

Configuring the Integration System User for Workday

- [Configure Workday Credentials in LYNX](#)
- [Configuring the Integration System User for Workday](#)
- [Creating the Student Transaction Log Outbound Connector in Workday](#)
- [Updating Registered Headcount With Workday](#)
- [LYNX for Workday - Architecture and Workflow](#)
- [LYNX for Workday - Assessments/Exam Import/Export](#)

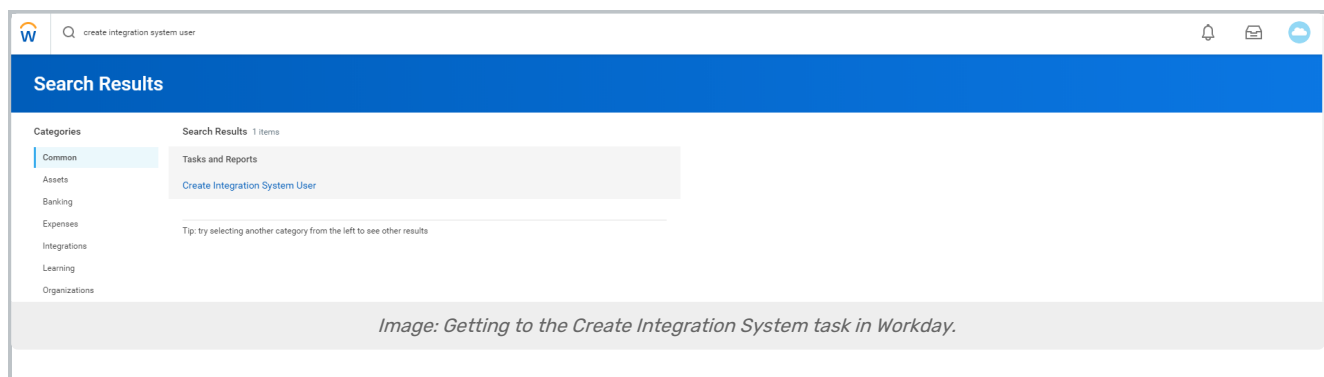
The Integration System User account is responsible for making Workday API requests to deliver academic data to the LYNX database. Please refer to the [Workday Documentation](#) for more detailed information and for the security requirements necessary to complete these steps.

In This Article:

- [Part 1: Create the Integration System User \(ISU\)](#)
- [Part 2: Create the Integration System Security Group](#)
- [Part 3: Apply Domain Security Policies](#)
- [Part 4: Apply Business Process Security Policies](#)
- [Part 5: Activate Pending Security Policy Changes](#)

Part 1: Create the Integration System User (ISU)

1. Run the *Create Integration System User* Task



2. Enter a Username and Password

Create Integration System User

Account Information

User Name

Generate Random Password ☐

New Password

Password Rules Your new password must not be the same as your current password or user name. Minimum number of characters required: 8. The following character types must be represented: alphabetic characters, uppercase characters, lowercase characters, Arabic numerals 0-9, special characters !"#\$%&'()*+,-./:;>?@[\]^_`{|}~.

New Password Verify

Require New Password at Next Sign In ☐

Session Timeout Minutes Enforced 120

Session Timeout Minutes

Do Not Allow UI Sessions ☒

Image: Entering information in the Create Integration User view.

Leave the **Session Timeout Minutes** set to zero to prevent session expiration. Enable **Do Not Allow UI Sessions** to prevent the ISU account from logging into the Workday UI. Special characters (such as ampersands) are allowed in the passwords.

Part 2: Create the Integration System Security Group

1. Run the *Create Security Group* Task

Search Results

Categories: Common, Assets, Banking, Expenses, Integrations, Learning, Organizations

Search Results 1 items

Tasks and Reports

[Create Security Group](#)

Tip: try selecting another category from the left to see other results

Image: Running the Create Security Group task in Workday.

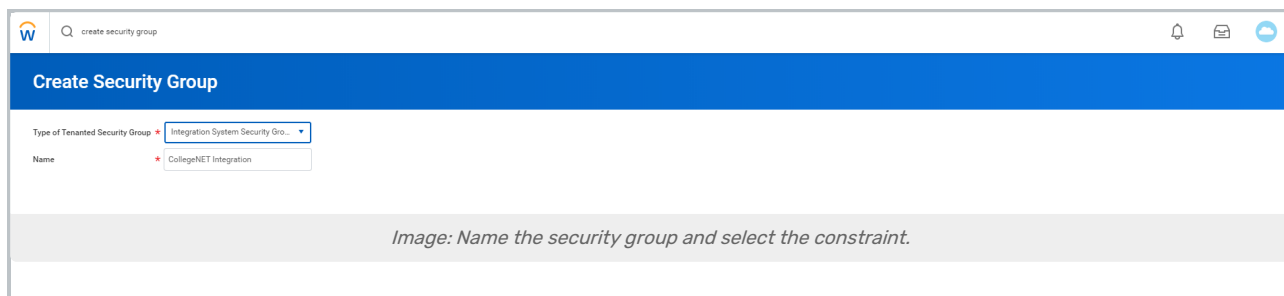


Using a Previously Created Group

If you already have a security group of type *Integration System Security Group (Unconstrained)* then you can skip Steps 1 and 2. Make sure you complete Step 3 to add the ISU account to the security group.

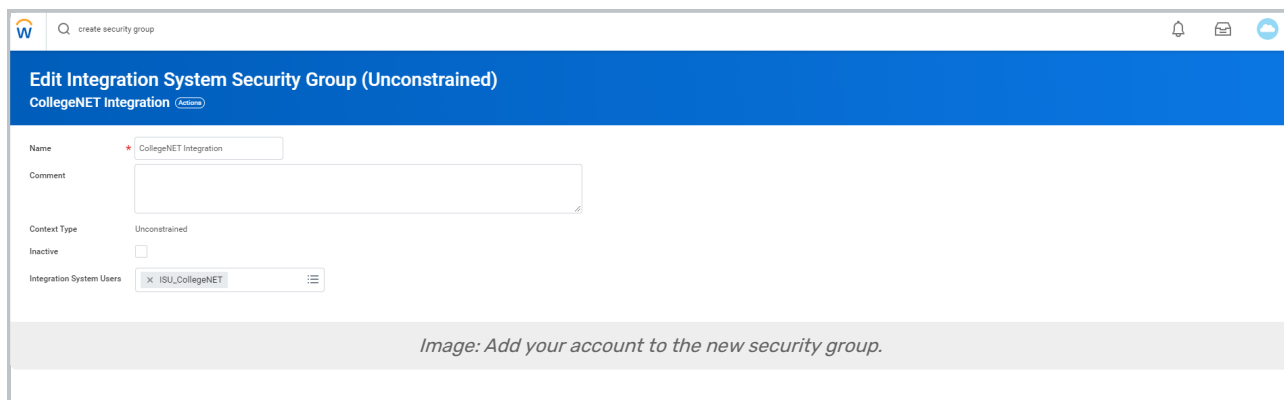
2. Name the Group and Select Type

Give your security group a name and select **Integration System Security Group (Unconstrained)** for the type. An unconstrained security group means that members will have access to data for all organizations.



3. Add the Account to the New Group

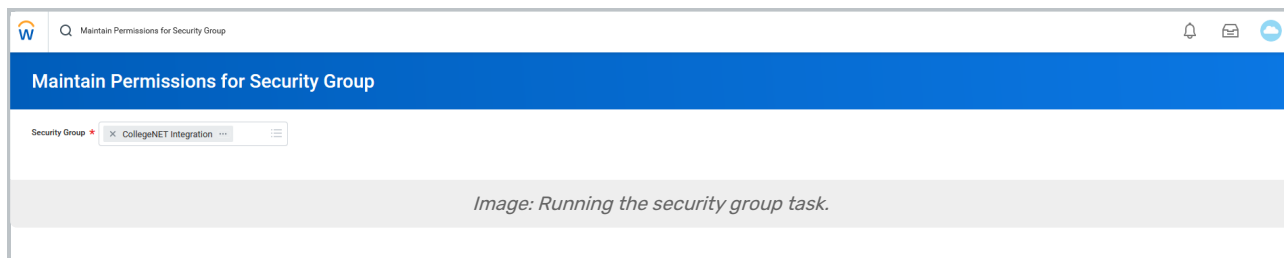
Add the ISU account that you created previously as a member of the security group.



Part 3: Apply Domain Security Policies

1. Run the Security Group Task in Workday

Run the **Maintain Permissions for Security Group** task for the ISU security group.



2. Add Domain Security Policies

Under **Integration Permissions**, add the domain security policies according to the lists below.

- **Domain Security Policies permitting GET and PUT access:**
 - Manage: Curriculum Management
 - Manage: Section Data
- **Domain Security Policies permitting GET access:**
 - Manage: Course Sections

- Manage: Preliminary Course Sections
- Set Up: Curriculum Management
- Worker Data: Public Worker Reports
- Set Up: Academic Units
- Set Up: Academic Appointments and Related Data
- Set Up: Course Tag Categories
- Set Up: Organization
- Manage: Location
- Integration Build
- Manage: Course Subjects
- Manage: Course Tags
- **Domain Security Policies permitting VIEW and MODIFY access:**
 - Custom Report Creation (required for [Updating Registered Headcount With Workday](#))



Why these specific policies?

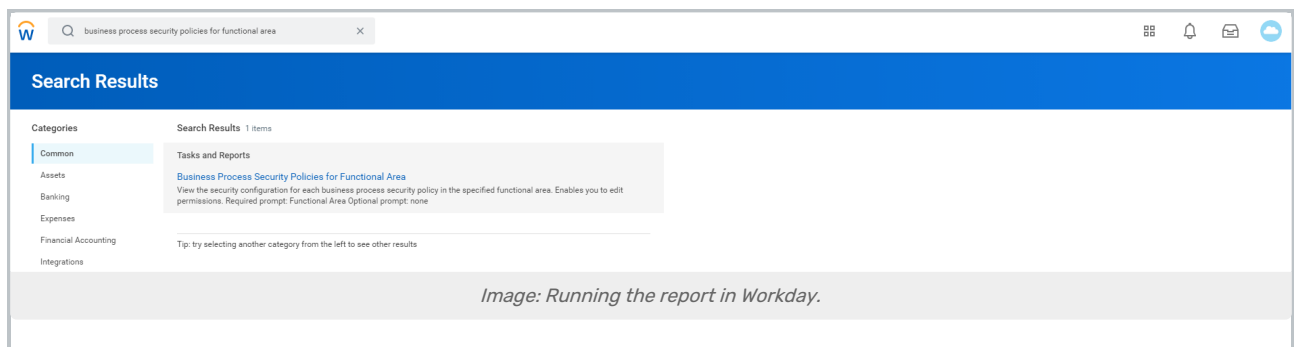
The domain security policies were determined by running the *View Security for Securable Item* report in the Workday UI for the Web Service Operations used by LYNX. Omitting any of them will prevent the LYNX integration from functioning properly.

Also, see [Using the Workday Course Section Tag to Add Location Feature Requirements Through LYNX](#) for permissions needed for that feature.

Part 4: Apply Business Process Security Policies

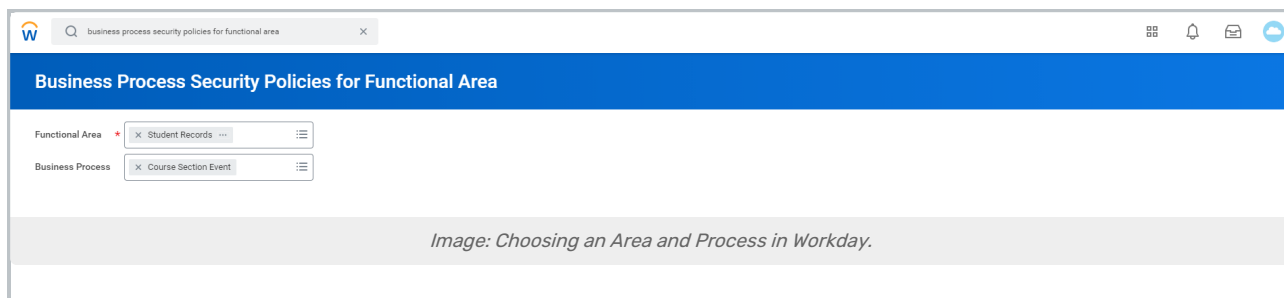
1. Run the Business Process for Functional Area Report

Run the **Business Process for Functional Area** report.



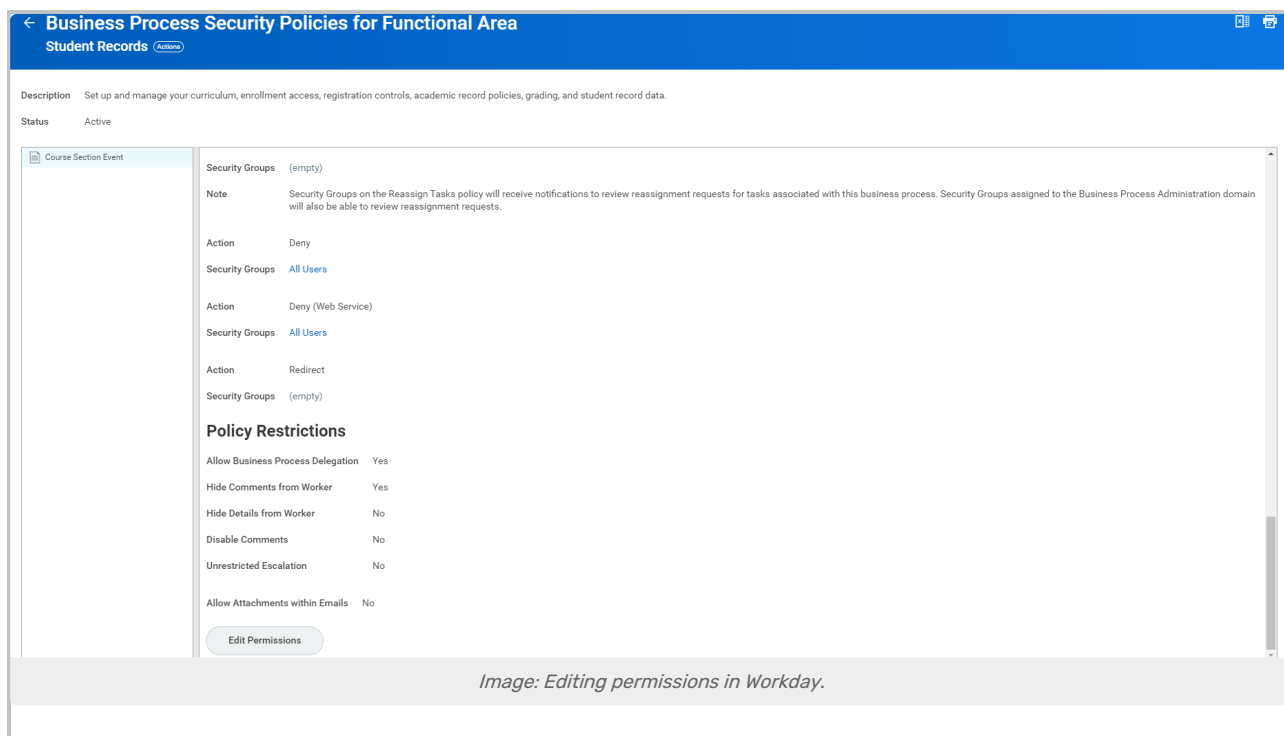
2. Select a Functional Area and Business Process

Select "Student Records" as the **Functional Area** and "Course Section Event" as the **Business Process**.



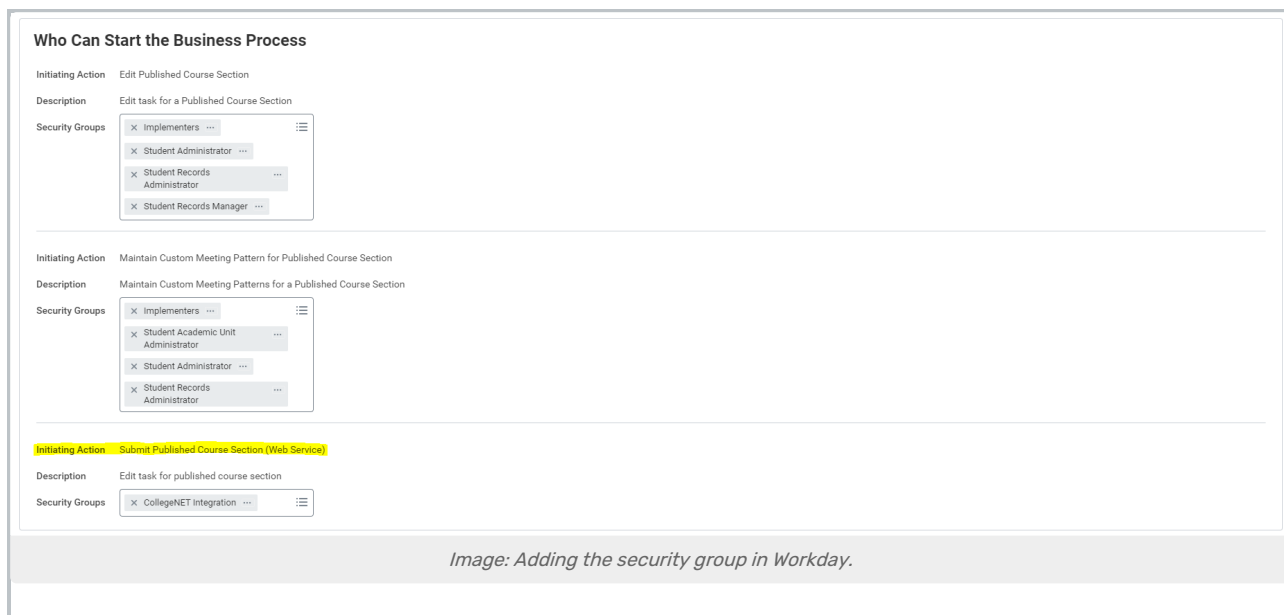
3. Edit Permissions

Scroll to the very bottom of the page and **Edit Permissions**.



4. Add the Security Group

Under *Initiating Action - Submit Published Course Section (Web Service)*, add the security group for the ISU account.



Why these specific policies?

The business process security policies were determined by running the *View Security for Securable Item* report in the Workday UI for the Web Service Operations used by LYNX. Omitting any of them will prevent the LYNX integration from functioning properly.

Part 5: Activate Pending Security Policy Changes

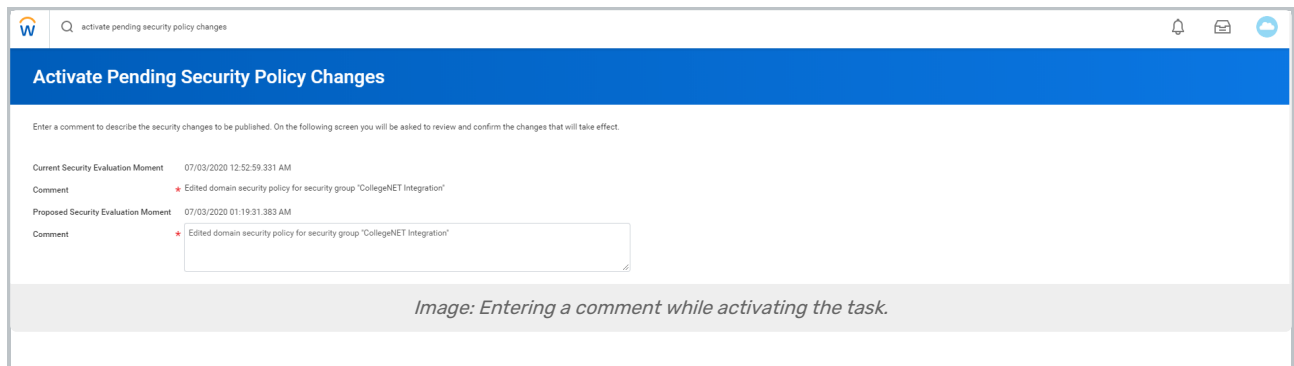
1. Activate the Pending Security Policy

Run the **Activate Pending Security Policy Changes** task.



2. Enter Comments

Enter a comment to describe the changes.



W activate pending security policy changes

Activate Pending Security Policy Changes

Enter a comment to describe the security changes to be published. On the following screen you will be asked to review and confirm the changes that will take effect.

Current Security Evaluation Moment 07/03/2020 12:52:59.331 AM

Comment Edited domain security policy for security group "CollegeNET Integration"

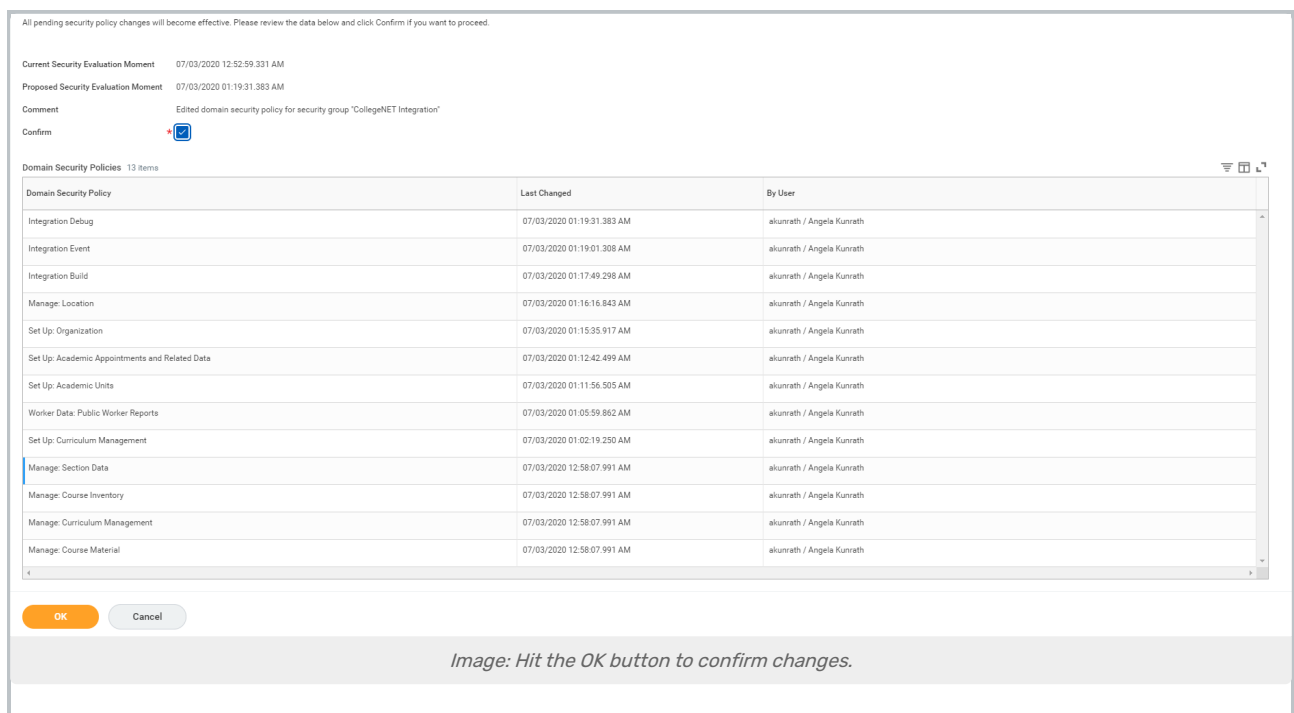
Proposed Security Evaluation Moment 07/03/2020 01:19:31.383 AM

Comment Edited domain security policy for security group "CollegeNET Integration"

Image: Entering a comment while activating the task.

3. Confirm the Changes

Confirm the changes using the **OK** button.



All pending security policy changes will become effective. Please review the data below and click Confirm if you want to proceed.

Current Security Evaluation Moment 07/03/2020 12:52:59.331 AM

Proposed Security Evaluation Moment 07/03/2020 01:19:31.383 AM

Comment Edited domain security policy for security group "CollegeNET Integration"

Confirm

Domain Security Policies 13 items

Domain Security Policy	Last Changed	By User
Integration Debug	07/03/2020 01:19:31.383 AM	akunrath / Angela Kunrath
Integration Event	07/03/2020 01:19:01.308 AM	akunrath / Angela Kunrath
Integration Build	07/03/2020 01:17:49.298 AM	akunrath / Angela Kunrath
Manage: Location	07/03/2020 01:16:16.843 AM	akunrath / Angela Kunrath
Set Up: Organization	07/03/2020 01:15:35.917 AM	akunrath / Angela Kunrath
Set Up: Academic Appointments and Related Data	07/03/2020 01:12:42.499 AM	akunrath / Angela Kunrath
Set Up: Academic Units	07/03/2020 01:11:56.505 AM	akunrath / Angela Kunrath
Worker Data: Public Worker Reports	07/03/2020 01:05:59.862 AM	akunrath / Angela Kunrath
Set Up: Curriculum Management	07/03/2020 01:02:19.250 AM	akunrath / Angela Kunrath
Manage: Section Data	07/03/2020 12:58:07.991 AM	akunrath / Angela Kunrath
Manage: Course Inventory	07/03/2020 12:58:07.991 AM	akunrath / Angela Kunrath
Manage: Curriculum Management	07/03/2020 12:58:07.991 AM	akunrath / Angela Kunrath
Manage: Course Material	07/03/2020 12:58:07.991 AM	akunrath / Angela Kunrath

OK Cancel

Image: Hit the OK button to confirm changes.