PIMS Administrators

Reference Guide
# Table of Contents

Pennsylvania Information Management System ................................................................. 4

PIMS .................................................................................................................................. 4

Overview ............................................................................................................................. 4

PIMS Security ....................................................................................................................... 4

PIMS Access .......................................................................................................................... 5

Initial Security Setup ........................................................................................................... 6

PDE User Registration ......................................................................................................... 6

Support Ticket ..................................................................................................................... 7

Authorization Email to PDE .................................................................................................. 9

PDE Reviews Request ......................................................................................................... 10

UserProfile ........................................................................................................................ 10

Authorization/Access ............................................................................................................ 11

Local Security or Pims Application Administrator ............................................................. 12

Group Overview .................................................................................................................. 12

Local Security or Pims Application Administrator – Add Users to Groups ......................... 13

Step 1 - Add Users to Group ............................................................................................... 16

Step 2 - Select an Institution .............................................................................................. 16

Step 3 - Group Membership Profile .................................................................................. 18

Local Security or Pims Application Administrator - Search ............................................... 18

Division of Data Quality
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>eScholar Data Manager</td>
<td>21</td>
</tr>
<tr>
<td>PIMS Template Names</td>
<td>22</td>
</tr>
<tr>
<td>Duplicate File Name</td>
<td>22</td>
</tr>
<tr>
<td>File Not Part of Submission</td>
<td>23</td>
</tr>
<tr>
<td>PIMS Template Upload</td>
<td>23</td>
</tr>
<tr>
<td>Home Page</td>
<td>24</td>
</tr>
<tr>
<td>File Manager</td>
<td>26</td>
</tr>
<tr>
<td>Validation Warning</td>
<td>29</td>
</tr>
<tr>
<td>Validation Failed</td>
<td>29</td>
</tr>
<tr>
<td>View Files</td>
<td>30</td>
</tr>
<tr>
<td>Download File Errors</td>
<td>32</td>
</tr>
<tr>
<td>Add to Batch</td>
<td>35</td>
</tr>
<tr>
<td>Batch Manager</td>
<td>37</td>
</tr>
<tr>
<td>Complete with Warnings</td>
<td>38</td>
</tr>
<tr>
<td>Complete with Errors</td>
<td>39</td>
</tr>
<tr>
<td>Cognos®</td>
<td>39</td>
</tr>
<tr>
<td>FAQ’s</td>
<td>41</td>
</tr>
<tr>
<td>PIMS User Manual and Training Guides</td>
<td>42</td>
</tr>
<tr>
<td>PIMS User Manuals</td>
<td>44</td>
</tr>
<tr>
<td>Volume 1</td>
<td>44</td>
</tr>
</tbody>
</table>
LOCAL SECURITY OR PIMS APPLICATION ADMINISTRATOR

FAQ’s .................................................................................................................. 45

VOLUME 2........................................................................................................... 45

PIMS HOW TO GUIDES AND TRAINING DOCUMENTS................................. 46

EMAIL .................................................................................................................. 47

WEBINARS......................................................................................................... 49

CURRENT WEBINARS ..................................................................................... 49

ARCHIVED WEBINARS .................................................................................. 52

USEFUL LINKS .................................................................................................... 52
Welcome to the PIMS team! PIMS, which is an acronym for the Pennsylvania Information Management System, can be challenging. This primer, along with the support of the team at PDE and PIMS Support Services, is designed to assist Local Security or PIMS Application Administrators with overcoming these challenges. More detailed information is available in the PIMS Manuals, eScholar Data Manager™ v3.0 PIMS Application User’s Guide, and other documents posted on the PIMS Website at www.education.state.pa.us.

PIMS

Overview

PIMS is a longitudinal data system (or data warehouse) that the Pennsylvania Department of Education (PDE) uses to collect student, staff, course, and other data from school districts and other local education agencies (LEAs) such as; charter schools, intermediate units, and career and technical centers.

PIMS data is used by PDE to send mandated reports to the federal government and to evaluate Pennsylvania programs. The collection of PIMS data replaces the annual collection of many separate reports by various PDE departments.

PIMS Security

The data collected in PIMS contains confidential information; therefore, to preserve the confidentiality of this data, secure access is required. The PDE Web Portal is the secure gateway to the PIMS applications. The PIMS applications secure access is designed to have
the PIMS Local Security Administrator or PIMS Application Administrator assign users to groups and to associate users with an institution.

There are four types of application security groups within the Web Portal.

- **Local Security Administrator** – The Local Security Administrator group is administered by PDE.
  - Responsibilities:
    - Overall Security of the Web Portal for the Institution
    - Administering the Local Application Administrator
    - Administering all Lower Groups in the Hierarchy

- **Local Application Administrator** –
  - Responsibilities:
    - Primarily Administering the Application Administrators
    - Administering all Lower Groups in the Hierarchy

- **Application – Local Administrator** –
  - Each PDE application will have an Application – Local Administrator group
  - Responsible for Administering the Application Groups
    - Example: PIMS – Local Administrator

- **Application Group** -
  - Membership in an Application Group provides access to the Application
  - Different Groups can Perform Different Functions within the Application

**PIMS Access**

PIMS data includes confidential information; therefore, a PDE log in and access to a PIMS
Group is required to access PIMS and PIMS Reports. The PDE log in is created by completing and submitting the PDE USER REGISTRATION form. The PDE USER REGISTRATION is required for PIMS application access and INITIAL SECURITY SETUP for the LEA.

**INITIAL SECURITY SETUP**

An Initial Security Setup is required for new LEAs and an LEA without a Local Security Administrator. The process for INITIAL SECURITY SETUP is:

1. Complete PDE USER REGISTRATION
2. Submit Support Ticket – Request Local Security Administrator Access for the Institution
3. Send Authorization Email to PDE – Must be submitted by the Chief School Administrator for the LEA
4. PDE Reviews Request – PDE may contact the Chief School Administrator for the LEA

**PDE USER REGISTRATION**

The first step to accessing PIMS or PIMS Reports is to create a PDE Web Portal log in. The USER REGISTRATION must be completed prior to requesting access for any application security group. Follow the instructions below for creating a PDE Web Portal log in:

1. Navigate to [www.education.state.pa.us](http://www.education.state.pa.us)
2. Click REGISTER
The REGISTRATION screen displays.

1. Complete Form
   a. All fields with a red asterisk (*) are required fields

2. Click REGISTER

When the request is received by PDE and access is granted, an email is sent to the email address submitted during the USER REGISTRATION process. Therefore, it is vital the email address is accurate.

Once the USER REGISTRATION confirmation email is received, log in to the PDE Web Portal with the USERID and PASSWORD created during the registration process. The USER PROFILE screen must be reviewed and saved before the Local Security Administrator or PIMS Application Administrator can add a user to a group.

**Support Ticket**

A SUPPORT TICKET must be submitted when requesting access for a Local Security Administrator. A SUPPORT TICKET should not be submitted if the LEA has a Local Security Administrator.
To submit a SUPPORT TICKET:

1. Go to [WWW.EDUCATION.STATE.PA.US](http://WWW.EDUCATION.STATE.PA.US)

2. Click HELP & SUPPORT

3. Scroll down to HELP & SUPPORT DOCUMENTS

   Complete and Submit the Support and Request Form by selecting:

4. Portal Security and Access

5. Security Administrator

6. No Security Administrator at my Institution
Authorization Email to PDE

If an LEA does not have a Local Security Administrator an authorization email must be sent to PDE by the Chief School Administrator for the LEA. The email request must contain the following information for the person selected as the Local Security Administrator for the LEA:

- Name
- UserID
- Title
- Phone Number
- Email Address – Must be Valid and Unique

The valid email must also contain the following information for the Chief School Administrator:

- Name
- Title
- Phone Number

Send the email to: RA-edhubadmin@state.pa.us

**NOTE:** Multiple PIMS users must submit a different email address for each user at the same LEA. PIMS users affiliated with multiple institutions must have a different UserID and email address for each location.

*Example: CEO operating multiple Charter Schools*
PDE REVIEWS REQUEST

Once the request is submitted, PDE will review the request, and if additional information is required, will contact the Chief School Administrator. An email notification is sent from PDE when the request has been approved, and the person selected as the Local Security Administrator for the LEA has been added to the group.

USER PROFILE

A USER PROFILE is required to obtain a PDE log in and to be granted access to PIMS applications. The USER PROFILE information is used by PDE for telephone and email correspondence, which includes; system availability, collection information, security for resetting a password, and other pertinent information. Therefore, it is essential for the USER PROFILE to contain accurate information.

The USER PROFILE screen must be viewed and saved before the Local Security or PIMS Application Administrator can add the user to a group.

To view or update the USER PROFILE:

1. Navigate to www.education.state.pa.us
2. Click LOG IN
3. Click My PDE

4. Click My Profile

![Image of My PDE interface]

5. Update User Profile

6. Click Save

**NOTE:** PDE and PIMS Support Services cannot update User Profile information.

**AUTHORIZATION/ACCESS**

The PDE Web Portal is the gateway to access all of PIMS’s applications. The initial access to PDE’s Web Portal is established through PDE’s Help Desk; however, access to a PIMS application, frequently referred to as **ADDING A USER TO A GROUP**, is established by the Local Security Administrator or the PIMS Application Administrator.
After gaining access to the PDE Web Portal, the LEA’s Local Security Administrator or the PIMS Application Administrator must grant access to the PIMS application. Each LEA must have at least one, but preferably two, Local Security Administrators to maintain the security and accuracy of the application through:

- **Add a User to Group** – Granting user security access to PDE applications
- **Review Registration Requests** – Email to Local Security or PIMS Application Administrator requesting access to a group
- **Delete Users from Groups** – Remove user security access to PDE applications

There are two methods of notifying the Local Security Administrator to grant access to a PDE application.

1. Directly notify Local Security or PIMS Application Administrator – PDE Preferred Method
2. Register for a Group – (See PDE Website Help and Support Documents)

**GROUP OVERVIEW**

There are three (3) components to a Group and there are three (3) Category Types. The components of a Group are:

- **Category Type** - Application
- **Group Category** – Abbreviation of the Application
- **Group Name** – User Role Within the Application
The Category Types are:

- Education Directory – Contains Security Administrator groups
  - Security Administrator Types include:
    - Local Security Administrator
    - Local Application Administrator
    - Application Administrator
- Application – Contains Application Groups (Roles)
  - Group Category – Application Abbreviation
  - Group Name – Application Role
- Portal Community – Groups Associated with Education Communities

**LOCAL SECURITY OR PIMS APPLICATION ADMINISTRATOR – ADD USERS TO GROUPS**

The Local Security Administrator or the PIMS Application Administrator can add a user to a group after the user has obtained a PDE log in.

To add a user to a group:

1. Log in to the PDE Web Portal
2. Click My PDE
3. Click USER/GROUP ADMINISTRATION

NOTE: If USER/GROUP ADMINISTRATION is not displayed, access was not granted by the Local Security Administrator to a Security Administration Group.

The My ADMINISTRATIVE GROUPS screen displays.

To search for a group:

1. Enter KEYWORDS
2. Click SEARCH
To view current members or to add new members to a group:

3. Click MANAGE USERS

<table>
<thead>
<tr>
<th>Category Type</th>
<th>Group Category</th>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education Directory</td>
<td>Chief Administrator</td>
<td>Chief</td>
<td>The chief executive officer and primary advisor to the board of education</td>
</tr>
<tr>
<td>Education Directory</td>
<td>Chief Administrator</td>
<td>Future Chiefs</td>
<td>Future chief executive officer and primary advisor</td>
</tr>
</tbody>
</table>

The MANAGE GROUP MEMBERSHIPS screen displays. To add a new user to a group:

1. Click ADD EXISTING USER

**NOTE**: Users can belong to multiple applications, but cannot have multiple roles.
STEP 1 – ADD USERS TO GROUP

The ADD USERS TO GROUP screen is displayed. This is the first of three steps to add a user to a group.

To begin the process:

1. Enter USERID

   Or

2. FIRST and LAST NAME

3. Click SEARCH

   Or

4. Select ADD from the list of users

The Select an Institution screen displays.

STEP 2 - SELECT AN INSTITUTION

The SELECT AN INSTITUTION is the second step in adding a user to a group. There are two
methods to add a user to a group. If the correct institution appears in the USE AN EXISTING EDUCATIONAL INSTITUTION AFFILIATION section:

1. Click Select

If there is no institution, or the incorrect institution is displayed, search for NEW EDUCATION INSTITUTION by keyword(s):

2. Enter INSTITUTION NAME
3. Click SEARCH

Locate the institution from the search results:

4. Click SELECT – (NOT SHOWN – Is available when search criteria is displayed)

The GROUP MEMBERSHIP PROFILE screen displays.

**NOTE:** If the new user is not located, verify the user has a PDE Web Portal log in, that the user has logged into the PDE Web Portal, and the USER PROFILE was reviewed and saved.
**STEP 3 - GROUP MEMBERSHIP PROFILE**

The **GROUP MEMBERSHIP PROFILE** is the final step in the process. This screen provides the ability to add group attributions, if applicable. To finalize the process:

1. Click **CREATE MEMBERSHIP**

**LOCAL SECURITY OR PIMS APPLICATION ADMINISTRATOR - SEARCH**

When the Local Security or PIMS Application Administrator is unknown, but needs to be notified to add a user to a group, or update an email address, a search can be performed from the PDE Web Portal. To conduct a search for the Local Security Administrator(s):

1. Log in to the PDE Web Portal
2. Click My PDE
3. Click APPLICATIONS
4. Click INFORMATION

5. Enter
   a. APPLICATION ABBREVIATION (PIMS)

   OR

   b. APPLICATION NAME (PIMS)

6. Click SEARCH
7. Click PIMS APPLICATION ADMINISTRATORS
The Security Administrators are displayed. To search for the Local Security or PIMS Application Administrator for a specific LEA:

8. Enter INSTITUTION NAME
9. Click SEARCH

The list of Local Security or PIMS Application Administrators for the selected LEA is displayed along with contact information. After receiving notification, the Local Security or PIMS Application Administrator can directly add a user to a group.
eScholar Data Manager™ (eDM), otherwise known as PIMS, is a secure web interface that manages and controls data as it moves through the data Extract, Transform, and Load (ETL) process; or commonly referred to as uploading templates into PIMS. eDM validates specific data submitted in the templates through up-front edits that are pre-determined by PDE.

Templates are files that load data into the PIMS data warehouse. Template specifications as detailed in the PIMS User Manual, Volume 1, define the fields required for each file submitted to PIMS. The data for the templates is extracted and uploaded into PIMS by the Local Security or PIMS Application Administrator.

**NOTE:** PIMS templates are also referred to as files or template files.

There are four methods to create PIMS template files:

1. **Student or Staff Information System (Source System)** – The software application purchased by the LEA from a software vendor to extract the templates identified in the PIMS User Manual, Volume 1.

2. **LEA Database - Extract or Export Data in the correct format as indicated in the PIMS User Manual, Volume 1.**

3. **PIMS Access Database** – Data-entry tool provided by PDE to create template files after data is entered into the PIMS Access Database.

4. **Excel® Spreadsheet or Text Editor** – Create PIMS templates manually.

**NOTE:** Prior to creating or editing PIMS template files in Excel®, contact PIMS Support Services at 1-800-661-2423.
PIMS TEMPLATE NAMES

The PIMS template name is required to be in the following format; AUN_TARGETTable_YYYYMMDDHHMM.xxx. The template name format provides the following information:

1. AUN - The 9-digit ADMINISTRATIVE UNIT NUMBER given to the LEA by PDE.
2. TARGET TABLE - The name of the template. This can be found at the beginning of the TEMPLATE SPECIFICATION in PIMS MANUAL VOLUME 1.
3. TIME AND DATE FORMAT YYYYMMDDHHMM is the 4-digit YEAR (YYYY), 2-digit MONTH (MM), 2-digit DAY (DD), 2-digit HOUR (HH) and 2-digit MINUTE (MM).
4. xxx - FILE EXTENSION
   a. SOURCE INFORMATION SYSTEM FILE - Typically a TAB delimited (.tab) file
   b. PIMS ACCESS DATABASE or EXCEL® SPREADSHEET - Should be a COMMA DELIMITED (.csv) file.

An example of a file name in:

- TAB DELIMITED FORMAT - 999999999_STUDENT_201103151134.tab
- COMMA DELIMITED FORMAT - 999999999_STUDENT_201103151134.csv

NOTE: See HOW TO MANUALLY EDIT A CSV TEMPLATE FILE WITHOUT LOSING FORMATTING document, which is located on PDE Website, PIMS Documents folder, for files created by hand.

DUPLICATE FILE NAME

Each file that is uploaded to PIMS must have a unique file name; therefore, the same file cannot be uploaded twice. For example, the first file uploaded has the unique file name of
LOCAL SECURITY OR PIMS APPLICATION ADMINISTRATOR

999999999_STUDENT_201207121139. If the same file is uploaded again, the file name needs to be revised or the file upload will fail. To prevent the file from failing for a duplicate file name, the MMDDHHMM section of the file name could be changed to: 999999999_STUDENT_201207151245.

FILE NOT PART OF SUBMISSION

If a file that is not part of the DATA SUBMISSION period is uploaded, the PIMS application will generate the FILE NOT PART OF SUBMISSION PERIOD error. If this error is generated, change the DATA SUBMISSION drop-down to the correct submission. If necessary, click HOME to verify which files are available for the data collection submission period.

PIMS TEMPLATE UPLOAD

The upload of the data collection templates begins with the submission of data to PDE. There are three sections to the PIMS template upload process.

1. PIMS HOME PAGE - List the data collections that are open for data submission

PIMS, through eDM, uploads templates in two steps:

2. FILE MANAGER – Templates were successfully uploaded and edits applied, possible errors

3. BATCH MANAGER – Files that passed File Manager edits, are batch processed, and additional edits applied, possible errors
   a. A batch may consist of 1 template or multiple templates
   b. A batch with multiple templates must be:
      i. For the same collection
      ii. Loaded in proper sequence (See PIMS User Manual, Volume 1)
The PIMS HOME page is where the process of submitting data begins. The HOME page includes the:

- Menu
- External Links
- System Messages
- Open Collections

To begin the process of uploading the PIMS templates, from the left menu bar:

1. Click UPLOAD
2. Select a DATA COLLECTION
3. Click BROWSE to locate the file
4. Click the **FILE/ALL FILES WITHIN ZIP FILE CONTAIN HEADERS** (Only if file contains a header row)

5. Click **UPLOAD**

If no errors are detected, the file is automatically moved to the **FILE MANAGER**.

If errors are detected, error messages will appear in:

- **SYSTEM MESSAGE FIELD**
- **Above SYSTEM MESSAGE FIELD**
- **Above FILE NAME**

The most common errors are:

- **File Name Incorrect**
- **File Name Duplicated**
- **File is not part of selected Data Collection**

**NOTE**: Templates must be uploaded in the order specified in the **PIMS USER MANUAL VOLUME 1.**
The System Message indicates the error, unless the file has advanced to the File Manager. The error message above the System Message field indicates an error occurred and the selected files need to be corrected and uploaded again. A message will also display above the file with errors. Files with errors are indicated by the message above the file name. The message states: Error – roll over with mouse to view.

The errors must be corrected before the file can be uploaded and moved to the File Manager.

**NOTE:** To maintain data accuracy and consistency, correct data in Student or Staff Information System prior to re-uploading the data file.

**FILE MANAGER**

The File Manager is the next step in the eDM (PIMS) process. The File Manager validates the structure of the file including:

1. PASecureIDs  
2. Snapshot Date  
3. District Codes (File – Column A)  
4. Various Code Sets
A file that successfully uploads will automatically move to the FILE MANAGER. The status of the file, indicated below, will change as it is processed through the FILE MANAGER.

<table>
<thead>
<tr>
<th>FILE STATUS</th>
<th>ICON</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECEIVED</td>
<td><img src="image" alt="file" /></td>
<td>File Received  &lt;br&gt; Validation in Process</td>
</tr>
<tr>
<td>VALIDATION OK</td>
<td><img src="image" alt="check" /></td>
<td>Validation Complete  &lt;br&gt; No Errors  &lt;br&gt; Ready for Batch Processing</td>
</tr>
<tr>
<td>VALIDATION WARNING</td>
<td><img src="image" alt="error" /></td>
<td>File Contains Errors, but less than the Threshold  &lt;br&gt; Records in Error Removed from the File  &lt;br&gt; Remaining Records can be Processed</td>
</tr>
<tr>
<td>VALIDATION FAILED</td>
<td><img src="image" alt="cross" /></td>
<td>File Contains more Errors than the Threshold  &lt;br&gt; File cannot be Processed</td>
</tr>
</tbody>
</table>

The FILE MANAGER screen displays with the RECEIVED status icon. This is the first status in the FILE MANAGER process. The file will remain in the RECEIVED status until the FILE MANAGER validations are processed.

**NOTE:** To verify the file has completed processing through the FILE MANAGER, the screen must be refreshed.
The status of the file does not automatically change when the validation process is complete. To update the status:

1. Click **REFRESH** 🔔 to view status changes

When the file has completed processing through the **FILE MANAGER**, and if has passed all of the PDE required validations, the **VALIDATION OK** icon will appear in the **STATUS** column:

2. **VALIDATION OK** ✅ indicates the file processed correctly, no errors were found

The file is ready to be added to a **BATCH**.

If the file failed some of the validations, a validation warning icon will appear in the status field. The failed icon will appear in the status if the file contains more errors than the limit designated by PDE.

**NOTE:** PDE recommends deleting the files with a warning or failed status and re-submitting, after the records with errors are corrected in the Source System.
**Validation Warning**

A **Validation Warning** indicates the file contains some errors but the errors are less than the threshold set by PDE. The file can be added to a batch, but the errors that caused the warnings are removed from the file. The records with errors need to be corrected and re-submitted to PIMS.

**Validation Failed**

A **Validation Failed** icon indicates the file contains more errors than the threshold set by PDE. The file cannot be processed as a batch. The file must be corrected and re-submitted to PIMS before it can be added to a batch.
**VIEW FILES**

The file contents need to be viewed to determine the errors when a VALIDATION WARNING or VALIDATION FAILED icon is displayed.

To view files:

1. Click VIEW

The page defaults to the GENERAL INFORMATION screen.

2. Click VALIDATION INFORMATION
3. Scroll to File Contents

4. Locate ERROR.ZIP
   a. View number of RECORDS IN ERROR, Errors and WARNINGS

5. Click View File Content

The FILE CONTENT screen displays in a view similar to an Excel® spreadsheet.

6. Use the scroll bars at the bottom and right side of the screen to view ERRORS and WARNINGS

7. ERRORS and WARNINGS are highlighted in red

Position the cursor over the highlighted field to view errors and warnings. A tool tip text displays with a message such as; *Failed ISO Date*. Fields will not be highlighted if the data is...
reported in the wrong column.

To correct the error(s):

1. Verify SOURCE FILE is in correct format
2. Correct errors and warnings in the SIS
3. Extract the corrected file and upload to PIMS

**NOTE**: The viewing screen is limited to 100 records. Files over 100 records need to be downloaded to view the entire list of errors.

**DOWNLOAD FILE ERRORS**

If the file has over 100 errors, the file will need to be downloaded to view the complete list of errors.

To download the file:

1. Click VIEW

The page defaults to the GENERAL INFORMATION screen.
2. Click Validation Information

3. Scroll to File Contents

4. Locate ERROR.ZIP
   a. View number of Records in Error, Errors and Warnings

5. Click View File Content

The File Content screen displays in a view similar to an Excel® spreadsheet.
6. Locate the **DOWNLOAD FILE**

7. Double click **ERROR.ZIP FILE**. If applicable, follow the instructions to:

   a. Unzip wizard to open and view the file

   OR

   b. Locate the unzipped document

      i. Double click the document to open it

8. Locate **ZIPPED FILE** saved to Computer

9. Locate **ERRORS or WARNINGS HIGHLIGHTED IN RED**

10. **Correct errors or warnings in Source System**

11. **Extract file from Source System**

12. **Upload corrected file to PIMS**
**ADD TO BATCH**

Once the file has uploaded successfully in the FILE MANAGER, the file can be added to a BATCH. A BATCH may contain one file or multiple files.

**NOTE:** Files must have a status of VALIDATION OK or VALIDATION WARNING to be added to a BATCH.

To add a file to BATCH:

1. Select the File(s)
2. Click ADD TO BATCH

![Add File to Batch]

The BATCH can be viewed after the screen refreshes.

3. Click VIEW BATCH

![View Batch]
The **View Batch** screen displays:

4. Select **FILE(s)**
5. Add **Batch Comments**
6. Click **Process Batch**

The **Batch Manager** screen displays.

**NOTE**: Add a **Batch Comment** to make searching for batches easier.
**Batch Manager**

The Batch Manager checks the contents of the data for validity and dependencies when loading the data into the PIMS Data Warehouse. Files added to a Batch from the File Manager screen are processed by the Batch Manager.

Currently, the Batch Manager checks:

- Required Dependencies – i.e. Student ID not in Student table
- Various Code Sets – i.e. CIP Codes or State Course Codes
- Other Validations – i.e. Location Codes of Residence or District Code of Residence

As the files are processed by the Batch Manager the status of the files are indicated by the following icons.

<table>
<thead>
<tr>
<th>BATCH STATUS</th>
<th>ICON</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready to Process</td>
<td></td>
<td>Indicates a Waiting or Queued Status</td>
</tr>
<tr>
<td>Processing</td>
<td></td>
<td>Batch Processing</td>
</tr>
<tr>
<td>Complete</td>
<td></td>
<td>Processing Complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No Errors Detected</td>
</tr>
<tr>
<td>Complete with Warnings</td>
<td></td>
<td>Processing Complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Load Plan Warnings Generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All Records Loaded</td>
</tr>
</tbody>
</table>
When a file is first added to a BATCH, the file is in the READY TO PROCESS or PROCESSING status. To update the processing status of the file click REFRESH. The VALIDATION OK (green checkmark) indicates the file processed correctly.

**NOTE:** Files with errors that were removed in File Manager are not included in BATCH PROCESS. The files with errors in FILE MANAGER need to be corrected in the SOURCE SYSTEM, and re-submitted to PIMS.

### Complete with Errors

<table>
<thead>
<tr>
<th>Complete with Errors</th>
<th>Processing Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Errors Found</td>
</tr>
<tr>
<td></td>
<td>Records Not Loaded</td>
</tr>
<tr>
<td></td>
<td>Review Errors</td>
</tr>
</tbody>
</table>

### Failed

<table>
<thead>
<tr>
<th>Failed</th>
<th>Processing Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System Error – Report to PIMS Support Services</td>
</tr>
</tbody>
</table>

### Complete with Warnings

There are three categories of warnings in BATCH MANAGER:

1. **Warn Child Accounting** – Indicates PIMS School Calendar Instructional Minutes Not Between 150 and 240.
   a. Correction –
      i. Verify the minutes are correct
2. **WARN STAFF** – Indicates Course Instructor template has instructors who were not uploaded in the Staff template
   
   a. Correction –
      
      i. Upload Staff template with instructors in the Course Instructor template
   
   ii. Verify Course Instructor and Staff templates have correct PPIDs

3. **WARN STUDENT** – A record in the Student or Student Snapshot template has a different Last Name and Birth Date with an associated PASecureID that already has a record in the PIMS Warehouse
   
   a. Correction -
      
      i. Verify the PASecureID has the correct name and date of birth

**COMPLETE WITH ERRORS**

Validation errors are generated when the file contains more errors than the maximum set by PDE. A batch with the status of **VALIDATION ERROR** cannot be processed. The file must be corrected in the Source System and re-submitted to PIMS.

**NOTE:** **COMPLETE WITH ERRORS** does not indicate ALL of the files have errors. Individual files without errors may have processed and were inserted into the data warehouse.
Cognos®, also known as PIMS Reports, is the application used to generate validation, production, and ACS reports. The reports are used to:

- Verify and Validate Data Submitted to PIMS
- Review Data in Production prior to Publication
- Generate the Accuracy Certification Statement (ACS)

**NOTE:** A signed ACS verifies the data submitted to PIMS is accurate and final to the best of the LEA’s ability.

The Collection and the related Cognos® folder for the PIMS reports are listed below.

<table>
<thead>
<tr>
<th>Collection</th>
<th>Cognos® Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access for ELLs/End of Year</td>
<td>LEP Reports</td>
</tr>
<tr>
<td>Child Accounting</td>
<td>Child Accounting Reports</td>
</tr>
<tr>
<td>Course</td>
<td>Course Reports</td>
</tr>
<tr>
<td>CTE</td>
<td>CTE Reports</td>
</tr>
<tr>
<td>Graduate, Dropout, Cohort</td>
<td>Graduation and Dropout Reports</td>
</tr>
<tr>
<td>HQT</td>
<td>HQT Reports</td>
</tr>
<tr>
<td>October Student Enrollment</td>
<td>Enrollment Reports</td>
</tr>
<tr>
<td>PATI</td>
<td>Low Income Reports</td>
</tr>
<tr>
<td>Precode or PSSA Refresh</td>
<td>PATI</td>
</tr>
<tr>
<td>Safe Schools</td>
<td>Precode Reports</td>
</tr>
<tr>
<td>Special Education</td>
<td>Safe Schools</td>
</tr>
<tr>
<td>Staff</td>
<td>Special Education Reports</td>
</tr>
<tr>
<td></td>
<td>Staff Profile Reports</td>
</tr>
</tbody>
</table>
FAQ’s

Q: Why do I get the SQL 121 Error when trying to run a report? Actual Error reads: An error occurred while performing operation 'sqlPrepareWithOptions' status='-121'.

A: Cognos has a refresh period two times a day. When an attempt to run a report during a refresh the SQL 121 Error is displayed. Sometimes the report will just spin or it might display another SQL error.

NOTE: The refresh occurs twice a day - once from noon to 2:00p.m., and again at 5:00 a.m.

Q: Why do I get the 3rd Party Provider Encountered an Unrecoverable Exception error when I try to log into Cognos?

A: The 3rd Party Provider error is a time out issue. Shut down the browser completely and then re-launch it. Then log back into the PDE Website and then back into Cognos.

NOTE: If Cognos®, PDE applications, or the PDE Website is left idle for several minutes, an error message is displayed.
PIMS USER MANUAL AND TRAINING GUIDES

The PIMS USER MANUALS and TRAINING GUIDES provide information on PIMS Collections, template requirements, and PIMS Reports. The USER MANUALS and TRAINING GUIDES are located on the PDE Website www.education.state.pa.us.

To locate the documents:

1. Click PROGRAMS
2. Select PENNSYLVANIA INFORMATION MANAGEMENT SYSTEM (PIMS)
3. Click Go
4. Click PIMS DOCUMENTS
Select the folder icons to view the documents associated with the folder name. It is highly recommended to view the PIMS User Manuals, the PIMS How to Guides and Training Documents, and the PIMS Webinars.

**NOTE:** The PIMS Question & Answer Webinar schedules are located on the PIMS Main page and the Documents page.
PIMS User Manuals

The PIMS User Manuals contain the information necessary for creating and submitting complete and accurate PIMS collection templates. The PIMS User Manual is comprised of two volumes. Volume 1 consists of template details and Volume 2 contains the appendices referenced in Volume 1.

Volume 1

The beginning of the PIMS User Manual Volume 1 includes general information such as:

- Pennsylvania Department of Education Administration
- Public Education Department PIMS Team
- PIMS User Manual Change Summary – Volume 1 and Volume 2
- Students to be Reported in PIMS
- Staff to be Reported in PIMS
- Race/Ethnicity: Federal Race and Ethnicity Standards
- Templates
- Extracting Data into Template Format
- Data Manager (eDM)

In addition, the manual provides template specifications and detailed information for each template listed in a PIMS Collection.

- Child Accounting Domain
- Location Domain
- Course and Grades Domain
- Survey Domain
- Discipline Domain
- Staff Domain
FAQ’s

Frequently Asked Questions (FAQ’s) are located after each template specification in a collection. In addition, guidance on extracting data into template format and a web link to detailed documentation on DATA MANAGER is provided at the end of THE PIMS USER MANUAL VOLUME 1.

VOLUME 2

The appendices that are referenced in the PIMS USER MANUAL VOLUME 1 are located in the PIMS USER MANUAL VOLUME 2. This includes everything from APPENDIX A – COURSE CODES to APPENDIX AC – PROGRAM PROVIDER TYPE CODES. The codes in the PIMS USER MANUAL VOLUME 2 must be used where indicated in the template specifications listed in the PIMS USER MANUAL VOLUME 1.
PIMS HOW TO GUIDES AND TRAINING DOCUMENTS

The PIMS HOW TO GUIDES and TRAINING DOCUMENTS folder contains a collection of resources that are often overlooked. The various documents provide guidance pertaining to PIMS that can be viewed on-line or downloaded to a computer.

The screen displays:

1. Document Format
2. Document Name
3. Date and Time Created
4. Download Document Icon

**NOTE**: Click document name to view without downloading document.
EMAIL

PDE frequently communicates with LEAs through emails. Therefore, it is extremely important for the Local Security or PIMS Application Administrator to maintain email addresses in the PDE Web Portal. Accurate email addresses ensure essential information is received.

Emails inform LEAs of:

- Collection Dates
- Missing Information
- Data Errors
- Webinars
- Updated/Revised Documents
- PIMS Maintenance

Local Security or PIMS Application Administrators can maintain email addresses through the PDE Website.

1. Go to [WWW.EDUCATION.STATE.PA.US](http://WWW.EDUCATION.STATE.PA.US)
2. Click HELP & SUPPORT
3. Scroll down to HELP & SUPPORT DOCUMENTS
4. Click Document Name to View
5. Click Help Desk Support

**NOTE:** This is *not* PIMS Support Services.

---

**NOTE:** Multiple PIMS users must submit a different email address for each user at the same LEA. PIMS users employed by multiple LEAs must submit a different email address for each LEA.
WEBINARS

Webinars are conducted for the individual PIMS collections, and for Questions and Answer sessions. The webinars are offered at different times and dates to allow LEAs the option to attend a webinar that best fits the LEAs schedule. PDE recommends that LEAs attend one session of each appropriate PIMS collections webinar and the Q & A webinars; or listen to the recording of the webinars.

**NOTE:** Webinars are limited in the amount of seats available for each session.

The individual PIMS collection webinars provide collection-specific information such as:

- Collection Schedule
- Accuracy Certification Statement (ACS) Due Date
- Best Practices
- Tips and Techniques

The Question and Answer (Q & A) webinars are open forums that include representatives from each of the PIMS collections. This webinar provides the LEAs an opportunity to ask the representatives questions in regards to any of the PIMS collections.

**CURRENT WEBINARS**

Current, future, and recorded webinar events are listed on [www.pdewebinars.org](http://www.pdewebinars.org). This Website allows an LEA to view and select current and future events, register for a webinar, or join a webinar session.
The PDE webinar web page defaults to show a list of current webinars that can be searched by:

1. **Search Field**
2. **Scroll Bar**
Each webinar listing provides the:

1. Webinar Name
2. Name of Presenter
3. Agency of Presenter
4. Description of Webinar
5. Target Audience
6. Available Sessions
7. Date and Time
8. Total Number of Seats
9. Number of Available Seats
10. More Information
11. Register

**NOTE:** Registering for a webinar is not required, nor does it guarantee a seat. However, it does provide notice in the rare event a webinar is canceled.
ARCHIVED WEBINARS

Webinars are recorded during the live presentations. The recorded webinars are archived for future reference, and are accessible at www.pdewebinars.org/archives.php or through the navigation bar at the top of the screen.

NOTE: To return to current webinars click CURRENT WEBINARS on the navigation bar.

USEFUL LINKS

PDE recommends that LEAs verify that their computer meet or exceed the minimum system requirements, and that the LEAs test their computer in advance of the webinars. Each webpage contains a section that provides access to:

- Presenter Proposal Form
- System Requirements
- Test Your Computer
- Elluminate Support

Performing these two tasks well in advance of the webinar provides the necessary time to correct the problem and still attend the webinar.

NOTE: This process is not necessary for future webinars unless a new or different computer is used to attend the webinar.