built according to regular expression rules using characters, parentheses, pipes ("|"), zero-or-more ("*"), one-or-more ("+"), and so on.
- *startsWith*. The attribute must start with the given string
- *startsWith(ignore case)*. The attribute must start with the given string, but case is ignored in making the comparison

Available user attributes

The attributes available for users when you build dynamic group expressions.

Depending on the type of attribute, the operators may be limited to a subset of the available operators. In some cases, a list of available values are presented when selecting a particular attribute and operator; in other cases, the administrator must enter the value to be checked by hand.

Attribute	Operators	Notes
Login Id	All	
Email	All	
Site Membership	=, contains, endsWith, exists, matches, startsWith	= operator presents a list of available sites. Evaluation is based on whether a user is a member of the given Luminis Site
Majors	=	
Role	All	= operator presents a list of available roles
Full Name	All	
Last Name	All	
First Name	All	
Date of Birth	=, <, <=, >, >=	The date of birth must be entered in the following format, *YYYY-MM-DD*. For example, 2011-05-05. The operators indicate: • = translates to ON • < translates to BEFORE • <= translates to ON or BEFORE • > translates to AFTER

Attribute	Operators	Notes
		- >= translates to ON or AFTER
Home Institution	All	The user's primary institution within a multi-campus system. For example, University of California, Berkley. The operator '= presents a list of available institutions

Manage dynamic groups

To add the **Luminis Group Manager** portlet to the layout, drag and drop the **Luminis Group Manager** from the **Add** menu's Luminis Admin sub-folder into your layout.

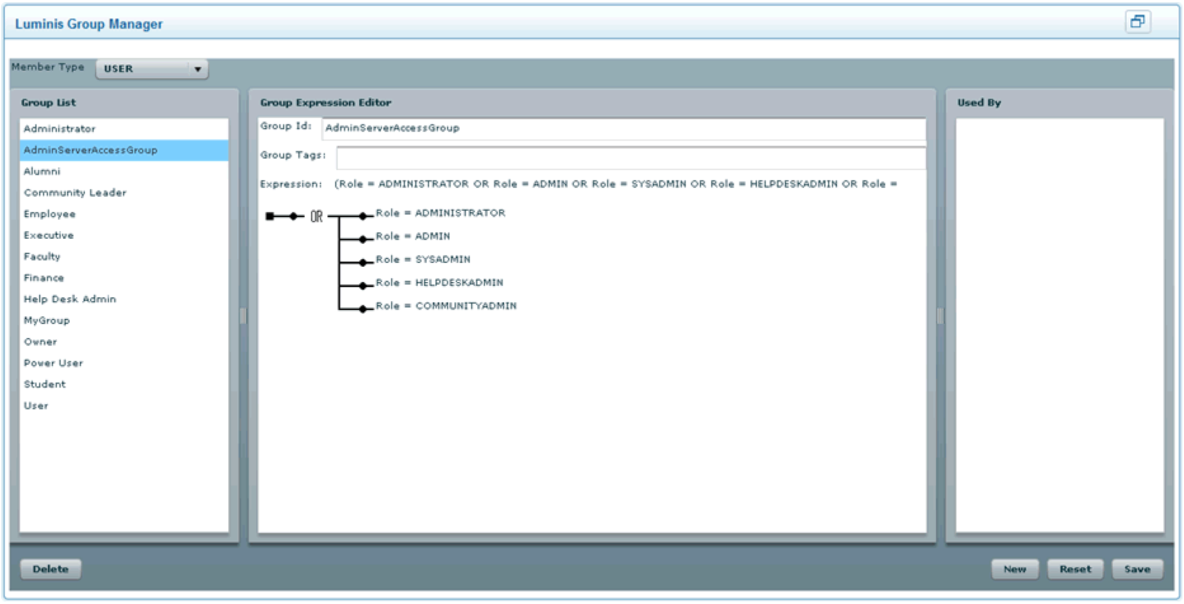
Group manager window

The Luminis Group Manager enables administrators to track changes made to a dynamic group and evaluate other dynamic groups that reference the group.

The Luminis Group manager consists of three primary window panes:

- a list of existing dynamic groups
- the view or edit area for the existing dynamic group you selected
- a list of dynamic groups that reference the current dynamic group

Note: You cannot delete a group that is referenced by another group. Performing such an action would break the evaluation of the referencing group, so the **Delete** button is disabled.



Member Type: USER

Group List: Administrator, AdminServerAccessGroup, Alumni, Community Leader, Employee, Executive, Faculty, Finance, Help Desk Admin, MyGroup, Owner, Power User, Student, User

Group Id: AdminServerAccessGroup

Group Tags:

Expression: (Role = ADMINISTRATOR OR Role = ADMIN OR Role = SYSADMIN OR Role = HELPDESKADMIN OR Role =

```
OR ─┬─ Role = ADMINISTRATOR
    ├─ Role = ADMIN
    ├─ Role = SYSADMIN
    ├─ Role = HELPDESKADMIN
    └─ Role = COMMUNITYADMIN
```

The group types currently available in the drop-down menu are User and User Group. The User type group evaluates the membership of users in the listed dynamic. The User Group type of group evaluates the membership of groups of dynamic groups of type user, or meta groups. In other words, when a dynamic user group definition is used as a group itself, it is a group of type User Group.

The function buttons **Delete**, **Create**, **Reset**, and **Save** are only active when their operation is allowed.

Create a new group

You can create a new user group in the Luminis Group Manager.

Procedure

1. Click **New**.
2. Enter a unique name in the **Group ID** field.

   To add to the group expression, click the empty node.

   A pop-up will display the option to add an operator , to insert an attribute, or to insert another dynamic group.
3. Select an operator to add nodes to the tree to perform the given operation.
   - And
   - Or
   - Not

   a) Select **Attr** to bring up an additional menu (the Expression Selector) to select the User attribute to use in the expression, such as LoginId, Email, and so on.

   b) When you select a specific attribute, a list of available attribute operators displays in the Expression Selector.
   c) When you select an operator, either a list of available attribute values displays, or the user must type in the string they wish to operate.
4. After you select or enter a value, click **Ok** to set the expression into the previously selected node in the **Group Expression Editor**.
5. After you add an expression to a node, the options on that node change to Insert And, Insert Not, Add Operand, and Delete Subtree. Use these options to edit and shape the expression as desired.
6. Continue to add or edit nodes to build the desired Boolean expression.
7. Click **Save** to store the dynamic group.

Related Links

Create User Group groups and other group types on page 200

Edit existing group

You can edit an existing user group in the **Luminis Group Manager**.

Procedure

1. In the **Group List** window, highlight the dynamic group you wish to change.
2. Edit the group expression similar to when you create a new group.
3. Once you are finished editing, click **Save**.

Related Links

Create User Group groups and other group types on page 200

Delete dynamic group

You can delete a user group in the **Luminis Group Manager**.

Procedure

1. Highlight the group in the **Group List** window, and then click **Delete**.
2. A dialog box will prompt for confirmation before the group is deleted.

Results

Warning! Care should be taken when deleting a dynamic group because it may be used in another application, such as Announcements or the Permission Manager. If the group is used in the definition of another dynamic group, then the **Delete** button is disabled. This is apparent by the existence of a group name in the Used By window of the group editor.

Create User Group groups and other group types

The User Group group type is a meta group, or a case where dynamic groups are being used as a dynamic group rather than determining if the user is a group member.

In other words, there are applications that wish to determine if a given dynamic group is a member of another dynamic group definition, in this case, groups made up of previously defined User groups.

Related Links

Edit existing group on page 199

Create a new group on page 198

Liferay roles and Luminis dynamic groups

Roles are used in Liferay to give permissions within the Liferay portal.

For example, portlets may be made available only to certain roles, or pages may be owned or edited by users with particular roles. In the Luminis Platform deployment of Liferay, the Liferay roles are tied explicitly to Luminis Dynamic Groups. A new group created in Luminis is propagated to Liferay, but the role name is appended with a suffix of *-LP-XXX*, where the *XXX* is the Luminis group ID. This makes it clear that these roles are Luminis Dynamic Groups.

Note: Pre-existing reserved Liferay role names, such as Administrator, do not have a *-LP-XXX* suffix, but they are still mapped to Luminis Dynamic Group with the matching name. Thus, assigning the Administrator role in Liferay is accomplished by a user with the appropriate attributes to make them a member of the Luminis Administrator dynamic group.

The default Liferay roles that do not have the Luminis *-LP-XXX* dynamic group extension include:

- Administrator
- Site Administrator
- Site Member
- Site Owner
- Guest
- Organization Member
- Organization Owner
- Owner
- Power User
- User

Permissions in Liferay may be delegated or assigned using Luminis Dynamic Groups within the Liferay context - they are simply called "roles" in the Liferay controls. Pages may be targeted, and permissions granted based on Luminis dynamic group membership, rather than a static role-based assignment. When a user accesses the system, Liferay determines if the user has that role by calling into the Luminis Dynamic Group evaluator. It does not use the Liferay role evaluation, and a

Luminis administrator should not use the Liferay control panel to assign roles to users, since those assignments are ignored.

Manage user sessions

Managing user sessions is a component of managing system resources. As long as a user is logged in, the session uses system resources. The resources are released for other users when a user logs out. If a user leaves a session open without logging out, they become unused resources.

You can configure user sessions to implement a timeout feature that automatically closes a session after it is idle for a specified amount of time. After a user is logged out, the system regains the session resources.

You can configure the timeout settings for all users using the **Session Management Console**. When defining the Session Management settings, you can allow users to set their own timeout setting in their **Luminis My Account** portlet. An individual user timeout is only used if the correct setting is checked in Session Management to allow users to set an individual timeout.

You can set a time for the system to display a timeout warning to users. This displays a warning message a specified number of minutes before the session times out. This gives the user an opportunity to perform an action that will keep the session active for an additional timeout period. You can also set an individual user's timeout in the **Luminis User Management** portlet.

Finally, you can define the URL where users will be redirected when they log out of a session.

Configure user session management

Configure the management of user sessions including session timeout period, timeout warning time period, and a logout landing page.

Procedure

1. Access the **Session Management Console** portlet located in the **Luminis Administrators Site**.

   If the portlet is not displayed in the **Luminis Administrators Site**, click **Add** > **Luminis Admin** to expand the folder. Then click **Session Management Console** > **Add** > .
2. From the **Add** menu, click **Luminis Admin** to expand the folder.
3. Click the **Add** link associated with the **Session Management Console** item, and enter appropriate information in the fields provided.

Field	Description
Default User Timeout	Set to the number of minutes a session can remain idle before the session times out. If a user has not defined a personal timeout, the global Default User Timeout is used.

Field	Description
Maximum User Timeout	Set the maximum number of minutes a user can set for the timeout.
Timeout Warning	Specify how many minutes before a session timeout occurs to display the warning message.
Logout Landing Page	Specify a URL that defines the Web page where the user will be redirected after they log out. By default, when a user logs out of the system, they are redirected to the Luminis portal login page. If after changing the logout landing page you wish to restore the default value set during system installation, delete the URL in the text box and click **Save Changes**.

4. Click **Save Changes** to apply the values you defined for Session Management.

Results

Changes only apply after the cache timeout of the configuration sub-system (30 minutes), or after a system restart.

Allow users to set their own timeout

Users may be allowed to set their own session timeout in the **MyAccount** portlet by setting the appropriate permission in the **Permission Grant Manager** portlet.

In the **Permission Grant Manager**, select the **User Management** category.

- Add a new permission of SET SESSION TIMEOUT with the **Allowed For** = SELF and **Granted To** = ALL USERS.
- To disallow setting their own timeout, remove that permission.
- To allow a sub-set of users to set their own timeout, modify the permission above as follows: leave the **Allowed For** to SELF, but change the **Granted To** to the dynamic group containing the users which should be allowed to set their own timeout.

Delegate User Session Management Settings

Luminis Platform allows for the Administrator to delegate which user(s) are capable of configuring User Session Management settings. These settings are modifiable using the **Session Management Console**.

If you wish a non-administrator user to have access to the **Session Management Console**, you must grant the user access to the following components:

- Administrator Portal
- Session Management Console portlet
- Configuration Web Service

Included in the example below are the steps needed to grant a non-administrator user full access to the **Session Management Console**.

For example, a Luminis role is used to distinguish user permissions. Although a Luminis role is used here, it is important to remember that any dynamic group could be used to assign a permission group to a set of users. The example below demonstrates one specific way to assign permissions to users.

Example: Create a role and group

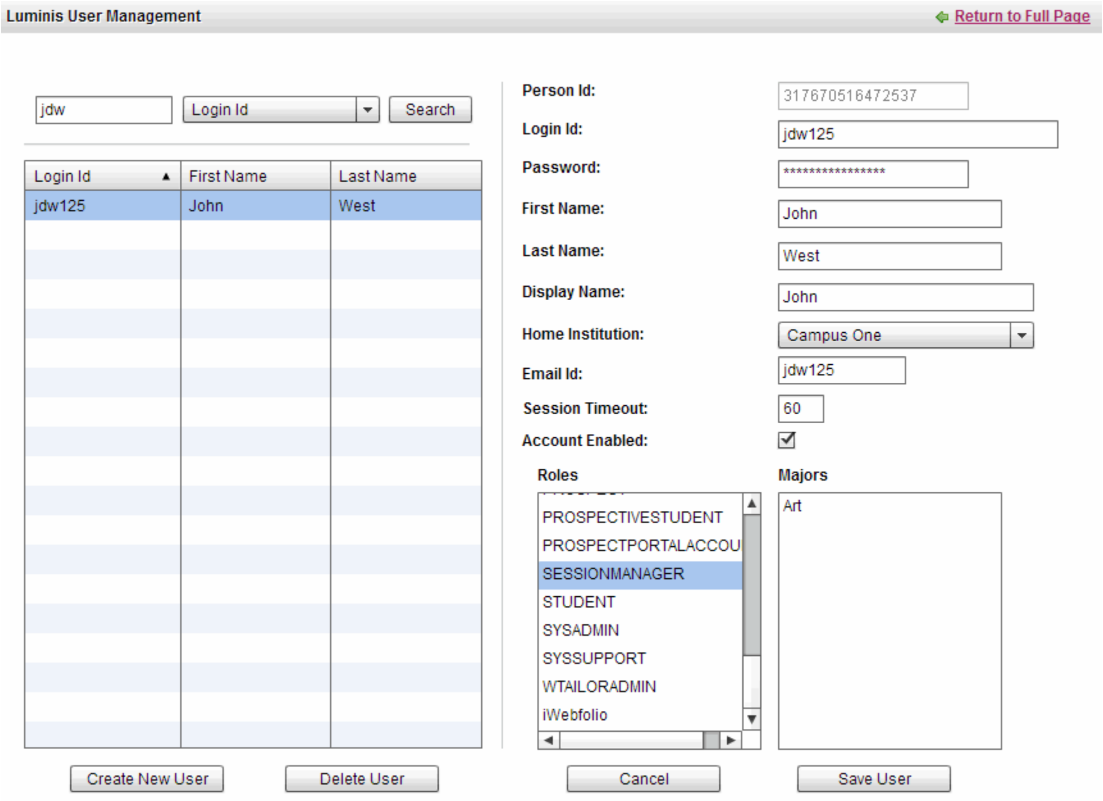
For this example you are going to need to create both a Luminis role and a Luminis dynamic group. The Luminis role will become the attribute which ties your users to the dynamic group.

About this task

To create a new Role and Group:

Procedure

1. Using the **Luminis Role Management** portlet, create a new role with appropriate description (for example, SESSIONMANAGER).
2. Open the **Luminis User Management** portlet and add that role to the desired users.



Search: jdw — Login Id

Login Id ▲	First Name	Last Name
jdw125	John	West

Person Id: 317670516472537

Login Id: jdw125

Password: ****************

First Name: John

Last Name: West

Display Name: John

Home Institution: Campus One

Email Id: jdw125

Session Timeout: 60

Account Enabled: ☑

Roles

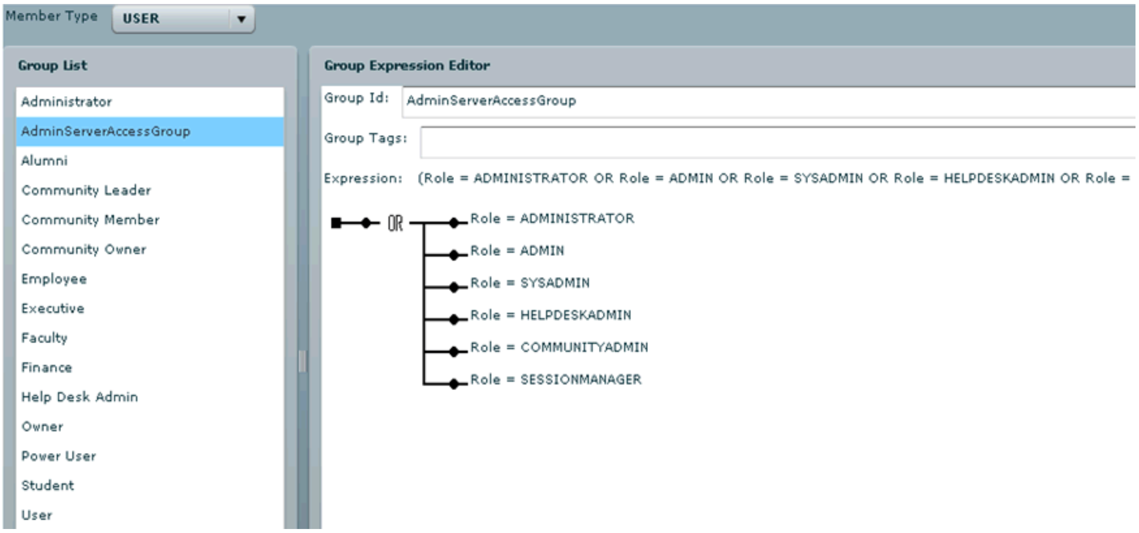
- PROSPECTIVESTUDENT
- PROSPECTPORTALACCOU
- SESSIONMANAGER
- STUDENT
- SYSADMIN
- SYSSUPPORT
- WTAILORADMIN
- iWebfolio

Majors

- Art

3. Create a Luminis dynamic group that includes the SESSIONMANAGER role.
4. Open the **Luminis Group Manager** portlet and create a new group under the User member type. The group should be created with an appropriate ID (for example, SessionManager). As an attribute to the group, you will want to add the SESSIONMANAGER role.
5. Once the Luminis role and Luminis dynamic group are created, grant user access to **Luminis Administrator Portal**.

   A user must be able to log into the **Administrator Portal** in order to use the **Session Management Console**. By default, Luminis Platform includes a dynamic group called AdminServerAccessGroup. All users associated with this group have access to the **Administrator Portal**. By opening the **Luminis Group Manager** portlet, you should be able to view and change the AdminServerAccessGroup. You will need to modify this dynamic group to include the SESSIONMANAGER role as an attribute.



Member Type: USER

Group Id: AdminServerAccessGroup

Group Tags:

Expression: (Role = ADMINISTRATOR OR Role = ADMIN OR Role = SYSADMIN OR Role = HELPDESKADMIN OR Role =

- Role = ADMINISTRATOR
- Role = ADMIN
- Role = SYSADMIN
- Role = HELPDESKADMIN
- Role = COMMUNITYADMIN
- Role = SESSIONMANAGER

Note: You may need to wait a few minutes for the changes to take effect.

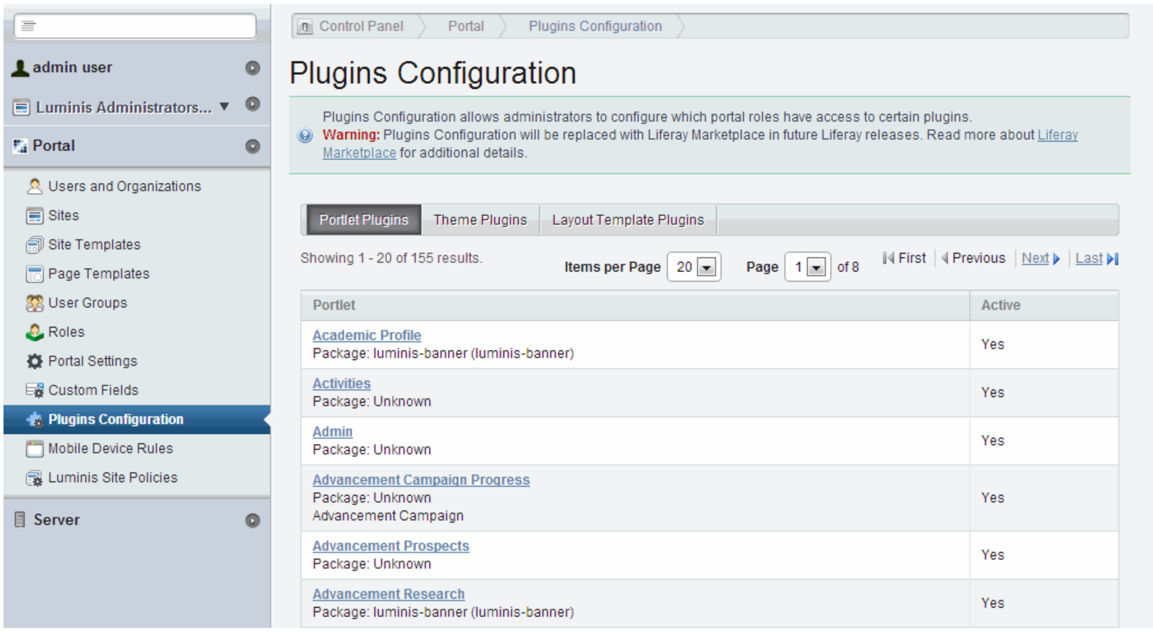
Any user with the Luminis role SESSIONMANAGER now has access to the administrator portal.

6. Grant user access to the **Session Management Console** portlet.

   The **Session Management Console** portlet may be restricted to certain users. You will want to check which users can access the portlet. You can do this through the **Control Panel**.

   a) In the **Control Panel**, under the Portal section, click the **Plugins Configuration** link.

   b) Select the **Portlet Plugins** tab to see a list of all the system portlets.



Plugins Configuration

Plugins Configuration allows administrators to configure which portal roles have access to certain plugins.
Warning: Plugins Configuration will be replaced with Liferay Marketplace in future Liferay releases. Read more about Liferay Marketplace for additional details.

Showing 1 - 20 of 155 results. Items per Page 20 Page 1 of 8

Portlet	Active
Academic Profile Package: luminis-banner (luminis-banner)	Yes
Activities Package: Unknown	Yes
Admin Package: Unknown	Yes
Advancement Campaign Progress Package: Unknown Advancement Campaign	Yes
Advancement Prospects Package: Unknown	Yes
Advancement Research Package: luminis-banner (luminis-banner)	Yes

7. Navigate to the entry for **Session Management Console** portlet and click the provided link. A view consisting of the plug-in configurations specific to the portlet will display.
8. Verify that the AdminServerAccessGroup portal role is listed in the Permissions section.

   Note: A Portal role is in essence the same as a dynamic group. Every time a dynamic group is created, a Portal role is also created. The name of the Portal role is essentially the name of the dynamic group followed by *-LP-XXX* (*XXX* represents a number). So the dynamic group SessionManager might map to a Portal role named SessionManager-LP-150.

9. To grant the Session Manager dynamic group permissions to the **Session Management Console** portlet:

   a) Login as the Luminis Platform administrator.

   b) Select **Go To** > **Control Panel**.

   c) In the Portal section, click **Roles**.

   d) Locate the role named *Session Manager-LP-XXX*.

   e) Select **Actions** > **Edit**.

   f) Click the **Define Permissions** tab.

   g) From the **Add Permissions** drop-down, navigate to Site Applications and select **Session Management Console**.

   h) Mark the check box next to the desired permissions.

   i) Click **Save**.
10. Grant user access to the Configuration Web Service.

    In order for the **Session Management Console** to function correctly, users need to have permission to read or write to the Configuration Web Service. This is where you will need the SessionManager dynamic group you created during setup.

    Open the **Luminis Permission Grant Manager** portlet. Change the category to Configuration Management. Create a new Grant that grants the WRITE CONFIG permission to the SessionManager group. Create another Grant that grants the READ CONFIG permission to the SessionManager group.

    Everyone with the Luminis role SESSIONMANAGER should now have access to read or write to the Configuration Web Service.

Secure the JMX Port

Portal and admin servers in the Luminis system are enabled with a JMX port. Access to this port using a JMX console, such as JConsole is protected with basic user name and password credentials.

After installation, the user name and password are those provided for the default administrator user and password in the installation properties file. You can change the default configuration and add more users with different access permissions.

Note: These users and passwords are not linked to users and passwords within the portal system. The JMX sub-system uses its own security mechanisms to protect access.

By default, two files are installed in the root directory of each Application Server of the Luminis system:

- `jmx.access` defines user names and access rights to the JMX port of the system
- `jmx.password` configures the password for each user defined in the `jmx.access` file

For example, the `jmx.access` file may contain:

user1	readonly
user2	readonly
adminuser	readwrite

The `jmx.password` file would then contain something similar to:

user1	mypassword
user2	password2
adminuser	adminpassword

Once the files are populated in the desired manner, restart the server for the changes to take effect.

Users, Roles, Groups, and Permissions

Users, roles, groups, and permissions are the building blocks for personalizing system content, information, services, and creating user-specific layouts and views.

About this task

This chapter provides information about setting up and maintaining the following:

- Content of the XML extracts and the system administrative commands used to import these extracts
- Procedures for performing ad hoc additions, modifications, or deletions of user records
- Procedures for configuring user password requirements and setting how passwords interact with integrated systems

One of the primary maintenance tasks is to update user profile records. You can import users and roles into the portal from a base ERP system, such as Banner®. You can also manually create users and roles in the **User Management** and **Role Management** portlet applications.

You can import new records at any time as your campus population changes. The user records for these periods are formatted as XML extract files, which are typically generated from your student information system.

Sometimes you may need to add, modify, or delete individual records and set up or modify password criteria to support system security. Instead of performing a full scale re-import of user records, you can modify selected records using the **User Management** and **Role Management** portlet applications or a number of specialized system administrative commands, for example, JMX.

After you set up users and roles, you can use the **Dynamic Group Manager** portlet application to build groups and segments of users. You can then target these groups with personalized content delivery, layouts, administrative permissions, and other system elements.

You can assign permissions at the portlet level to determine who does or does not have access to certain portlets in the layouts or views. To assign portlet-level permissions to select user groups:

Procedure

1. Login as the Luminis Platform administrator.
2. Select **Control Panel** from the **Go To** menu.
3. In the Portal section, click **Roles**.
4. Locate the role you want to assign, then select **Edit** from the **Actions** menu.
5. Click the **Define Permissions** tab.
6. From the **Add Permissions** drop-down, navigate to the Site Applications heading and select the desired application or portlet.
7. Check the check box next to the permissions you want users with the selected role to have.
8. Click **Save**.

   For additional information about roles and permissions, see Liferay's documentation.

If users do not have view permissions, the default system behavior is to make the portlets visible to users with the message "You do not have the roles required to access this portlet." To hide the portlet from the layout for these users, add this to the `portal-ext.properties` file:

```
layout.show.portlet.access.denied=false
```

Note: Make sure that you configure the time zone before adding or importing users into the system.

Related Links

Java Management Extensions on page 17

Import users into Luminis Platform

You can use a command-line tool to import an LDISP 2 XML into Luminis® Platform.

About this task

For example:

```
 # lptool importims -v <filename>
```

The `import xml` file can contain user data, course data, institutions, and so forth. You can import any XML import file that is supported by JConsole's IMSFileImporter by using the command-line tool.

Note: The file `<filename>` exists on the Admin server.

You can also use the JMX to import users into Luminis Platform. A JMX bean is provided from the Luminis Platform administration server. You can access the bean using the Java Console tool, also known as jconsole.

Note: These steps assume you are using the Windows Operating System (OS).

Use these steps to import users from a LDISP 2.0 compliant XML file. LDISP 2.0 is the only supported format for importing users into Luminis Platform.

Procedure

1. Open jconsole and connect to a running Luminis Platform administration server by typing this from the command line:

   ```
    c:/jconsole
   ```

> **Note:** The `jconsole` executable is located in the `<JAVA_HOME>/bin` directory where `<JAVA_HOME>` is the directory in which the JDK is installed. If this directory is in your system path, type `jconsole` in a command prompt. If the directory is not in your path, type the full path to the executable file.

The `jconsole` connection window displays.

For more information about jconsole, see "Configuration management with JMX."

2. Select **Remote Process** and enter the <*host name:port*> for the Luminis Platform administration server.
   - Enter `9002` for the port, as this is the JMX port for the Luminis Platform administration server.
   - For example, if the Luminis Platform administration server is running on the `slc0600221` server, enter `slc0600221:9002` in the **Remote Process** field.
3. In the **Username** and **Password** fields, enter the Luminis Platform administrator credentials.

   After connecting to the Luminis Platform administration server, the main JConsole window displays.
4. Select the **MBeans** tab to view the Managed Beans for the Luminis Platform administration server.
5. Select **Luminis |** > **IMSFileImporter |** > **Operations |** > **importFile** in the directory tree.
6. Under the Operation invocation area, in the **fileName** field, enter the full path and file name of the file you want to import.

   Enter `c:\CreateUser10` to import the `CreateUser10` file located in the `cdirectory`.
7. Click **importFile**.

   When the import is finished, a window displays the number of users that were imported.
8. Click **OK** to acknowledge the user number.

Related Links

Java Management Extensions on page 17

Monitor user import progress

You can subscribe to the notifications in the JConsole window to enable the import process. The import process sends notifications while it is in progress.

About this task

You need to subscribe to the `imsImporter` bean to receive the import notifications.

To subscribe to the notifications:

Procedure

1. Select the **MBeans** tab.
2. Select **Luminis | imsFileImporter | Notifications** in the directory tree.

3. Click **Subscribe**.

View notifications

Notifications are displayed from the **Notifications** node.

About this task

You receive notifications during the import process:

- When the import process starts
- Each time a group of ten records is imported
- When the import finishes

Note: Notifications node is a page in JConsole.

To view notifications:

Procedure

1. Select the **MBeans** tab.
2. Select **Luminis | imsFileImporter | Notifications** in the directory tree.
   The Notification buffer displays any notifications.

User Identifiers

Luminis Platform stores user attributes in the LDAP directory server and the relational database that supports certain system components.

The "Import users into Luminis Platform", section illustrates a number of user attributes that are set through the System Administration Center or through XML imports.

These attributes are used to:

- Describe the characteristics of a given user, such as name or date of birth
- Associate the user with courses, groups, or with other integrated systems, such as e-mail
- Provide consistent identifiers for the user that the Luminis Platform and its integrated systems can use to grant access to services and manage the user's account.

Changes to most user attributes do not adversely impact the integration of other systems with the Luminis Platform or the user's ability to interact with the system. For example, you could change the user's date of birth in the system and it would not cause adverse affects.

However, there are a few critical attributes that the Luminis Platform and its integrated applications consider as primary user identifiers for which changes have broader implications. These include:

Attribute	Description
Login name	The primary identifier for a Luminis Platform user. This value is also used in: • The Login Name field when Administrators search for and identify a user • The `Logon ID useridtype` attribute in XML imports that conform to the `ldisp-2.0.dtd` Changes to a Login Name should be performed infrequently and with caution. Possible reasons are: • The value corresponds closely to a user's actual name, and Sally Smith changes her name to Sally Jones • The Login Name is a PIN number derived from a common application, such as a records management system, and there is a changeto the system that governs the PINs **Note:** The `ldisp-2.0.dtd` file is an XML schema file that defines how the import file is parsed.
Person ID	While most user attributes are designed to accommodate change, systems will typically maintain one or more unique, non-changeable attributes used to permanently identify a given user and manage their account. The Luminis Platform uses a single identifier called the person ID, which cannot be changed.

Manage Login Names

The login name is the primary user identifier for the Luminis Platform. Since it is available for use by system users, system administrators, and integrated systems in a variety of ways, there are a number of ways in which the login name can be referred.

Term	Associated application
Login ID	Used in various fields and displays presented through the **Luminis User Management** portlet.

Term	Associated application
	A useridtype attribute used to specify the Luminis user's login name through XML imports that conform to the LDISP 2 DTD.

Change the login name for a single user

The **Luminis User Management** portlet is the best way to change the login name for a single user.

About this task

To change a user's login name:

Procedure

1. Log in to Luminis Platform.
2. Access the **Luminis User Management** portlet.
3. Enter the search criteria of the user to be changed, then click **Search**.
4. Select the user from the list.
5. Select the **Login Id** field and enter the new login id.
6. Click **Save User** to save the changes.

Work with person IDs

The Luminis Platform uses a single unique attribute called the Person ID to permanently and definitively identify a user and manage their account.

You can only assign a specific Person ID to a user using an XML import. The Person ID is automatically assigned through the Luminis User Management portlet.

Assign person IDs through XML import

When you create a user, you can set a Person ID.

You can only import using the `LDISP 2` format.

To set the Person ID, create a user record and specify a Person ID *useridtype* attribute in the person element. In this example, the user's login name and Person ID are set in addition to a number of other aspects of the user's account that would typically be provided when you create the record.

```
<person>
  <sourcedid>
    <source>Wasatch College LMS</source>
    <id>139</id>
  </sourcedid>
  <userid useridtype=”Logon ID”>sasmith</userid>
  <userid useridtype=”ImmutableID”>123456</userid>
  <userid useridtype=”SCTID”>710000028</userid>
  <userid useridtype=”Email ID”>sasmith</userid>
  <name>
    <fn>Sally Smith</fn>
    <n>
     <family>Smith</family>
     <given>Sally</given>
  </n>
</name>
<demographics>
  <gender>1</gender>
</demographics>
<email>sasmith</email>
<institutionrole primaryrole=”No” institutionroletype=”Student”/>
<extension>
  <luminisperson>
    <academicmajor>English</academicmajor>
  </luminisperson>
  </extension>
</person>
```

Once the file is imported, a user account for Sally Smith is created and her login name is set to sasmith and the Person ID for her account is set to `123456`. While you can change the login name at a later date, the Person ID cannot be modified. If the record you are generating contains a Person ID already in use by another system user, the account is not created and an error is written to a log file.

Note: If you did not specify a Person ID as part of the record, one will automatically be assigned.

Manage user accounts

The **Luminis User Management** portlet enables you to add, delete, or modify user information for users in Luminis Platform.

The portlet is located under the **Add** > **Administration** section of the menu. To access the **User Management** portlet, users must be added to the `AdminServerAccessGroup` as described in "Admin server access group."

After you add the **User Management** portlet to your portal page and open the portlet, you see that the portlet has two panes. The left-hand pane enables you to search for a user or users in the system and select that user, and the right-hand pane displays information specific to the selected user.

Before you can access the **Luminis User Management** portlet, the system administrator must grant certain permissions to allow other users to access the different features of the **Luminis User Management** portlet.

For each user that will access the **User Management** portlet, you must set each of the permissions.

User Management Action	Granted User Management Permissions
Read Users	Read User, Read User Permissions
Read User Protected Data	Permission to read all user fields without granting read permission on them individually.
Create Users	These Set permissions are the required minimum: Read User, Read User Permissions, Create User, Set Login Id, Set Password, Set First Name, Set Last Name, Set Display Name, Set User Roles. Grant other Set permissions to allow the logged in user to enter additional user information.
Update Users	Read User, Read User Permissions, Update Users. There is no minimum. Grant only the Set methods that you want the user to be able to change. If no Set permissions are granted, the user information will not change.
Delete Users	Read User, Read User Permissions, Delete Users

Warning! When you grant the Set User Roles permission you allow the setting of any user roles. This could unintentionally allow or remove user access to specific features. For example, a student user might accidentally be assigned the Administrator role.

Related Links

User management on page 189

Create user accounts

The **Luminis User Management** portlet enables you to create user accounts.

Procedure

1. Log in to the Luminis Platform as an administrator.
2. Click **Go to**, then select **My Public Pages** from the drop-down list.
3. Access the **Luminis User Management** portlet.
4. Click **Create New User**.
5. Enter the mandatory user account details such as, **Login id**, **Password**, **First Name, Last Name**, and **Display Name**.
6. Select the roles for the user from Roles list box.

Note: Use the **Ctrl** key to select multiple roles for a user. Ensure the **Account Enabled** check box is checked.

7. Click **Save User**.

   You have added a user account to the system.
8. **Optional:** Click **Cancel** to stop the user account creation.

   Note: This operation adds the user to the Luminis Platform. It does not add the user to any integrated system such as Banner or an Identity Management system.

Modify user account

The **Luminis User Management** portal enables you to manage user accounts.

Procedure

1. Log in to the Luminis Platform as an administrator.
2. Click **Go to**, then select **My Public Pages** from the drop-down list.
3. Access the **Luminis User Management** portlet.
4. Search for the user account to be modified.

   The user account details appear in edit mode.
5. Edit the user account details.
6. **Optional:** Change roles for the user from the Roles list box.

   When you change a user's role, the change may not take effect until the Liferay user cache expires. The role change may also cause a system error to display the next time the user logs in. The system error will go away after the Liferay user cache expires.
7. Click **Save User**.

Delete user account

The **Luminis User Management** portal enables you to delete user accounts.

Procedure

1. Log in to the Luminis Platform as an administrator.
2. Click **Go to**, then select **My Public Pages** from the drop-down list.
3. Access the **Luminis User Management** portlet.
4. Search for the user account to be deleted.

   The user account details will appear in edit mode.
5. Click **Delete User**.
6. Click **OK** in the confirmation pop-up box to confirm the user deletion was successful.

Search for user

Search for a user in the **User Management** portlet.

About this task

The **User Management** portlet contains two panes. The left-hand pane enables you to search for a user or users in the system and select that user, and the right-hand pane displays information specific to the selected user.

To find a user in your system:

Procedure

1. Log in to the Luminis Platform as an administrator and locate the **Luminis User Management** portlet.
2. Enter the first few letters of the Login ID, first name, or last name in the search box. Enter an asterisk (*) for the search character if you wish to search for all users.
3. From the pull-down menu, select **Login ID**, **First Name**, or **Last Name**.
4. Click **Search**.

   The results of your search appear in the columns below the search field.

   Note: The search for users will only list fifty records at a time. To list more click **Additional Users** at the bottom of the search result list.
5. Click to select the desired user.

   The specific information for that user appears in the right-hand pane and includes the Person ID, Login ID, Password, First Name, Last Name, Email Address, Session Timeout, Preferred Language, and Roles. The roles for this specific user are highlighted.

Create role in Luminis Platform

The **Luminis Role Management** portlet enables you to add roles to a user.

About this task

A role's Admin Managed value controls how the role is evaluated during an import. The role will not be processed -- either added or removed -- during import if an Admin Managed role is part of the user import, or the user has been assigned an Admin Managed role.

- If the **Admin Managed** check box is not selected and the role is part of the user import, the role will be processed during import.
- If the **Admin Managed** check box is checked and the role is part of the user import, the role will not be processed during import.

You can only add or remove the Admin Managed role for a user within the **User Management** portlet or by using the PersonService JMX bean described "Manage user roles through JMX."

To add roles to a user:

Procedure

1. Log in to the Luminis Platform as an administrator and locate the **Luminis Role Management** portlet.
2. Click to select the role(s) that you want to create.
3. Click **New**.
4. In the **Create New Role** pop-up window, enter the new role details.
5. Click **Save**.

Modify role in Luminis Platform

The **Luminis Role Management** portlet enables you to modify existing role details.

Procedure

1. Log in to the Luminis Platform as an administrator and locate the **Luminis Role Management** portlet.
2. Click the edit icon next to the role record you want to edit. ✎
3. In the **Edit Role Properties** pop-up window, perform the necessary changes.
4. Click **Save**.

   Note: You may not perform maintenance on the system role.

Delete role in Luminis Platform

The **Luminis Role Management** portlet enables you to delete existing roles.

Procedure

1. Access the **Luminis Role Management** portlet.
2. Select the role you want to delete.

   Note: You cannot delete system roles.

3. Click **Delete**.
4. Click **OK** to confirm the role deletion.

Manage user roles through JMX

The following sections describe how to manage user roles using the JMX import tool..

Related Links

Configuration management with JMX on page 26

Add a Luminis Platform user role using JMX

Use the JMX console to add a single role to Luminis Platform users.

About this task

A JMX bean is provided from the Luminis Platform administration server. You can access the bean using the Java Console tool, also known as jconsole.

Note: The following steps assume you are using the Windows Operating System (OS).

To add a single role to a Luminis user:

Procedure

1. Open jconsole and type this from the command line to connect to a running Luminis Platform administration server:

   ```
   c:/jconsole
   ```

   Note: The jconsole executable is located in the `<JAVA_HOME>/bin` directory where `<JAVA_HOME>` is the directory in which the JDK is installed. If this directory is in your system path, type `jconsole` in a command prompt. If the directory is not in your path, type the full path to the executable file.

2. In the jconsole connection window, select **Remote Process** and enter the *<host name:port>* for the Luminis Platform administration server.

   Enter `9002` for the port, as this is the JMX port for the Luminis Platform administration server.

   If the Luminis Platform administration server is running on the `slc0600221` server, enter `slc0600221:9002` in the **Remote Process** field.
3. In the **Username** and **Password** fields, enter the Luminis Platform administrator credentials. After connecting to the Luminis Platform administration server, the main JConsole window displays.
4. Click the **MBeans** tab to view the Managed Beans for the Luminis Platform administration server.
5. Select **Luminis** > **PersonService** > **Operations** in the directory tree.
6. Under the Operations invocation area, in the **LoginId** field, enter the login ID of the Luminis person you want to add a role to. This is the login ID the Luminis user enters to log into Luminis Platform.
7. In the **roleName** field enter the role name of the role you want to add.

   Warning! The role name has to be an exact match or the role will not be added to the Luminis Platform user.

8. Click **addRoleToPerson**. A dialog appears when the process is finished. The dialog does not tell you whether the process was successful. To see the result, you must monitor the person service bean.

Remove a Luminis Platform user role using JMX

To remove a Luminis platform role from a user:

Procedure

1. In the **loginId** field in the Operation invocation area, enter the login ID of the Luminis person you want to add a role to. This is the login ID the Luminis user enters to log into Luminis Platform.
2. In the **roleName** field, enter the name of the role to be added.

   Warning! The role name has to be an exact match or the role will not be added to the Luminis Platform user.

3. Click **removeRoleFromUser**. A dialog appears when the process is finished. The dialog does not tell you whether the process was successful. To see the result, you must monitor the person service bean.

Monitor progress of added or removed user roles

You can subscribe to the notifications in the JConsole window to monitor the success of role operations. The add or remove a user role process sends notifications of success or failure.

About this task

You need to subscribe to the PersonService bean to receive the import notifications.

To subscribe to the notifications:

Procedure

1. Select the **MBeans** tab.
2. Select **Luminis** > **PersonService** > **Notifications** in the directory tree.
3. Click **Subscribe**. The Notifications item changes to indicate the number of notifications received.
4. After you have subscribed to the person service bean to view the notifications, click the **Notifications** option in the directory tree.

Manage Sites and Collaboration

Luminis® Platform sites provide portal users at your institution tools to create, manage, and participate in dynamic online sites.

Luminis Platform sites, known prior to Luminis Platform 5.1 as "communities", provide dedicated portal areas for both academic and non-academic collaboration for courses, clubs, affiliations, and other interests. System users create and manage non-academic sites. Course events from back-end Enterprise Resource Planning (ERP) systems create academic sites for all courses offered at your institution.

The Sites area of Luminis Platform provides these features:

- Administration
- Content creation and workflow
- A suite of collaboration tools

Academic sites are configurable collaboration rooms (virtual class room or site). Academic sites are also referred as Course sites and represent different courses that are scheduled for an academic year.

Non-academic sites represent virtual groups available for online collaboration. They are created by system users through approved requests to administrators or by administrators themselves for special types of sites.

All sites have an owner. Typically, a site owner is the person who initially requested the site creation. Site owners:

- Create and manage the group homepage, including the layout of the homepage, as well as the available collaboration applications such as file sharing, Web logs, photos, and discussion threads
- Create and manage the Welcome and Guest view messages, including the site description and information, and any links or photos that would be appropriate to be viewed by members or potential members
- Set up and manage the site applications with relevant and compelling content
- Add and remove site members as necessary, including approving or denying membership requests for restricted sites

Luminis Platform provides several portlets for access to site features:

- **Luminis Site**. Users can access each of the sites of which they are members.
- **Luminis Site Welcome**. Users can view and join additional sites.
- **Create Luminis Site**. Users can create new sites.
- **My Courses**. Users can access the sites for courses in which they are registered.

To allow system users easy access to the site features, the Luminis Platform site portlets can be added to a dedicated "Sites" page in the Home site.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Related Links

Academic sites on page 314
Non-Academic sites on page 316

Luminis Sites portlet

From the **Luminis Sites** portlet, users can manage the sites they administer or belong to.

From this portlet, users can join sites, navigate to the homepage of sites to which they belong, and manage sites of which they are owner.

Luminis Sites portlet features:

- The My Sites snapshot view and navigation mechanism to sites that the user is a member of
- Site icons that provide quick-links to pre-defined site homepages
- Site search functions
- An option to join or request membership to a site

When the user clicks **Join** to request membership to a site, a pop-up window displays. The window includes a welcome or guest message for the site, the site membership policy, and a check box for the user to agree with the policy. If the site is a restricted site, a text area is also included so the user can write to the sight owner. Once the user selects the check box and optionally gives a reason to join, they click the second **Join** button. The server either adds the user to the public site, or sends a request for the site owner to approve the user's membership in the restricted site.

The **Manage** button next to sites the user owns enables the owner to edit, activate, or delete messages for their sites. You can only activate or delete messages that are marked inactive.

Asset Publisher

Publish a mixed group of various kinds of assets such as images, documents, blogs, and Web content. You can place user-created wiki entries, blog posts or message board messages in context with your content.

Note: The **Calendar Event** option applies only to the **Liferay Calendar** portlet and not to the Luminis Calendar. If you are using the Luminis Calendar, Ellucian® recommends that you deactivate the **Liferay Calendar** portlet from the **Portlet Configuration** option in the **Control Panel** to avoid confusion. This will remove the Liferay Calendar Event from the Asset Publisher.

Add a portlet

To work with most portlets, you must add the portlets to your site's basic layout.

About this task

To add a portlet:

Procedure

1. In the Luminis Platform main menu, mouse over or click **Add** > **More** to search for the application that you wish to add to the layout. For example, Luminis Blog, Create Luminis Site, and so on.
2. Click **Add**.

   Note: You can also drag and drop the portlet on to the page layout.

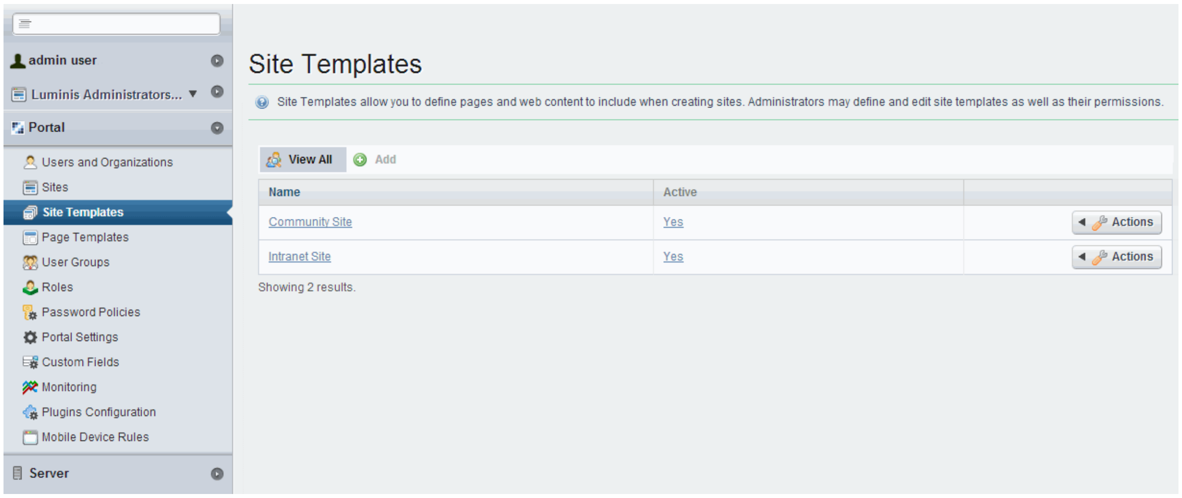
Site templates

Templates are a set of pages which are automatically populated with portlets and content.

Two ready-made site templates are available through Liferay. You also have the option to create a unique template to fit the needs of your institution. If your institution chooses to use the Site Template feature, create one or more site templates. For instructions on creating a new template, see the Liferay documentation at liferay.com.

Note: If you have additional questions about Luminis Platform or associated third-party software, or you want to report defects in the system, contact Ellucian Customer Support.

Liferay's default templates are located through the **Control Panel**:



Site Templates

Site Templates allow you to define pages and web content to include when creating sites. Administrators may define and edit site templates as well as their permissions.

Name	Active	
Community Site	Yes	Actions
Intranet Site	Yes	Actions

Showing 2 results.

By default, courses and sites are not created using a template. If the administrator chooses to not use site templates, courses and sites are created with blank pages.

To enable the site template within Luminis Platform, configure this JConsole property:

- Site Example:

  ```
  key: luminis.community.creation.template
  ```

  ```
  value: Community Site
  ```

  Note: Community Site is the exact name of the site template, as shown in the image above. When a user creates a site, the system automatically assigns the specified template to that site.

- Course Example:

  ```
  key: luminis.course.creation.template
  ```

  ```
  value: SLCC Course Template
  ```

  Note: SLCC Course Template is the name of the site template that you must manually create. When courses are imported, the system automatically assigns the specified Site Template to the imported courses. This only affects new imported courses; existing courses are unchanged.

Related Links

Manage JMX-enabled Java in JConsole on page 27

Manage the My Courses portlet

The **My Courses** portlet provides an aggregate view of the terms and courses that are relevant for both students and faculty.

These conditions apply to the **My Courses** portlet:

- Displays the terms and course details. It does not participate in terms and courses life cycle in any other way. Terms and course details are retrieved from Banner®. Banner application integration must be working before course details are displayed. Data for My Courses comes from Banner as an XML message. For more information on setting up Banner integration, refer to the *Luminis Platform Banner Integration Setup Guide.*
- User must be registered for the available terms and courses. Registration information must be imported into Luminis through a properly formatted ldisp-2.dtd extract.

Select Term

Select Term displays the terms for which the user has registered. Appropriate course details are displayed once a term is selected.

Courses I'm attending

Course information details include Course Title, Course Id, and Instructor.

This section is available only for students who have registered for courses in a given term.

If a valid e-mail address was entered into the instructor's profile, an e-mail button displays next to the instructor's name. When the user clicks the icon, their default e-mail client opens to allow the user to e-mail the instructor.

Courses I'm teaching

Additional course details such as Course Title and Course Id are displayed.

This section is available for faculty members who are teaching courses in a given term.

Create a site

Create a new site for those who share your academic or non-academic interest.

About this task

If a site is created by an administrator, the administrator becomes the owner of that site with all the rights of an owner. If a site is created by a non-administrative user such as, students, faculty, alumni, and so on, it must be approved by the Luminis Site Administrator. Once approved, the site will be available to the person who requested it, making that person the owner.

Sites can be created two ways:

- Through course events
- Manually by portal users using the **Create Luminis Site** portlet

  Note: A Student is not allowed to create a hidden site.

To create a Luminis site:

Procedure

1. Log in to the Luminis Platform as an administrator and locate the **Create Luminis Site** portlet.
2. In the **Create Site** page, designate a **Site Name** for the site.

   The **Site Name** must be unique, and can have up to 25 characters. It can include numbers but cannot be all numbers.

3. From the drop-down menu, select a **Site Category**.

   The list is populated with these default categories: Academic, Athletic, Cultural, Intramural, Political, Service, and Social.

4. Click **Next**.
5. Set **Site Options**.

Field	Description
Type	Used to set the site as one of the three types: • Public. Public sites will be listed to the public and will be available for all to join. • Restricted. Restricted sites will be displayed to the public, but membership requests will be subject to approval from the Site Owner. • Hidden. Hidden sites will not be listed for the public to search and join. Only the Site Administrator or the Site Owner can add members to the site. Select the desired type for the new site.
Site Status	Indicates whether the site is currently available to the members. Select either of these choices: • Active • Inactive
Sort Membership Lists By Last Name	If you check the check box, members are sorted by their last name in the Site's **Member List** portlet. If unchecked, users are sorted by their first name. By default, this box is unchecked.

6. Click **Next**.
7. Enter Site Guest Message information in the text blocks.

Field	Description
Guest Message Name	The title or name of the guest message. After the site is created, the site owner can create additional welcome messages.
Guest Message Content	The welcome message that displays to a guest in the Welcome portlet.

8. Click **Next**.

9. Enter Site Member Message information in the text blocks.

Field	Description
Member Message Name	The title or name of the welcome message. After the site is created, the site owner can create additional welcome messages.
Member Message Content	The welcome message that displays to members in the Welcome portlet.

10. Click **Next**.
11. In the **Create Site** page, enter text in the **Creation Comment** field to describe why the site is being requested.
12. Read the Site Policy and check the box indicating that you have read and understood the policy.
13. Click **Next**.
14. Review the Summary.

    To make changes before you finish creating the site, click **Previous**.
15. Click **Finish**.

    Note: Sites created by administrators are available immediately and you will see the new site in your **Luminis Site** portlet. You can also use the **Welcome** and **Member List** portlets to see and begin modifying the content for the active, newly created site. Sites created by non-administrators must be approved by an administrator before they can be made available for use.

Approve or deny a site request

A request for the creation of a site is sent to the site owner for approval. The **Luminis Site Request Approval** portlet lists all the newly requested sites and is used to approve or deny a request.

About this task

To approve or deny a request:

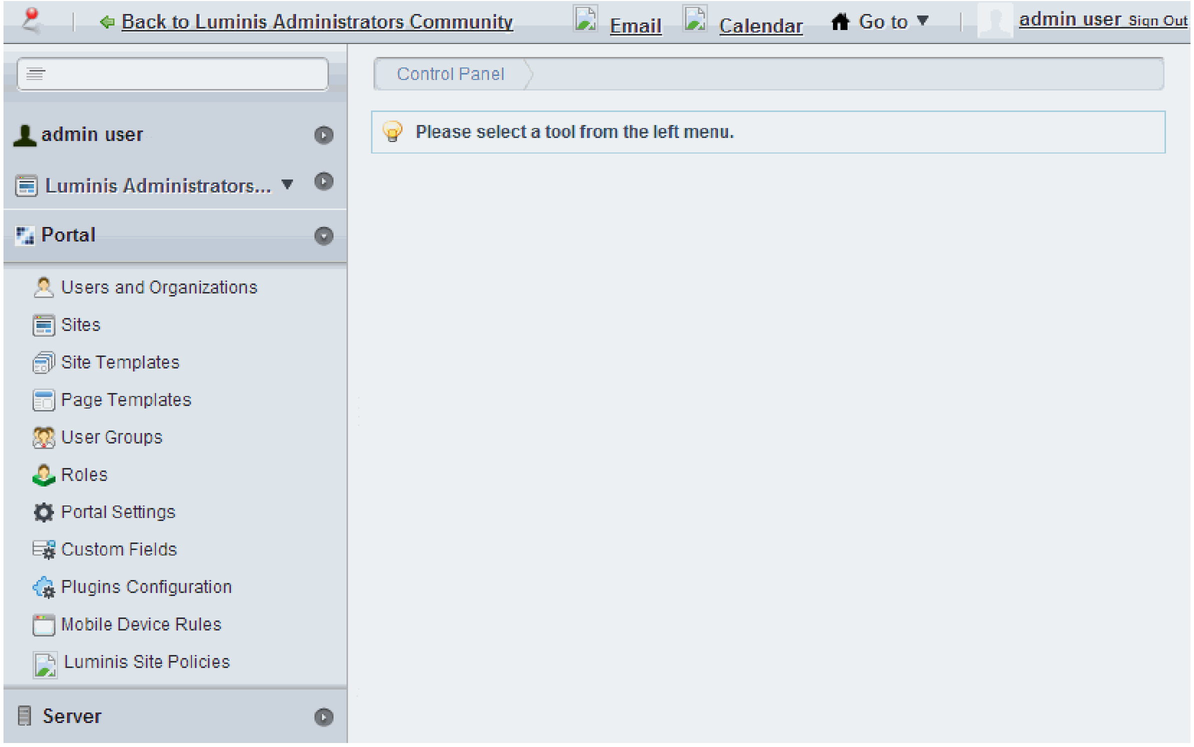
Procedure

1. In the **Luminis Site Request Approval** portlet, select the site you wish to approve.
2. To approve, click **Approve**.
3. **Optional:** To deny, click **Deny**.

    Note: As part of the approval process, the Site Administrator can modify the site status, name, category, type, and guest and member messages.

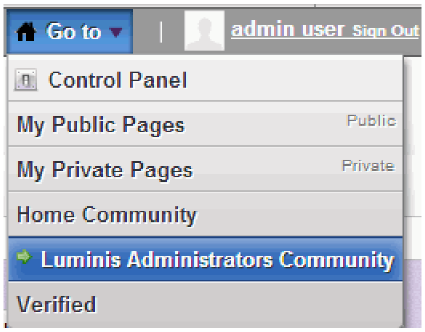
Manage sites through the Control Panel

As an administrator, you will use the **Control Panel** to manage sites.



Please select a tool from the left menu.

To access the **Control Panel**, mouse over or click **Go to**, and select **Control Panel** from the drop-down menu.



Management of a site includes:

- Manage Site Pages
- Manage Site Content
- Edit the site name, description, and type

- Edit the memberships
- Edit the categorization for the site
- Activate or deactivate a site
- Delete a site

Manage site policy administration

The **Manage Site Policy** page can be accessed only by the Administrator through the **Luminis Site Policies** link found in the Portal section of the Liferay Control Panel. Use this link to modify the Site Policy and Site Member Policy information. These policies are read and agreed to by users while creating or joining a site.

There are two types of site policies:

- A Site Policy governs the creation of sites
- A Site Membership Policy specifies the rules that each user should follow as a site member

The first time you access the **Control Panel** and click on the **Policy** menu, the Luminis Site Policies displays a default set of Site Policy and Site Member Policy values.

Field	Description
Site Policy Title	Header for the site policy.
Site Policy	Site policy information. When a Luminis user creates a site the Site Policy information is displayed. The user must agree to the policy before the site will be created.
Site Member Policy Title	Header for Site Member Policy. While joining a site, the Site Member Policy is displayed to the user.
Site Member Policy	Site member policy information. Before Luminis users join a site, they must agree to the Site Member Policy.

When you create a new site, or update the Site Policy and Site Member Policy, click **Save** to save the information.

Change the default site name

Default site names are included with Luminis Platform installation.

About this task

Default site names and URLs:

- Luminis Administrators Community

  Site URL = `/luminis-admin-group`
- Home Community

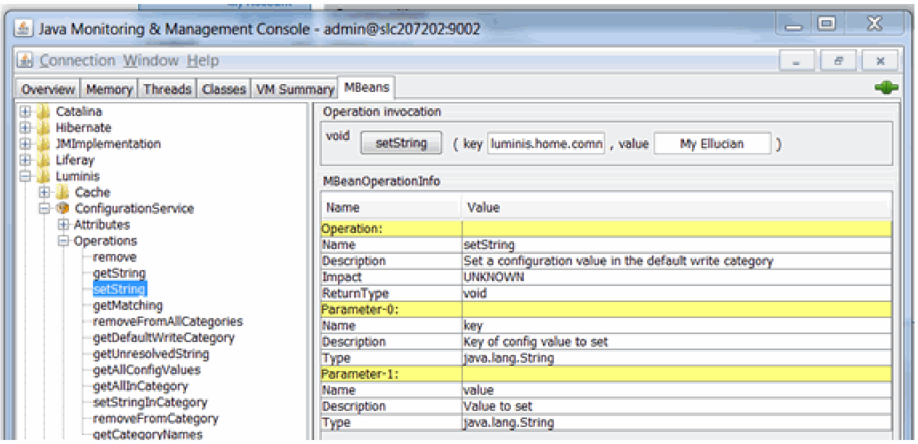
  Site URL = `/home-community`

To change the default settings after Luminis Platform has been installed:

Procedure

1. Log into Luminis Platform as an administrator
2. Click **Go to** > **Control Panel**.
3. Click **Site** in the Portal section.
4. Click **Actions** > **Edit Settings** for the site you want to update.
5. In the **Site Settings** page, edit the **Name** and **Description** fields, as desired.
6. To edit the URL, click the **Site URL** link in the Basic Information menu and edit the Friendly URL.
7. Click **Save**.
8. Using JConsole, set the following properties with the same values set in the **Control Panel**:

```
luminis.admin.community
luminis.admin.community.url
luminis.home.community
luminis.home.community.url
```



void setString (key luminis.home.comn , value My Ellucian)

Name	Value
Operation:	
Name	setString
Description	Set a configuration value in the default write category
Impact	UNKNOWN
ReturnType	void
Parameter-0:	
Name	key
Description	Key of config value to set
Type	java.lang.String
Parameter-1:	
Name	value
Description	Value to set
Type	java.lang.String

9. Edit the site names and URL values in the `portal-ext.properties` file for each node:

```
# Default landing page for the Portal
community.default.home=Home Community
company.default.home.url=/web/home-community
company.default.web.id=ellucian.edu
```

Note: Do not remove the `/web` from the `company.default.home.url` value.

The `portal-ext.properties` file is located in the following directories:

`$CP_ROOT/products/tomcat/tomcat-admin/webapps/ROOT/WEB-INF/classes`

`$CP_ROOT/products/tomcat/tomcat-portal/webapps/ROOT/WEB-INF/classes`

10. Restart the Luminis Platform system.

    Note: The `portal-ext.properties` file is overwritten when the Luminis system is patched.

Results

For information on how to change the default settings prior to installation, see "Customize the installation values" in the *Luminis Platform Installation Guide*.

Edit site details

Once a site has been created you may need to modify its settings, or delete the site.

About this task

To edit a site:

Procedure

1. Click **Go to** > **Control Panel**.
2. Click **Site** in the Portal section.
3. Click **Actions**, then select **Edit Settings** for the site you want to update.
4. Make the required changes on the **Site Settings** page.
5. Click **Save**.

Add members to a site

In some cases you may need to manually add members to a site, particularly if the site is a private site and there are no automatic functions for joining.

About this task

To add members to a site:

Procedure

1. Click **Go to** > **Control Panel**.
2. Click **Site** in the Portal section.
3. Click **Actions**, then select **Manage Memberships** for the site you want to update.

4. On the Site Memberships page, click **Add Members** > **User**.
5. Check the box next to the user(s) you want to add and click **Save**.
6. **Optional:** Click the **Advanced** link to search for a user based on the first name, middle name, last name, page name, or e-mail address.

Manage Site Categories

Each site must be created under a category. Only an administrator can create and manage categories, which is done through the **Control Panel**.

During Luminis Platform installation, a default set of categories are created. Additionally, categories can be created and edited using the Global scope in the Luminis Platform Control Panel. The default categories are:

- Academic
- Athletic
- Cultural
- Intramural
- Political
- Service
- Social

Each site can have multiple categories and sub-categories, and sub-categories can be assigned to multiple sites. You can create a category under Luminis Categories, which is the vocabulary for all the categories.

Once a category is created, edited or deleted, the changes will be reflected in the category tree displayed within.

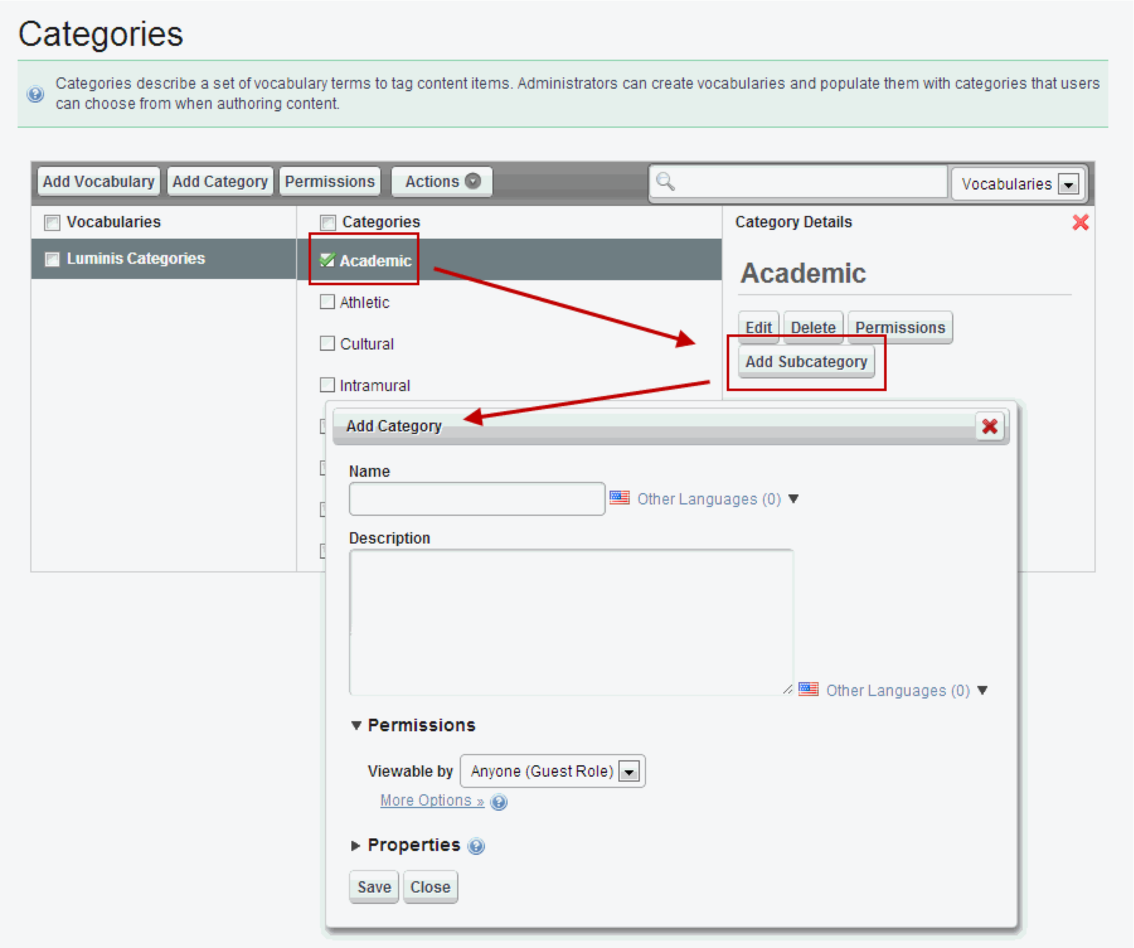
Create Luminis category

To create a Luminis category:

Procedure

1. Click **Go to** > **Control Panel**.
2. Click **Categories** in the Global section.
3. Ensure that **Luminis Categories** is selected on the **Categories** page, then click **Add Category**.
4. Enter a name and optional description for the category in the **Add Category** pop-up window.
5. Click **Save**.
6. To create a subcategory, check the box next to an existing category, then click **Add Subcategory**.

   You see the **Add Category** pop-up window.



Categories

Categories describe a set of vocabulary terms to tag content items. Administrators can create vocabularies and populate them with categories that users can choose from when authoring content.

Viewable by: Anyone (Guest Role)

7. Enter a name and optional description, and click **Save**.

Edit Luminis category

To edit a Luminis category:

Procedure

1. From the list of Luminis Categories, select a category that you want to edit.
2. Click **Edit**.

   Note: The category names can be modified to a non-English language, such as Spanish, French, or Arabic.

3. Make the desired updates in the **Edit Category** pop-up window, and click **Save**.

   The modified category name is reflected in all the portlets.

Delete Luminis category

To delete a Luminis category:

Procedure

1. From the list of Luminis Categories, select a category that you want to delete.
2. Click **Delete**.

Activate, deactivate, or delete a site

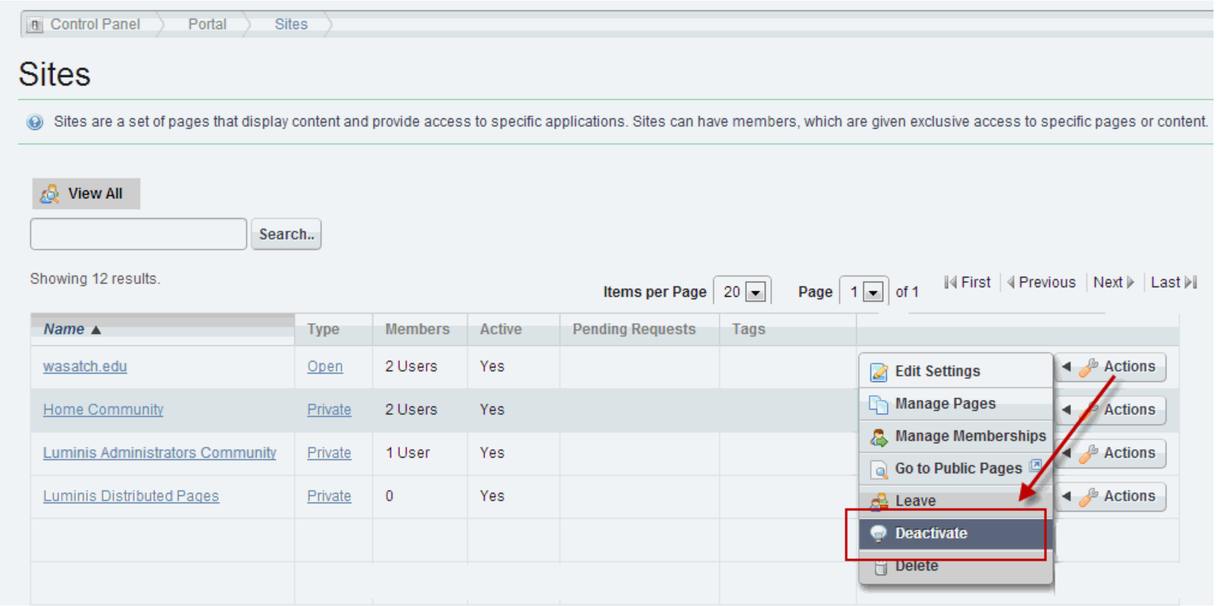
Deactivate an active site, activate an inactive site, or delete the site.

About this task

To either activate or deactivate a site, depending on the current status:

Procedure

1. Click **Go to** > **Control Panel**.
2. Click **Site** in the Portal section.
3. To activate or deactivate the site, click **Actions**, then select either **Activate** or **Deactivate** from the drop-down menu. Only one of the options will be available.



Sites

Sites are a set of pages that display content and provide access to specific applications. Sites can have members, which are given exclusive access to specific pages or content.

Showing 12 results.

Name ▲	Type	Members	Active	Pending Requests	Tags	
wasatch.edu	Open	2 Users	Yes			Actions
Home Community	Private	2 Users	Yes			Actions
Luminis Administrators Community	Private	1 User	Yes			Actions
Luminis Distributed Pages	Private	0	Yes			Actions

4. To delete the site, click **Actions**, then select **Delete** from the drop-down menu.
5. Click **OK** in the confirmation pop-up window.

Collaboration tools and applications

Luminis Platform has a number of tools that help people with common interests interact with each other. The **Control Panel** enables the Site Owner or Administrator to manage the site content in one central location.

For example, a **Documents and Media** portlet can share site-related files or be added to a non-site area of the system and configured by the end user for personal use.

Review the Liferay documentation for the "Collaboration Suite" on the Liferay Web site for information about configuring the portals.

Note: The links on the Liferay Web site are subject to change without notice.

These baseline Liferay portlets are available in Luminis Platform:

- Blog
- Bookmarks
- Documents and Media
- Message Boards
- Web Content
- Wiki

See "Glossary" for descriptions of these portlets.

Dynamic membership in sites

You can map a Luminis dynamic group so that all of the users in the group are assigned to be members of a Luminis site, or create a custom field for a site.

Map Luminis dynamic groups to Luminis sites

Map a Luminis dynamic group so that all of the users in the group are assigned as members of a Luminis site.

About this task

To map a Liferay site to a Luminis dynamic group.

Procedure

1. Create a Luminis Site using the **Create Luminis Site** portlet. For details about creating Luminis sites, see "Create a site."

   When you create a Luminis dynamic group, a matching Liferay role is automatically created. The Liferay role is used to map a site to a Luminis dynamic group.
2. From the **Liferay Control panel** In the Portal category, click **Roles**.

3. Locate a role that was automatically created with the Luminis dynamic group you created.

   The description for these roles is Mapped Luminis Dynamic Group and the role name includes `-LP-` followed by an associated number. Note the role name used to map the Liferay site. For example, Alumni-LP-100.
4. From the **Liferay Control** panel in the Portal category, click **Sites**. Find the new site that was created for the Luminis Site.
5. Click **Action** and select **Edit Settings** for the site you want to map.
6. In the **Basic Information** menu, click the **Custom Fields** link under Miscellaneous.
7. Enter the Liferay role name that is mapped to a Luminis dynamic group. This is the name of the Liferay role that was created when the Luminis dynamic group was created. For example, Alumni-LP-100.
8. Click **Save**.

Results

The next time a user who belongs to the affected Luminis dynamic group logs into Luminis Platform, the user is added as a member of the site and can access the site from the **Go to** menu.

If the option for Luminis Dynamic Group mapping is removed from the Liferay site, the site becomes a regular site available to all users for membership. The users who are already members of the site remain members unless the Administrator manually removes the site membership.

If the group does not display when the user logs in, here are some options to help you troubleshoot the problem:

- The mapping of Liferay sites to Luminis dynamic groups is held in a cache that expires after 15 minutes. If a site mapping is created during the time the cache is active, wait for the cache to expire before you can add new site mapping.
- Ensure that the custom field key is set to `luminis_dynamic_group`. For instructions, see "Create a custom field for a site."
- Ensure that the permissions for the Luminis dynamic group custom field are set to View and Update for the User role. For instructions, see "Create a custom field for a site."
- Ensure that the Searchability value is set to As Keyword. For instructions, see "Create a custom field for a site."
- Ensure that the Liferay role was entered correctly in the site's custom field. For instructions, see "Create a custom field for a site."
- Ensure whether pages are available within the site, and that correct page permissions are set. For more information about pages, see "Overview of Creating and Publishing Pages and Content to Users."

Related Links

Overview of Creating and Publishing Pages and Content to Users on page 157

Create a custom field for a site

The manual process to create a custom field for a site when you need to create additional or backup fields.

About this task

The Liferay site field is automatically created during the Luminis Platform startup process at installation and during patch updates.

Note: When you start Luminis Platform, the system checks to ensure the **luminis_dynamic_group** custom field is available. If the custom field is not found, the system creates it. If you delete the **luminis_dynamic_group** custom field, all values are also removed and the field is automatically created the next time Luminis Platform is restarted. If any Liferay sites were mapped to Luminis Dynamic groups when the field was deleted, those sites are no longer mapped. The site memberships will not change, but additional members cannot be added until the site is once again mapped to a Luminis dynamic group.

Procedure

1. Click **Go to** > **Control Panel**.
2. In the Portal category, click **Custom Fields**.
3. Click the site you want to add the field to.
4. Click **Add Custom Field**.
5. Enter the custom field information.
    a) In the **Key** field, enter luminis_dynamic_group in all lower case letters, including the underscores. If the key is not entered correctly, the Luminis site is not recognized as mapped site.
    b) In the Type drop-down, select **Text Field - Indexed**.
6. Click **Save**.
7. Click **Actions** and select **Edit** from the drop-down for the new Luminis Dynamic Group field.
8. Select **As Keyword** from the Searchability drop-down.
9. Click **Save**.
10. Click **Actions** and select **Permissions** for the Luminis Dynamic Group field.
11. Enable **View** and **Update** for the User role.

    Warning! If these permissions are not set the value for this field cannot be accessed during user log in.

12. Click **Save**.

Related Links

Overview of Creating and Publishing Pages and Content to Users on page 157

Integrate Google with Luminis Platform

Integrated with Google™, Luminis® Platform system provides a full implementation of e-mail and calendar standards, backend integration for data and account provisioning, and a set of e-mail and calendar portlets.

One of the key objectives of Luminis Platform is to provide better interoperability and more flexibility throughout the system where appropriate. Institutions can integrate external e-mail and calendaring systems providing a unified and open experience between the institutional-driven portal and external e-mail and calendar systems. GoogleApps calendar and e-mail offerings include these key features:

- Single sign-on option for Google mail and calendar
- Check and send e-mail and manage calendars directly through the portal
- Packaged e-mail and calendar portlets that deliver snap shots of e-mail and calendar data
- ERP data integration, account provisioning, and Banner® ERP event processing to and from Google
- UI integration with event synchronization and color coded events

Note: The Luminis portlet used for the Google calendar supports only the Gregorian calendar.

Luminis Platform calendar and e-mail strategy for Google

The topics in this section explain the options available to you when you configure Luminis Platform e-mail and calendars using Google, and prerequisites required to successfully implement the portlets.

Luminis calendar configuration using Google

Luminis Platform provides prepackaged configuration for Google-based calendar integration.

This topic applies to schools with an understanding of the hosted Google calendar environment for hosting school calendar data (for example, Education Google Apps accounts).

To achieve this integration, the configuration parameters and setup noted in "Integrate Google mail and calendar integration with Luminis Platform tools" are required to be completed.

You use the **Calendar Configuration** portlet to configure Luminis Platform with the login and logout URL parameters for Google.

The parameters in the **Calendar Configuration** portlet, combined with the parameters defined in the **External Services Configuration** portlet for your Google domain account, will provide these functionalities for Luminis users:

- Calendar portlet integration
- Single sign-on (SSO)

- Enterprise Resource Planning (ERP) event support, and full user and account provisioning between connection with an existing Google account when they are added via your backend ERP
- Automatically created course calendar and Google groups based on ERP course events

Prerequisites for the calendar configuration:

- This operation is performed within the context of a running Luminis instance. The school must have the Luminis Platform installed and running as well as an existing relationship with Google for calendar hosting (GoogleApps account - Education edition).
- Luminis Platform relies on properly configured CAS or Ellucian Identity Service (EIS), SAML, and network for communication and SSO between Luminis and Google

Luminis mail configuration using Google

Luminis Platform provides pre-packaged configuration for Google-based e-mail integration. This topic applies to schools with an understanding of the hosted Google mail environment for hosting school e-mail data (for example, Education Google Apps accounts).

To achieve this integration, the configuration parameters and setup noted in "Integrate Google mail and calendar integration with Luminis Platform tools" are required to be completed.

You use the **Luminis Mail Configuration** portlet to configure Luminis Platform with the login and logout URL parameters for Google mail.

The parameters in the **Luminis Mail Configuration** portlet, combined with the parameters defined in the **External Services Configuration** portlet for your Google domain account, will provide these functionalities for Luminis users:

- Mail portlet integration
- Single sign-on (SSO)
- Enterprise Resource Planning (ERP) event support, and full user and account provisioning between connection with an existing Google account when they are added via your backend ERP

Prerequisites for the Luminis mail configuration:

- This operation is performed within the context of a running Luminis instance. The school must have an existing relationship with Google for e-mail hosting (Google Apps account - Education edition).
- Luminis Platform relies on properly configured CAS or Ellucian Identity Service (EIS), SAML, and network for communication and SSO between Luminis and Google.

Calendar and e-mail configuration for multiple groups

You can define multiple calendar configurations and assign each configuration to a Luminis dynamic group.

By default, the first calendar configuration that is saved to Luminis will be assigned to the All Users group. Use the **Manage calendar Groups** tab to assign a Luminis dynamic group to a calendar configuration.

You can define multiple e-mail configurations and assign each configuration to a Luminis dynamic group. By default, the first e-mail configuration that is saved to Luminis will be assigned to the All Users group. Use the **Manage e-mail Groups** tab to assign a Luminis dynamic group to a e-mail configuration.

Integrate Luminis Platform with Google

To integrate Google e-mail and calendaring systems, you must complete certain prerequisites and configure the tools within Luminis Platform.

Google integration prerequisites

This section outlines the fundamental pre-requisite steps you must complete before you can use the Luminis Platform tools to integrate Google.

Items here include base Google Account setup for your institution, configuration required to ensure your Google Apps account interacts with Luminis using CAS or EIS, steps to generate all appropriate public and private keys and certificates, steps required to configure Single Sign-On (SSO) authentication with Google, steps required to configure OAuth authentication, and steps required to enable the appropriate Google APIs.

Luminis portlets are granted access to the user's data through Google service accounts and OAuth 2.0 implementation. This enterprise application is an alternative to requiring users to manually give consent for Luminis access to the mail and calendar data.

Sign up for a Google Apps for Education account

Sign up for a Google Apps for Education account for your domain using the URL http://www.google.com/enterprise/apps/education/.

Note: You must be an administrator of the domain to create a Google apps education account.

Follow the steps in Google to validate ownership of your domain and initial Google Apps account setup.

Generate public and private keys and upload the certificates

Follow one of these sets of steps to generate public and private keys and upload the certificates for Google Single Sign-on (SSO) setup. This certificate must contain the public key used by either CAS or EIS/WSO2 to sign the SAML requests.

About this task

- To generate the certificate for Google, use the `keytool` command to export the certificate from the WSO2 keystore. The location of the keystore used by WSO2 for this public key is defined in the `<IS_HOME>/repository/conf/carbon.xml` file (look for the `<KeyStore>` element).
- `keytool -export -alias <alias> -file for_google.cert -keystore <keystore_file> -storepass <store_password> -rfc`
- To generate public and private Digital Signature Algorithm (DSA) keys using openssl in CAS, complete these steps. The location of this key for CAS is defined in the `<CP_ROOT>/products/tomcat/cas-server/webapps/cas-web/WEB-INF/spring-configuration/argumentExtractorsConfiguration.xml` file.

Procedure

1. Navigate to this location in the CAS server:`$CP_ROOT/products/tomcat/cas-server/webapps/cas-web/WEB-INF/classes`.
2. Create a DSA parameter file.

   ```
   openssl dsaparam -out dsaparam.pem 1024
   ```
3. Use the parameter file to create a private key.

   ```
   openssl gendsa -out dsaprivkey.pem dsaparam.pem
   ```
4. Extract the public key into the DER format. Place both generated keys into the CAS classpath.

   ```
   openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
   ```
5. Convert the private key into pkcs8 and DER format. Once complete, keys can be used to create the certificate to be uploaded to Google.

   ```
   openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out
   dsaprivkey.der -nocrypt
   ```
6. Using the public and private key, create the certificate. After you answer a set of questions, a certificate will be created and saved as `dsacert.pem`.

   ```
   openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
   ```

   Warning! When you generate the certificate, you must specify the domain name. The domain name must be the same as the domain indicated in the URLs you enter in the Google Admin console for the sign-in, sign-out, and change-password URLs. Also, make sure to use the associated external domain and not the machine name of the server when you generate the certificate. After you generate the certificate, inspect the certificate to verify that it is correct. The domain specified in the certificate supports a trust relationship that allows the HTTPS protocol required by Google when it communicates with the CAS server.
7. Inspect the generated key using the openssl utility.

```
openssl x509 -in dsacert.pem -noout -text
```

For more information, go to the Security section of the Google admin console for your education domain account, as described in "Configure Single Sign-on with Google."

For more information about viewing of generated certificate content, see http://www.mkssoftware.com/docs/man1/openssl_x509.1.asp.

8. Restart Luminis Platform.

Configure single sign-on with Google

Single Sign-On (SSO) between Luminis and your Google Apps domain account will use SAML for authentication through either CAS or through Ellucian Identity Service (EIS). Steps listed below cover setup for SAML with CAS and EIS using the WSO2 identity service. If your Luminis Platform is configured to use EIS with an alternate Identity Service (other than WSO2) please refer to the IS documentation for instructions to configure SAML for Google Apps.

Procedure

1. Log in to the Google Admin console.
2. Navigate to **Security** > **Set up single sign-on (SSO)**.
3. In the **Sign-in page URL** field, the URL should point to your CAS login page for Luminis, or to the EIS SAML endpoint for your Google Service Provider.
   - CAS:

     `https://<cas-host-name>:<port>/cas-web/login`
   - WSO2:

     `https://<EIS-host-name>:<port>/samlsso`
4. In the **Sign-out page URL** field, the URL should point to your CAS logout page for Luminis, or to the EIS logout page. For example in CAS, `https://<cas-host-name>:<port>/cas-web/logout`.

   Note: If using EIS with WSO2, there may be some additional customizations needed to create a logout and change password page. For instructions, see the WSO2 documentation.
5. To set the **Change password URL** field for CAS, use the URL `https://<cas-host-name>:<cas-port>/cas-web/changepassword`. With SSO enabled between Luminis and Google, you cannot change password in the Google system. You must change the password in Luminis Platform only.

   Note: If using EIS with WSO2, there may be some additional customizations needed to create a logout and change password page. For instructions, see the WSO2 documentation.
6. In the required **Verification certificate** field, upload the certificate file that is created in "Generate public and private keys and upload the certificates."

Create the service account and credentials

As you create the service account, gather the information to access Google Apps domain-wide delegation of authority and to authorize your service account in Luminis Platform.

About this task

- Client ID
- Private key file
- E-mail address

To create these accounts:

Procedure

1. Create a new project and application for Luminis Platform in the Google Developers Console. This console is located at https://console.developers.google.com. Name the project Ellucian Luminis.
2. When you create the new project, several of the Google APIs are automatically enabled in the new project application. You must also enable the mail and calendar APIs. If Google user accounts are provisioned through Luminis, you must also enable the Admin SDK API.

   Note: New Google API comes with strict quota assignments. You may need to request a quota increase to fit your institution's needs. Monitor quota usage via the Google Developers console at https://console.developers.google.com.

3. Click **Credentials** under the API Manager menu to generate credentials for a service account.
4. To set up a service account:

   Click **Create Credentials**.

   Click **Service Account Key**

   Select **New Service Account** and select **p12** for the key type.

   For the name, enter `ellucianLuminis`

   Click **Create** to generate the p12 private key file. Google automatically generates the file and downloads it through your browser.

   Copy the new p12 key to the Luminis Admin application server in `$CP_ROOT/products/tomcat/tomcat-admin/shared/classes`.

   Note: If the file name contains a space, rename the file to remove the space.

   You can get the service account's e-mail address and client ID after you have downloaded the file.

   If you provision Google user accounts and course calendars through Luminis Platform, you can create a second service account specifically for provisioning. If you create a second service account, you must copy the p12 key file for this account to the Luminis application servers in `$CP_ROOT/products/tomcat/tomcat-admin/shared/classes`.

A second service account allows you to narrow the scope in your domain account in Luminis so that the OAuth access token generated for the user portlets only have access to the mail and calendar APIs, and access to the directory API is limited to the Luminis provisioning processes.

Apply service account credentials

Steps a Google Apps domain administrator must complete to grant your service account access to the Google Apps domain's user data.

Procedure

1. In the Google Apps domain's Admin Console, click **Security**. The console is located at https://admin.google.com.

   If **Security** is not listed in the control panel, click **More controls** in the gray bar at the bottom of the page, then click **Security** from the list of controls.
2. Click **Advanced settings**.
3. In the Authentication section, click **Manage API Client access**.
4. In the **Client name** field, enter the service account Client ID you created in "Create the service account and credentials."
5. In the **One or More API Scopes** field, enter a comma-delimited list of scopes Luminis Platform needs access to. Luminis Platform requires that you add the mail and calendar scopes. For example, `https://mail.google.com`, and `https://www.goggleapis.com/auth/calendar`.
6. Click **Authorize**.
   - If you provision Google user accounts and course calendars through Luminis and you choose to maintain only one service account, then you must add the URLs for the directory APIs to the scope at the beginning of this topic.

     For example, `https:/www.googleapis.com/auth/admin.directory.group`, `https://www.googleapis.com/auth/admin.directory.group.member`, `https://www.googleapis.com/auth/admin.directory.user`
   - If you choose to add a second service account specific to provisioning, repeat the steps in "Create the service account and credentials" to grant access to the directory APIs with the second service account Client ID.

Enable APIs

You must enable the calendar and e-mail APIs before you integrate Google with Luminis Platform.

Procedure

1. Log in to the Google Admin console.
2. Select **Security** > **API reference**.

3. Check the **Enable API access** check box.
4. Click **Save Changes**.

Add a new service provider for Google

About this task

Warning! These steps do not apply to a CAS configuration.

In the WSO2 Management Console, under the **Inbound Authentication Configuration** tab, add a SAML2 Web SSO Configuration.

Procedure

1. Enter google.com for the issuer, unless you have selected domain specific issuer on the Google side.
   a) Enter `https://www.google.com/a/<your-domain>/acs` for the Assertion Consumer URL.
   b) Select **Enable Response Signing**.
   c) Select **Enable Attribute Profile**.
   d) Click **Register**.
2. Under the **Claim Configuration** tab, add a claim for the e-mail address.
   a) Select **Use Local Claim Dialect**.
   b) Click **Add Claim URL** to add a new Requested Claim. Select http://wso2.org/claims/emailaddress.
   c) In the **Subject Claim URL** drop-down, select http://wso2.org/claims/emailaddress (the same as the Add Claim URL).
   d) Click **Update**.

Add a secondary user store

In the WSO2 Management Console, on the **Configure** tab, go to the **User Store Management** page to add a Secondary User Store.

About this task

Warning! These steps do not apply to a CAS configuration.

Procedure

1. The User Store Manager Class should be the default value, ReadWriteLDAPUserStoreManager.
2. Enter PRIMARY-ATTRIBUTE-STORE for the Domain Name.

3. Enter the property values. Once saved, these properties are written to a file called `PRIMARY-ATTRIBUTE-STORE.xml` located in `<IS_HOME>/repository/deployment/server/userstores` directory. This is a sample of the XML file:

```
<?xml version="1.0" encoding="UTF-8"?>

<UserStoreManager
class="org.wso2.carbon.user.core.ldap.ReadWriteLDAPUserStoreManager">

<Property name="ConnectionName">cn=Directory Manager</Property>

<Property name="ConnectionURL">ldap://slctestv4.ellucian.com:389</
Property>

<Property name="ConnectionPassword">cp.admin</Property>

<Property name="UserSearchBase">ou=People,o=cp</Property>

<Property name="Disabled">false</Property>

<Property name="UserNameListFilter">(objectClass=person)</Property>

<Property name="UserNameAttribute">uid</Property>

<Property name="UserNameSearchFilter">(&amp;(objectClass=person)
(uid=?))</Property>

<Property name="UserEntryObjectClass">user</Property>

<Property name="GroupEntryObjectClass">groupOfNames</Property>

<Property name="ReadGroups">true</Property>

<Property name="GroupSearchBase">ou=People,o=cp</Property>

<Property name="GroupNameAttribute">cn</Property>

<Property name="GroupNameListFilter">(objectClass=groupOfNames)</
Property>

<Property name="MembershipAttribute">member</Property>

<Property name="GroupNameSearchFilter">(&amp;
(objectClass=groupOfNames)(cn=?))</Property>

<Property name="MaxUserNameListLength">100</Property>

<Property name="MaxRoleNameListLength">100</Property>

<Property name="UserRolesCacheEnabled">true</Property>

<Property name="SCIMEnabled">false</Property>

<Property name="PasswordHashMethod">SHA</Property>

<Property name="UserDNPattern">uid={0},ou=People,o=cp</Property>

<Property name="PasswordJavaScriptRegEx">^[\S]{5,30}$</Property>

<Property name="UserNameJavaScriptRegEx">^[\S]{3,30}$</Property>

<Property name="UserNameJavaRegEx">[a-zA-Z0-9._-|//]{3,30}$</Property>

<Property name="RoleNameJavaScriptRegEx">^[\S]{3,30}$</Property>
```

```
<Property name="RoleNameJavaRegEx">[a-zA-Z0-9._-|//]{3,30}$</Property>
<Property name="WriteGroups">true</Property>
<Property name="EmptyRolesAllowed">true</Property>
<Property name="MemberOfAttribute"/>
<Property name="DomainName">PRIMARY-ATTRIBUTE-STORE</Property>
<Property name="Description">attribute store</Property>
</UserStoreManager>
```

After you complete this step, each user is listed twice in the WSO2 Users page, once with the prefix `PRIMARY-ATTRIBUTE-STORE/`. In the User Profile for each user, you should see the user's e-mail address from Luminis.

4. Edit the `<IS_HOME>/repository/conf/carbon.xml` file. Make sure this element is uncommented and is true:

```
 <EnableEmailUserName>true</EnableEmailUserName>
```

5. Restart WSO2.

Integrate Google mail and calendar integration with Luminis Platform tools

Instructions for using the Luminis Platform tools and portlets for Google Mail and Calendar integration.

Note: You must configure the **Luminis External Services Configuration**, **Luminis Mail Configuration**, and **Luminis Calendar Configuration** portlets in Luminis Platform.

Create a Google service

Using the **External Services Configuration** portlet, create a Google service.

Procedure

1. Login to Luminis Platform as an administrator.

   If needed, use the **Add** menu to add the **Luminis External Services Configuration** portlet to the Luminis Administrators Site.
2. In the **Luminis External Services Configuration** portlet, click the **External Services Configuration** link.
3. Click **New** to create a new Google Service.
4. Select **Google** in the **Type** drop-down list.
5. In the **Service Name** page, enter a name and a description for the Google service.

6. Click **Next**.
7. On the **Portlet Support** page, enter the properties for the Google service.

Field	Description
Google Account Domain	The name of the domain that is registered for an Education account at Google.
Service Account Email	The e-mail for the account.
Service Account P12 Key Filename	The private key filename for the account.
Google Administrator ID	The Google administrator account. You can have multiple administrator user accounts on your Google domain account. The user who initially requests the account sets up the first admin user account as part of requesting the account from Google. Any one of these admin user accounts will work in this field in the **External Services Configuration** portlet. **Note:** The entry in this field must include the domain. For example: mailto:john.smith@demosystem.wasatch.com.

8. Click **Next**.
9. On the **Provisioning Support** page, mark the **Enable Luminis user account setup for Google** check box to enable the provisioning options. This check box is unmarked by default. When this check box is checked, you can access these radio buttons:
   - If you select **Luminis controls account provisioning**, then when you use the IMS importer, the LDI importer, or the **User Management** portlet UI to create new users, Luminis Platform sends a request to provision a new Google user account. This button is selected by default. If you choose this option, you can enter information into the **Delete external Google user accounts when deleting Luminis user accounts** and **Connect Luminis user accounts to existing Google user accounts** fields described in the Google user account fields table below.
   - If new user accounts for Google are provisioned outside of Luminis Platform, for example, through your IDM system or Google's Directory Sync application, select the **External System controls account provisioning** radio button. When you use the IMS or LDI importer or the **User Management** portlet UI to create new users, Luminis Platform assumes the Google user account already exists and creates the data necessary for the Luminis Platform user portlet to connect to the Google account.

     Note: When you select **External System controls account provisioning**, Luminis Platform does not create Google course calendars and events during LDI import.

Field	Description
Delete external Google user accounts when deleting Luminis user accounts	Mark this check box to delete external Google user accounts at the same time you delete the corresponding Luminis user accounts.
Connect Luminis user accounts to existing Google user accounts	Mark this check box to enable Luminis user Email IDs set in the **User Management** portlet or through import to link with the corresponding external Google accounts. When a new user is created by either using the IMS or LDI importer or **User Management UI** and the check box to **Connect Luminis User Accounts to Existing Google User Accounts** is marked, the Luminis system will send a request to provision a Google user account for the new Luminis user. If the user already exists in Google, the Luminis system will link the new Luminis user to the existing Google user account. **Note:** When you enable provisioning, you must be cautious to prevent inadvertent access to a Google user account by different Luminis users.
Provisioning Service Account Email	The email for the account.
Provisioning Service Account P12 Key Filename	The private key filename for the account.

10. Click **Next**.

    The system will automatically send a test request to Google to validate the properties entered for the Google service. The results will display on the **Save Service** page.

11. On the **Save Service** page, click **Save** to save all the details that you have entered and view a page that lists all services.

    Note: You can save the properties regardless of whether the validation fails. However, the **Save** button will be disabled until the results of the validation are returned.

12. To modify and update the fields mentioned in the Google user account fields table above, click **Edit**.

13. To make sure the keys required for the set up are correct, click **Validate**.

Configure the Luminis/Google calendar

Customize the **Luminis Calendar Configuration** portlet to meet the needs of your institution.

Procedure

1. Using the **Add** menu, add the **Luminis Calendar Configuration** portlet to the Luminis Administrators Site.
2. In the **Luminis Calendar Configuration** portlet, click on the **Calendar Configuration** link.

   Note: You must have created an external service configuration before creating a calendar configuration.
3. In the **Luminis Calendar Configuration** portlet, click **New**.
4. Enter the mandatory fields.

Field	Description
Name	A short name to identify the configuration (User Defined, Free Text).
Calendar Service	Service defined in the **External Services Configuration** portlet. The items in the drop-down list are generated from the setup completed using the **External Services Configuration** portlet. Each new service you create will now be available here.
Description	More descriptive name (User Defined, Free Text).
Application URL	The URL used to access the calendar application at Google. This value can be found on the Google Admin console. For example, www.google.com/calendar/hosted/demosystem.sct.com
Application Logout URL	The URL Luminis uses to ensure proper logout from Google calendar. The Logout URL is http://www.google.com/calendar/logout
Update Interval (sec)	The frequency that the **Calendar** portlet will check with Google for new calendar event data. The default is 300 seconds.
Properties Global to all Calendar Configurations	Mark the **Use this configuration to provision course calendars** check box to make the configuration the default for all site calendars. If provisioning is enabled,

Field	Description
	this configuration will be used to provision a course calendar in Google when the course is imported into Luminis. Only one configuration can be set as the default for site calendars. When you mark the check box for a specific configuration, check marks in any other configurations are cleared. You can also provision inactive courses in the **Calendar Configuration** portlet. Mark the **Provision Calendars for Inactive Courses** check box to create course calendars on the import even if the course is not active. **Note:** If you are using an External System to control account provisioning, this setting does not apply.

5. Click **Save**.

   Note: **Manage Calendar Configuration** tab is used to create, edit, validate, and delete all calendar configurations.

6. To make changes to the portlet, click **Edit or Double-click the name to edit calendar configuration** in the **Manage Calendar Configuration** tab.
7. To test the Single Sign-On settings, click **Validate**.

   This process will attempt to launch the Google calendar application using the value from the application URL field in a new browser window using the currently logged in Luminis user credentials.
8. To delete a calendar configuration, click **Delete**.

Assign a Luminis dynamic group to a Google calendar configuration

To assign a Luminis dynamic group to a calendar configuration:

Procedure

1. In the **Luminis Calendar Configuration** portlet, select the **Manage Calendar Groups** tab.
2. Select a calendar configuration from the left panel.
3. Double-click on the desired group in the left panel, **Available Groups** box.

   The members of the Selected Group will be assigned to a given calendar configuration under **Selected Group** box.

Note: You can only add one group to the Selected Group column. If a group matching the rules you require does not already exist in the list of available groups, you must use the **Luminis Group Manager** to create a new group for provisioning.

4. If the selected calendar configuration already has a group associated, click the delete icon next to the group to remove before you select a new group. ☒
5. Click **Save** to save the changes.

   If you have multiple calendar configurations assigned to multiple groups, they must be given a priority for the Luminis system to use when provisioning user accounts in the external calendar provider system.

   If there is a calendar configuration named Student, which is associated with a Student group, and a calendar configuration named Faculty associated with the Faculty group. If a new user is added to Luminis that belongs to both the Student and Faculty groups, the system would use the priority to determine which calendar configuration to use to provision the new user account in Google.

Related Links

Calendar and e-mail configuration for multiple groups on page 240

Configure Luminis/Google e-mail

To configure the **Luminis Mail Configuration** portlet:

Procedure

1. In the **Luminis Mail Configuration** portlet, click the **Mail Configuration** link.

   Note: You must have created an external service configuration before creating a mail configuration.

2. In the **Luminis Mail Configuration** portlet, click **New**.
3. Enter the fields as described.

Field	Description
Name	A short name to identify the configuration (User Defined, Free Text).
Mail Service	Service defined in the **External Services Configuration** portlet. The items in the drop-down list are generated from the setup completed using the **External Services Configuration** portlet. Each new service you created will now be available here.
Description	More descriptive name (User Defined, Free Text).

Field	Description
Application URL	The URL used to access the e-mail application at Google. This value can be found on the Google Admin console. For example: http://mail.google.com/a/demosystem.wasatch.com
Application Logout URL	The URL Luminis uses to ensure proper logout from Google e-mail. For example: http://mail.google.com/?logout
Update Interval (sec)	The frequency that the **Mail** portlet will check with Google for new messages.
Mail List Size	The number of messages to display in the **Mail** portlet.

4. Click **Save**.

   Note: **Manage Mail Configuration** tab is used to create, edit, validate, and delete all mail configurations.

5. To make changes to the portlet, click **Edit or Double-click the name to edit a mail configuration** in the **Manage Mail Configuration** tab.
6. To test the Single Sign-On settings, click **Validate**.

   This process will attempt to launch the Google e-mail application using the value from the application URL field in a new browser window using the currently logged in Luminis user credentials.
7. To delete a mail configuration, click **Delete**.

Assign a Luminis dynamic group to a Google e-mail configuration

Assign a Luminis dynamic group to a mail configuration.

Procedure

1. In the **Luminis Mail Configuration** portlet, select the **Manage Mail Groups** tab.
2. Select a mail configuration.
3. Double-click the desired group, **Available Groups** box.

   The members of the Selected Group will be assigned to a given mail configuration under **Selected Group** box.

   Note: You can only add one group to the Selected Group column. If a group matching the rules you require does not already exist in the list available groups, you must use the **Luminis Group Manager** to create a new group for provisioning.

4. If the selected mail configuration already has a group associated, use the ☒ icon next to the group to remove before selecting a new group.
5. Click **Save** to save the changes.

   If you have multiple mail configurations assigned to multiple groups, they must be given a priority for the Luminis system to use when provisioning user accounts in the external e-mail provider system.

   Note: By default, the external provisioning is disabled.

   If there is a mail configuration named Student, which is associated with a Student group, and a mail configuration named Faculty associated with the Faculty group. If a new user is added to Luminis that belongs to both the Student and Faculty groups, the system would use the priority to determine which mail configuration to use to provision the new user account in Google.
6. You can add the **Luminis Calendar** portlet and **Luminis Mail** portlet using the **Add** menu, and validate by accessing Google calendar and Google mail applications respectively from Luminis Platform.

Related Links

Luminis mail configuration using Google on page 239
Provisioning on page 256

Confirm the CAS server is configured for Google single sign-on

Validate that the CAS server is configured properly for Single Sign-on.

Procedure

1. Log into the CAS Management page.

   `https://<cas server>:<port>/cas-web/services/manage.html`
2. If necessary, add the Google domain to the Service URL for Google Apps.

   For example, if `testlp.wasatch.com` is the Google domain, the Service URL would be `https://www.google.com/a/testlp5.wasatch.com`.

Support sub-domains with Google

Luminis Platform supports multiple domains on your Google Apps for Education account.

About this task

For example, if your primary domain with Google is wasatch.edu, you may want to also create a student.wasatch.edu sub-domain for students and faculty.wasatch.edu for faculty. These sub-domain options allow Luminis Platform to assign student users an e-mail address such as joseph.smith@student.wasatch.edu.

Procedure

1. Create the domains in the Google Admin Console located at https://admin.google.com. Complete the steps within the console to verify ownership of the domains.
2. Create a separate service configuration in Luminis Platform for each domain. The value of the **Google Account Domain** field must be similar to one of these example domains:
   - wasatch.edu
   - student.wasatch.edu
   - faculty.wasatch.edu

   Note: All Google configurations can use the same Google service account email and key file.
3. After you create the Google services in the **External Services Configuration** portlet, create one mail configuration and calendar configuration for each domain.

   To find the correct URLs, navigate to the Google Apps page on the Google admin console, then choose **Calendar** or **Gmail** to view the URLs for each application.

   Warning! It is critical that you assign the correct URL for the sub-domain as the value of the **Application URL** field for the mail or calendar configuration. The correct URL for each sub-domain ensures that SSO works correctly for your users.

   When you create the mail configuration for students, enter a URL such as http://mail.google.com/a/student.wasatch.edu.
4. After you complete the mail and calendar configurations, associate the mail configurations with the user groups, such as student.wasatch.edu with the Students group, faculty.wasatch.edu with the Faculty group, or wasatch.edu with ALL USERS.

   Note: If the Luminis user is a member of two or more groups, each associated with a separate mail configuration, the priority in the Manage Mail Groups tab of the **Luminis Mail Configuration** portlet determines the domain of the e-mail address for that user.

   If Sally is both a student and faculty member, and the mail configuration for the Student group was priority 1, then Sally would be provisioned with the email address mailto:sally@student.wasatch.edu.

Provisioning

Information about provisioning Google objects in your Google account, accessing user accounts, and processing user accounts or course calendar objects.

Automatically provision Google objects from Luminis Platform

The Luminis system can be configured to automatically provision objects in your Google domain account after these configurations are complete:

- Google service configuration
- Mail and Calendar service configurations

  Note: By default, external provisioning is disabled. It must be enabled before you create a new user or a new course in Luminis for the provisioning to occur automatically. To enable external provisioning, see "Create a Google service" and confirm that the **Luminis controls account provisioning** option is marked. The other option, **External System controls account provisioning**, prevents Luminis Platform from creating the Google objects detailed in this section.

Luminis Platform supports provisioning of these Google objects:

User account. You can create a new user in Luminis using one of these methods:

- **User Management** portlet
- IMS file importer
- LDI person event

After you create a new user, a new account is provisioned at Google for the user.

- Course calendar. When you import a course section using an IMS file importer or using an LDI course section event, a new Google group and course calendar is provisioned at Google for the course. If the class times are included with the course section, the class times schedule is added as a calendar event at Google on the course calendar.

  The default Liferay time zone is assigned to a course calendar when the calendar is created. The user sets the Google calendar's time zone the first time that user logs into Google Calendar. The course calendar automatically inherits the Liferay time zone.
- Enrollment. When you import a membership or an enrollment using the IMS file importer or through an LDI membership event (to enroll a user to a specific course or assign a user as the instructor of the course), the user account at Google is granted access to the course calendar.

Related Links

Create a Google service on page 247

Process provisioning requests

The Luminis system processes requests for provisioning user accounts or course calendar objects at Google asynchronously.

When a user is created or a course section is imported and provisioning is enabled, a request for provisioning will be created. A separate provisioning engine will pick up the provisioning request and will communicate with Google to handle the object creation. During times of high volume (for example, during a large IMS file import), provisioning requests will be in queue in the Luminis database, to be processed by the provisioning engine.

Thus, when you create a new user in Luminis, the corresponding Google user account will not be created immediately. It is important to provide both the Luminis provisioning engine and Google necessary time to process the new user account before attempting to login to Luminis with the newly created user account.

Integrate Microsoft Office 365 with Luminis Platform

Integrated with Microsoft Office 365, the Luminis® Platform system provides single sign-on (SSO) to a full implementation of e-mail and calendar standards.

One of the key objectives of Luminis Platform is to provide better interoperability and more flexibility throughout the system where appropriate. Mail and calendar are two of those areas. Institutions can integrate external e-mail and calendaring systems to provide a unified and open experience between the institutional-driven portal and external e-mail and calendar systems. Microsoft Office 365 calendar and e-mail offerings include these key features:

- SSO option for Office 365 mail and calendar
- ERP data integration and Banner® ERP event processing to and from Office 365

The current integration with Microsoft Office 365 does not provide support for the following portlets:

- Luminis Calendar Portlet
- Luminis Mail Portlet

Luminis Platform provides SSO to Microsoft Office 365 for portal users through SAML 2.0 authentication. Shibboleth will be installed with the patch to Luminis Platform 5.1.1 on the CAS tier, or during installation of Luminis Platform 5.2 and above.

Luminis Platform calendar and e-mail strategy for Microsoft Office 365

The topics in this section explain the options available to you when you configure Luminis Platform e-mail and calendars using Microsoft Office 365, and prerequisites required to successfully implement the portlets.

Luminis calendar configuration using Office 365

Luminis Platform provides prepackaged configuration for Office365-based calendar integration. Configuration parameters and setup are noted in "Install and Configure Shibboleth". This topic applies to schools with an understanding of the hosted Office365 calendar environment for hosting school calendar data.

Note: If you choose to use the Office 365-based calendar, configuration is optional.

This topic is dependent on first completing the External Services Configuration for Office365.

You use the **Calendar Configuration** portlet to configure Luminis Platform with the login and logout URL parameters for Office 365 calendar.

The parameters in the **Calendar Configuration** portlet, combined with the parameters defined in the **External Services Configuration** portlet for your Office 365 domain account, will provide these functions for Luminis users:

Enterprise Resource Planning (ERP) event support, and full user connection with an existing Office 365 account when they are added by your backend ERP.

Prerequisites for the calendar configuration:

- This operation is performed within the context of a running Luminis instance. The school must have the Luminis Platform installed and running in addition to an existing relationship with Office365 for calendar hosting.
- This system relies on a properly configured CAS, SAML and network for communication between Luminis and Office365

Luminis mail configuration using Office 365

Luminis Platform provides pre-packaged configuration for Office 365 based e-mail integration.

To achieve this integration, the configuration parameters and setup noted in "Install and Configure Shibboleth" are required to be completed. This topic applies to schools with an understanding of the hosted Office 365 mail environment for hosting school e-mail data.

This topic is dependent on first completing the External Services Configuration for Office 365.

You use the **Luminis Mail Configuration** portlet to configure Luminis Platform with the login and logout URL parameters for Office 365 mail.

The parameters in the **Luminis Mail Configuration** portlet, combined with the parameters defined in the **External Services Configuration** portlet for your Office 365 domain account, will provide these functionalities for Luminis users:

- Single sign-on
- Enterprise Resource Planning (ERP) event support, and full user connection with an existing Office 365 account when they are added via your backend ERP

Prerequisites for the Luminis mail configuration:

- This operation is performed within the context of a running Luminis instance. The school must have an existing relationship with Office 365 for e-mail hosting.
- This system relies on a properly configured CAS and network for communication between Luminis and Office 365

Integrate Luminis Platform with Microsoft Office 365

This section provides step-by-step instructions for using the Luminis Platform tools and portlets for Microsoft Office 365 Mail and Calendar integration.

Office 365 integration prerequisites

Steps to integrate Luminis Platform with Office 365.

Procedure

1. Sign up for an Office 365 Standard account.

   For more information, see "Office 365 Education plans and pricing" on the Microsoft Web site.

   Note: The links on the Microsoft Web site are subject to change without notice.

2. Enable Single Sign-On (SSO) authentication.
   a) Install and configure Shibboleth with your CAS server.
   b) Validate Shibboleth and CAS configuration using TestShib.
   c) If needed, request a subscription to Microsoft Office 365 services from the Microsoft Store.
   d) Configure a federated authentication server to work with Office 365, as explained in "Create Domain entries for SSO at Microsoft."
   e) Complete the steps in "Integrate Office 365 mail and calendar integration using the Luminis Platform tools" to set values needed for the Office 365 environment.

Install and Configure Shibboleth

Luminis Platform automatically installs software to enable a Shibboleth server to support Microsoft Office 365 integration on the Luminis Platform CAS tier.

If you integrate with Office 365, the following configuration values for the Shibboleth server must be set in the `$CP_ROOT/install/resolved.properties` file. If your environment was preconfigured with IDP settings during the initial Luminis Platform 5.2 and above installation, or during a Luminis Platform 5.1.1 upgrade, these configuration values may already be set:

```
idp.host=<host name of server hosting the Shibboleth server>
idp.http.port=<http port of Shibboleth server>
idp.https.port=<https port of Shibboleth server>
idp.soap.https.port=<soap port of Shibboleth server>
idp.ajp.port=<AJP port of Shibboleth server>
idp.scope=<domain covered by Shibboleth operation>
idp.immutableid.name=<Default value is objectGUID>
idp.entity.id=<URL to access the Shibboleth webapp. For example:
 https:// [your server name]/idp/shibboleth>
```

```
idp.userid.name=<Default is userPrincipalName>
```

After you have configured the above IDP* settings, run `$CP_ROOT/install/scripts/config_shib.sh` to automatically update configuration within the Shibboleth server.

To configure Shibboleth to start automatically with Luminis Platform, copy the `15-shib-webserver` script file from `CP_ROOT/install/bin/15-shib-webserver` to `CP_ROOT/bin/15-shib-webserver`.

For more information about configuring Microsoft Office 365, see "Microsoft Office 365 Tips" in the *Luminis Platform Installation Guide*.

Validate Shibboleth and CAS configuration

Luminis Platform includes the configuration and metadata to interact with a Shibboleth testing facility called TestShib.

TestShib, located at www.testshib.org, is a testing service intended for new installations of Shibboleth. All SAML 2.0 implementations are welcome and may be tested against Shibboleth at the Web site.

The Web site contains steps to achieve an independent test for your Shibboleth installation. This testing system is not related to any other service or provider using SAML and is solely intended as a system to test shibboleth installations. Luminis Platform supports testing by use of TestShib with several of the steps already accomplished in the pre-delivered Luminis Platform Shibboleth.

Note: In the Luminis Platform 5.2 deployment, the Shibboleth server is installed as a component of the CAS tier. If an external Shibboleth server has already been integrated with Office 365 in your environment, and you choose to use external CAS configuration in your Luminis install, complete the steps in the "External CAS Installation and Configuration" chapter in the *Luminis Platform Installation Guide*, and integrate with your existing Shibboleth server, following the *JASIG Shibboleth-CAS Integration guide* at https://wiki.jasig.org/display/CASUM/Shibboleth-CAS+Integration

Once the external Shibboleth server is integrated with CAS, validate functionality using the TestShib steps.

Install PowerShell for access to remote online services

Windows PowerShell is a tool developed by Microsoft to allow for command line control of windows servers. Additional remote access `cmdlets` have been created that can be installed into standard PowerShell allowing remote access to Microsoft Azure online services.

Note: As PowerShell is a Microsoft product, and the `cmdlets` for PowerShell access to Office 365 online are also Microsoft products, they are neither installed nor supported by Ellucian.

For instructions on installing PowerShell, see http://technet.microsoft.com/en-us/library/hh847837.aspx.

For information about managing Microsoft online via PowerShell, see:

- http://technet.microsoft.com/en-us/library/jj151815.aspx

- http://social.technet.microsoft.com/Forums/windowsserver/

Note: The links on the Microsoft Web site are subject to change without notice.

Create Domain entries for SSO at Microsoft

Create managed domains at Microsoft for single sign-on (SSO) in Luminis Platform.

Procedure

1. Follow the steps on described on Microsoft.com (https://portal.microsoftonline.com/Domains/DomainManager.aspx) to create a domain name and domain name services entries, and to validate the domain.

   To link your domain to Microsoft Online Services, follow the steps outlined in the Microsoft Azure online Portal.

   Note: You must login to complete this task. To log in or create a new organizational account, see http://office.microsoft.com/en-us/office365-suite-help/set-up-your-organization-on-office-365-small-business-HA102818317.aspx.The links on the Microsoft Web site are subject to change without notice.

2. Login to the Microsoft Online Portal.
3. Once the domain is created and verified in the portal, convert the domain to a federated SSO domain. This happens from the PowerShell interface, because externally federated domains cannot be managed in the Microsoft Online portal.

   - If more than a single sub-domain is desired, then all domains must be created using PowerShell; the result of creating these domains in the portal is a lack of recognition by Office 365 that multiple domains are registered and users may accidentally cross domains during authentication, content retrieval and administration. The `new-MsolDomain` command must be used with the -*SupportMultipleDomains* flag.
   - Because federated domains are not directly manageable in the Microsoft portal, we recommend that you use the PowerShell command line to create new domains. To connect the new domain with Windows, enter the commands listed in "Install Powershell for access to remote online services." Then, enter the PowerShell command `New-MsolFederatedDomain -DomainName $dom -Confirm -SupportMultipleDomains` where the variable *$dom* is defined by `$dom = "<your domain name>"`.

     For example, `New-MsolFederatedDomain -DomainName $dom -Confirm -SupportMultipleDomains` where the variable *$dom* is defined by `$dom = "wasatch.edu"`

     Domain-related commands:

     ```
     $dom = "shib.ellucian.com"
     
     $url = https://shib.ellucian.com/idp/profile/SAML2/POST/SSO
     
     $ecpUrl = "https://shib.ellucian.com/idp/profile/SAML2/SOAP/ECP"
     
     $uri = "https://shib.ellucian.com/idp/shibboleth"
     ```

```
$logouturl = "https://shib.ellucian.com/idp/logoutredir.jsp"

$certData = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2

("C:\Users\Administrator\Desktop\base64_shib.cer")

$cert = [system.convert]::tobase64string($certdata.rawdata) Convert-
msolDomainToStandard -domainname $dom

Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName

$dom -Authentication Federated -PassiveLogOnUri $url -
SigningCertificate $cert -IssuerUri $uri -ActiveLogOnUri $ecpUrl -
LogOffUri $logouturl -PreferredAuthenticationProtocol SAMLP

Convert-msolDomainToFederated -domainname $dom
```

Results

If Shibboleth is configured to use non-standard ports using the `idp` properties, these ports must be present in all URLs relating to Shibboleth.

Related Links

Install PowerShell for access to remote online services on page 261

Install the new domain certificate into the metadata cache at Microsoft

When you create a new domain, the certificate used during Luminis Platform installation must be installed into the metadata cache at Microsoft. The certificate must match the one used by the Web server running Shibboleth.

About this task

To install the certificate:

Procedure

1. Use the commands listed in "Create Domain entries for SSO at Microsoft" to reference the certificate file. Click the certificate button in the URL bar to save the certificate file locally on the windows machine that is running PowerShell.
2. Once the file is saved onto the PowerShell machine, use the following certificate loading command:

   ```
   $certData = New-Object
   System.Security.Cryptography.X509Certificates.X509Certificate2
   ("C:\Users\Administrator\Desktop\base64_shib.cer")
   $cert = [system.convert]::tobase64string($certdata.rawdata)
   ```

   This command loads the certificate from the identified file, then converts the certificate into a 509 certificate for use in the PowerShell commands.

Link your domain to the Microsoft Azure online portal

Follow the steps on https://portal.microsoftonline.com/Domains/DomainManager.aspx to link your domain to Microsoft Online Services.

Note: You must log in to complete this task. To log in or create a new organizational account, see http://office.microsoft.com/en-us/office365-suite-help/set-up-your-organization-on-office-365-smallbusiness- HA102818317.aspx.The links on the Microsoft Web site are subject to change without notice.

ObjectGUID issue

When Microsoft Office 365 is configured, a Microsoft product called DirSync is used to provision accounts in the online system.

This DirSync product creates online accounts then synchronizes data with the user's Active Directory account, specifically updating the e-mail address and the ObjectGUID field. The account is created at outlook.com.

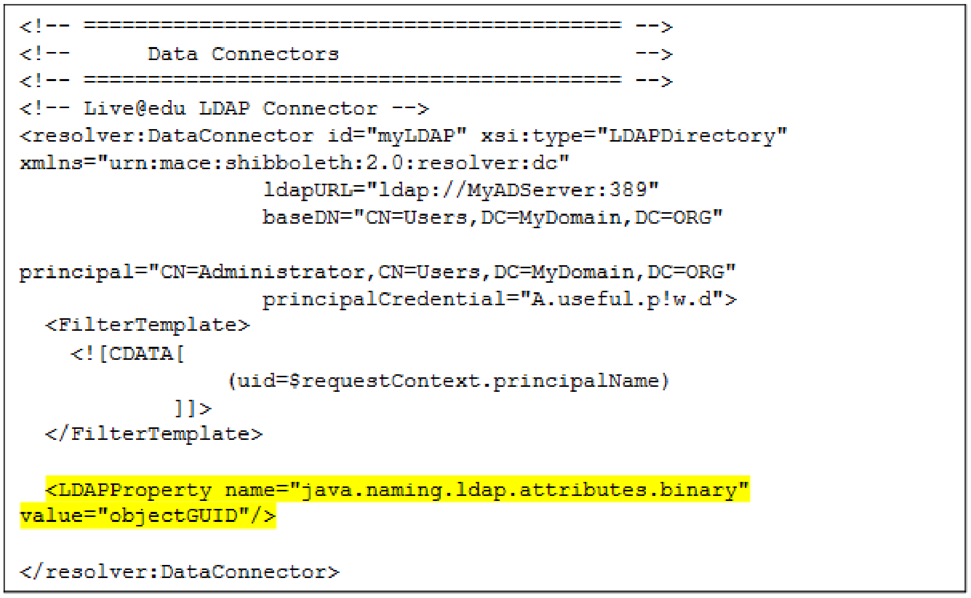
The resulting value is a globally unique identifier (GUID), a string of numbers and characters with dashes separating four groups of values to create a globally unique identifier. Modification of the Shibboleth deployment is required when setting up an Active Directory DirSync based deployment because DirSync base64 encodes the GUID value before storing it in the directory server.

The LDAP configuration in Shibboleth uses a binary field reader that has intrinsic operations to encode and decode base64 contents.

- If the field contains values that are encoded, it will decode
- If the contents are not encoded, they are encoded before they are sent
- If the following modification is omitted, the user's e-mail landing page will fail to render at Outlook but will succeed during SSO login:

  Add a single line to the `attribute-resolver.xml` file found at `CP_ROOT/products/shib-home/conf/attribute-resolver.xml`.

  Changes to the file should appear where the required change is highlighted below:



```
<!-- ========================================== -->
<!--      Data Connectors                       -->
<!-- ========================================== -->
<!-- Live@edu LDAP Connector -->
<resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory"
xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                   ldapURL="ldap://MyADServer:389"
                   baseDN="CN=Users,DC=MyDomain,DC=ORG"

principal="CN=Administrator,CN=Users,DC=MyDomain,DC=ORG"
                   principalCredential="A.useful.p!w.d">
  <FilterTemplate>
    <![CDATA[
                (uid=$requestContext.principalName)
            ]]>
  </FilterTemplate>

  <LDAPProperty name="java.naming.ldap.attributes.binary"
value="objectGUID"/>

</resolver:DataConnector>
```

Additional changes are required in the same file where the field name **udcid** is used in the attribute configuration. When using DirSync, the field name must be changed to objectGUID instead of udcid. This configuration is required for Luminis Platform testing and operations but should not be used in production.

For more information about Microsoft configuration using Shibboleth for single sign-on, see the Microsoft Web site.

Note: The links on the Microsoft Web site are subject to change without notice.

Integrate Office 365 mail and calendar integration using the Luminis Platform tools

To use the Luminis Platform tools for Office 365 mail integration, you must configure the **External Services Configuration** and **Luminis Mail Configuration** portlets.

Create a Microsoft Office 365 service

Use the **External Services Configuration** portlet to create a Microsoft Office 365 service.

Procedure

1. Login to Luminis Platform as an administrator.

   If needed, use the **Add** menu to add the **Luminis External Services Configuration** portlet to the Luminis Administrators Site.

2. In the **Luminis External Services Configuration** portlet, click the **External Services Configuration** link.

3. Click **New** to create a new Office 365 Service.
4. Select **Microsoft** in the **Type** drop-down list.
5. In the **Service Name** page, enter a name and a description for the Office 365 service.
6. In the **Domain** field, enter the fully qualified domain name for Microsoft Office 365. For example, `myuni.onmicrosoft.com`.
7. On the **Save Service** page, click **Save** to save all the details that you have entered.

   Luminis Platform displays the main page of the **External Services Configuration** portlet (listing all services).
8. **Optional:** Click **Edit** to modify and update the fields.
9. **Optional:** Click the **X** to delete a configuration.

   Warning! After Luminis user accounts have been linked with an external mail and calendar system such as Microsoft Office 365, you cannot delete any configurations used to link the external mail and calendar integration in the **Luminis External Services Configuration**, **Luminis Mail Configuration**, or **Luminis Calendar Configuration** portlet. If no users are linked with a selected configuration, then deletion is allowed.

Configure the Luminis/Office 365 calendar

Use the **Luminis Calendar Configuration** portlet to customize calendars for institutions and groups.

About this task

Note: The properties for displaying events in the **Luminis Calendar** portlet and the settings for Calendar provisioning will be disabled when the Calendar Service is set to use a Microsoft configuration.

Procedure

1. Use the **Add** menu to add the **Luminis Calendar Configuration** portlet to the Luminis Administrators Site.
2. In the **Luminis Calendar Configuration** portlet, click on the **Calendar Configuration** link.

   Note: You must have created an external service configuration before creating a calendar configuration.
3. In the **Luminis Calendar Configuration** portlet, click **New**.
4. In the **Create New Calendar Configuration** page, enter the mandatory fields.

Field	Description
Name	A short name to identify the configuration (User Defined, Free Text).

Field	Description
Calendar Service	Service defined in the **External Services Configuration** portlet. The items in the drop-down list are generated from the setup completed using the **External Services Configuration** portlet. Each new service you create will now be available here.
Description	More descriptive name (User Defined, Free Text).
Application URL	The URL used to access the calendar application at Office 365. For example, `https://login.microsoft.calendar.com`
Application Logout URL	The URL Luminis uses, to ensure proper logout from Office 365 calendar. The Logout URL is `https://login.microsoft.calendar.com/logout.`

5. Click **Save**.

   Note: **Manage Calendar Configuration** tab is used to create, edit, validate, and delete all calendar configurations.

6. In the **Manage Calendar Configuration** tab, click **Edit or Double-click the name to edit calendar configuration.**
7. Click **Validate** to test the single sign-on settings.

   This process will attempt to launch the Office 365 calendar application using the value from the application URL field in a new browser window using the currently logged in Luminis user credentials.
8. Click **Delete** to delete a calendar configuration.

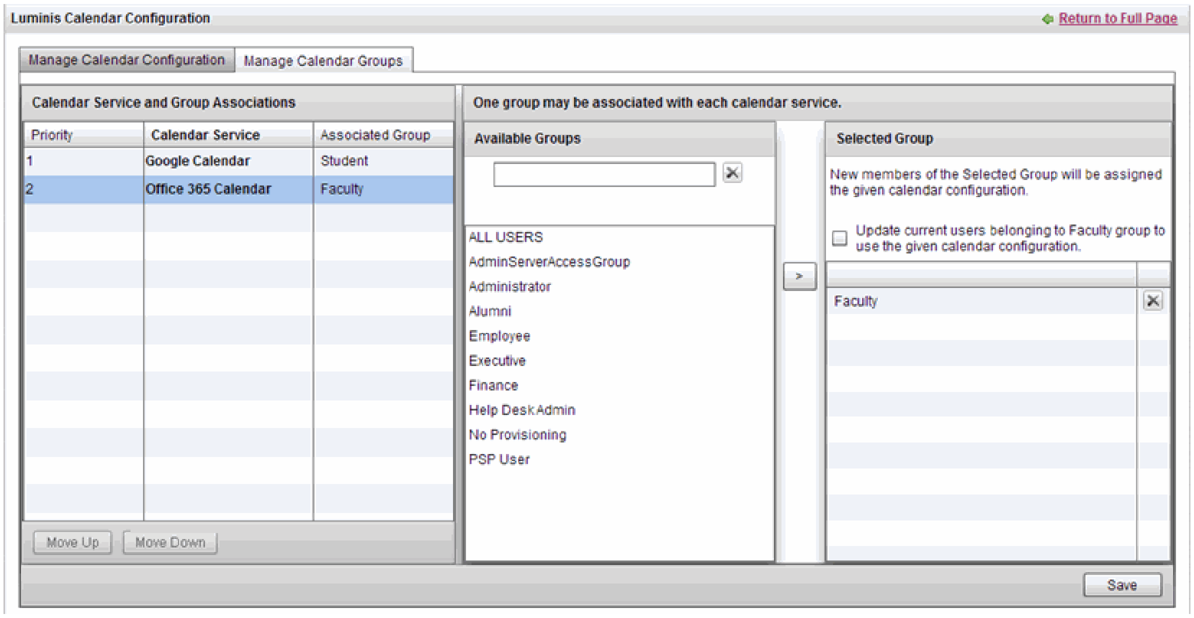
   Note: After Luminis user accounts have been linked with an external calendar system such as Microsoft Office 365, you cannot delete any configurations used to configure the calendar integration in the **Luminis Calendar Configuration** portlet.

Assign a dynamic group to an Office 365 calendar configuration

Assign a Luminis dynamic group to one or more calendar configurations.

Procedure

1. In the **Luminis Calendar Configuration** portlet, select the **Manage Calendar Groups** tab.


Luminis Calendar Configuration
Return to Full Page
Manage Calendar Configuration
Manage Calendar Groups
Calendar Service and Group Associations
Move Up
Move Down
One group may be associated with each calendar service.
Available Groups
Selected Group
>
Save

Priority	Calendar Service	Associated Group
1	Google Calendar	Student
2	Office 365 Calendar	Faculty

Available Groups: ALL USERS, AdminServerAccessGroup, Administrator, Alumni, Employee, Executive, Finance, Help Desk Admin, No Provisioning, PSP User

New members of the Selected Group will be assigned the given calendar configuration.

□ Update current users belonging to Faculty group to use the given calendar configuration.

Selected Group: Faculty ☒

2. Click to highlight a calendar configuration from the **Calendar Service and Group Association** box.
3. Double-click the desired group in the **Available Groups** box.

   Warning! If the selected calendar configuration already has a group associated, click the **X** next to the group to remove before you select a new group.

   The members of the Selected Group will be assigned to a given calendar configuration under **Selected Group** box.

   Note: You can only add one group to the **Selected Group** column. If a group matching the rules you require does not already exist in the list available groups, you must use the **Luminis Group Manager** to create a new group.

4. Mark the **Update current users belonging to [selected group] to use the given calendar configuration** check box to update the calendar for all users in the selected group. If the box is left unchecked, Luminis users who belong to the group will remain connected to their current calendar configuration.

   Note: The check box is only enabled when you add a group to the **Selected Group** list. After a **Save**, the option and check box are disabled. If you make an additional change, such as removing the selected group and adding another, the check box is re-enabled.

5. Click **Save** to save the changes.

   If you have multiple calendar configurations assigned to multiple groups, they must be given a priority for the Luminis system to use when configuring user accounts with the external calendar provider system.

   If there is a calendar configuration named Student, which is associated with a Student group, and a calendar configuration named Faculty associated with the Faculty group. If a new user is added to Luminis that belongs to both the Student and Faculty groups, the system would use the priority to determine which calendar configuration to use to configure the new user account in Office365.

Configure Luminis/Office 365 e-mail

Use the **Luminis Mail Configuration** portlet to configure e-mail for your institution.

Procedure

1. Using the **Add** menu, add the **Luminis Mail Configuration** portlet to your page.
2. In the **Luminis Mail Configuration** portlet, click the **Mail Configuration** link.

   Note: You must have created an external service configuration before creating a mail configuration.

3. In the **Luminis Mail Configuration** portlet, click **New**.
4. Enter the fields as needed.

   Table 21: Mandatory Mail Configuration portlet fields

Field	Description
Name	A short name to identify the configuration (User Defined, Free Text).
Mail Services	Service defined in the **External Services Configuration** portlet. The items in the drop-down list are generated from the setup completed using the **External Services Configuration** portlet noted above. Each new service you created will now be available here.
Description	More descriptive name (User Defined, Free Text).
Application URL	The URL used to access the e-mail application at Office 365. For example, `https://outlook.com/owa/<testlp5>.wasatch.com`
Application Logout URL	The URL Luminis uses to ensure proper logout from Office 365 e-mail. For examples, see the following options: • `https://outlook.com/owa/auth/logoff.aspx?Cmd=logoff&src=exch` • `https://outlook.com/owa/<testlp5>.wasatch.com`

5. Click **Save**.

6. In the **Manage Mail Configuration** tab, click **Edit or Double-click the name to edit a mail configuration.**

   The **Manage Mail Configuration** tab is used to create, edit, validate, and delete all mail configurations.

7. Click **Validate** to test the Single Sign-On settings.

   This process will attempt to launch the Office365 e-mail application using the value from the application URL field in a new browser window using the currently logged in Luminis user credentials.

   Note: To validate in an Internet Explorer 10 or 11 browser window, you must first import the certificate into the local certificate store. Otherwise, the validation test will fail.

8. Click **Delete** to delete a mail configuration.

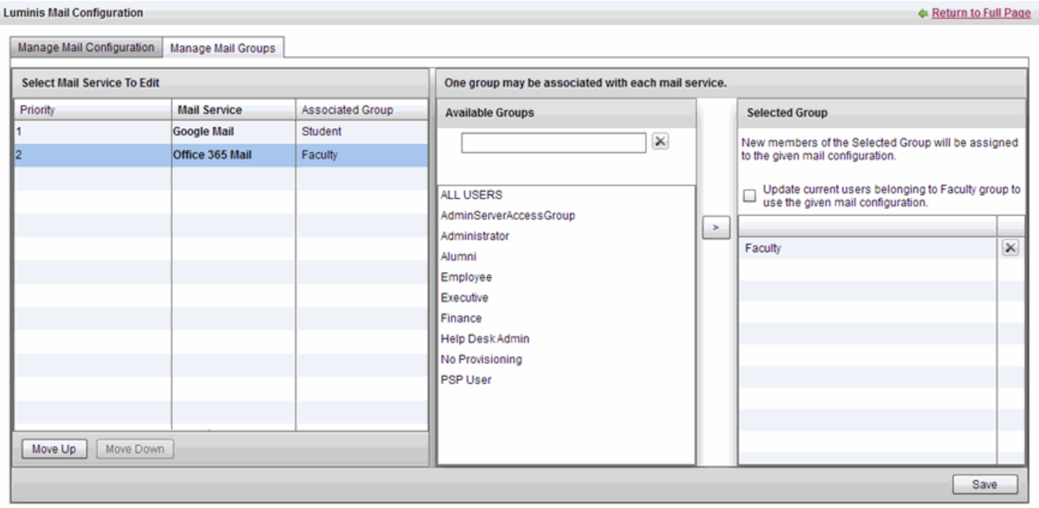
   Warning! After Luminis user accounts have been linked with an external mail system such as Microsoft Office 365, you cannot delete any configurations used to configure the mail integration in the **Luminis Mail Configuration** portlet.

Assign a Luminis dynamic group to an Office 365 calendar configuration

Use the **Luminis Mail Configuration** portlet to assign a Luminis dynamic group to a mail configuration.

Procedure

1. In the **Luminis Mail Configuration** portlet, select the **Manage Mail Groups** tab.



Luminis Mail Configuration

Select Mail Service To Edit

Priority	Mail Service	Associated Group
1	Google Mail	Student
2	Office 365 Mail	Faculty

One group may be associated with each mail service.

Available Groups

ALL USERS
AdminServerAccessGroup
Administrator
Alumni
Employee
Executive
Finance
Help Desk Admin
No Provisioning
PSP User

Selected Group

New members of the Selected Group will be assigned to the given mail configuration.

☐ Update current users belonging to Faculty group to use the given mail configuration.

Faculty

2. Select a mail configuration from the **Select Mail Service to Edit** box.
3. Double-click on the desired group in the left panel, **Available Groups** box.

Warning! If the selected mail configuration already has a group associated, use the **X** icon next to the group to remove before selecting a new group.

Note: You can only add one group to the **Selected Group** column. If a group matching the rules you require does not already exist in the list available, you must use the **Luminis Group Manager** to create a new group.

The members of the Selected Group will be assigned to a given mail configuration under **Selected Group** box.

4. Mark the **Update current users belonging to [selected group] to use the given mail configuration** check box to update the mail for all users in the selected group. If the box is left unchecked, Luminis users who belong to the group will remain connected to their current mail configuration.

   Note: The check box is only enabled when you add a group to the **Selected Group** list. After a **Save**, the option and check box are disabled. If you make an additional change, such as removing the selected group and adding another, the check box is re-enabled.

5. Click **Save** to save the changes.

   If you have multiple mail configurations assigned to multiple groups, they must be given a priority for the Luminis system to use when configuring user accounts in the external e-mail provider system.

   Note: Luminis Platform does not provision Microsoft Office 365 accounts.

   Warning! For the current iteration of Office 365, Luminis Platform does not support the **Mail** and **Calendar** portlets.

   If there is an e-mail configuration named Student, which is associated with a Student group, and an e-mail configuration named Faculty associated with the Faculty group. If a new user is added to Luminis that belongs to both the Student and Faculty groups, the system would use the priority to determine which e-mail configuration to use to configure the new user account in Office365.

Related Links

Luminis mail configuration using Office 365 on page 259

Confirm the CAS server is configured for Office 365 single sign-on

Validate that the CAS server is configured properly for Office365 single sign-on (SSO).

Procedure

1. Log into the CAS Management page: `https://<cas server>:<port>/cas-web/services/manage.html`
2. If necessary, add the Office365 domain to the Service URL for Office365.

For example, if `wasatch.school.com` is the Office365 domain, the Service URL would be `https://wasatch.school.com/idp/**.`

Automatically connect Luminis users to Microsoft accounts

If the Luminis Platform system has been integrated with Microsoft, new Luminis users are automatically assigned a Microsoft e-mail address using the configured domain.

You can create a new user in Luminis with one of these methods:

- User Management portlet
- IMS file importer
- LDI person event

Once you create a new user, the user is assigned a Microsoft e-mail address based on the user's Email ID.

In addition, existing users are also assigned a Microsoft e-mail address when you use the methods listed above to update the users.

Integrate Learning Management Systems with Luminis Platform

Luminis® Platform provides single sign-on to Blackboard and Moodle external learning management systems (LMS) via CAS configuration and authentication.

The LMS enhancements are supported by a step-by-step configuration process completed directly through the **External Configuration Services** portlet.

The LMS feature also includes an easy-to-use interface in the **My Courses** portlet for instructor and teaching assistants to configure each course for single sign-on to integrated external learning management systems.

In order to integrate the LMS with Luminis Platform, the Luminis Platform admin user must first configure their LMS to enable single sign-on (SSO) through the Luminis Platform CAS server. Next, the admin user creates an LMS service in the **External Services Configuration** portlet, with their institution's property values. Finally, the instructors for each of the courses choose the LMS service they need for the **My Courses** portlet for their course.

Create an LMS service

Once the single sign-on (SSO) is enabled, the Luminis Platform admin user creates an LMS service in the External Services Configuration portlet.

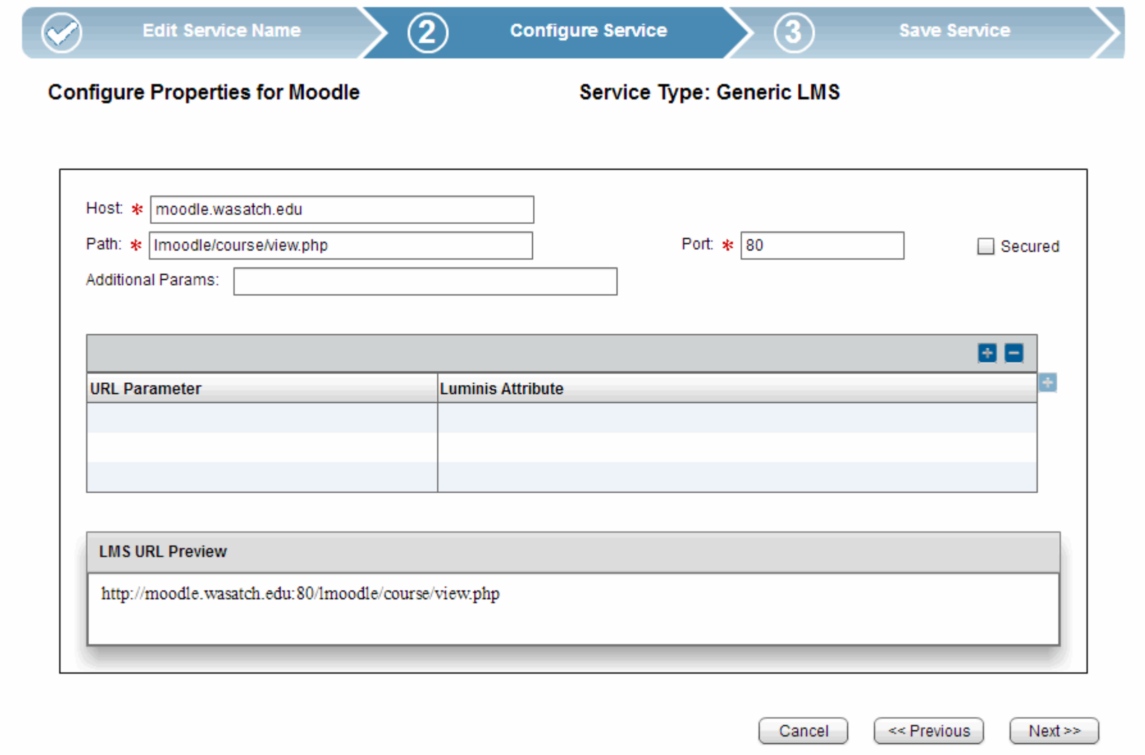
Procedure

1. Login to Luminis Platform as an administrator and navigate to the **Luminis External Services Configuration** portlet and the Luminis Administrators Site.
2. In the **Luminis External Services Configuration** portlet, click **External Services Configuration**.
3. Click **New**.
4. Select an LMS option from the **Type** drop-down list. These LMS options are available:
   - Blackboard 9.x
   - Generic LMS
   - Moodle 2.x

   Note: The LMS external service configuration defines the URL that the system will use to access the LMS for SSO. If you choose either type Blackboard 9.x or Moodle 2.x, the generated URL pre-populates with default URL paths and parameters as known at the time of the most recent Luminis Platform. If you must access the Blackboard or Moodle system with a URL path or additional parameters other than the default, or if future releases of Blackboard or Moodle changes the URL path or parameters, then choose the Generic LMS and configure the URL path and parameters appropriately. Other options in the drop-down list, such as Google and Microsoft, are intended for mail and calendar integration.

5. Enter a name and a description for the LMS service in the **Edit Service Name** page.
6. Click **Next**.

   The **Configure Service** page displays for Moodle or Generic.



Configure Properties for Moodle

Service Type: Generic LMS

Host: * moodle.wasatch.edu

Path: * lmoodle/course/view.php

Port: * 80

□ Secured

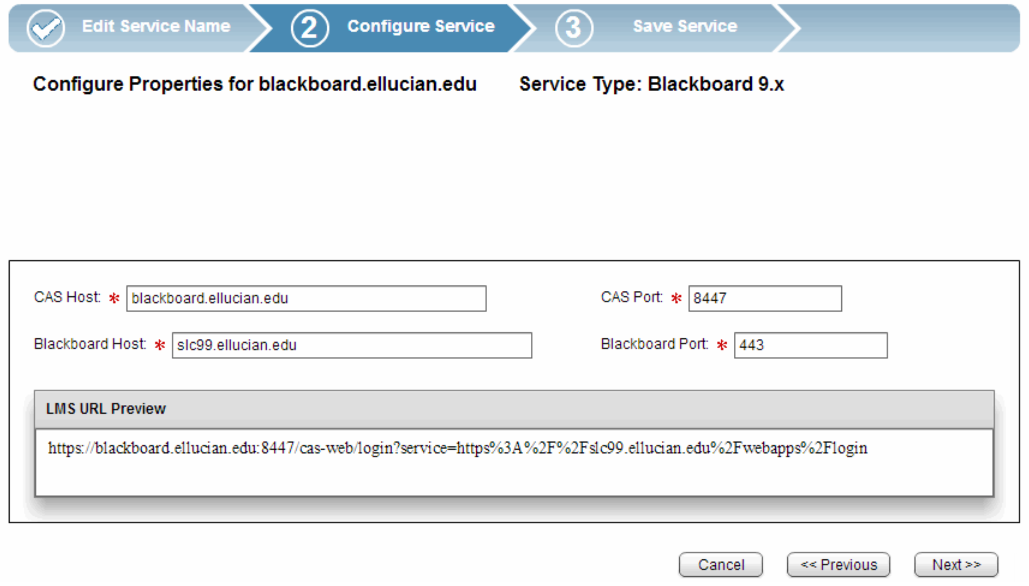
Additional Params:

URL Parameter	Luminis Attribute

LMS URL Preview

http://moodle.wasatch.edu:80/lmoodle/course/view.php

The **Configure Service** page displays for Blackboard Learn.



Configure Properties for blackboard.ellucian.edu

Service Type: Blackboard 9.x

CAS Host: * blackboard.ellucian.edu

CAS Port: * 8447

Blackboard Host: * slc99.ellucian.edu

Blackboard Port: * 443

LMS URL Preview

https://blackboard.ellucian.edu:8447/cas-web/login?service=https%3A%2F%2Fslc99.ellucian.edu%2Fwebapps%2Flogin

7. Enter the properties for the LMS service. Enter all of the information the system needs in order to build the URL to a specific course within the LMS system. The URL will display in the **LMS URL Preview** box.

Table 22: LMS fields

Field	Description
Additional Params	URL parameters for which the value is not stored in Luminis.
Blackboard Host	The server hostname for the LMS instance created using Blackboard Learn. For example: blackboard.wasatch.edu **Note:** The host name of the Luminis CAS server should be the same CAS server with which the Blackboard 9.x Learn system is integrated.
Blackboard Port	The port number for the URL.
CAS Host	The hostname for the CAS server.
CAS Port	The number for the CAS port.
Host	The server hostname for the LMS instance.
Path	The URL path to a course in the LMS. • For Generic, the LMS default is empty. • For Moodle, the default is /moodle/course/view.php
Port	The port number for the URL. For Moodle, the default is port 80.
Secured	For a secured Web site, mark the check box. A secured Web site displays as https. A non-secure Web site displays as http.

8. The URL Parameter grid allows the user to map parameters on the URL to specific attributes within Luminis. Each row in the grid is a parameter on the URL.

   - To add a URL parameter, click the add icon:⊞
   - To remove a URL parameter, click the remove icon:⊟

   a) In the **URL Parameter** box, enter the name of the URL parameter.

   b) In the **Luminis Attribute** box, select the name of the attribute in Luminis to be mapped to the parameter.

   c) **Optional:** To create a single URL parameter using multiple Luminis attributes, click the add icon to the right of the **Luminis Attribute** column. A separator column and a second

Luminis Attribute column will be added to the grid. You can add up to three **Luminis Attribute** columns.

The default parameter for Blackboard anticipates multiple attributes. The *course_id* URL parameter uses two Luminis Attributes in its mapping:

- Course Reference Number
- Course Term Number - separated by a dot.

The result in the URL is as follows:

```
course_id=<Course Reference Number.Course Term Number>
```

Table 23: URL parameter mapping attributes

Field	Description
Course Department ID	Provided in the IMS import file. **Note:** The import file is generated by the admin from Banner®. The admin creates the XML file using Banner tools and then uses that XML file to populate within Luminis Platform. For information about importing the IMS file, see "Import LDISP or IMS data with jconsole."
Course ID	Provided in the IMS import file.
Person UDC ID	Provided in the IMS import file.
Course Reference Number	The course ID concatenated with the course section separated by a dot.
Person Login ID	Luminis Platform user login ID.
Person Static ID	The immutable ID assigned to a Luminis user when the user profile is created.
Course Term Number	Provided in the IMS import file.
Course Section ID	Provided in the IMS import file.

9. Click **Next**.

   Luminis Platform automatically sends a request to the hostname and port provided to validate the name and port properties. The results will display on the **Save Service** page. The path, additional params, and attribute mappings properties cannot be validated.

10. On the **Save Service** page, click **Save** to save all the details that you have entered.

    Note: You can save the properties regardless of whether the validation succeeds or fails. However, the **Save** button will be disabled until the results of the validation are returned.

    Luminis Platform displays the main page of the **External Services Configuration** portlet, listing all services.

Note: If you configure a Moodle or Blackboard service, additional configurations are required.

11. **Optional:** Click **Edit** or double-click the service in the grid to modify and update the fields.

Related Links

Integrate Google with Luminis Platform on page 238
Integrate Microsoft Office 365 with Luminis Platform on page 258
Import LDISP or IMS data with jconsole on page 31
Configure a Moodle service on page 283
Configure a Blackboard service on page 280
Configure a Moodle service on page 283

LMS association during import

You can automatically assign an LMS to a coursesection group using an extension node with this form:

```
<extension>
    <luminisgroup>
        <deliverysystem>myValidLMSSystem</deliverysystem>
    </luminisgroup>
</extension>
```

This section provides example codes that include LMS associations during the import process. The deliverysystem attribute value is freeform text which must match the name of an existing LMS.

- To import successfully, enter a code similar to:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE enterprise SYSTEM "ldisp-2.0.dtd">
<enterprise>
    <properties>
        <datasource>SUNGARDHE University SCT Banner</datasource>
        <datetime>2004-01-01</datetime>
    </properties>
    <group recstatus="2">
        <sourcedid>
            <source>SUNGARDHE University SCT Banner</source>
            <id>200250</id>
        </sourcedid>
        <grouptype>
            <scheme>Luminis</scheme>
            <typevalue level="1">term</typevalue>
        </grouptype>
        <description>
            <short>200250</short>
            <long>Summer Quarter 2002</long>
        </description>
        <timeframe>
            <end restrict="0">2002-08-16</end>
        </timeframe>
        <enrollcontrol>
            <enrollaccept>0</enrollaccept>
        </enrollcontrol>
        <extension>
            <luminisgroup>
                <sort>200250</sort>
            </luminisgroup>
        </extension>
    </group>
    <group recstatus="2">
        <sourcedid>
            <source>SUNGARDHE University SCT Banner</source>
            <id>1070.200250</id>
        </sourcedid>
        <grouptype>
            <scheme>Luminis</scheme>
            <typevalue level="2">coursesection</typevalue>
        </grouptype>
        <description>
            <short>1070</short>
            <long>LIS-4700-2</long>
            <full>Tpc Public Libraries</full>
        </description>
        <org>
            <orgunit>Library &amp; Information Science</orgunit>
        </org>
        <relationship relation="1">
            <sourcedid>
                <source>SUNGARDHE University SCT Banner</source>
                <id>200250</id>
            </sourcedid>
            <label>term</label>
        </relationship>
        <extension>
            <luminisgroup>
                <deliverysystem>myValidLMSSystem</deliverysystem>
            </luminisgroup>
        </extension>
    </group>
</enterprise>
```

- To delete the LMS association, import a file with a new extension similar to:

```
        <extension>
            <luminisgroup>
                <events>
                    <recurringevent>
                        <eventdescription>Course Meeting Time</
eventdescription>
                        <begindate>2002-06-17</begindate>
                        <enddate>2002-07-08</enddate>
                        <daysofweek>M</daysofweek>
                        <begintime>16:00</begintime>
                        <endtime>18:30</endtime>
                        <location>STURM 124</location>
                    </recurringevent>
                </events>
            </luminisgroup>
        </extension>
```

- To update the code to navigate to a different valid LMS, use an extension similar to:

```
        <extension>
            <luminisgroup>
                <deliverysystem>myUpdatedValidLMSSystem</
deliverysystem>
            </luminisgroup>
        </extension>
```

Choose the LMS service for the My Courses portlet

After the administrator configures the LMS service in Luminis Platform, instructors for each of the courses can choose the LMS service they want to use for their course in the **My Courses** portlet. When a course is configured to use an LMS service the site home page for that course in Luminis automatically navigates to the URL within the LMS system for that course. In addition, when a student clicks the home icon for the course in their **My Courses** portlet, the student is automatically signed into the LMS system and the course page displays. 🏠

About this task

Note: If the course is configured to use Blackboard, users are directed to the Blackboard Learn main page instead of the course’s main page.

Instructors will use the **My Courses** portlet to choose an LMS service for a specific course.

Warning! If you configured a Moodle service, you must configure CAS before the instructors can select a Moodle LMS page in the **My Courses** portlet.

Procedure

1. Log into Luminis Platform and navigate to **My Courses**.
2. Under the "Courses I'm Teaching" header, select the LMS config icon next to a course: 🔧

   The LMS config icon should only appear if an External LMS service is configured in the **External Configuration Services** portlet. The icon also only appear for the instructor to set up the LMS for any course.
3. In the **LMS Configuration** page, mark the radio button for the LMS service you choose.

   The default LMS service is Luminis Site. This option indicates that the home page will be the default Luminis Site home page for that course because no external LMS service was applied.
4. Click **Save**.

Related Links

Configure a Moodle service on page 283

Configure a Blackboard service

Luminis Platform 5.x offers single sign-on (SSO) integration with the Blackboard Learn 9.x system. This includes the ability for students and instructors to SSO to the Learn system and access the correlating Learn home page.

After you configure an integration with Learn, the default Blackboard values automatically populate in the **Configure Services** page. The host name of the Luminis CAS server should be the same CAS server with which the Blackboard 9.x Learn system is integrated. Enter in the host name of the Blackboard Learn system. If either CAS or Blackboard servers are running on different ports than the default, change the port fields to reflect the correct ports.

Note: When the user completes a Blackboard user session, the user must log out of Blackboard. Failure to do so allows subsequent users who use the same browser and computer to remain logged into Blackboard with the previous user's credentials.

If you log out of Blackboard, then click on the **Home** icon without logging out of Luminis Platform, the CAS login page displays. Enter your user name and credentials to access Blackboard.

Related Links

Create an LMS service on page 273

Add the Blackboard service URL to CAS

After you have configured the Blackboard Learn LMS within Luminis Platform, add your Blackboard service URL to CAS.

Procedure

1. Log into CAS.
2. Navigate to the **Manage Services** page.
3. Click **Add New Service**.
4. Add your Blackboard Learn service URL.

   The service URL will appear similar to the following, where <*your Blackboard host*> is the fully qualified host name of your Blackboard Learn system:

   ```
   https://<your Blackboard Host>/webapps/login*
   ```

Configure Blackboard SSO with Luminis Platform

To configure Blackboard Lean to single sign-on (SSO) with Luminis, you must ensure that the affected users and courses are either created or imported into Blackboard.

Import users into Blackboard

A user profile must be created or imported into the Blackboard Learn system for each student and faculty member that you want to access Blackboard Learn.

See the Blackboard documentation for information on how to complete bulk imports.

Note: The following operations are performed with Blackboard Learn as your Administration user.

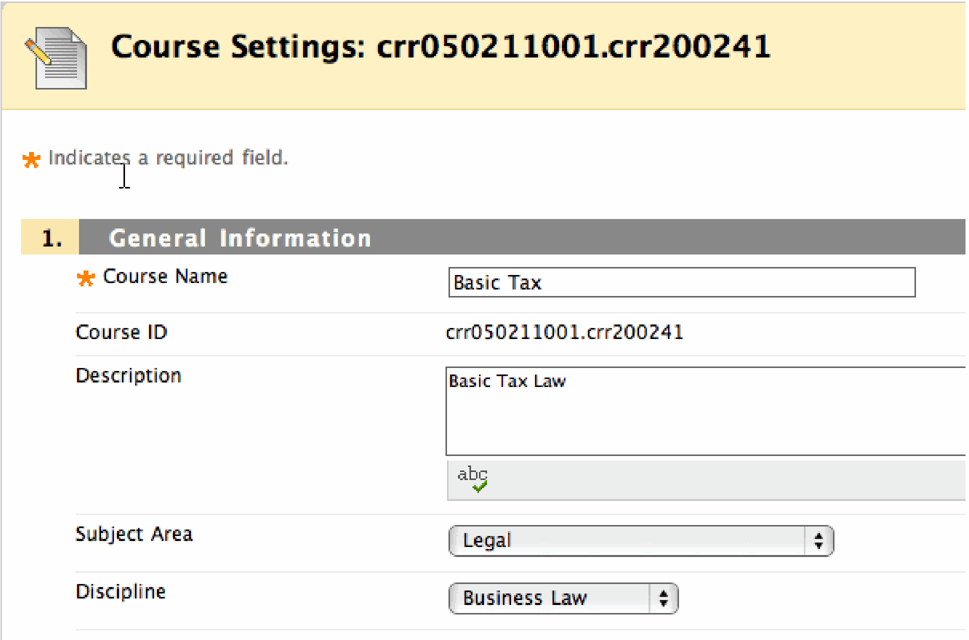
For Luminis Platform to be able to single sign-on to Blackboard Learn, the Username fields must match the login ID of the user in Luminis. If you import the users in Luminis Platform via the IMS importer, the Learn Username must match the userId of type Login Id of the user. In the example below, the user name is myloginid.

The IMS snippet for the user is as follows:

```
<person recstatus="1">
    <sourcedid>
      <source>WASATCH University SCT Banner</source>
      <id>crr050211.103</id>
    </sourcedid>
    <userid useridtype="Logon ID" password="l3tm31n">myloginid</userid>
    <userid useridtype="Email ID" password="l3tm31n">myemailid</userid>
    <userid useridtype="SCTID" password="l3tm31n">crr050211.usr103</
userid>
    <name>
…
```

Import course IDs into Blackboard

Your Blackboard Learn Course IDs must match the CRN.Term ID pair from your Banner system.



Course Settings: crr050211001.crr200241

* Indicates a required field.

1. General Information

* Course Name: Basic Tax

Course ID: crr050211001.crr200241

Description: Basic Tax Law

Subject Area: Legal

Discipline: Business Law

In this example, the IMS snippet would appear as follows:

```
<group recstatus="2">
    <sourcedid>
        <source>SUNGARDHE University SCT Banner</source>
        <id>crr050211001.crr200241</id>
    </sourcedid>
    <grouptype>
        <scheme>Luminis</scheme>
        <typevalue level="2">coursesection</typevalue>
    </grouptype>
    <description>
        <short>crr050211001</short>
        <long>LAWS-4100-1</long>
        <full>Basic Tax</full>
    </description>
    <org>
        <orgunit>College of Law</orgunit>
    </org>
…
```

The CRN.TermID for the above course can be found in the sourcedid id node.

Configure Blackboard courses

Once an instructor has selected Blackboard Learn for a given course, the Home icon for the course single signs members on to the Blackboard Learn system and navigates to the Blackboard Learn home page.

Once you have configured your courses in your Blackboard Learn system and have created an integration for the Learn system, your instructors can setup their courses to access the Learn system.

Related Links

Choose the LMS service for the My Courses portlet on page 279

Configure a Moodle service

If you configure a Moodle service, additional configurations are required to the CAS server, single sign-on (SSO), and courses to support a Moodle environment.

Moodle integration supports linking users directly to Moodle LMS course pages. Blackboard integration links users to the Blackboard Home page which then offers the course schedule and links. Moodle is one-click access to course pages. Blackboard is two-click access.

The default Moodle values automatically populate in the **Configure Services** page.

Note: When a user SSO's into Moodle, it is important that the user logs out of Moodle before closing the Moodle window when they finish. If they do not log out, Moodle will remember the user's session. Consequently, the next user that logs in and attempts to access the same course on the same computer will log in as the first user.

Related Links

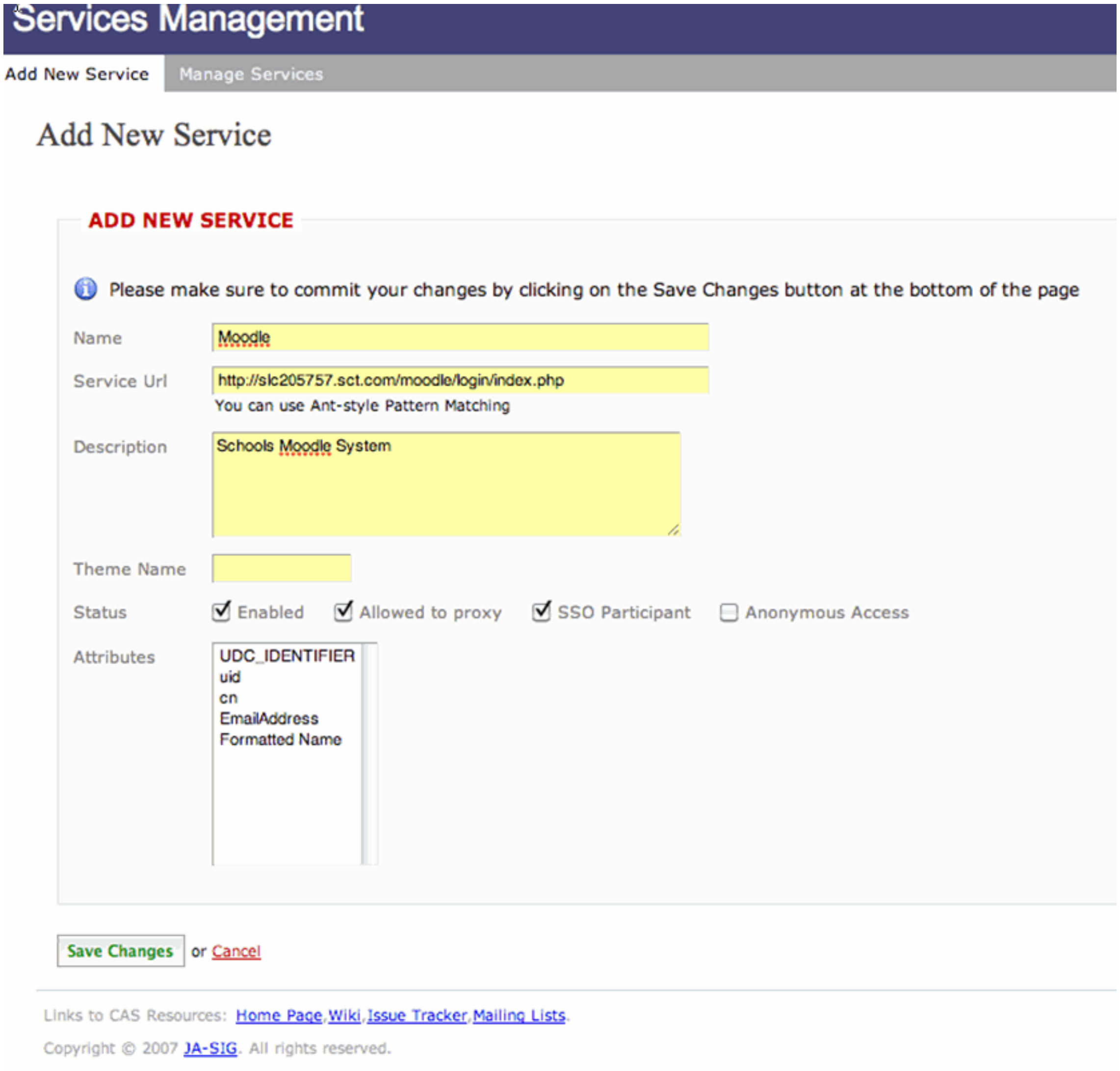
Create an LMS service on page 273

Add the Moodle service URL to CAS

After you have configured the Moodle LMS within Luminis Platform, add your Moodle service URL to CAS.

Procedure

1. Log into CAS.
2. Navigate to the **Manage Services** page.
3. Click **Add New Service**.
4. Add your Moodle service URL to CAS.



Add New Service

ADD NEW SERVICE

Please make sure to commit your changes by clicking on the Save Changes button at the bottom of the page

Name	Moodle
Service Url	http://slc205757.sct.com/moodle/login/index.php You can use Ant-style Pattern Matching
Description	Schools Moodle System
Theme Name	
Status	☑ Enabled ☑ Allowed to proxy ☑ SSO Participant □ Anonymous Access
Attributes	UDC_IDENTIFIER uid cn EmailAddress Formatted Name

Links to CAS Resources: Home Page, Wiki, Issue Tracker, Mailing Lists.

Copyright © 2007 JA-SIG. All rights reserved.

Service URL:

```
http://<host name>/moodle/login/index.php
```

In this example, <*host name*> is the fully qualified host name of your Moodle server.

Note: Depending on the Moodle configuration, the `/moodle` piece of the URL may not be needed.

Configure Moodle for SSO in Luminis Platform

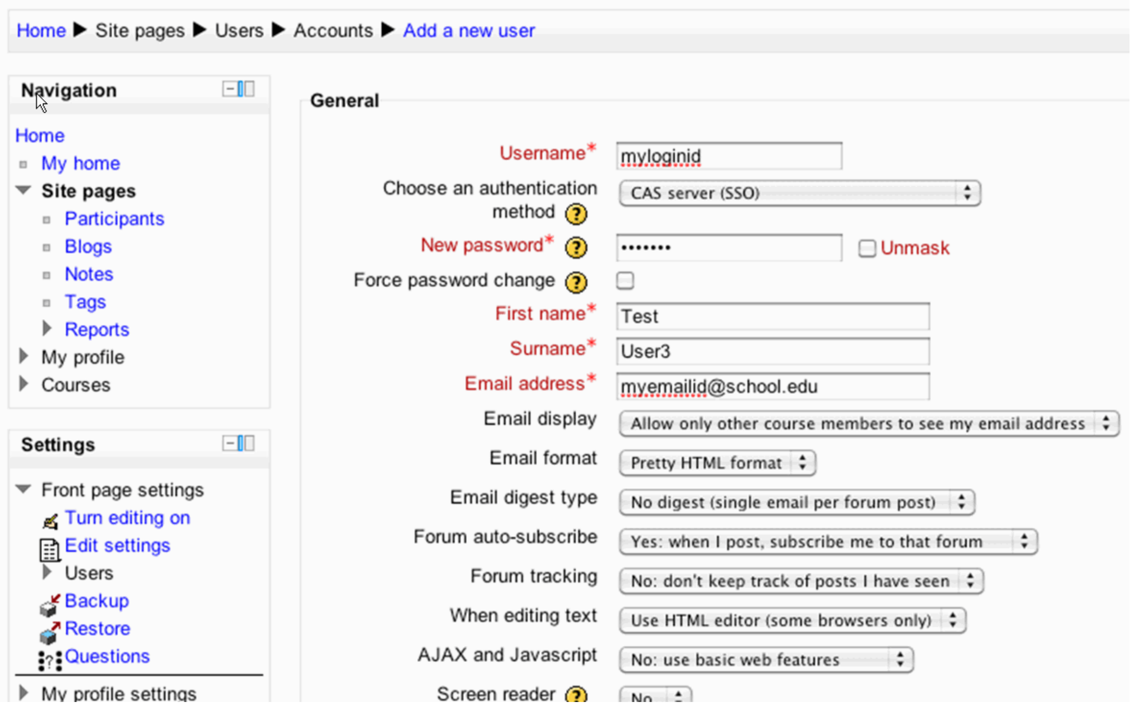
To configure Moodle to single sign-on (SSO) with Luminis, you must ensure that the affected users and courses are either created or imported into Moodle.

Import users into Moodle

Create or import all of your student and instructor logins in Moodle.

For single sign-on to work properly for these users within Luminis Platform, the **Username** field in Moodle must match the login ID of the user in Luminis Platform. If you import the users in Luminis Platform via the IMS importer, you will want the Moodle **Username** value to match the `userId` of type Login ID of the user.

For example, if the username is myloginid, enter the account information as follows:



General

Username* mylogininid

Choose an authentication method CAS server (SSO)

New password* ••••••• □ Unmask

Force password change □

First name* Test

Surname* User3

Email address* myemailid@school.edu

Email display Allow only other course members to see my email address

Email format Pretty HTML format

Email digest type No digest (single email per forum post)

Forum auto-subscribe Yes: when I post, subscribe me to that forum

Forum tracking No: don't keep track of posts I have seen

When editing text Use HTML editor (some browsers only)

AJAX and Javascript No: use basic web features

Screen reader No

The corresponding section of the IMS import file displays as follows:

```
<person recstatus="1">
 <sourcedid>
      <source>WASATCH University SCT Banner</source>
      <id>crr050211.103</id>
    </sourcedid>
    <userid useridtype="Logon ID" password="l3tm31n">myloginid</userid>
    <userid useridtype="Email ID" password="l3tm31n">myemailid</userid>
    <userid useridtype="SCTID" password="l3tm31n">crr050211.usr103</
userid>
    <name>
```

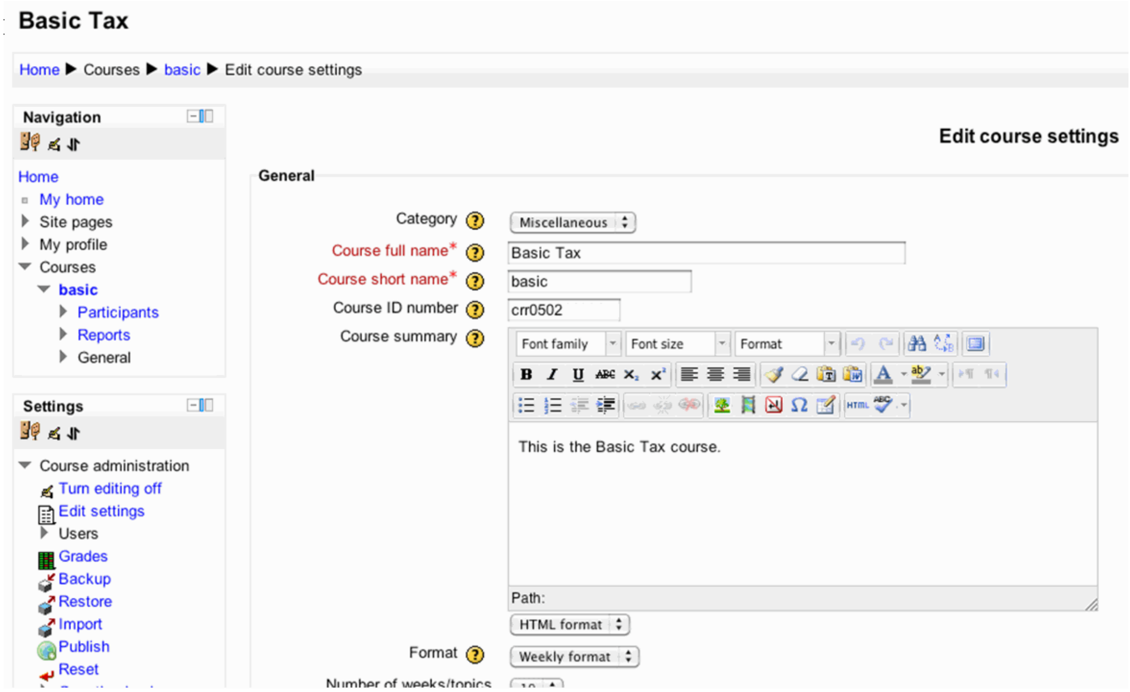
```
        <fn>crr050211.usr103</fn>
```

Import courses into Moodle

In addition to configuring the user accounts in Moodle, create or import the courses in Luminis Platform that you want to use Moodle system. All of the membership information in Moodle must match the information in Luminis Platform.

For the courses included in Moodle, ensure that your Moodle Course ID Number value matches the `CRN.TermID` of the Luminis course.

For example, `CRN.TermID` for the above course is the sourcedid ID node:



Basic Tax

Home ▶ Courses ▶ basic ▶ Edit course settings

Edit course settings

General

Category: Miscellaneous

Course full name*: Basic Tax

Course short name*: basic

Course ID number: crr0502

Course summary: This is the Basic Tax course.

Path:

HTML format

Format: Weekly format

Number of weeks/topics

The corresponding section of the IMS import file displays as follows:

```
 <group recstatus="2">
     <sourcedid>
         <source>WASATCH University SCT Banner</source>
         <id>crr050211001.crr200241</id>
     </sourcedid>
     <grouptype>
         <scheme>Luminis</scheme>
         <typevalue level="2">coursesection</typevalue>
     </grouptype>
     <description>
         <short>crr050211001</short>
         <long>LAWS-4100-1</long>
         <full>Basic Tax</full>
     </description>
```

```
        <org>
            <orgunit>College of Law</orgunit>
        </org>
   …
```

Configure the Moodle, Luminis, and CAS Logout

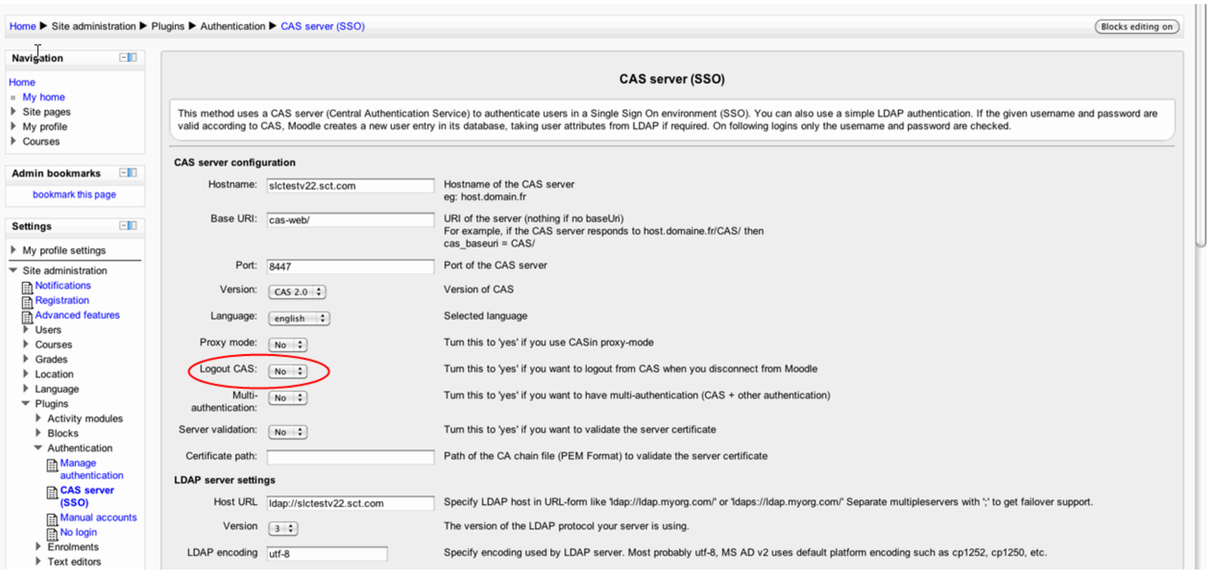
When you configure Moodle to run with CAS, you have the option to change the default setting.

About this task

By default, when you logout of Moodle, Moodle will logout of CAS as well. This also causes you to log out of Luminis Platform. Prevent the Moodle session from logging out at the same time you log out of the CAS session.

Procedure

1. Within Moodle, navigate to **Site administration** > **Plugins** > **Authentication** > **CAS server (SSO)**.



CAS server (SSO)

This method uses a CAS server (Central Authentication Service) to authenticate users in a Single Sign On environment (SSO). You can also use a simple LDAP authentication. If the given username and password are valid according to CAS, Moodle creates a new user entry in its database, taking user attributes from LDAP if required. On following logins only the username and password are checked.

CAS server configuration

Hostname:	slctestv22.sct.com	Hostname of the CAS server eg: host.domain.fr
Base URI:	cas-web/	URI of the server (nothing if no baseUri) For example, if the CAS server responds to host.domaine.fr/CAS/ then cas_baseuri = CAS/
Port:	8447	Port of the CAS server
Version:	CAS 2.0	Version of CAS
Language:	english	Selected language
Proxy mode:	No	Turn this to 'yes' if you use CASin proxy-mode
Logout CAS:	No	Turn this to 'yes' if you want to logout from CAS when you disconnect from Moodle
Multi-authentication:	No	Turn this to 'yes' if you want to have multi-authentication (CAS + other authentication)
Server validation:	No	Turn this to 'yes' if you want to validate the server certificate
Certificate path:		Path of the CA chain file (PEM Format) to validate the server certificate

LDAP server settings

Host URL	ldap://slctestv22.sct.com	Specify LDAP host in URL-form like 'ldap://ldap.myorg.com/' or 'ldaps://ldap.myorg.com/' Separate multipleservers with ';' to get failover support.
Version	3	The version of the LDAP protocol your server is using.
LDAP encoding	utf-8	Specify encoding used by LDAP server. Most probably utf-8, MS AD v2 uses default platform encoding such as cp1252, cp1250, etc.

2. For the **Logout CAS:** option, select No.
3. Save the configuration.

   When you log out of Moodle, you will not concurrently log out of Luminis Platform.

Configure Moodle courses

Once you have configured a Moodle installation, your instructors can select the Moodle option from a list of possible landing pages for their courses.

Manage Targeted Content

The Targeted Content application is a tool to create, personalize, publish, and manage content of all types.

The Targeted Content application adds to the existing web content development tools available in Luminis® Platform. The Targeted Content application enables you to develop content, including the ability to create a publish role-based sections and subsections. . This feature is similar to the Targeted Content Channel application and includes a few feature and usability enhancements.

- For administrators, this application includes personalization capabilities at the portlet level, and simplified content management processes.
- For end users, this application includes easy-to-use content selection, ability to place multiple Targeted Content portlets on one or multiple separate pages, and dynamic content selection of institution-driven information and services.

Authorized content authors can create, edit, and delete content, and target the content to specific groups of users. Administrators can apply the Targeted Content application to user layouts by default, or enable users to add them to their respective pages. Users can customize which content blocks are shown in their views, but they cannot modify the content. Users can drag one or more Target Content applications to one or more pages in their portal.

Refer to the "Glossary" for descriptions of the targeted content terminology.

Apply the Targeted Content application to your page

For administrators, the first step is to apply the Targeted Content application to your page using the **Add** menu.

Procedure

1. Log in to the Luminis Platform with administrative privileges.
2. From the **Add** menu, locate the **Targeted Content** portlet in the Content Management folder and click **Add**.

Create a content block

Build a block of content. A definition of blocks and other targeted content terms are in c_glossary.xml

About this task

Procedure

1. In the Targeted Content portlet, click **Select a display block**.

The system displays options associated with various permissions and only appear to authorized users.

Table 24: Targeted Content administrator menu options

Field	Description
Create New Block	Permission-based control that allows the authorized user to begin the process to create a new block of content. Click the create new icon to create or configure new blocks. ⊕
View targeted content block list	Permission-based control that allows the authorized user to view the blocks of content that they are allowed to work with. ▤
Select a display block	Link used to display a block of content within the **Targeted Content** portlet.

2. Create a new block and supply the basic block information such as a name, category, administrator, and language.
3. Add sections to the block.
4. Add sub-sections of content to the sections.
5. From the default content author page, click the create new block icon.⊕You can also start a new block of content by selecting **View targeted content block list** and then selecting the create new block icon.
6. Complete the **Block** properties pane:
   a) In the **Block Name** field, provide a name for the content block.
   b) Select a category.
   c) **Optional:** Assign a block Administrator from the **Block Administrator** list. If the appropriate permissions have been assigned to the chosen Luminis groups, then members of those groups will be able to work with this block of content.
   d) If your institution offers multi-language support, click **Language**.
7. Press **Save** to create the block.

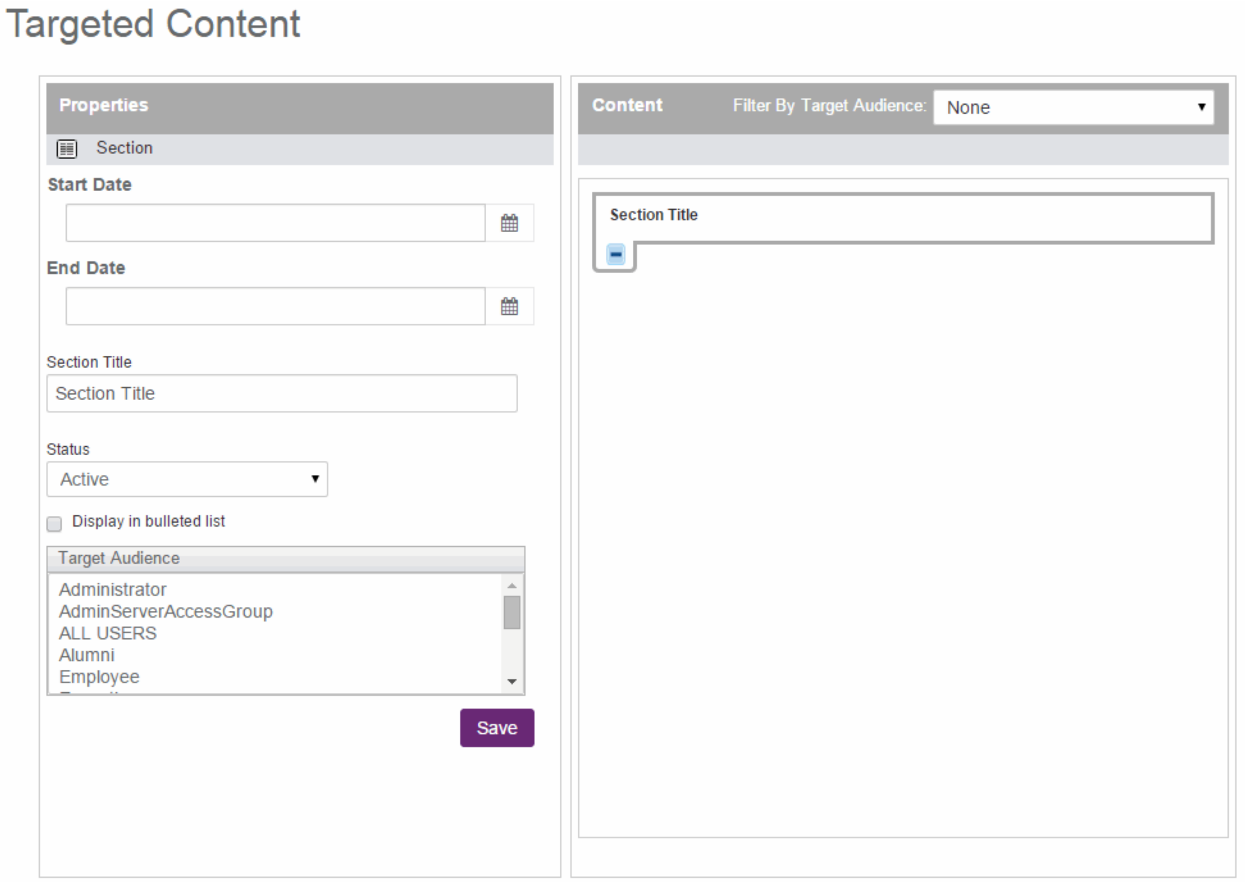
   You can now proceed to the next task of adding sections to the block.

Create a Targeted Content section

Create a targeted content section.

Procedure

1. After you save the content block and click the **Section Title** field in the **Content** panel, this page displays:



Targeted Content

Properties

Section

Start Date

End Date

Section Title: Section Title

Status: Active

☐ Display in bulleted list

Target Audience

Administrator
AdminServerAccessGroup
ALL USERS
Alumni
Employee

2. In the Properties panel, select the **Start Date** and **End Date**.
   - If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
   - If the subsection is saved with start date alone then it will post on the selected date and will not expire.
   - If the subsection is created with only an end date, the content will post immediately and expire on the selected date.
3. Enter a **Section Title**.
4. By default, all sections are active from the start to end dates. You have the option to inactivate the section if needed.
   - Active. Displays the section to the audience.
   - Inactive. Hides the section from the audience and stages section content for future publishing.

   You may choose inactivate the section after it has been published so you can edit a web link or make editorial changes without otherwise interrupting the viewer experience.

   Within the section, you may also click the Set section as inactive icon.👁

5. Mark the **Display in Bulleted List** check box to display the subsections in the form of a bulleted list.
6. Select the target audience for the section. The target audiences that appear here come from the groups you managed using the **Luminis Group Manager** portlet.
7. Click **Save** to save the section.
8. To create a duplicate of the section, click the copy icon.
9. To remove a section, click the subsection and then click the delete icon.

Change the section title

After you create the section, you can change the Title.

Procedure

1. Click the section's title in the Content panel to enable inline edit.
2. Enter the new title for the section.
3. Click ✓ to save or ✗ to cancel.

Add additional sections

Add sections to the content pane to target to different audiences.

Procedure

1. To add additional sections, click anywhere in the white space region in the editor's content pane. The **Subsection Content Types List** icon appears.
2. Click the icon.

Results

A new section appears in the content pane. You can target this section to a different audience.

Create subsection content

Create subsection content with the section controls. After you create your subsections, you can drag and drop subsections within the section to reorder them as needed.

Procedure

1. Log in to Luminis Platform with administrative privileges.
2. Click the View targeted content block list icon in the **Targeted Content** portlet.

3. Click the block you want to edit.
4. Click the section you want to edit.
5. Click the Add subsection to section icon and choose one of the content types. +▾
   a) Choose one of the content types.
   b) Enter the information as needed.
   c) Click **Save** for a new section or **Update** for an edited section.
6. To remove a section, click the subsection and then click the delete icon. −
7. Click **Update** to save the changes.

Related Links

Content types on page 292

Content types

The Targeted Content application offers a portfolio of six different content types to support your content development needs.

Free form HTML/Text

Click the **Free Form HTML/Text** link from the subsection dropdown in the Section Controls to create almost any type of content including rich text, photos, videos, and hyperlinks.

About this task

Procedure

1. Select the **Start Date** and **End Date** for the subsection.
   - If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
   - If the subsection is saved with start date alone, the content will post on the selected date and will not expire.
   - If the subsection is created with only an end date, the content will post immediately and expire on the selected date.
2. Enter the content in the editor in the Content Panel, using one of these methods:
   - Rich HTML
   - Source Code
3. Click **Save** to create the subsection.
4. Click **Cancel** to return to the section view.

Create a link with a teaser and photo

Link references to remote sites and an image along with an optional description for the content.

About this task

Note: With the exception of the step to save the subsection, none of the steps are reliant upon each other. All are optional, depending on the desired result.

Procedure

1. Select the **Start Date** and **End Date** for the subsection.
   - If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
   - If the subsection is saved with start date alone, the content will post on the selected date and will not expire.
   - If the subsection is created with only an end date, the content will post immediately and expire on the selected date.
2. Enter a title or heading for the referenced link.
3. Enter the URL for the link. When a user clicks the link, the referenced page opens in a new browser tab.
4. Choose the file to upload for the image. This image file appears with the link and content.

   By default the image link is active. To hide the image from the end user, clear the **Active** check box.
5. Select an alignment or location for the image in the **Align** field.
6. Enter the caption for the image.

   The image caption is limited to no more than 35 characters.
7. Click **Save**.

Link with Photo

Add or edit subsection content that includes an optional link to a remote site and a photo. Link references to remote sites and an image.

About this task

Note: With the exception of the step to save the subsection, none of the steps are reliant upon each other. All are optional, depending on the desired result.

Procedure

1. Select the **Start Date** and **End Date** for the subsection. The start date should be less than the end date.

- If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
- If the subsection is saved with start date alone then it will post on the selected date and will not expire.
- If the subsection is created with only an end date, the content will post immediately and expire on the selected date.

The start date may be September 1, and the end date September 15.

a) Click the calendar icon to select the required date.

b) Click the remove icon to clear the selected date.

2. Enter a title or heading for the referenced link.
3. Enter the URL for the link. This is a hyperlink which when clicked opens the referenced link in a new browser tab.

   The link description supports up to 4000 characters.
4. Choose the file to be uploaded for the image. This image file displays with the link and content. By default the image link is active.

   To hide the image from the end user, uncheck **active**.
5. Select an alignment or location for the image from the **Align** drop-down menu.
6. Enter the caption for the image.

   The image caption is limited to no more than 35 characters.
7. Click **Save**.

Remote HTML

Dynamically render the content from a given URL. When the Remote HTML content is displayed in Luminis Platform, it will render using the look and feel from the portal.

About this task

The Targeted Portlet application uses an AJAX request to render the HTML content from the remote server. The rules of same-origin policy apply (see https://en.wikipedia.org/wiki/Same-origin_policy for more information). Because of this, the remote content must be configured for Cross Origin Resource Sharing (CORS) and must allow access to your Luminis domain as the origin of the request. For more information about CORS, see https://en.wikipedia.org/wiki/Cross-origin_resource_sharing.

The remote HTML content should be rendered from a secure https page with a properly signed certificate. Otherwise, users will be subject to browser “mixed content” policies.

Procedure

1. Select the **Start Date** and **End Date** for the subsection.

- If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
- If the subsection is saved with a start date alone, the content will post on the selected date and will not expire.
- If the subsection is created with only an end date, the content will post immediately and expire on the selected date.

2. Enter the URL.
3. Click **Display** to preview the content of the referenced URL in the Content panel.
4. Click **Save**.

Remote Image

Display remote images from external sites or systems.

About this task

Procedure

1. Select the **Start Date** and **End Date** for the subsection.
   - If the subsection is saved without a start date and end date, the content will post immediately and will not expire.
   - If the subsection is saved with a start date alone, the content will post on the selected date and will not expire.
   - If the subsection is created with only an end date, the content will post immediately and expire on the selected date.
2. Enter the URL.
3. Enter the width, height, border, Vspace, Hspace, and alignment.
4. Click **Save**.

File/Image Upload subsection

Add or edit subsection content that references remote images from external sites or systems.

About this task

Procedure

1. Select the **Start Date** and **End Date** for the subsection.
   - If the subsection is saved without a start date and end date, the content will post immediately and will not expire.

- If the subsection is saved with start date alone. the content will post on the selected date and will not expire.
- If the subsection is created with only an end date, the content will post immediately and expire on the selected date.

2. Enter the file or image by browsing to the source location for the file.
3. Click **Save**.

Reorder subsections

After you create your subsections, you can prioritize or reorder the sections as needed.

Procedure

1. Log in to Luminis Platform with administrative privileges.
2. Click the View targeted content block list icon in the **Targeted Content** portlet.
3. Click the block you want to edit.
4. Click the section you want to reorganize.
5. Click and drag a subsection to move it into the desired position within the section.
6. When the subsections are arranged, click **Save** to save the subsection priority.

Targeted Content Blocks

From the **Targeted Content Manager** page, authorized users can perform the management tasks.

Click the view targeted content block list icon under **Manage Targeted Content Blocks** to navigate to the **Targeted Content Manager** page.

▤

Click **Done** to redirect to the TC admin page in minimized state.

Table 25: Targeted Content Manager management tasks

Field	Description
Manage published or staged content	Click the block name to navigate to the content editing pages. Use these pages to modify the content block, sections, and subsections.
Duplicate content blocks for reuse	To duplicate an existing content block and its sections and subsections, select the check box next to a given content block and then click the copy icon.⧉The appendage `_Copy` is added to the newly created block name and `_Copy` is localized for user configured languages. When

Field	Description
	you select the copied block name, you are redirected to the content editing pages.
Add new content block	Click the new block icon to start new content blocks from within the Targeted Content Manager.⊕This action creates a new block with the title Untitled Block. Click the **Untitled Block** link to redirect to the content editing pages.
Delete a content block	To delete content blocks from within the Targeted Content Manager, select the check box next to a given content block, then click the delete icon.✖
Configure the number of content blocks to display	To configure the number of content blocks to be displayed on the page, use the **Items per page** field.
Sort the content list	Click any one of the column headings, such as **Block Name**, or **Target Audience**, to sort the list by that selection.
Page through content	Use the pagination tools to jump through pages. Click the refresh page icon to reload the content in the Targeted Content Manager. ⟳

End user instructions

How portal users view and manage their delivered content.

Portal users sign into Luminis Platform and drag the Targeted Content application onto their page using the **Add** menu. Users can add the Targeted Content application to one or more pages according to their personal preference. They can then select different sets of content to display in any given instance of the Targeted Content application.

On pages where users have permissions, non-content authors will see a link, **Select a display block**. When users click this link, they can navigate the targeted content categories to view the content blocks. When they click on a block, the **Content Preview** window appears, and users can choose to set the current block as the display block. Alternatively, users can continue to navigate the categories to view additional blocks, or click cancel to return to the portlet default view.

If the user navigating the categories is an administrator or authorized content author but not part of the target audience for that piece of content, they see a There is currently no content to display message.

After a content block is selected as the display block, the portlet is populated with the appropriate content and the portlet title changes to reflect the name of the block.

Targeted content permissions

You can assign permissions to groups of users to allow them to schedule targeted content.

Note: By default, only administrators can perform these duties.

The block owner is the user who initially created the content block.

Block owners can limit the content blocks available for the group to edit. To determine which user groups have access to manage and maintain the block, select a value from the **Block Administrator** field.

Targeted blocks can be edited by the Luminis Platform administrator, block owner, block administrator, and users that have been granted access to the “manage block” or “edit block” permissions. Possible edits include the following:

- Choose from a list of options to reset the block administrator for the block
- Update the block values

The Luminis Platform administrator can manage all blocks in the system regardless of the value set in the block administrator field for the blocks.

Users who are granted the “set block admin” permission can set the block administrator to the group determined by the permission’s **allowed for** value.

Related Links

Schedule a targeted announcement on page 140
Targeted Content on page 192

Targeted Content permissions practical example

In this example, a Help Desk Administrator is granted permission to target content to students and faculty users. For this example, a user must be available, and assigned the Help Desk Admin role.

Procedure

1. Sign in as the Luminis Administrator, and navigate to the **Luminis Group Manager** portlet.
2. In the Group Expression Editor, create a group with the name FacultyStudent that includes both Faculty and Student roles.
3. Navigate to the **Luminis Permission Grant Manager**, and select **Targeted Content** from the category drop-down menu.
4. In the Luminis Permission Grant Manager table, add the permissions necessary for creating and managing targeted content.
   a) Add a permission for Create block and grant it to Help Desk Admin.

   b) Add a permission for Manage block and grant it to Help Desk Admin.
   c) Add a permission for Set section target audience and grant it to Help Desk Admin.
   d) In the **Allowed For** field, select **FacultyStudent**.
5. If necessary, add the **Targeted Content** portlet to the Home Community Welcome page.
6. Configure the **Targeted Content** portlet to enable the HelpDesk Admin to configure permissions.
   a) Click the configuration icon and select **Configuration** from the drop-down list. ⚙▾
   b) In the **Targeted Content Permissions** list, locate the Help Desk Admin role and set the Configuration option for the Help Desk Admin.
7. Sign out as the Luminis Administrator.
8. Sign in as the Help Desk Admin user, and navigate to the **Targeted Content** portlet.

   Note: The view targeted content block list icon appears only if existing blocks are present.

9. Click the add block icon and add the targeted block values. ⊕
10. Enter `Faculty and Student Block` as the block name, and then click the **Academic Targeted Content** category.
11. Click **Save** to save the new block.
12. Assign a section title to the new block and add the targeted block section values.

    Click **Section Title** and enter `Faculty and Student` as the section title, and select **FacultyStudent** from the Target Audience list. The Target Audience list is controlled by the Set section target audience permission. The only group the Help Desk Admin can target is the FacultyStudent group.
13. Click **Save** to continue.
14. After the section is saved, you can add content to the section. Click the section in the Content pane, then click +▾, and select **Free Form HTML/text**.
15. Add content, then click **Save**.
16. Click **Done** to close the portlet.

Related Links

Manage dynamic groups on page 197
Targeted Content on page 192

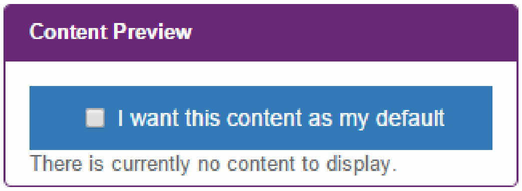
Preview Targeted Content

After you have created the targeted content block and sections, you can preview the information to see how the targeted content will appear to the user.

Procedure

1. Log in as the Help Desk Admin user.

2. Select the **Select a display block** link on the **Targeted Content** portlet. From the **Block Category** list, select the **Academic** category.
3. In the Academic category, click the **Faculty and Student Block** link to set the block to display. The system automatically refreshes the window and displays the Targeted Content portlet with a new title of “Faculty and Student Block”.

   Content Preview

   □ I want this content as my default

   There is currently no content to display.

4. Click the preview icon to enter into preview mode.🔍

   The portlet displays a preview of the content that will be visible to the intended targeted audience. You can select different Target Groups to view the content intended for each group.
5. Click the return icon to reload the page and see the default portlet view.
6. Sign in as a student or faculty user and navigate to the Home Community to view the targeted content portlet configured with the **Faculty and Student Block**.

Configure Targeted Content

Configure permissions on the portlet to enable users with Targeted Content permissions access to icons to view and create blocks and the link to select a display block.

Procedure

1. Sign in as the Luminis Administrator.
2. In the **Targeted Content** portlet, click the configuration icon, and then select **Configuration**.⚙
3. Find the groups who have been granted targeted content permissions.
4. Select the **Configure** check box. The Configuration permission enables users with permissions to access the **Create New Block** and **View targeted content block list** icons, and to configure a display block.
5. Click **Submit** to save the changes.

View content targeted to users

Users in a targeted audience can view the content targeted to them.

About this task

The targeted content is displayed in the **Targeted Content** portlet. In this example, the user uses the **My Profile** or **My Dashboard** pages and is assigned the Faculty or Students roles.

Procedure

1. Sign in to Luminis Platform.

   In this example, the user is assigned the Faculty or Student roles.
2. Navigate to the user's **My Profile** page.
3. Click **Add** > **Applications**, and from the Content Management category drag the **Targeted Content** portlet to the page.
4. Click **Select a display block**.
5. From the **Block Category** list, click the **Academic** folder.

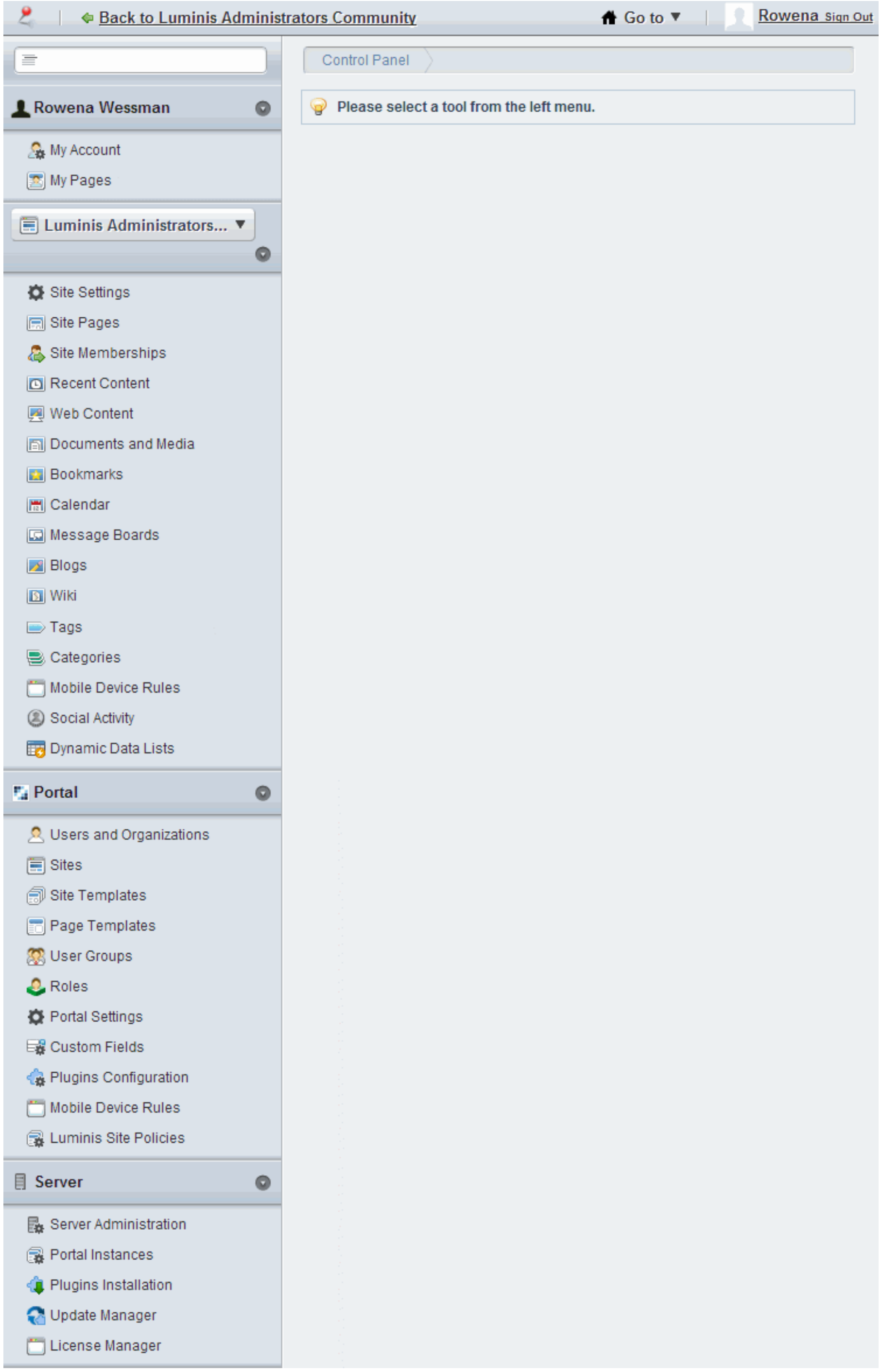
   Luminis displays the **Faculty and Student Block** link.
6. Click **Faculty and Student Block**.

Results

Luminis displays the targeted content in the **Faculty and Student Block** portlet.

Control Panel

The **Control Panel** is used in addition to the administrative portlets and tools to maintain and administer various system functions.



Please select a tool from the left menu.

It is used in support of functions such as creating, pushing, and maintaining pages and content to users, managing Web Content developed using the **Web Content Display** portlet, managing academic and non-academic sites, and managing certain system settings such as, changing language, timezone, and the global logo and color scheme for your portal.

Administrative users and non-administrative users have a **Control Panel** entry point under the **Go to** menu. Administrative users have a robust set of functions within their **Control Panel**, whereas non-administrative users have limited functions.

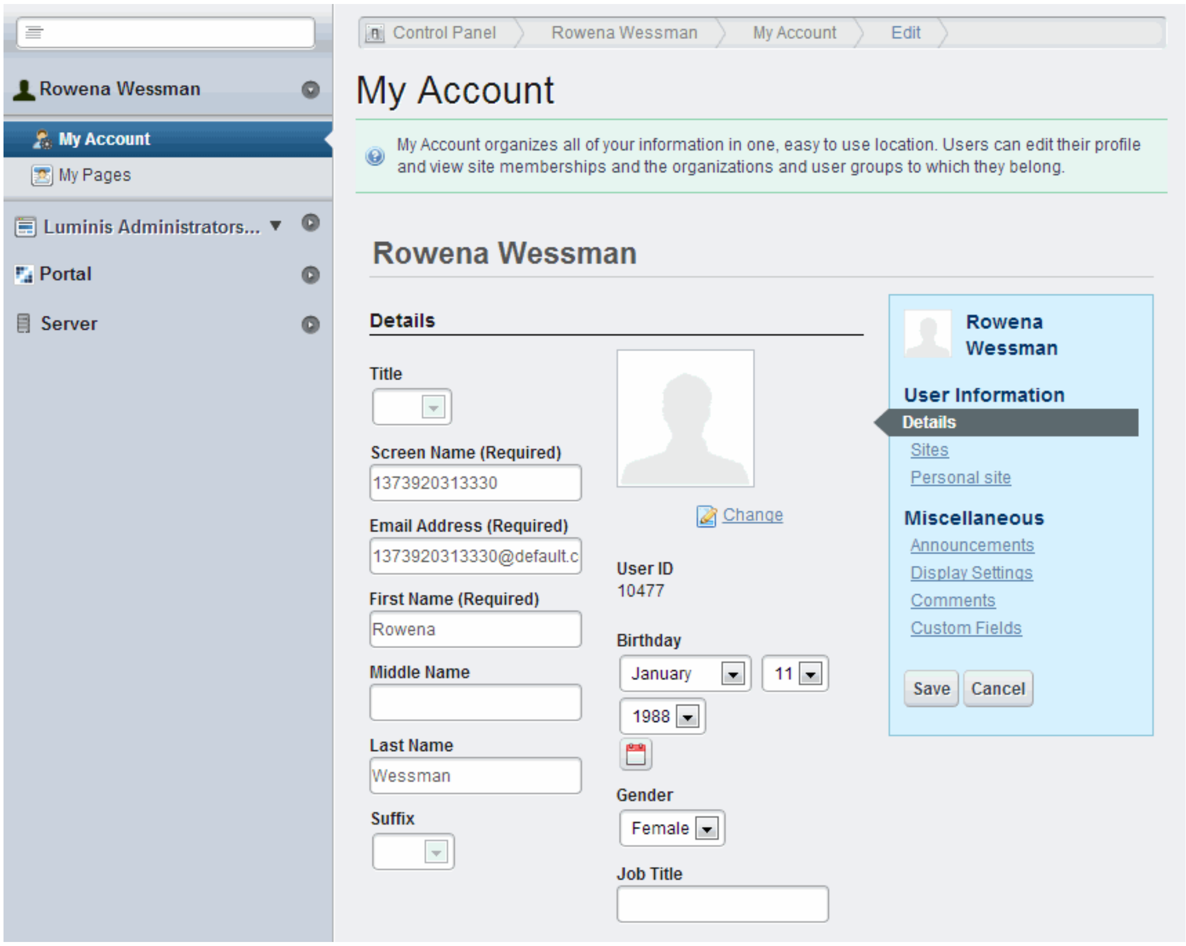
Manage personal page options

All system users have **My Account** and **My Pages** options they can access through the **Control Panel**.

Depending on system privileges, the functionality varies in these areas.

My Account options

View the sites you belong to, your role(s) within the portal, manage personal photos, and change how the system greets you.



My Account

My Account organizes all of your information in one, easy to use location. Users can edit their profile and view site memberships and the organizations and user groups to which they belong.

Rowena Wessman

Details

Title:

Screen Name (Required): 1373920313330

Email Address (Required): 1373920313330@default.c

First Name (Required): Rowena

Middle Name:

Last Name: Wessman

Suffix:

User ID: 10477

Birthday: January 11 1988

Gender: Female

Job Title:

The following User Information **Detail** fields are read-only:

- Title
- Screen Name
- Email Address
- First Name
- Middle Name
- Last Name
- Suffix

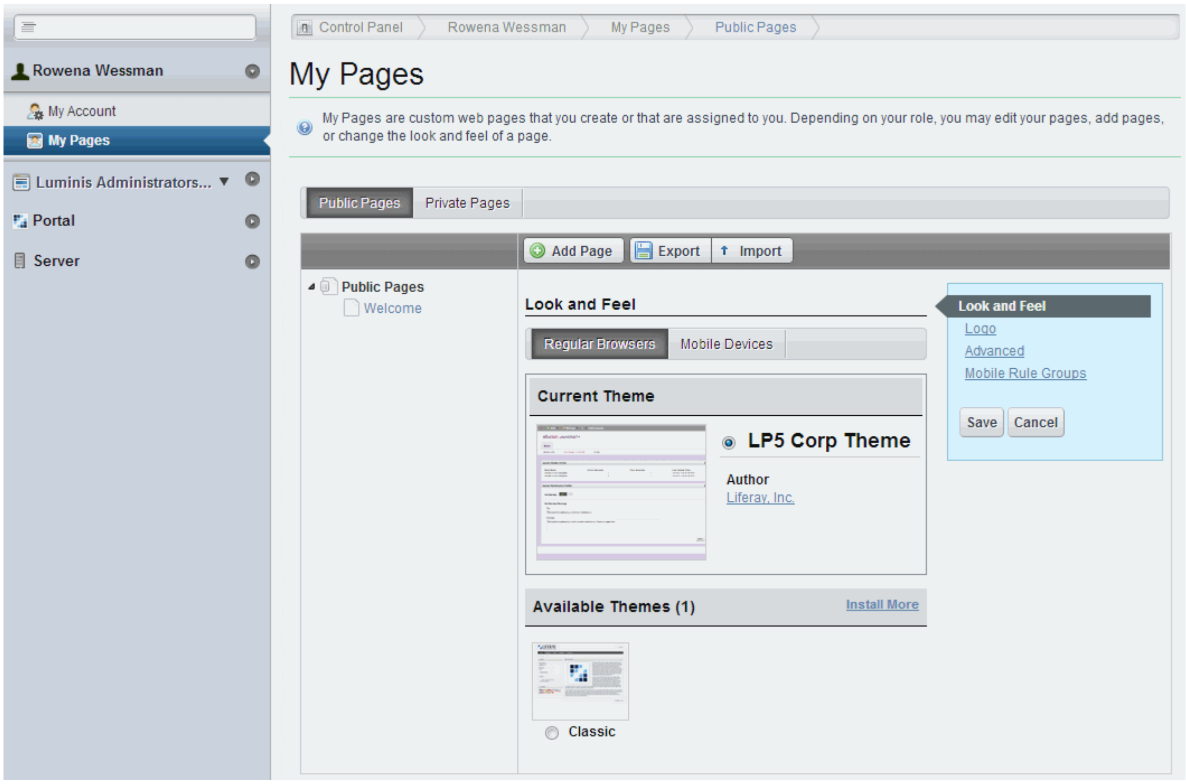
> **Note:** Any changes to settings on the **Miscellaneous** > **Announcements** page only apply to Liferay's alerts and announcements. They do not apply to Luminis Platform announcements.

The **My Account** area is available to all system users with varying functions based on role.

My Pages options

Manage personal pages and content.

The **My Pages** area is available to all system users with varying functions based on role.



My Pages are custom web pages that you create or that are assigned to you. Depending on your role, you may edit your pages, add pages, or change the look and feel of a page.

This area is not used to manage the pages and content published by the institution. Institution controlled pages are managed through**Control Panel** > **Portal** > **Sites**.

Manage Web content

Manage site content using the **Web Content Display** portlet, which uses the **Web Content** area of the **Control Panel**.

For example, if you create a new piece of content and add it to the Home Site, it can be managed here.

Administrators can easily switch between sites and view all Web Content content created for that site. Select a site from the drop-down on the left, then the click the **Web Content** link. You can edit, modify permissions, preview, copy, or delete the content.

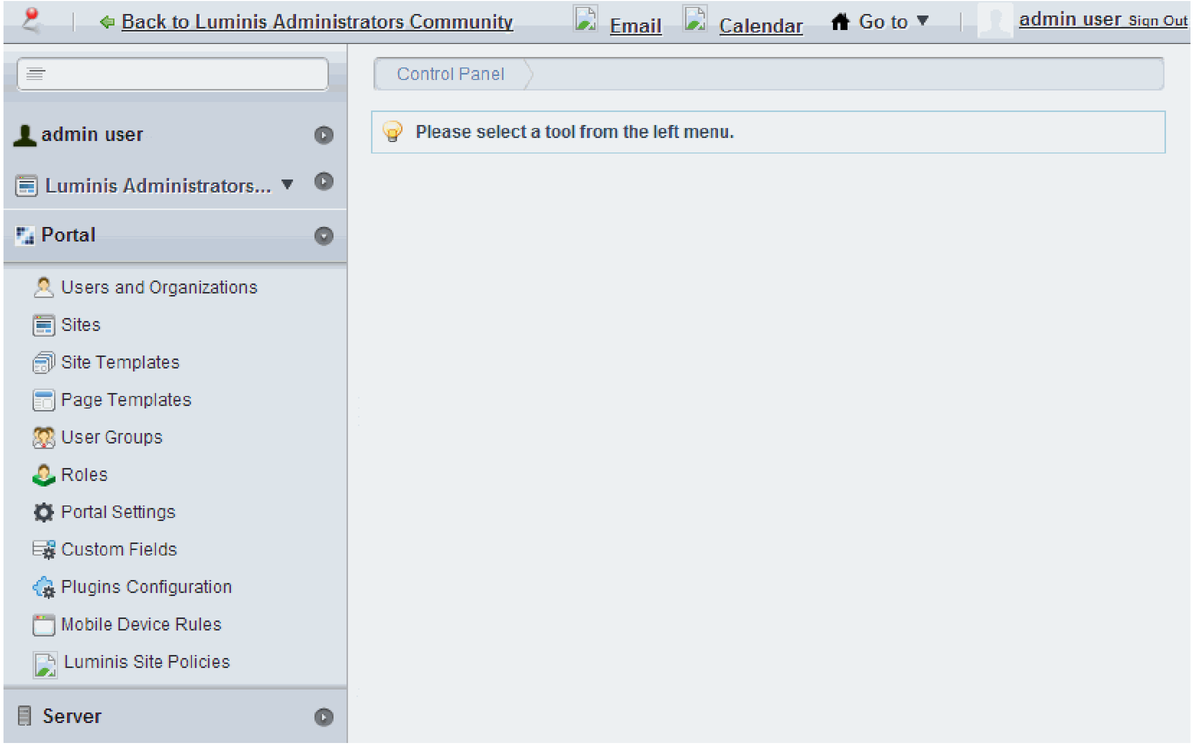
Non-administrative users can add the **Web Content Display** portlet to one of their personal pages to create content in. Only the user can view and manage this personal page content.

Manage portal content

A menu to lead you to management options for Users, Institution, Sites, Roles, Settings, and Plugins Configuration.

You are most likely to use the Users and Sites options as you administer Luminis Platform.

Figure 8: Control Panel - Portal

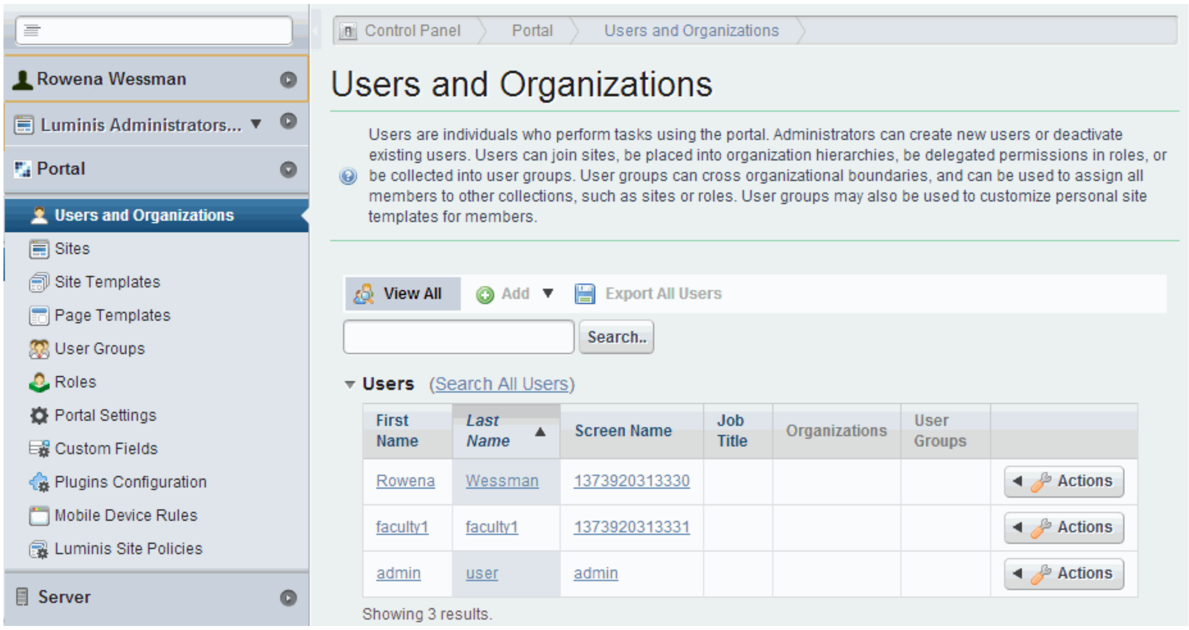


Please select a tool from the left menu.

Users and Organizations content

Review information about system users.

Warning! Do not modify users using the **Control Panel**. Please manage system users using the **Luminis User Management** portlet.



Users and Organizations

Users are individuals who perform tasks using the portal. Administrators can create new users or deactivate existing users. Users can join sites, be placed into organization hierarchies, be delegated permissions in roles, or be collected into user groups. User groups can cross organizational boundaries, and can be used to assign all members to other collections, such as sites or roles. User groups may also be used to customize personal site templates for members.

Users (Search All Users)

First Name	Last Name ▲	Screen Name	Job Title	Organizations	User Groups	
Rowena	Wessman	1373920313330				Actions
faculty1	faculty1	1373920313331				Actions
admin	user	admin				Actions

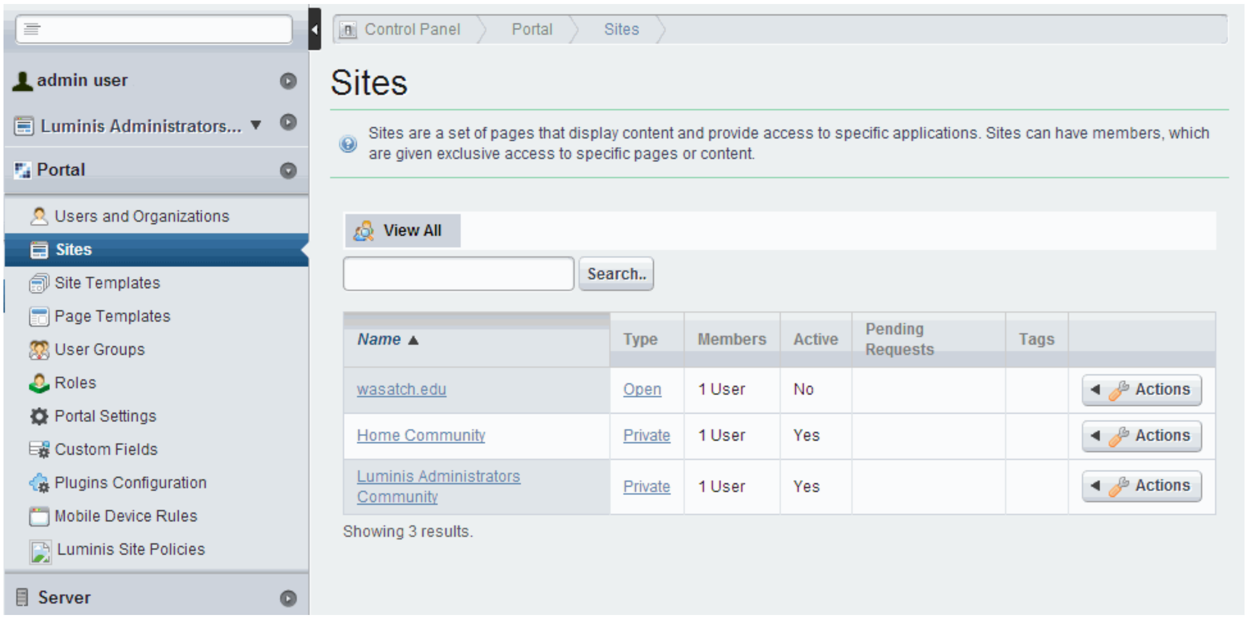
Showing 3 results.

Sites content

Create and publish pages and content, and manage user layouts.

When Luminis Platform is installed, these sites are available by default:

- Guest
- Home Community
- Luminis Administrators Community



Sites

Sites are a set of pages that display content and provide access to specific applications. Sites can have members, which are given exclusive access to specific pages or content.

Name ▲	Type	Members	Active	Pending Requests	Tags	
wasatch.edu	Open	1 User	No			Actions
Home Community	Private	1 User	Yes			Actions
Luminis Administrators Community	Private	1 User	Yes			Actions

Showing 3 results.

Depending upon a user's role in the system, the user will automatically become a member of the Home Community or the Luminis Administrators Community. There are three types of sites:

Type	Description
Open	An open or public site appears in the **Luminis Community** portlets and users can join the site without restriction.
Restricted	A restricted site appears in the **Luminis Community** portlets, but users must request membership. A site owner must then grant or deny users' requests to join.
Private	A private site does not appear in the **Luminis Community** portlets and users must be added to it manually by a site administrator.

As additional sites and courses are added to the system, the list of sites in the **Control Panel** will be updated to display each of these sites. From the **Sites** area of the **Control Panel**, administrative users will be able to view and manage the pages for each of these sites.

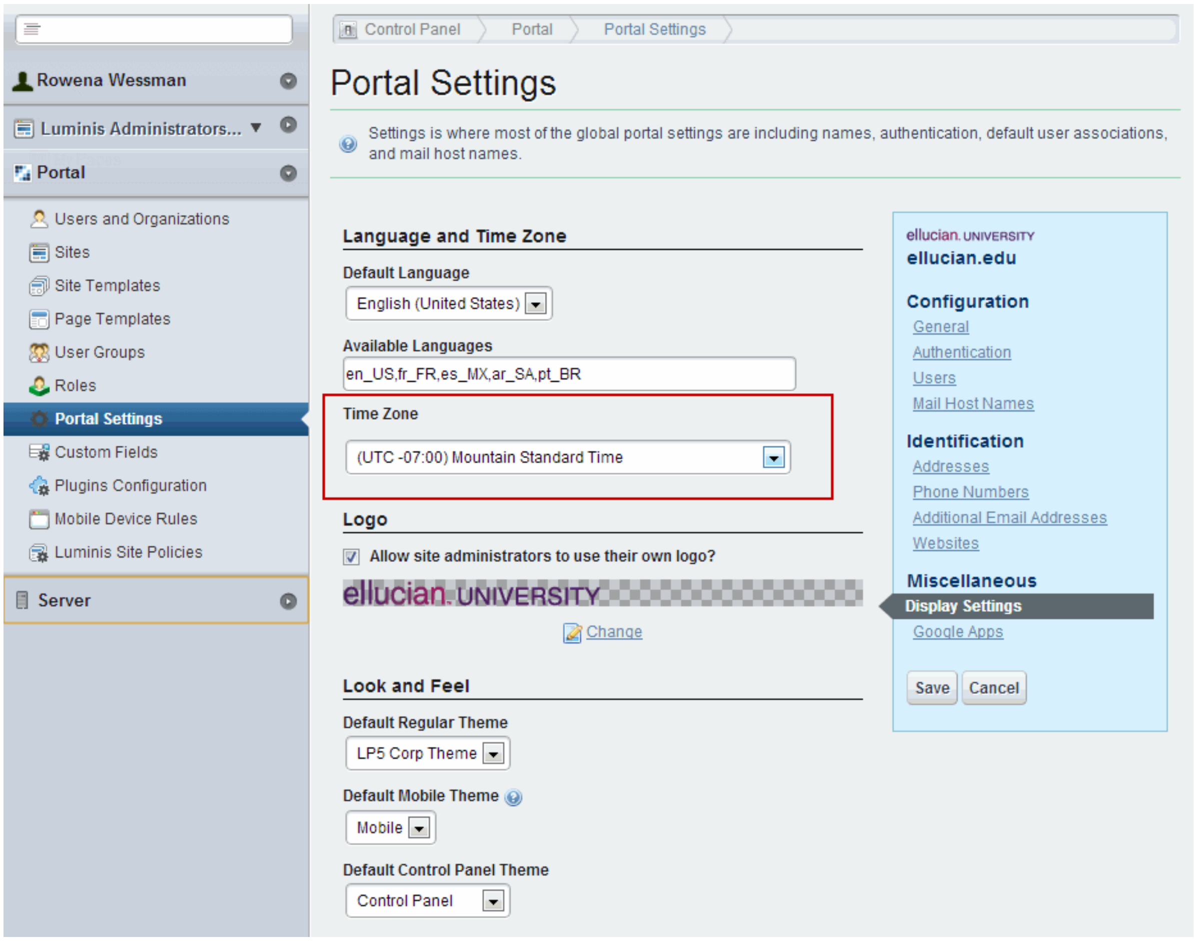
For each site, options are present under the **Actions** menu.

Action options	Description
Edit Settings	Review site details
Manage Pages	Create and manage pages for the selected site
Manage Memberships	Add members, add site roles to members, remove membership, and so forth
Go to Public Pages	Navigate to the pages available to the public
Deactivate	Disable, do not delete, the site
Delete	Remove the site

Portal Settings - Display Settings

Change the default timezone.

Edit file `$CP_ROOT/products/tomcat/tomcat-[admin|portal]/lib/classes/system-ext.properties`. Change the `user.timezone` property to the desired time zone, then restart the server.



Portal Settings

Settings is where most of the global portal settings are including names, authentication, default user associations, and mail host names.

Language and Time Zone

Default Language: English (United States)

Available Languages: en_US,fr_FR,es_MX,ar_SA,pt_BR

Time Zone: (UTC -07:00) Mountain Standard Time

Logo

☑ Allow site administrators to use their own logo?

Look and Feel

Default Regular Theme: LP5 Corp Theme

Default Mobile Theme: Mobile

Default Control Panel Theme: Control Panel

You must make the change to every node where the time zone is to take effect. Additionally, you should also edit the `$CP_ROOT/install/resolved.properties` file if the new value is to remain in effect after a Luminis system patch.

The default time zone option set in the Liferay portal **Display Settings** is the time zone assigned to users when they are created or imported. This changes the default time zone used under Liferay, but this does not change the Java system property setting for `user.timezone`. Any portlet accessing the system property will still see the value that was set during installation in the install property `user.timezone`.

Internationalization and Localization in Luminis Platform

Luminis® Platform supports multiple languages, such as US English, French, Spanish, Arabic in the presentation of content.

Administrators can select which languages are available for the users. Users in turn can select from the list of languages to view the portal in their preferred language.

Note: In Luminis Platform, the list of specific languages available for a particular release is documented in the release notes for that version.

Language and country codes

Languages are specified in Luminis configuration using the ISO 639-1 standard, and countries are specified by the ISO 3166 standard.

Each language specification consists of a language code and a country code. For example, the code to specify U. S. English is `en_US`. Other examples would be, `fr_FR` for French (France), `de_DE` for German (Germany), and `es_ES` for Spanish (Spain). Refer to the release notes to know which languages are supported in your version of Luminis Platform.

Select languages during installation

In the installation setup properties file, there are properties that may be set to specify which languages should be available for all users of the Luminis Platform deployment, and which language is the default language to be presented to all users.

To set the default language during installation, set these two properties to the desired language and country codes:

```
default.language.code=en
default.country.code=US
```

To specify all available languages, set the following property with a comma-delimited list of languages using the format <*language_code*>_<*country_code*>:

```
supported.locales=en_US,es_ES
```

Post-installation settings

Specify Internationalization settings prior to installation.

Select languages post-installation

Once the system is installed, you can add new languages from the list of languages supported by the Luminis Platform.

Modify property files in the deployed system directories. A restart of the Luminis Platform system is required to take effect.

Change the default language

To change the default portal language, edit these files on the admin and portal nodes:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/lib/classes/system-
ext.properties
```

Set the values:

```
user.language=<language code>
user.country=<country code>
```

Enable other languages

Change the supported portal languages.

Edit these files on each admin and portal node:

```
$CP_ROOT/products/tomcat/tomcat-[admin|portal]/webapps/ROOT/WEB-INF/
classes/portal-ext.properties
```

Set the locales configuration value with a comma-delimited list of values of the form *<language>_<country>* as in the following example:

```
locales=en_US, it_IT, fr_FR
```

Select a personal language

Once a set of languages is configured, a user may select their language.

On the **My Account** page, select the **Display Settings** tab from the right column. A drop-down list becomes available to select the language.

Glossary

Terms used in this document.

Academic sites

Academic sites are configurable collaboration rooms (virtual class room or site) that provide online supplements to course instruction. Online portal sites are automatically built for each course offered at the institution based on back-end Enterprise Resource Planning (ERP) course events. Membership and authorization privileges are also created by the backed ERP events. Programmatic creation of academic sites provides a course site environment for all students and faculty and eases the administrative burden associated with creating online sites for each course.

Custom academic site home pages can be created by the instructor, teaching assistant, or other Course Leader. End users or course members can also create custom pages in which to interact with their academic (or non-academic) sites.

Related Links

Manage Sites and Collaboration on page 221

Block

A content block is the parent content container for the sections and the sections' subsections. All content starts with a content block. Content blocks are usually involved with targeted content.

Related Links

Manage Targeted Content on page 288

Block Category

The content blocks are categorized. Content blocks are usually involved with targeted content.

There are two types of categories:

- Default Categories created during installation. These are system categories, localized for different language bundles where applicable. They should not be deleted.
- Custom Created Categories: These categories can be created at any depth and can be modified or deleted thereafter.

Related Links

Manage Targeted Content on page 288

Block Name

A targeted content block name is the unique name representing the content block and its sections and subsections.

Related Links

Manage Targeted Content on page 288

Blog

A blog is a public space where users posts writings of any kind. It is used as an individual or site-based tool. This portlet functions in user and site levels.

Bookmarks

The **Bookmark** portlet allows users to create, manage, and share bookmarks. This portlet functions in user and site levels.

Content

Text, pictures, and video used in the content blocks, sections, and subsections. Content blocks are usually involved with targeted content.

Related Links

Manage Targeted Content on page 288

Content Author

Portal users with authorization to create and manage content within the Targeted Content application.

Related Links

Manage Targeted Content on page 288

Documents and Media

The **Documents and Media** portlet allows users to upload, manage, and share photos, videos, and all other files within course sites, general sites, or on personal pages. More information about compatible global document types are found at liferay.com/documentation.

Note: The links on the Liferay Web site are subject to change without notice.

Language

Language (English, Spanish, French, Arabic, Portuguese) used within the portal for any given user.

Member list

The Site Member list is an application that allows users to view a list of all the members associated with a site. The member list can be sorted.

Message Boards

The **Message Boards** portlet is a forum application with many configuration options.

Non-Academic sites

Non-academic sites are for all site collaboration that may not be directly related to courses. Student government, executive sites, areas of study such as Anthropology or Chemistry, and special interests such as ski or chess clubs are common examples.

Non-academic sites are created by system users instead of integrated system events. Non-academic sites, are configured in the same manner as academic sites and inherit all site and collaboration functions available in academic sites.

Related Links

Manage Sites and Collaboration on page 221

Role Preview

Admin feature to quickly preview content as a given audience would see it. Role preview is usually involved with targeted content.

Related Links

Manage Targeted Content on page 288

Site Administration

Administrators and site owners can manage individual sites from the **Control Panel**. Options include managing site pages, memberships, and site content. Administrators can also manage global site and membership policies.

Site categories

Site Categories are placeholders for various non-academic sites that are created in Luminis Platform. They are used to logically group all related sites.

Site member

A site member can use the collaboration tools to interact with other members of the site, to share content, images, files, and so on. Depending on the site application being used, members may be required to submit content for approval to the site owner. Members can view the approved content posted by other site members.

Site types

A site allows students, faculty, or employees of an institution the ability to create and manage group home pages for clubs or other affiliations and interests. A site is categorized as public, restricted, or hidden.

Public groups are open for anyone to join a site. Restricted groups are subject to certain membership criteria. Hidden sites do not appear in the portlet; only an administrator or site owner can choose the members for a hidden site.

Site welcome or guest portlet

When a site is selected, the **Welcome** portlet displays information about the site. This includes a message for guests who are not members of the site and the option to join.

Once the person is a member, a welcome message appears in the portlet. The Owner of the site can create and set guest or welcome messages for a site.

Sites

Known prior to Luminis® Platform 5.1 as "communities", sites provide portal users at your institution tools to create, manage, and participate in dynamic online sites. Luminis Platform Sites provide dedicated portal areas for both academic and non-academic collaboration for courses, clubs, affiliations, and other interests. System users create and manage non-academic sites. Course events from back-end Enterprise Resource Planning (ERP) systems create academic sites for all courses offered at your institution.

Related Links

Manage Sites and Collaboration on page 221

Target Audience

The segment of portal users in which the content block or sections is targeted.

Targeted messaging

Targeted Messaging is a tool used to send announcements to all the system users.

Targeted Messaging supports the following activities:

- Sending Personal Announcements to selected users or groups based on the role, major, or other custom attributes
- Sending Campus Announcements to all system users
- Administering and managing the announcements (delete, archive, sorting, and filtering)
- Delegate publishing and creation of an announcement
- Restricting the audience to the authorized authors

Related Links

Luminis Announcements on page 134

Web Content

The **Web Content** portlet allows for a simplified method for publishing content to a site. You can manage content using templates with dynamic or static elements.

Wiki

The **Wiki** portlet helps in creating pages using a WYSIWYG text editor or in plain text. At any time, a person can view the pages as they will look to other members. Each page can be altered and a member can contribute their information to the specific Wiki topic.