FLORIDA DEPARTMENT OF EDUCATION

SLDS Program
Race to the Top
FLDOE Single Sign-on
LEA Integration and
User Provisioning Specification

Version 1.0

Revision Date:	June 10, 2013
Sponsor:	Accountability, Research, and Measurement
Program:	Statewide Longitudinal Data Systems (SLDS) Program
Project:	RTTT Portal and Single Sign-On Initiative
Document Control #:	SLDS-00065

Revision History

Date	Version	Description of Revision	Author
5/9/2012	.02	Initial Draft	Joshua Richmond
5/11/2012	.03	Updated with input from leadership	Joshua Richmond
7/6/2012	.04	Reduced the number of application attributes	Joshua Richmond
7/16/2012	.05	Multiple user information files; spelling changes	Joshua Richmond
7/30/2012	.06	Changed Proginet to TIBCO. Synced with the RTTT_SSO User Information v.12 document.	Joshua Richmond
7/31/2012	.07	Removed reference to the Readiness Cert. Settled on a file naming convention.	Joshua Richmond
8/6/2012	.08	Added ftp info, onboarding/training, existing apps.	Joshua Richmond
8/13/2012	.09	FIM portal info; Provisioning process precedence; Deprovisioning; ValidUser flag.	Joshua Richmond
8/14/2012	.10	Updates from the Custom Development Requirement and SSO Committee meetings.	Joshua Richmond
08/21/2012	.11	Prepared for LEA testers.	Robin Borschel
08/28/2012	.12	Added section for LEA authorization to use specific applications	Robin Borschel
10/23/2012	.13	Removed SchoolType Attribute and added description of UserType attribute	Christopher Webb
02/18/2013	.14	Removed provisioning method combining with transmission file. Update transmission file. Update Appendix A, B & C	Edwin Hurley
3/11/13	.15	Updated on-boarding tasks, document name, added authorization file specs for each application, removed Appendix A.	Andrea Latham
5/23/13	.16	Updated on-boarding steps, added key contacts, updated user provisioning data with new identity and authorization formats; updated FIM Portal information; removed Appendix A and B.	Andrea Latham
6/10/13	1.0	Added SSO Reports; finalized all information.	Andrea Latham

Approvals Page

FLDOE SSO LEA Integration & User Provisioning Specification

Version 1.0

Program Sponsors

Todd Clark	Date
Kit Goodner	Date
David Stokes	Date

Project Manager

Gar Schafer	Date

TABLE OF CONTENTS

Revision History ..... **I**

Approvals Page ..... **II**

1 Introduction **4**

2 On-boarding Steps **4**

3 Key Contacts **5**

4 Authentication **5**

4.1 FLDOE-Hosted 6
4.2 WS-Federation 6
4.3 Comparison of WS-Federation versus FLDOE-Hosted 7

5 User Provisioning Data **8**

5.1 Identity Attributes 8
5.2 Authorization Attributes 10

6 Data Submission **11**

6.1 File Transmission 11
6.2 File Encryption 11
6.3 File Formats 12
6.3.1 CSV 12
6.3.2 Identity File CSV Example 12
6.3.1 Authorization File CSV Example 12
6.3.2 XML 13
6.3.3 Identity File XML Example 13
6.3.4 Authorization XML Example 13
6.4 Forefront Identity Manager (FIM) Portal 14
6.4.1 How to Access the FIM Portal 14
6.4.2 View or Modify your Profile 17
6.4.3 Add New User 20
6.4.4 Modify User 24
6.4.5 Add User Authorizations 27
6.4.6 Modify Authorizations 30
6.4.7 Delegating Administrators 35
6.4.8 Password Reset 38
6.4.9 Delete or Disable Users 41

7 SSO Reports **46**

1 Introduction

The Florida Department of Education Single Sign-On (FLDOE SSO) is one web address, www.fldoe.org/sso, which enables users to access a selection of FLDOE resources with one username and password. The list below identifies the six FLDOE resources that will be available via single sign-on by June 2014; after which, additional resources will be integrated.

- CPALMS – Statewide Standards & Instructional Resource Tool
- eIPEP – Educator Preparation Institution Reporting Tool
- English Language Arts Formative Assessment System
- FloridaSchoolLeaders.org – Leadership Development Tool
- Interim Assessment Item Bank Test Platform
- PMRN – Florida Interim Assessment for Reading (FAIR)

All local education agencies (LEAs) requiring access to any of the resources in the FLDOE SSO must provision user accounts. Provisioning means to create, update, or disable a user's access to FLDOE resources. This *FLDOE SSO LEA Integration & User Provisioning Specification* details the on-boarding steps, identity and authorization data required for each user, and information about the ways this information can be submitted to the Department. The FLDOE SSO includes a variety of methods to meet the needs of all types and sizes of LEAs.

LEA Administrators are encouraged to visit the FLDOE SSO website periodically for news, information, training resources, and the latest versions of all FLDOE SSO specifications at: www.fldoe.org/sso/communications.asp. The FLDOE SSO team can be reached at (850) 245-9776 or fldoe-sso@fldoe.org.

2 On-boarding Steps

There are a number of steps that need to be taken in order for an LEA to participate in the FLDOE SSO. First and foremost, the LEA should navigate to the FLDOE SSO website at www.fldoe.org/sso/communications.asp to access on-boarding materials and review training videos. The LEA must determine their key contacts and authentication method before initiating on-boarding steps.

1. Submit the Memorandum of Understanding (MOU) and LEA Participation Form to fldoe-sso@fldoe.org.
    - The FLDOE SSO team will provide the LEA Functional and Technical Leads with their unique SSO ID and secure file transfer account information to support the provisioning process.
    - If WS-Federation is selected as the LEA's authentication method, documentation will be provided on how to establish a trust. The LEA will work with the FLDOE SSO team to establish the connection before proceeding to Step 2.

2. Upload **staff** identity file to the secure file transfer account (CD to TEST); email the FLDOE SSO team when complete.
    - The FLDOE SSO team will provide feedback on the results of the file. Accounts will not be created.

3. Verify the IT Helpdesk information that will be published online for user support.

4. Upload **lead** identity file (for the two leads only) to the secure file transfer account (CD to PROD); email the FLDOE SSO team when complete.
    - The FLDOE SSO team will elevate the leads to LEA Admin status and provide training on how to use the system. This allows the leads to get familiar with the system before initiating accounts for the entire LEA.

5. Complete user provisioning training.

6. Schedule a cutover date.

7. Notify the LEA Helpdesk staff and end users.

8. Submit the Certificate of Readiness form to fldoe-sso@fldoe.org.
    - The Certificate of Readiness is required to satisfy a grant deliverable for public school district LEAs participating in the Race to the Top grant. Upon receipt of the form, the FLDOE SSO team will review, sign, and return a scanned copy via email. The document may be uploaded to the grants management system as evidence the deliverable has been met, or you may select the "no upload" option and indicate the details of when it was sent and to whom (ex: sent June 1, 2013 to fldoe-sso@fldoe.org).
    - If the LEA is not participating in the Race to the Top grant, skip this step and proceed to Step 9.

9. On the scheduled cutover date, upload production-ready user provisioning information to the LEA's secure file transfer account (CD to PROD).
    - Successful receipt of user provisioning information triggers automated emails to FLDOE-Hosted users with their username and password prompting them to complete their account registration and WS-Federated users will be enabled to utilize applications as authorized (notification will not be sent from FLDOE).

10. Log into the FIM Portal and review SSO Reports for PROD file processing results; continue to manage LEA users and support FLDOE SSO.

3 Key Contacts

FLDOE SSO requires two key contacts from each LEA to participate, a Functional Lead and a Technical Lead, each having their own responsibilities. The Functional Lead serves as the primary point of contact for policy, process, and approval requirements related to participation in the FLDOE SSO. The Technical Lead serves as the sole secure transfer file account user and primary LEA Admin within the FIM Portal. If WS-Federation is selected, the Technical Lead is also responsible for establishing the WS-Federation connection and managing certificate information. These two roles cannot be held by the same person.

4 Authentication

There are two configuration options available when it comes to how users are authenticated. LEAs are responsible for selecting one authentication method for all its users at all sites within their purview. For public school district LEAs, this includes charter schools. The LEA must

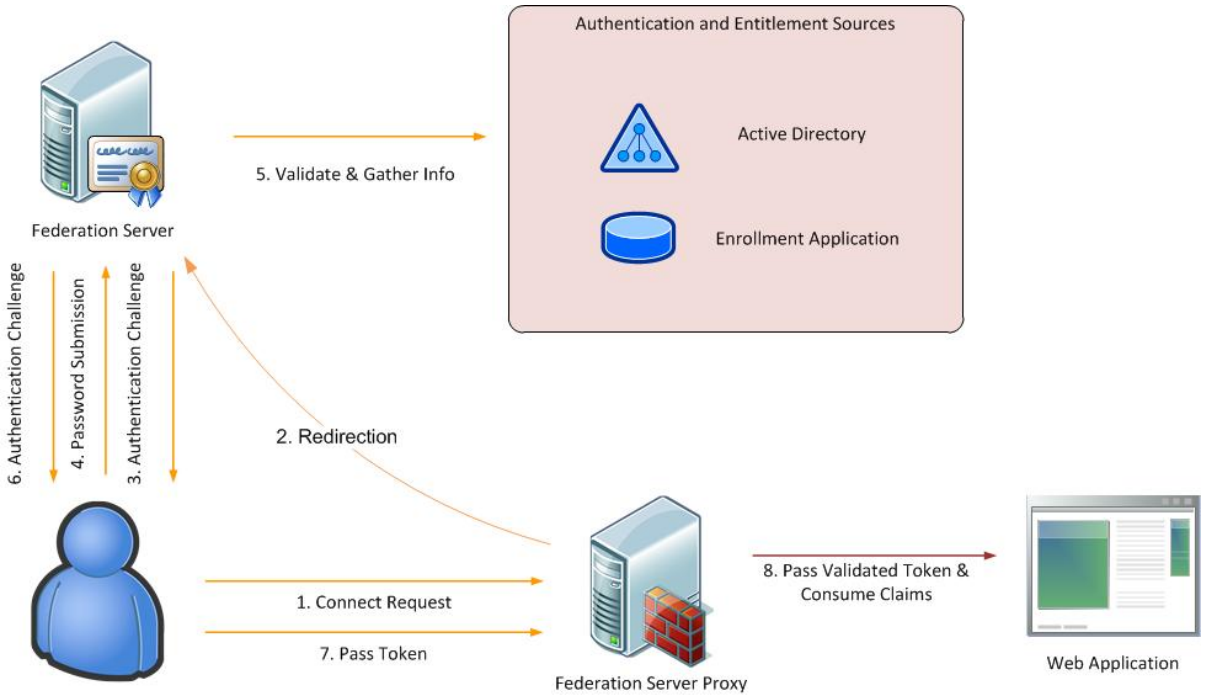
choose which authentication option is right for them prior to on-boarding with the FLDOE SSO. The two authentication options available for LEAs are as follows:

4.1 FLDOE-Hosted

This method requires the LEA Technical Lead to provide user provisioning information for each person who requires access to the applications integrated into the FLDOE SSO environment. With this information the system will create an SSO username and issue email notifications to the user to complete the account registration process. Users will navigate to www.fldoe.org/sso and log in to access the applications. User accounts and passwords are maintained in the FLDOE SSO Active Directory and follow the same security policies for all hosted entities. If an LEA prefers to control password policies (such as length and frequency of change) for its users, then the WS-Federation option should be explored.

The diagram below shows how authentication and claims work in the Hosted scenario. Note: the "Web Application" below represents any of the WIF-enabled applications participating in FLDOE SSO such as Florida School Leaders, CPALMS, and eIPEP.

FLDOE- Hosted User Authentication Model



4.2 WS-Federation

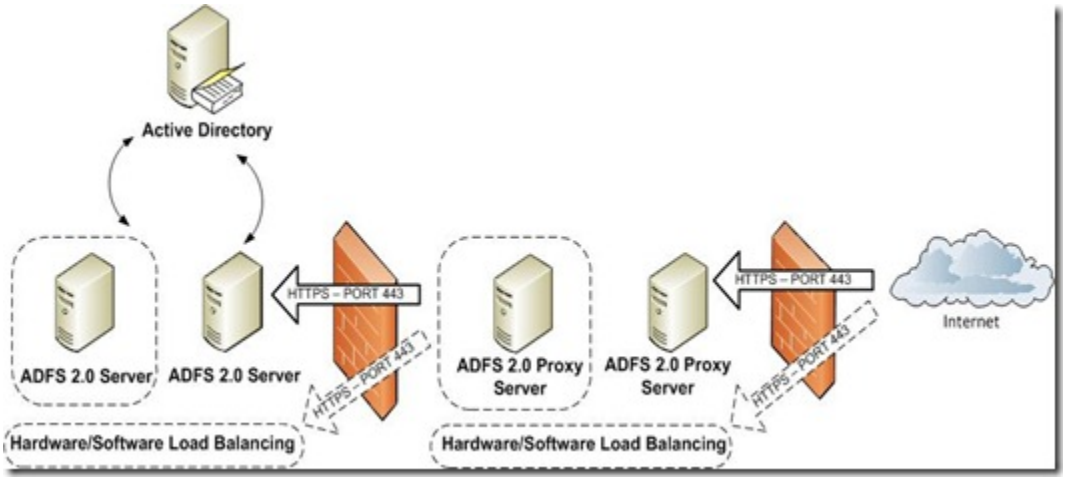
This method requires the LEA Technical Lead to provide user provisioning information for each person who requires access to the applications integrated into the FLDOE SSO environment. Additionally, the LEA must maintain current SAML 2.0 compliant federation service, an SSL certificate, and a code signing certificate. A one-way trust is established between FLDOE and the LEA. Users will log in to the local LEA system first (authenticating with the same username and password they currently have) and then navigate to the FLDOE portal to access the applications. WS-Federation supports any SAML 2.0 compliant Identity

provider, the example below is with Microsoft's ADFS 2.0 services but other Identity Providers can also be used.

An ADFS 2.0 solution consists of the following components:

- ADFS server(s) (internal network joined to AD forest)
- ADFS Proxy Server(s) (perimeter network used to support remote users)

WS-Federation using Microsoft ADFS 2.0



To request additional information regarding WS-Federation requirements, please email the FLDOE Administration Team at fldoe-sso@fldoe.org.

4.3 Comparison of WS-Federation versus FLDOE-Hosted

LEAs should carefully consider the pros and cons of each authentication option. WS-Federation has the benefits of utilizing the LEAs current security and authentication directory, but also requires extra effort such as setting up your Identity provider. FLDOE-Hosted has the benefit of allowing control through the provisioning files with no need to maintain passwords, but does require some planning around how applications will be assigned to users (centrally through the authorization file or delegated through the FIM Portal).

FLDOE-Hosted	WS-Federation
Requires user provisioning information	Requires user provisioning information
One username and password issued by **FLDOE** using one security policy	One username and password issued by the **LEA** using the LEA security policy Note: LEA Admins and Location Admins using the FIM Portal will have an additional username and password used for administration only**.**

Users authenticate with **FLDOE** to access FLDOE applications (www.fldoe.org/sso)	Users authenticate with **LEA** to access FLDOE applications (i.e.: www.yournetwork.org)
No additional technology required	Requires current SAML 2.0 compliant federation service, an SSL certificate, and a code signing certificate. Certificates must be issued from a third party certificate authority such as GoDaddy, Symantec, Comodo, Global Sign, etc.
No local Directory requirements	Local Directory must include user email addresses

5 User Provisioning Data

Regardless of the authentication method selected above, user provisioning information is required for each person who needs access to the applications integrated into the FLDOE SSO environment. There are two types of information used for the provisioning process: identity and authorization. The identity information is about "who" the person is and authorization information is about "what" the person can access.

5.1 Identity Attributes

The FLDOE SSO requires a selection of attributes about each user to be provisioned. The following is a list of the identity fields with rich descriptions. Attributes are limited to staff at this time.

Field Name	Order	Description	Example	
SSO ID	1	The SSO ID is a unique identifier for each trusted source of provisioning information. The FLDOE SSO team will provide this number to the LEA during the on-boarding process.	54	Required
Email Address	2	The email address of the user. *If the WS-Federation is selected, it is critical that the email address provided match the email address recorded in the LEA's local Directory.	John@doe.org	Required
Valid User	3	Valid User may be True or False.	True	Required

User Type	4	User Type may be Staff.	Staff	Required
First Name	5	The legal first name of the user.	John	Required
Middle Name	6	The legal middle name of the user.	Fitzgerald	Optional
Last Name	7	The legal surname of the user.	Smith	Required
Name Suffix	8	The academic, religious, generational, or professional suffix that follows the user's full name.	Jr.	Optional
State ID Number	9	Reserved for the Florida Education Identification Number available in 2014.	FL888888888888	Optional
Birth Date	10	The date of birth of the user (MMDDYYYY).	09171974	Optional
Site ID	11	The primary administrative reporting unit to which the user is assigned. For public school district LEAs, the Site ID is the state assigned four-digit school number (0001-9899) from the MSID; commonly reported on Surveys as (School Number, Primary/Home)[1]. http://doeweb-prd.doe.state.fl.us/EDS/MasterSchoolID/ For public and private postsecondary LEAs, the Site ID is the six-digit IPEDS ID number. http://nces.ed.gov/globallocator/	1234	Required
Job Category	12	The primary job code assignment to which staff is assigned. Only one job category is permitted. For public school district LEAs, the Job Category is the survey code associated with the primary job assignment of the employee (Job Code, Primary). http://www.fldoe.org/eias/dataweb/database_1213/208750.pdf For public and private postsecondary LEAs, the Job Category is a SOC code. http://www.bls.gov/soc/	53002	Optional
Local ID Number	13	The unique local identification number assigned to staff within the LEA. This number may be alphanumeric, up to 50 characters.	755741	Required

[1]For public school district LEAs, the Site ID must be a valid number listed in the MSID. Finer grain site numbers, such as those assigned to staff working at the district level, should be rolled up to the Superintendent's office Site ID published in the MSID.

5.2 Authorization Attributes

At a minimum, authorization attributes determine which applications a user may access. Individual applications will determine if additional attributes (up to 10) are needed, such as defined roles for access or additional identity information. The following is a list of the authorization fields with rich descriptions. Specific information about each application's authorization attributes are available in the secure transfer file account (SSO DOCS folder – accessible to the LEA Technical Lead only) or through the FLDOE SSO Portal (accessible to LEA Administrators and Location Administrators).

Field Name	Order	Description	Example	
SSO ID	1	The SSO ID is a unique identifier for each trusted source of provisioning information. The FLDOE SSO team will provide this number to the LEA during the on-boarding process.	54	Required
Local ID Number	2	The unique local identification number assigned to staff within the LEA. This number may be alphanumeric, up to 50 characters.	755741	Required
Application ID	3	The Application ID is a unique identifier generated by the SSO for each application.	4	Required
Role	4	The basic role or roles that a user is able to perform within the application.	45	Required
Attribute1	5	Defined by application.		
Attribute2	6	Defined by application.		
Attribute3	7	Defined by application.		
Attribute4	8	Defined by application.		
Attribute5	9	Defined by application.		
Attribute6	10	Defined by application.		
Attribute7	11	Defined by application.		
Attribute8	12	Defined by application.		
Attribute9	13	Defined by application.		
Attribute10	14	Defined by application.		

6 Data Submission

LEAs may submit provisioning information in a variety of ways, either through file transmissions or using the Forefront Identity Management (FIM) Portal.

The following sections outline how the identity and authorization information may be submitted and the content of each.

6.1 File Transmission

Provisioning files (identity and authorization) may be sent through the use of two available options, secure file transfer via appropriate client or file upload through provider's HTTPS portal. Both methods require the establishment of a secure file transfer account to upload provisioning files to the LEA's secure account for processing.

Using the secure file transfer account, LEAs have the option of selecting from either the SFTP or FTPS protocols to securely upload provisioning files. Based on the secure file transmission option selected, the LEA Technical Lead would use an appropriate secure FTP client to establish a secure connection to their secure FTP account. With a secure connection established, the provisioning files can be uploaded to FLDOE. Additional information about the secure options follows:

- SFTP – Secure FTP is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. It is functionally similar to FTP, but because it uses a different protocol, a standard FTP client cannot be used to communicate with an SFTP server. Likewise a client that supports SFTP cannot be used to communicate with a FTP server.

- FTPS – FTP Secure and FTP-SSL is an extension to the commonly used FTP that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. FTPS should not be confused with the SSH File Transfer Protocol (SFTP), an incompatible secure file transfer subsystem for the Secure Shell (SSH) protocol. It is also different from Secure FTP, the practice of tunneling FTP through an SSH connection. Both the source (LEA) and the destination (FLDOE) will require a secure service to be in place to use this option. SSL keys will have to be exchanged.

- The HTTPS option allows LEAs to log into the provider's portal, browse, and select a file from their local device to be uploaded to their account.

For all methods, LEAs must establish a secure file transfer account with the FLDOE by completing FLDOE SSO LEA Participation Form. Keep in mind, LEA locations are not permitted to use the secure transfer file account; therefore, if data is needed from locations they must submit the data to the LEA Technical Lead and the Technical Lead will utilize the account to send data on their behalf.

6.2 File Encryption

As discussed in the File Transmission section, files are transmitted using a secure transmission path; the files themselves do not require encryption. Although not required, LEAs may choose to encrypt provisioning files before uploading via secure transmission option. To facilitate this option FLDOE SSO will support the Pretty Good Privacy (PGP) protocol for encrypted file transmission. If this option is selected, LEAs must upload their public credential to their secure file transfer account, allowing for decryption of uploaded provisioning files.

6.3 File Formats

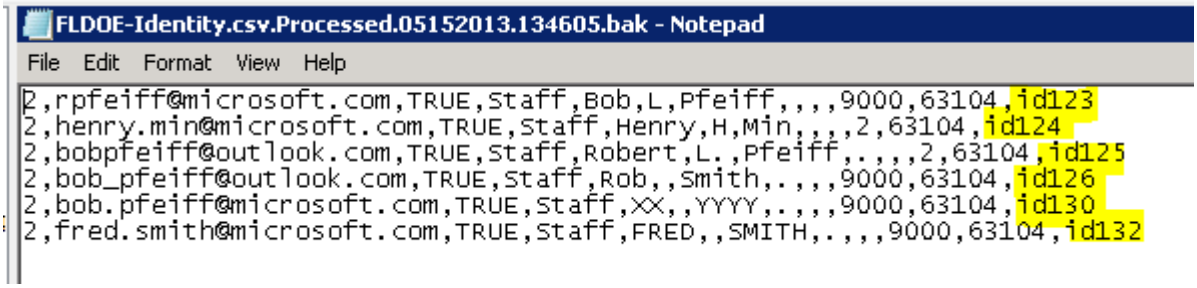
LEAs may choose between two different file formats to submit provisioning files to FLDOE. The first is a comma-separated values flat file format based on the FLDOE SSO CSV Schemas. The second is an XML file format based on the FLDOE SSO XML Schemas. The schemas and sample files are explained in this document and examples are provided. While LEAs may choose between .XML or .CSV file formats, the two types of provisioning files (identity and authorization) must be sent in the same format.

Each user will have one record in the identity file and one record in the authorization file per application that they should be able to access. Account disablement shall only occur explicitly. In other words, access revocation records must be sent in order to remove a user's access. The following sections detail the guidelines for preparing each file type.

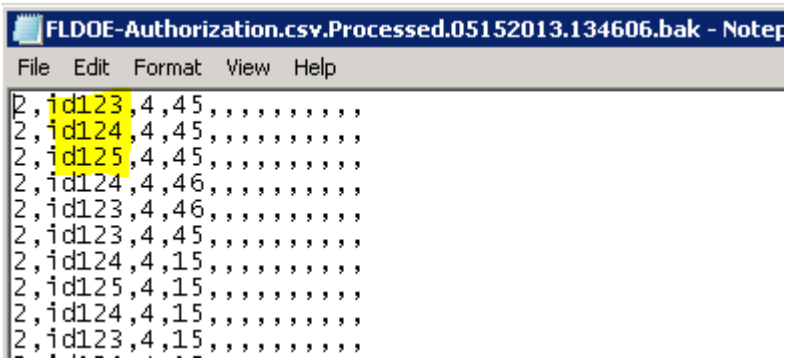
6.3.1 CSV

- The files must follow the naming convention of "SSOID-YYYYMMDDHHmm-FileType.csv". The time represented by HHmm for hour and minute will be entered using standard 24 hour time and the file type will be either "Identity" or "Authorization". If the file name is incorrect, the entire file will be rejected.
- Each record is located on a separate line, delimited by a line break.
- Field/column headers are not supported; specified order is mandatory.
- The use of double quotes is not supported.
- The use of an apostrophe or hyphen in a record is supported without the use of double quotes. Examples:
    - 34,aohurley@bay.k12.fl.us,true,staff,Aaron,J,O'Hurley,,,,21,51013,id123
    - 34,rhernandez-gonzales@bay.k12.fl.us,true,staff,Rose,J,Hernandez-Gonzales,,,,161,51002,id124

6.3.2 Identity File CSV Example



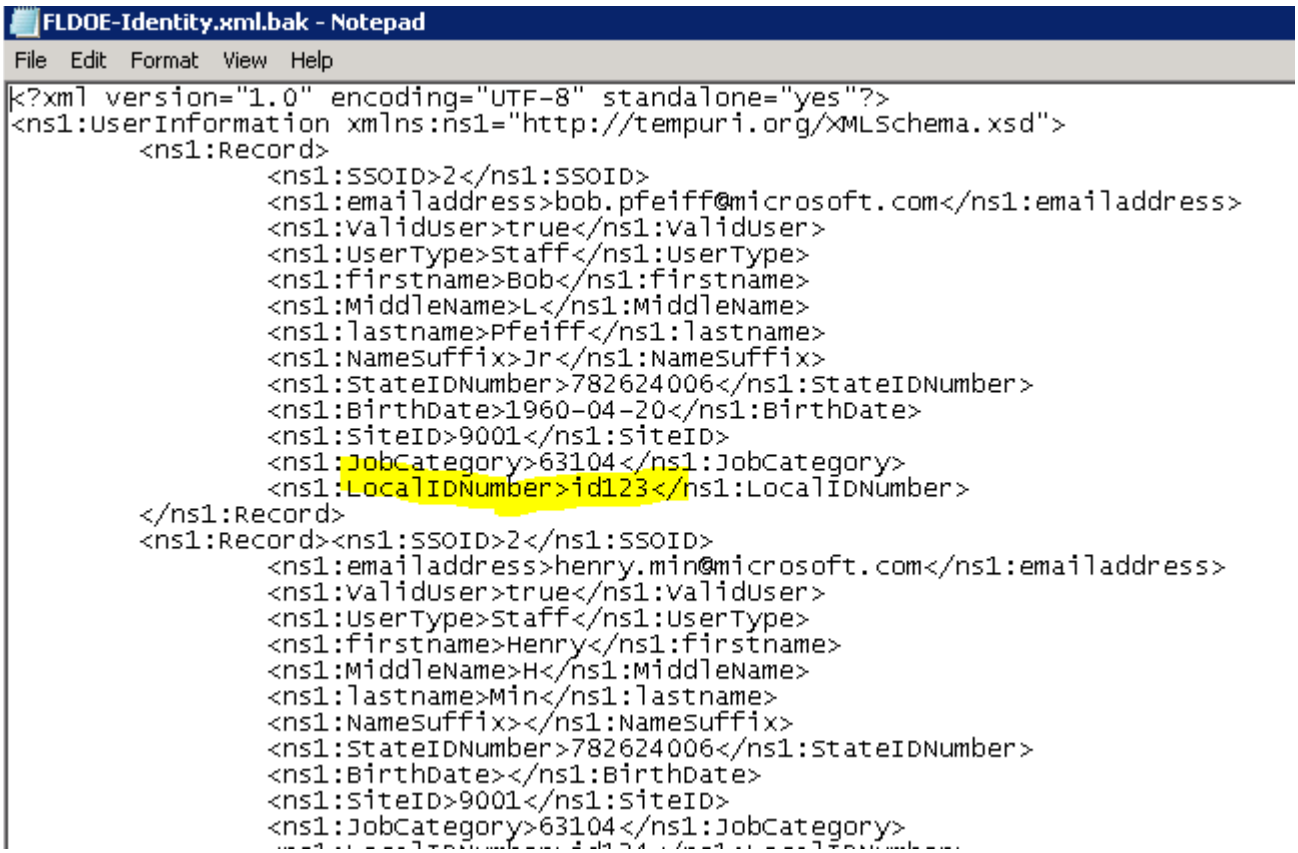
6.3.1 Authorization File CSV Example



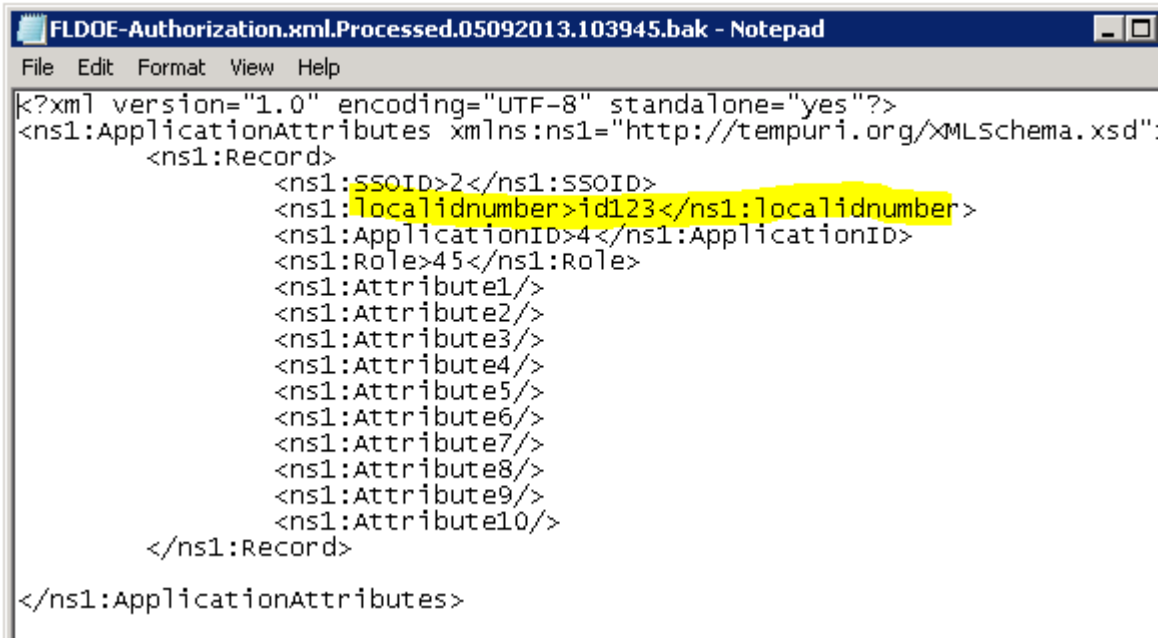
6.3.2 XML

- The files must follow the naming convention of "SSOId-YYYYMMDDHHmm-FileType.xml". The time represented by HHmm for hour and minute will be entered using standard 24 hour time and the file type will be either "Identity" or "Authorization". If the file name is incorrect, the entire file will be rejected.
- The files must be well formed.
- Field/column headers are not supported; specified order is mandatory.
- The files must follow the FLDOE SSO XML Schemas.

6.3.3 Identity File XML Example



6.3.4 Authorization XML Example



6.4 Forefront Identity Manager (FIM) Portal

As an alternative to provisioning users solely based on the file upload process, the LEA Administrator may use the tools provided by the Forefront Identity Manager (FIM) Portal. The primary LEA Administrator can navigate to the FIM Portal and perform the following tasks:

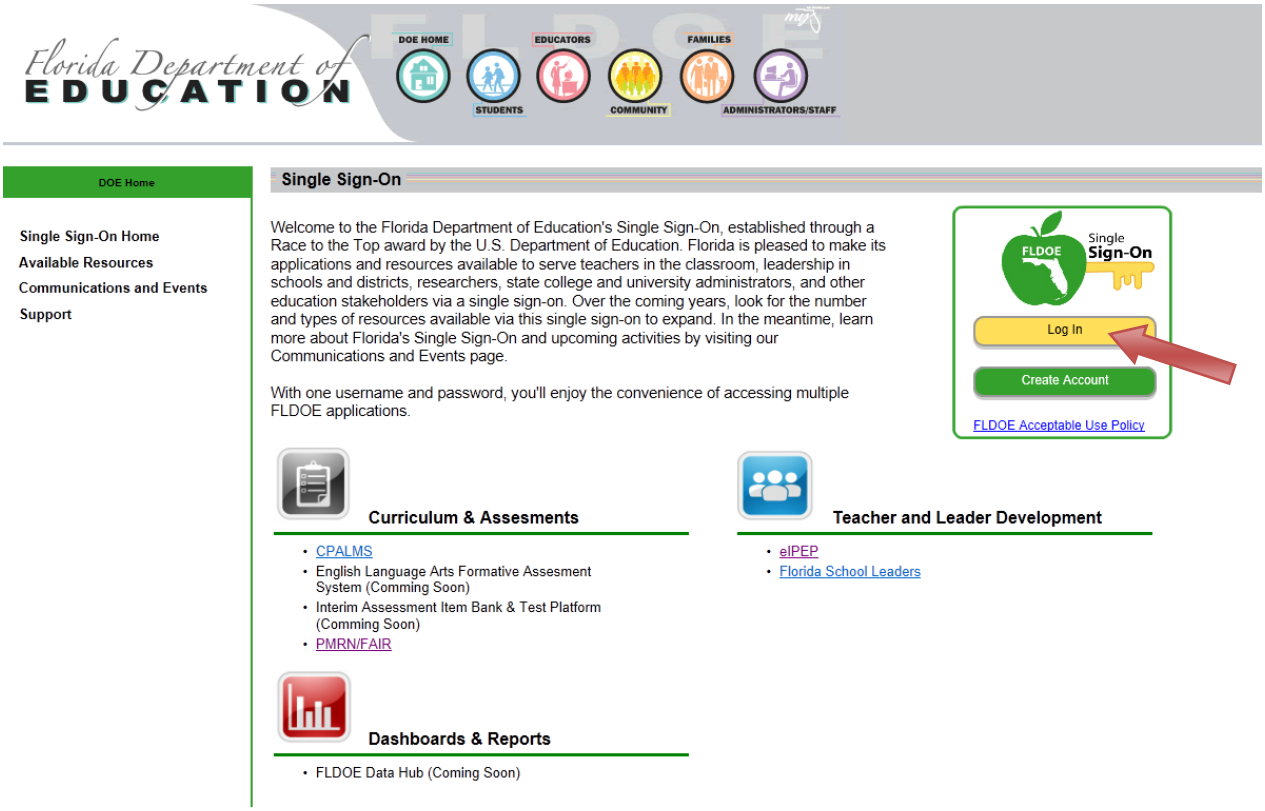
- Create, modify, or disable users
- Add, modify, or remove user authorizations
- Designate LEA Administrators or Location Administrators
- Reset a user's password

IMPORTANT:

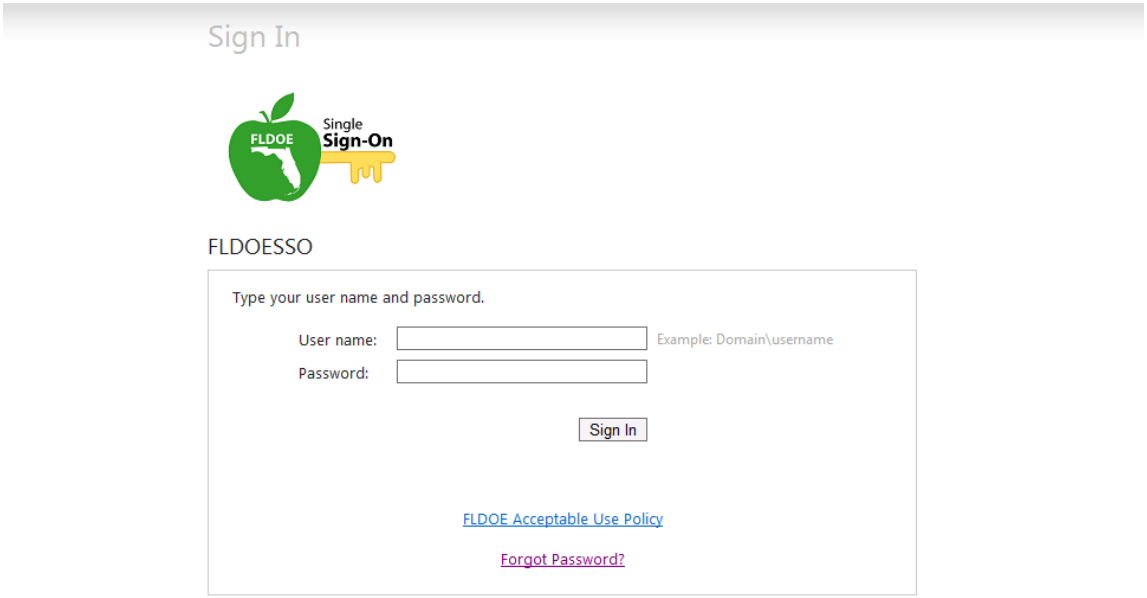
1. While the FIM Portal may be used to create or modify the user provisioning information, those modifications will be overwritten by the file upload process when it is next initiated. Therefore, it is vitally important to modify the source data of the user provisioning files to match information entered into the FIM Portal.
2. The FIM Portal only supports the Internet Explorer browser 7.0 and above (i.e. Chrome and Firefox browsers are not supported).
3. It takes time to process items entered in the FIM Portal. Sync times may vary from minutes to hours depending on the number of records being processed (submitted cumulatively by all LEAs statewide).

6.4.1 How to Access the FIM Portal

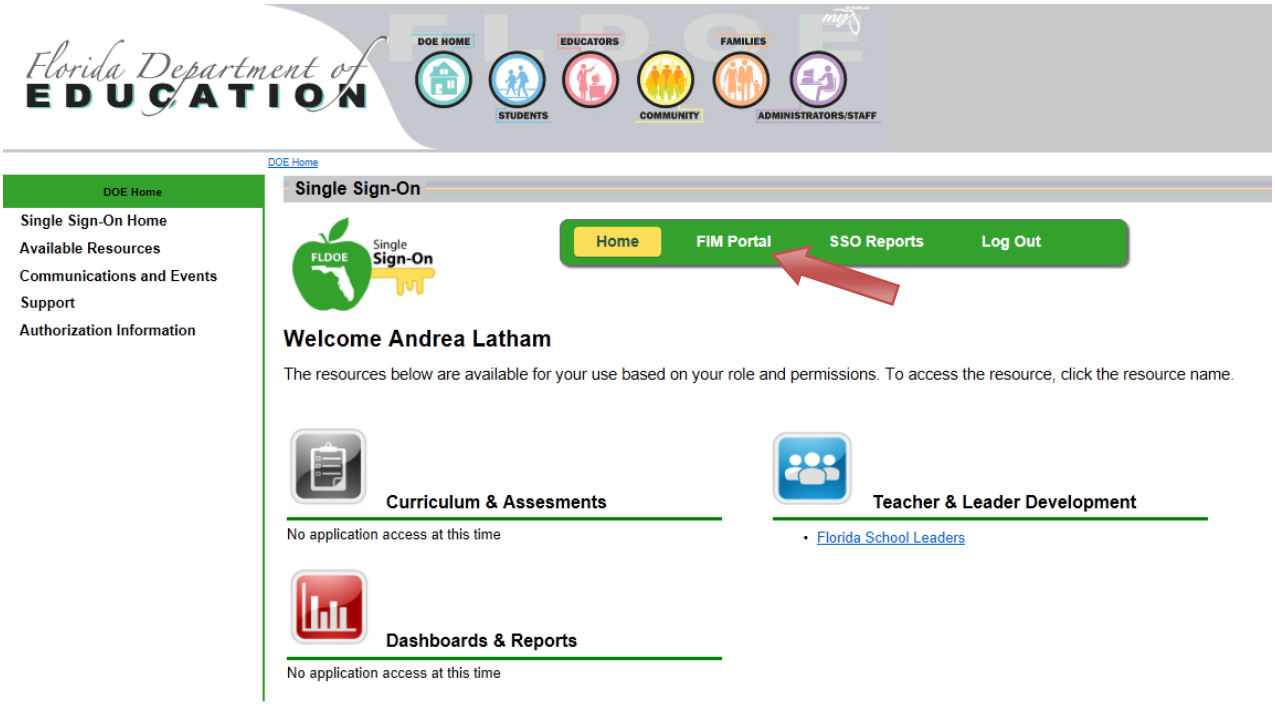
1. Go to www.fldoe.org/sso
2. Select "Log In"



3. Enter your FLDOE SSO username and password

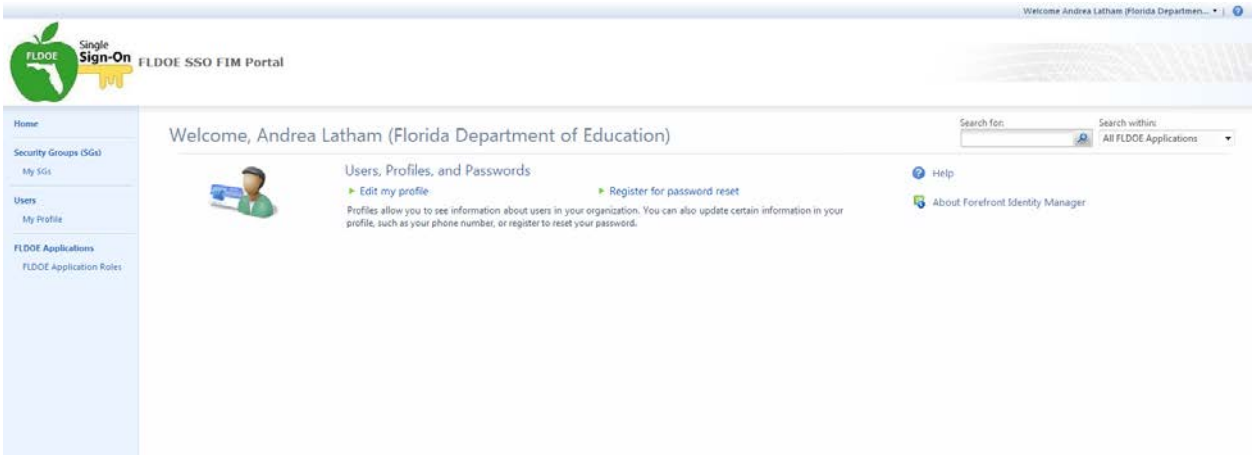


4. Select “FIM Portal” from the main menu bar at the top of your screen.



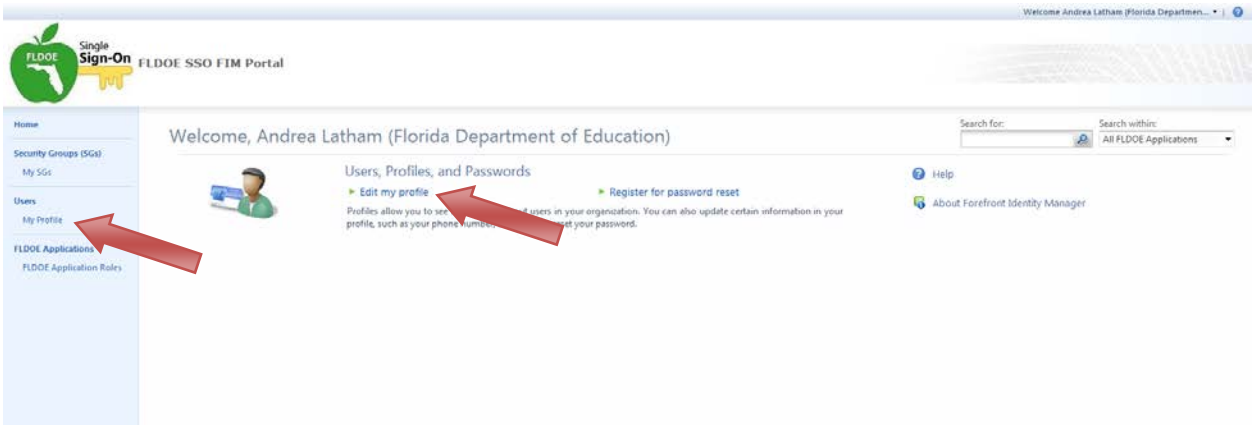
5. Enter your password and select “OK”

6. FIM Portal Home Page



6.4.2 View or Modify your Profile

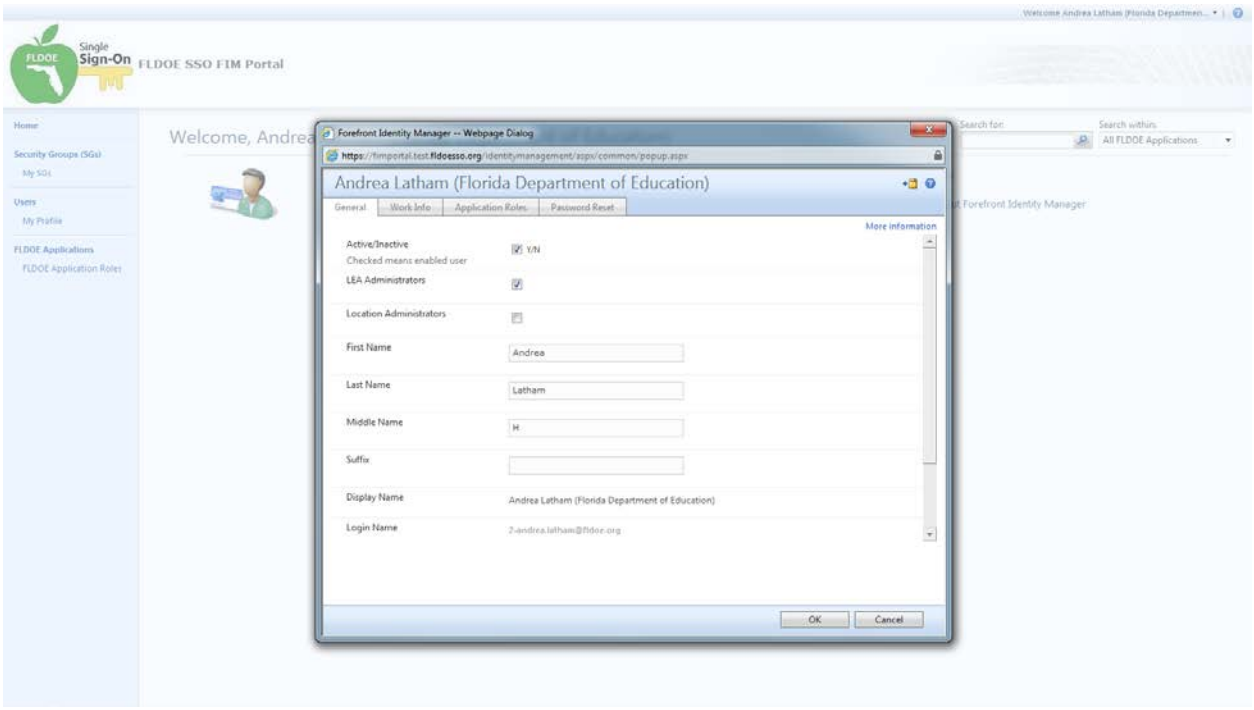
1. Click on “My Profile” from the left side menu or “Edit my profile” in the center area



There are four tabs to a user profile: General, Work Info, Application Roles, and Password Reset.

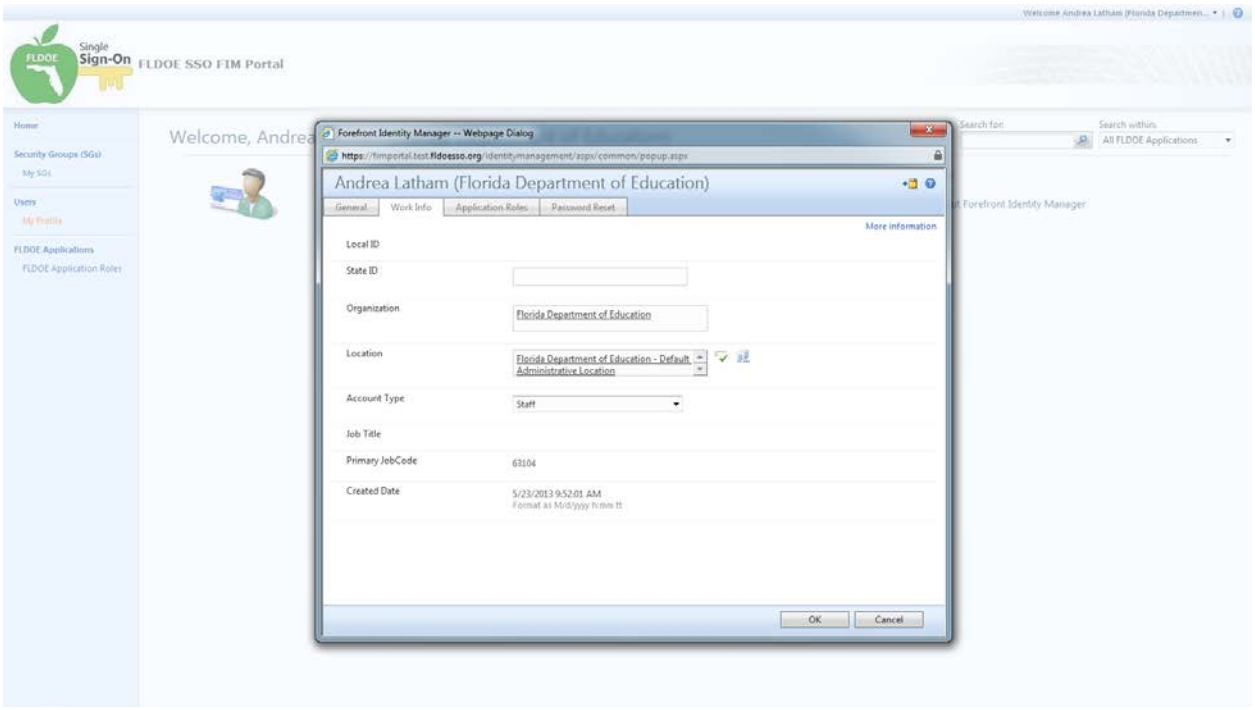
General Tab

- Active/Inactive = Checked means the user is enabled; un-checking this will disable a user from the FLDOE SSO.
- LEA Administrator = Checked means the user is an LEA Administrator with rights to view, modify, or disable all users within the LEA.
- Location Administrator = Checked means the user is a Location Administrator with rights to view, modify, or disable users at their assigned location within the LEA.
- First Name = The legal first name of the user. This field is required; it can be modified. The user’s name will appear in the system exactly as entered; proper sentence case is suggested.
- Last Name = The legal surname of the user. This field is required; it can be modified. The user’s name will appear in the system exactly as entered; proper sentence case is suggested.
- Middle Name = The legal middle name of the user. This field is optional; it can be modified.
- Suffix = The academic, religious, generational, or professional suffix that follows the user’s full name. This field is optional; it can be modified.
- Display Name = The user’s first and last name (appears as entered) and their organization in parenthesis.
- Login Name = A concatenation of the user’s organization SSO ID and email address.



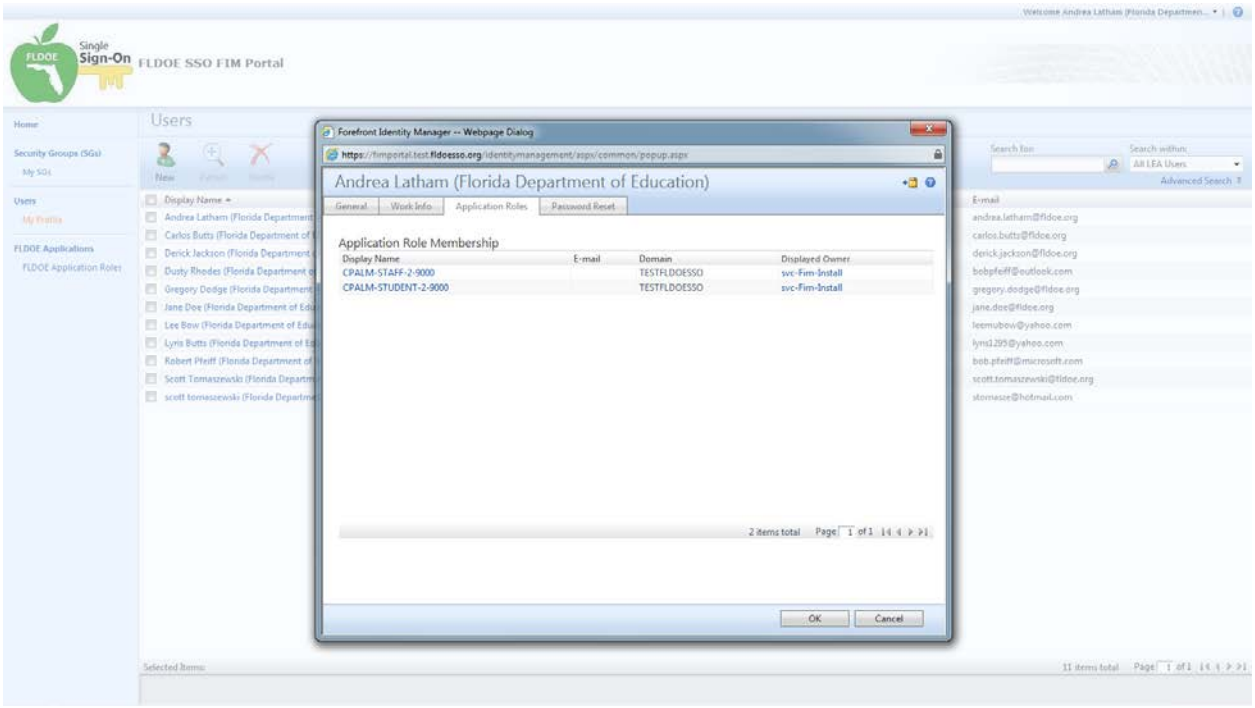
Work Info Tab

- Local ID = The unique local identification number assigned to staff within the organization. This number represents the primary key for user identification. This field is required; it cannot be modified.
- State ID = Reserved for the Florida Education ID Number. This field is optional; it can be modified.
- Organization = The sponsoring organization or LEA providing the user provisioning information. This field is required; it can be modified. However, modifying the organization will remove the user from the LEA Administrator's purview.
- Location = The primary administrative reporting unity to which the user is assigned. This field is required; it can be modified. However, modifying the organization will remove the user from the Location Administrator's purview.
- Account Type = The user type may be staff or student. This field is required; it can be modified. However, the FLDOE SSO is not taking student accounts at this time.
- Job Title = The job title is populated based on the Primary Job Code provided. This field is optional; it can be modified by editing Job Category in the identity file.
- Primary Job Code = The primary job assignment code to which staff is assigned. Only one job code is permitted. This field is optional; it can be modified by editing Job Category in the identity file.
- Created Date = Represents the date the user account was initially created.



Application Role

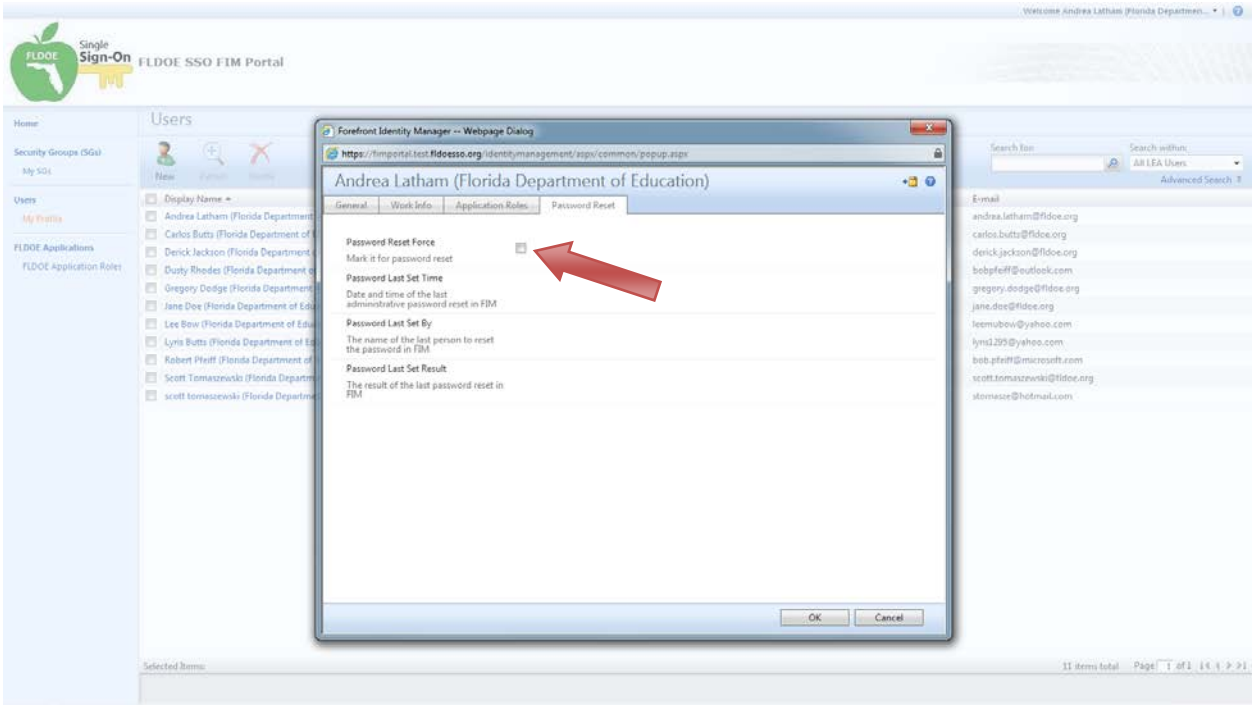
1. Displays the applications of which the user is a member.



Password Reset

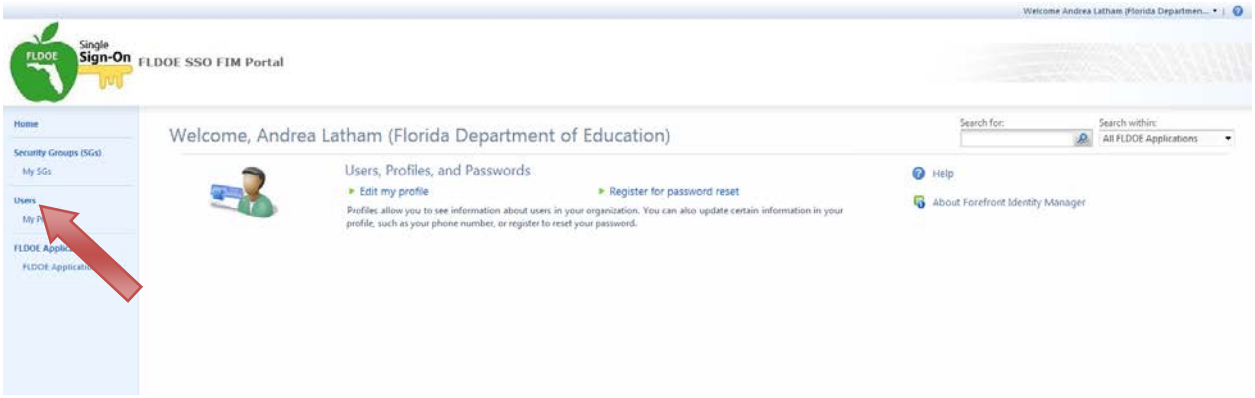
1. Displays password set history.

2. Checking “Password Reset Force” will reset the user’s password and initiate a system email notifying them of the change and directions for registering their security questions and resetting the password.

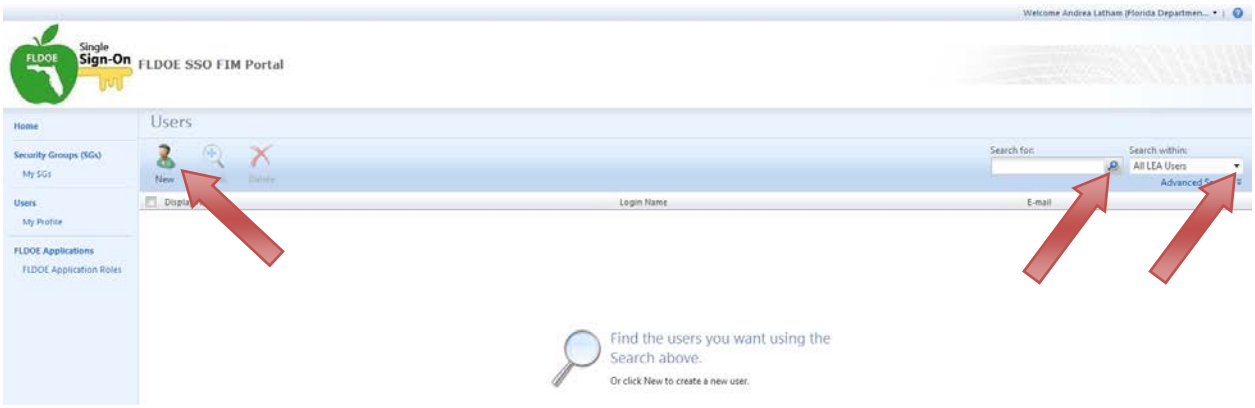


6.4.3 Add New User

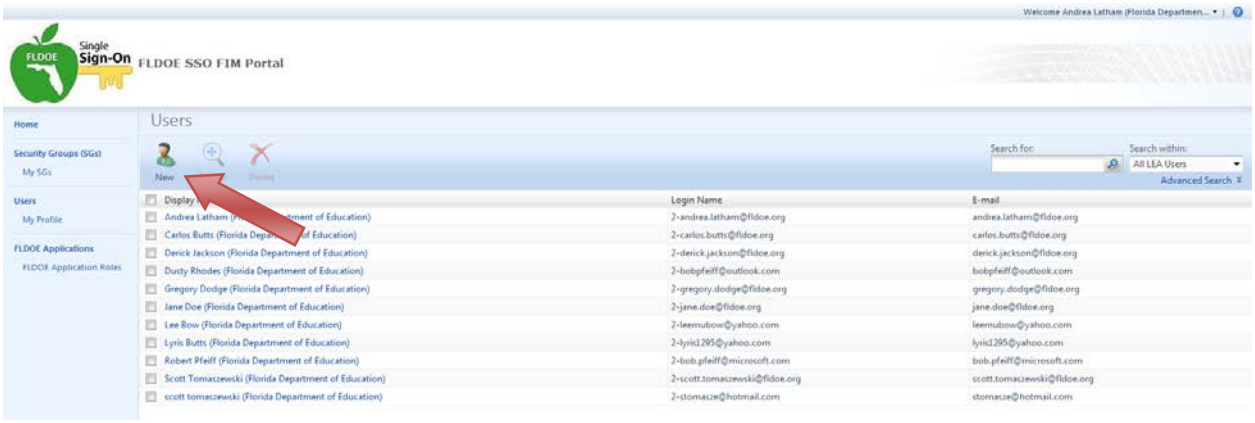
1. Click on “Users” from the left side menu



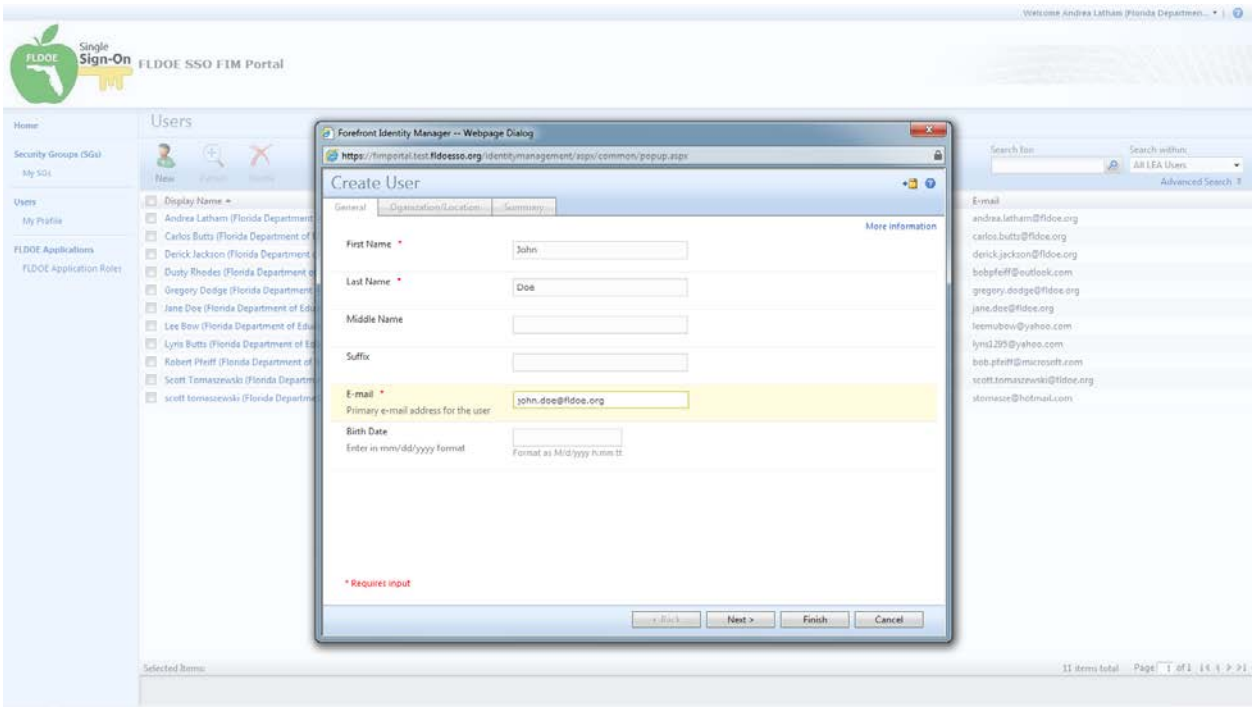
2. Click “New” to create a new user. However, it is recommended to first use the search options on the right to verify the user is not already created.
    - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
    - Select the “Search for:” magnifying glass icon to begin the search.



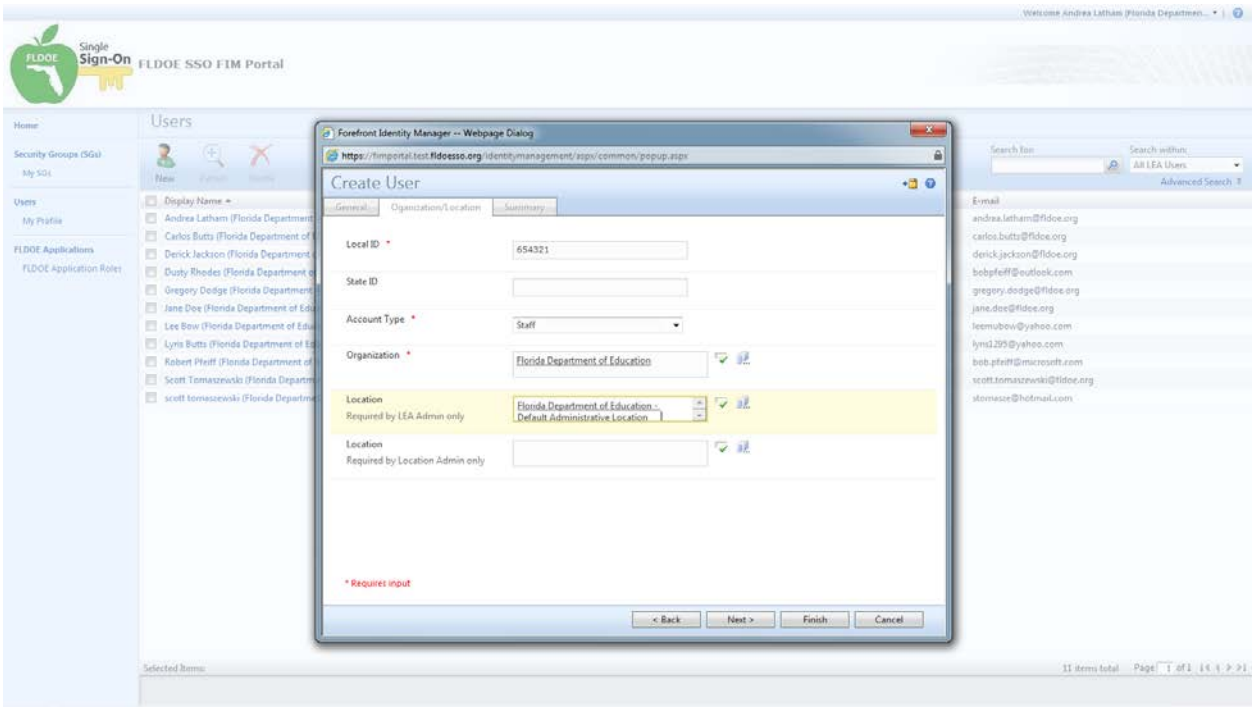
3. A list of users is presented. Verify the user account has not been created.
4. To add a new user, select “New”



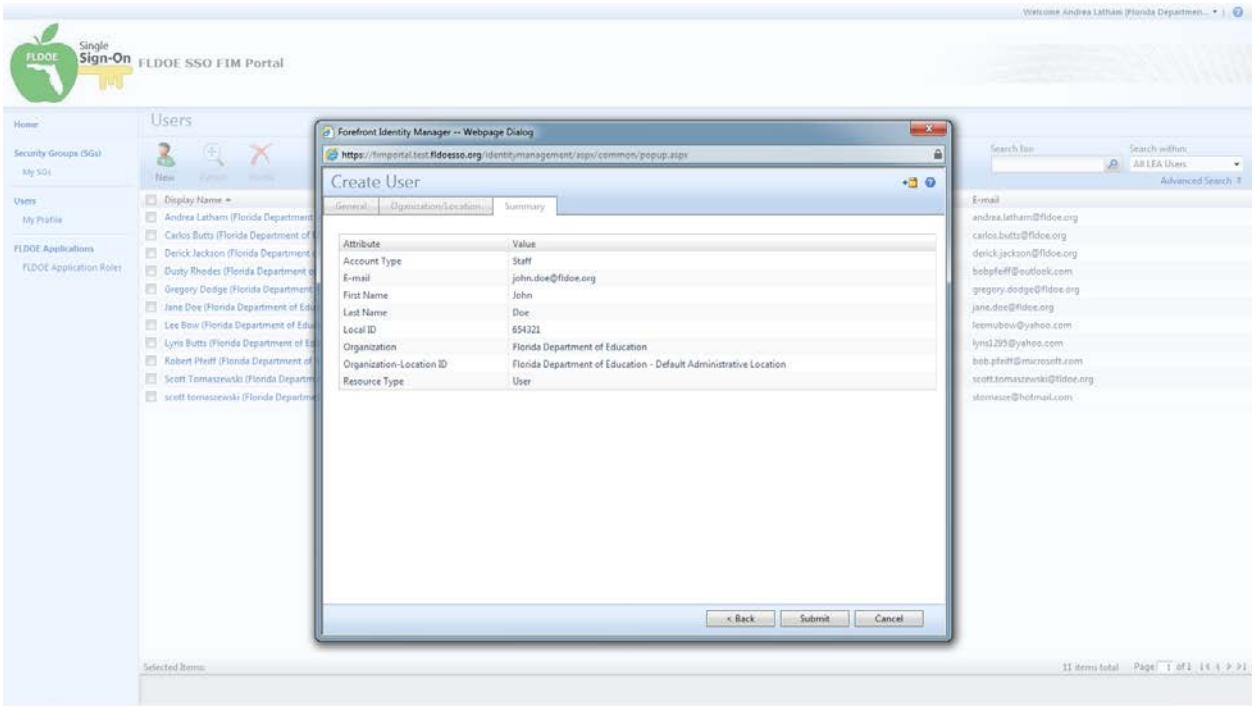
5. Enter the required fields
   - First Name
   - Last Name
   - Email Address
6. Select “Next”



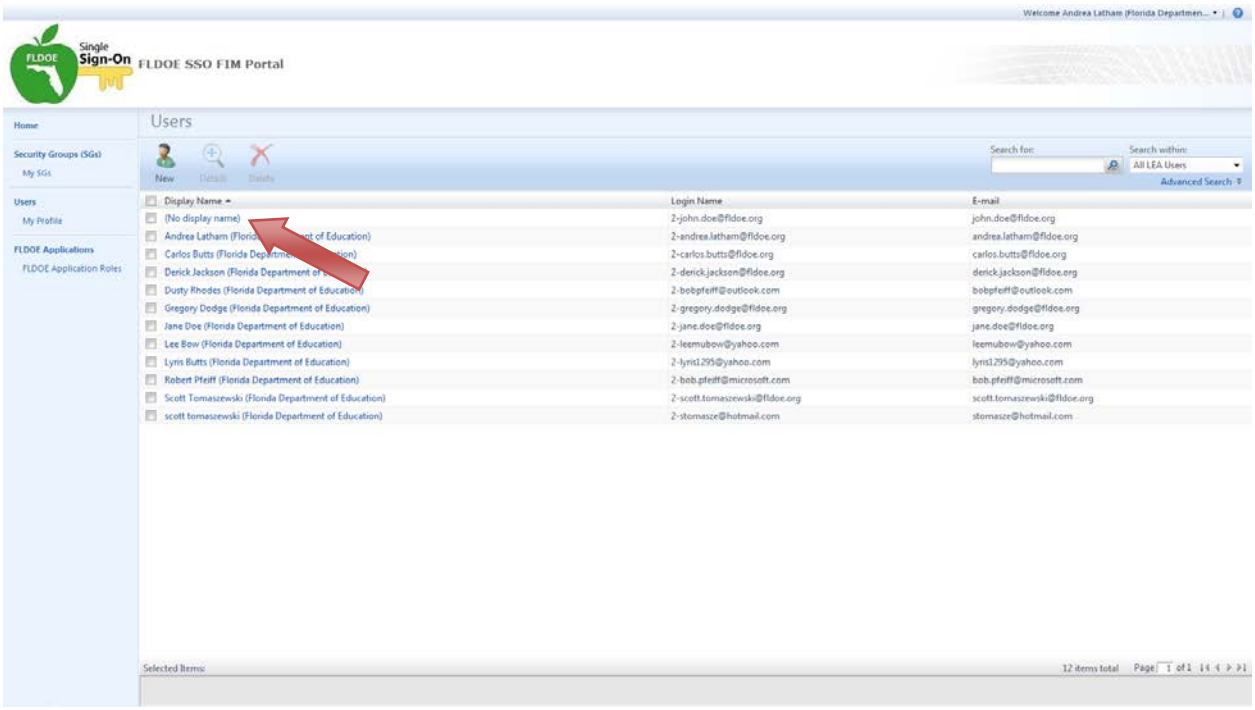
7. Enter the required fields
   - Local ID
   - Account Type
   - Organization
     - Browse for Organization by selecting the browse icon to the right of the field.
   - Location
     - There are two location fields. You must use the appropriate location field based on <u>your</u> role. If you are an LEA Administrator, use the first location field. If you are a Location Administrator, use the second location field.
     - Browse for the Location by selecting the browse icon to the right of the appropriate location field based on <u>your</u> role.
8. Select “Next”



9. The final screen will display a summary.
10. If correct, select “Submit” otherwise you may select “Back” to make corrections.

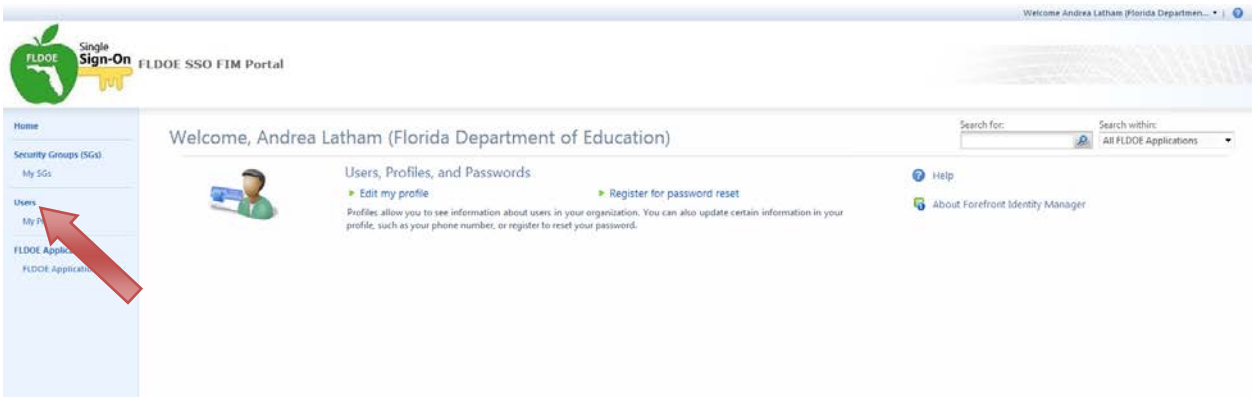


11. You will now see the new user added to the Users screen. However, their account will not be fully processed until the sync occurs. This may take a few minutes. Once the sync is finished, the (No display name) will change to the user information.

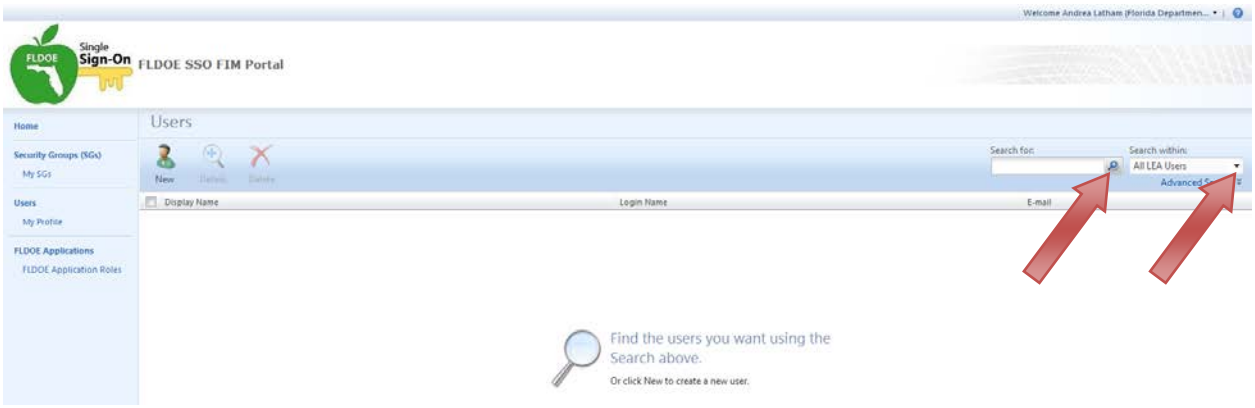


6.4.4 Modify User

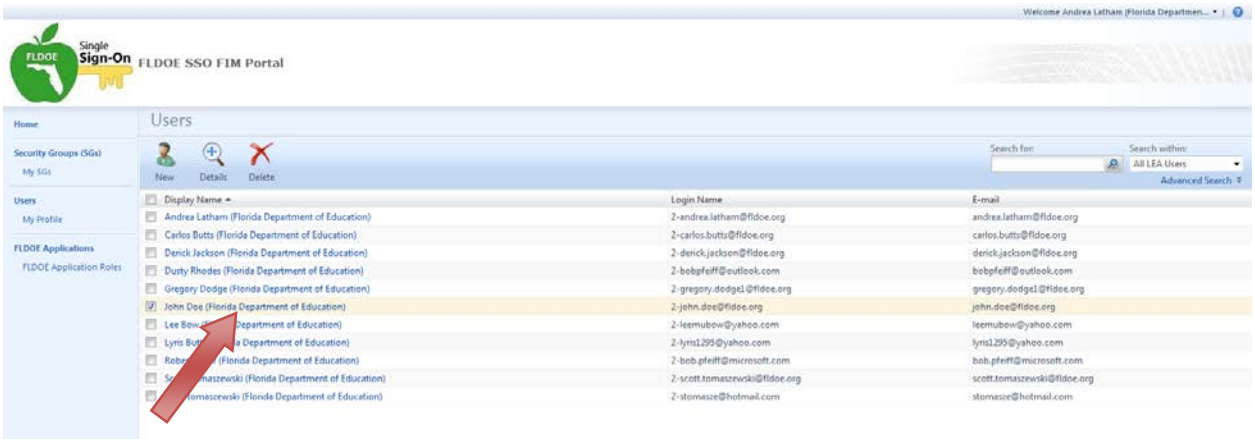
1. Click on “Users” from the left side menu



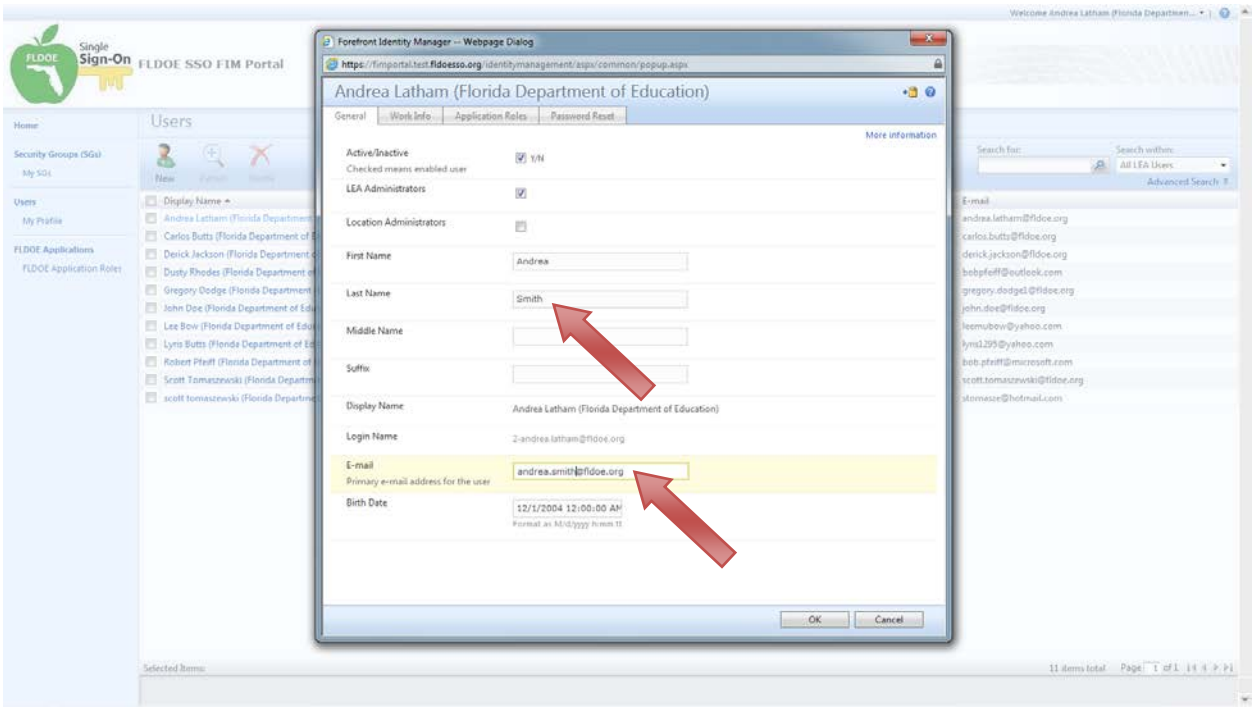
2. Search for the user
   - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
   - Select the “Search for:” magnifying glass icon to begin the search.



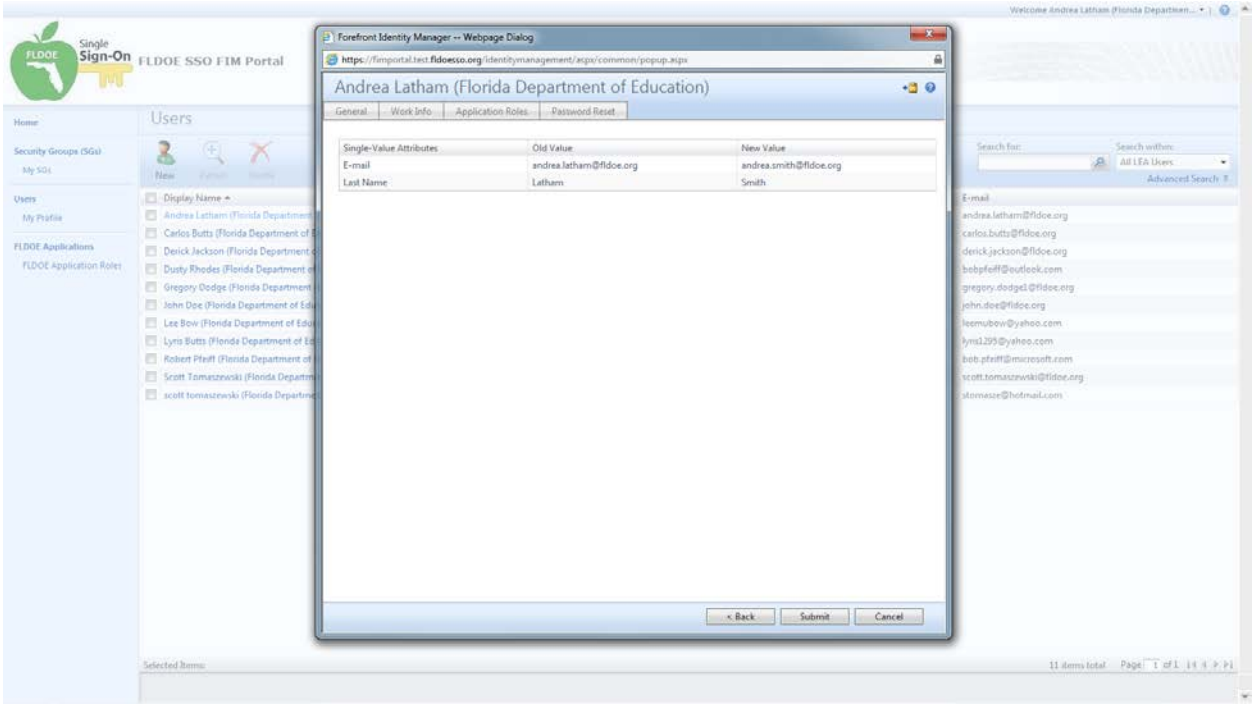
3. A list of users is presented
4. Click on the user name



5. There are four tabs to a user profile: General, Work Info, Application Roles, and Password Reset (described in section 6.4.2). Select the relevant tab to make a change. For example, to change the user's last name and email address, open the General tab. Keep in mind you may need to scroll to see all the fields.
6. Click "OK"

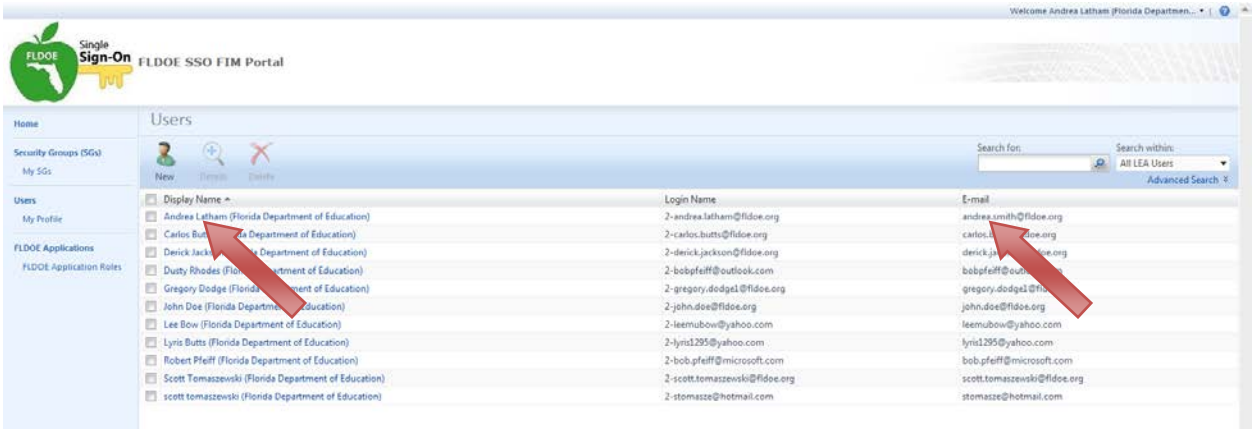


7. The final screen will display a summary.
8. If correct, select “Submit” otherwise you may select “Back” to make corrections.



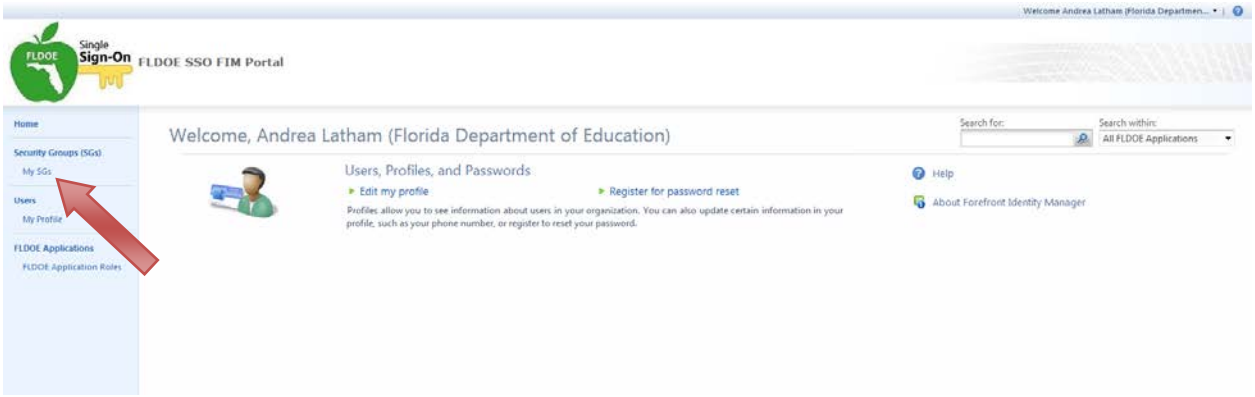
9. In this example, you can see some of the new user information has updated on the Users screen. However, the account will not be fully processed until the sync occurs. This may take a few minutes. Once the sync is finished, the display name, login name, and email address will change to the modified user information.

- It is important to note in this example, the user's email address was changed. Consequently, this changed the user's login name. The system only sends notifications for new account creation, not modifications. So, system will not notify the user of their new login name. As the LEA Administrator or Location Administrator that made the change, it is your responsibility to notify the user. (This is true for email address modifications submitted through the provisioning files, too. They system only sends notifications for new account creation, not modifications.)

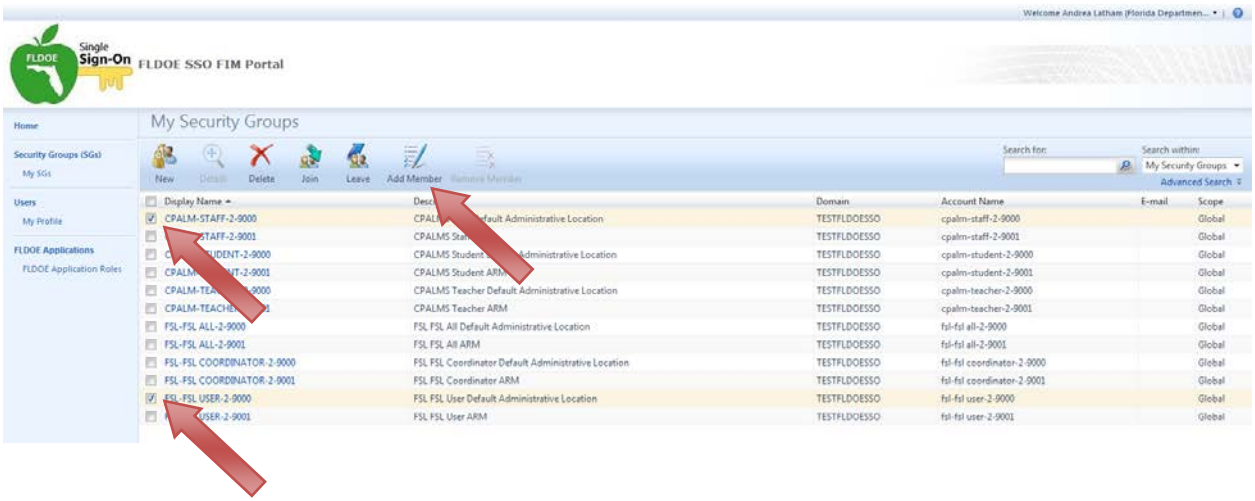


6.4.5 Add User Authorizations

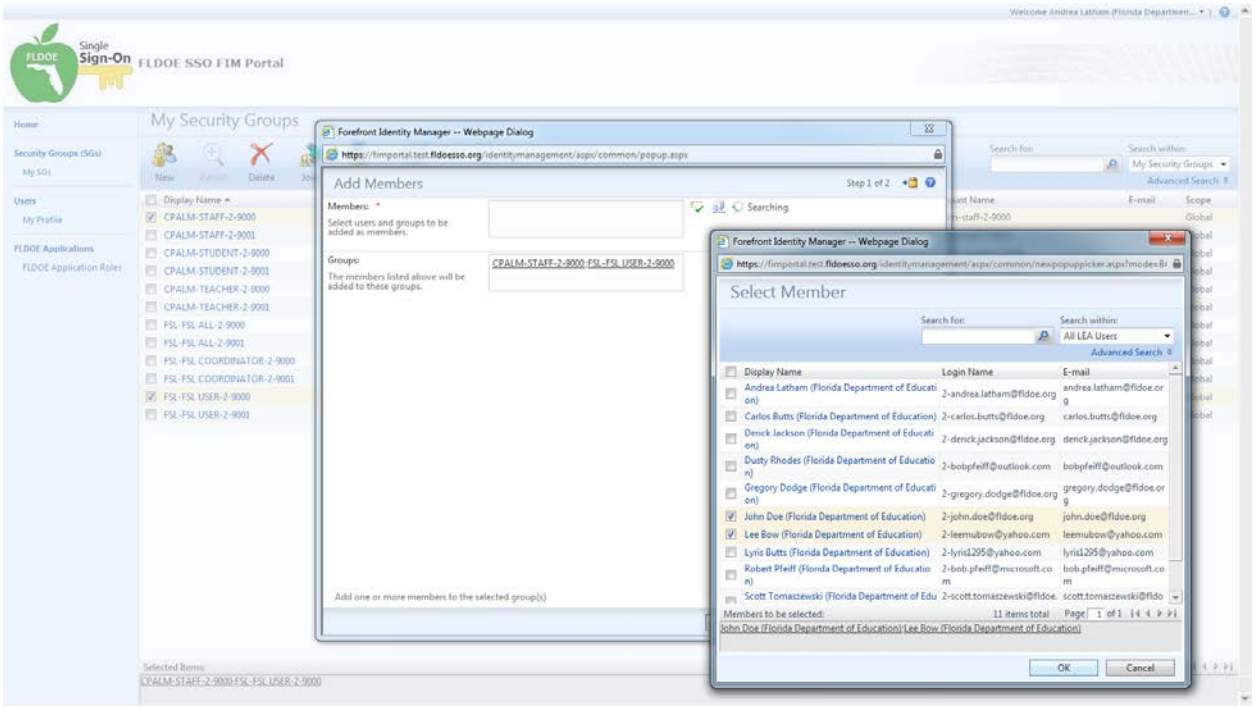
1. Click on "My SGs" from the left side menu



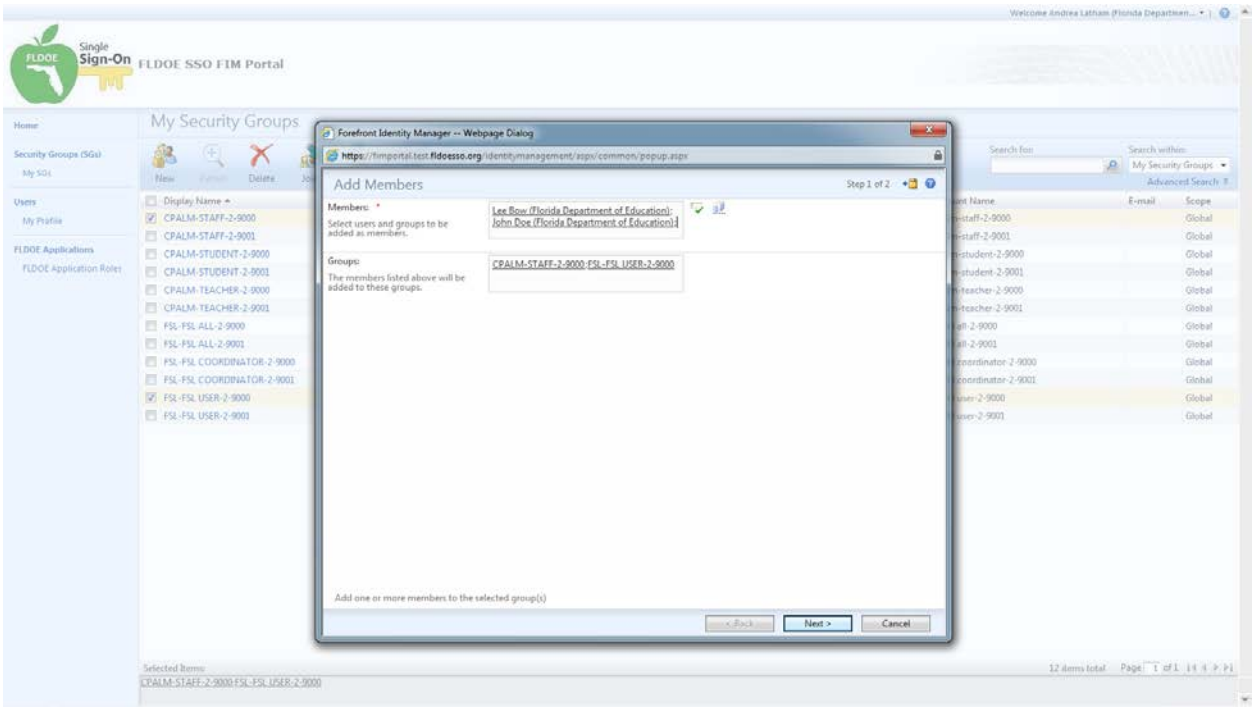
2. Select the application(s) to which a user will be added.
   - There will be multiple listings of applications appended with the SSO ID and Location ID. To add the user to the right group, you must select the group with their Location ID.
   - To view the user's Location ID, you may look them up in Users.
3. Select "Add Member" from the ribbon.



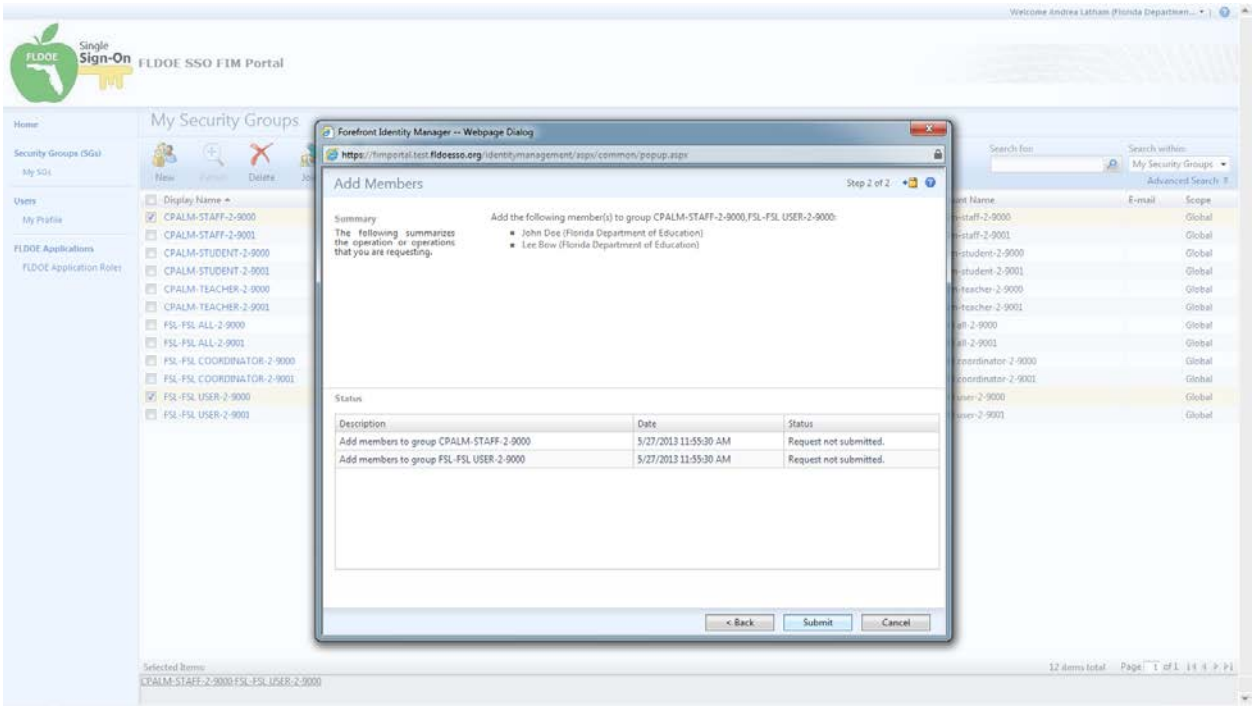
4. Browse for Members by selecting the browse icon to the right of the field.
5. In the next window, search for members.
   - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
   - Select the “Search for:” magnifying glass icon to begin the search.
6. Select the member(s) to add to the group(s) and click “OK”



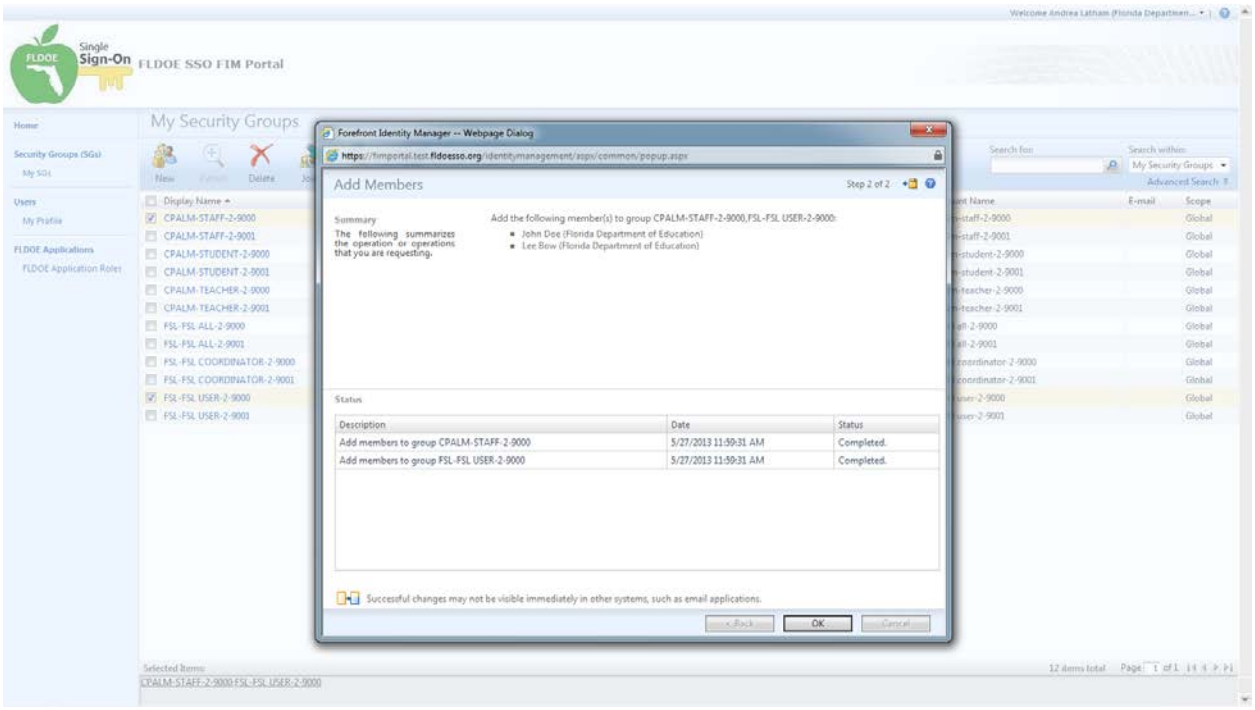
7. Once all the members have been selected, click “Next”



8. The final screen will display a summary.
9. If correct, select “Submit” otherwise you may select “Back” to make corrections.

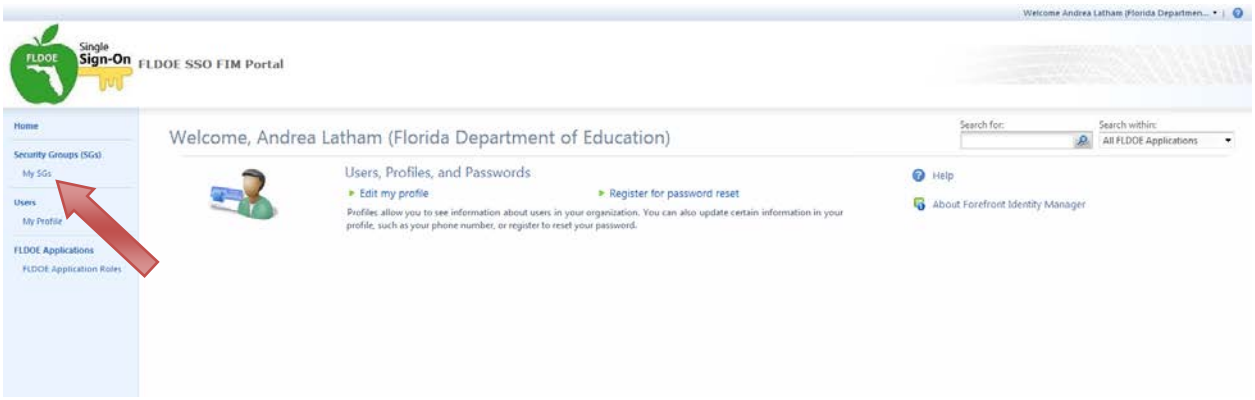


10. When the processing is complete, click “OK”

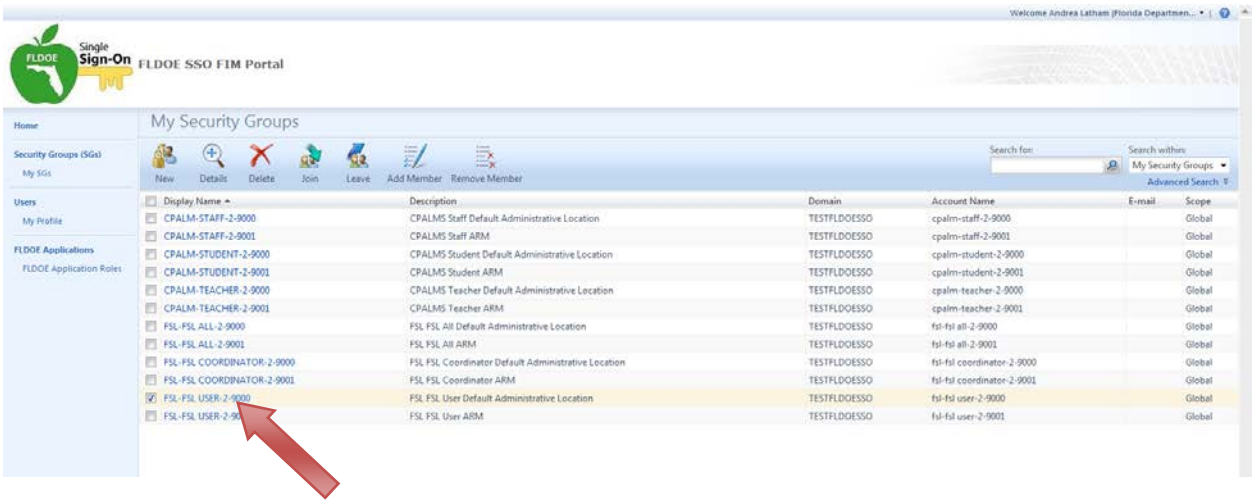


6.4.6 Modify Authorizations

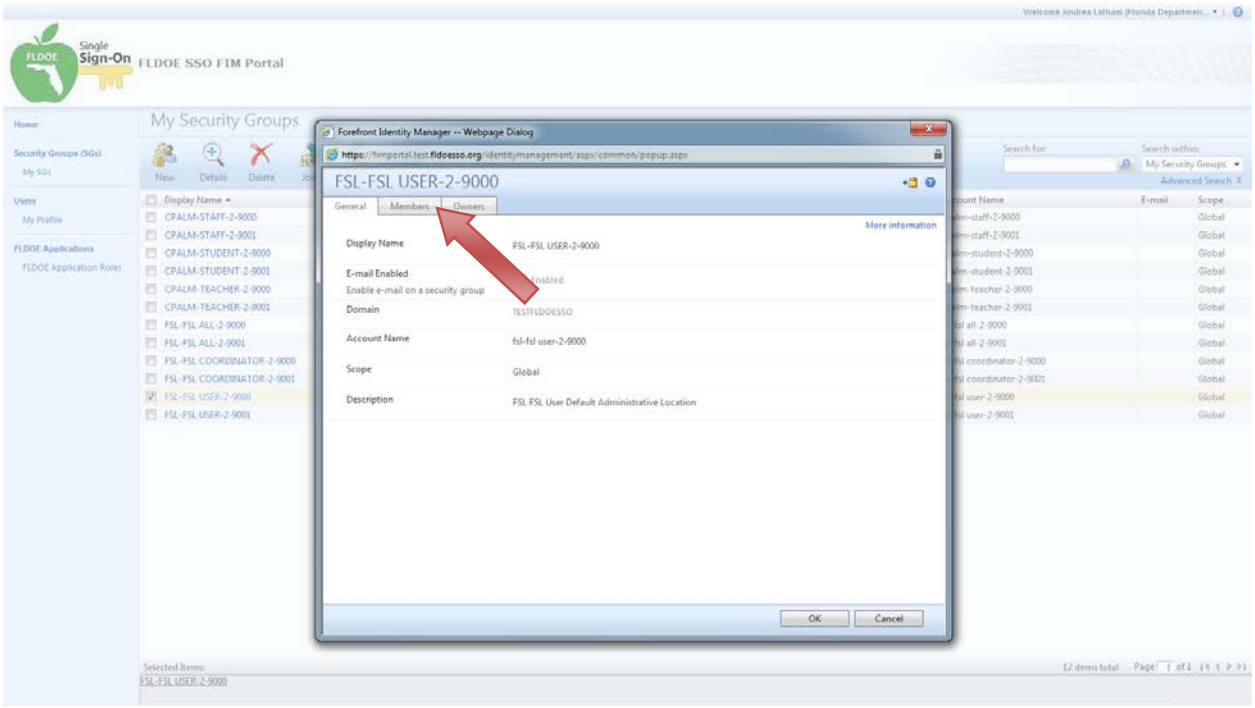
1. Click on “My SGs” from the left side menu



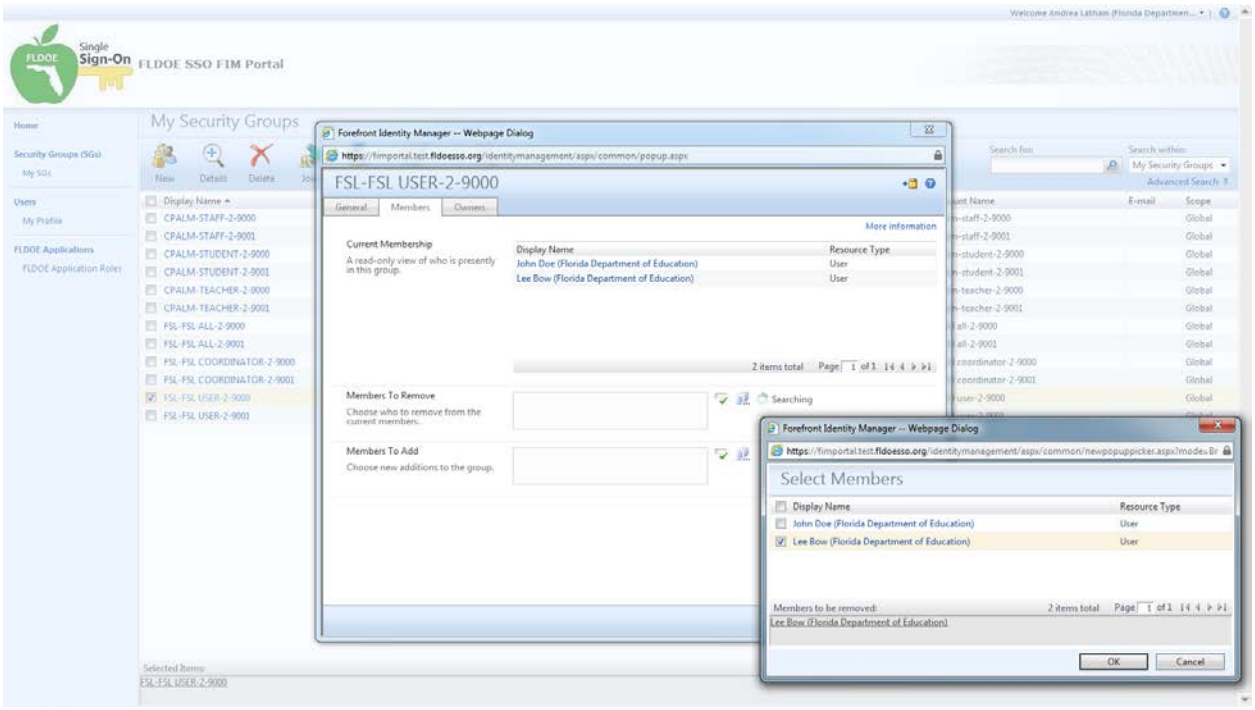
2. Select the application to be modified and click on its name.
    - There will be multiple listings of applications appended with the SSO ID and Location ID. Select the appropriate group based on the user’s Location ID you are adding.
    - To view the user’s Location ID, you may look them up in Users.



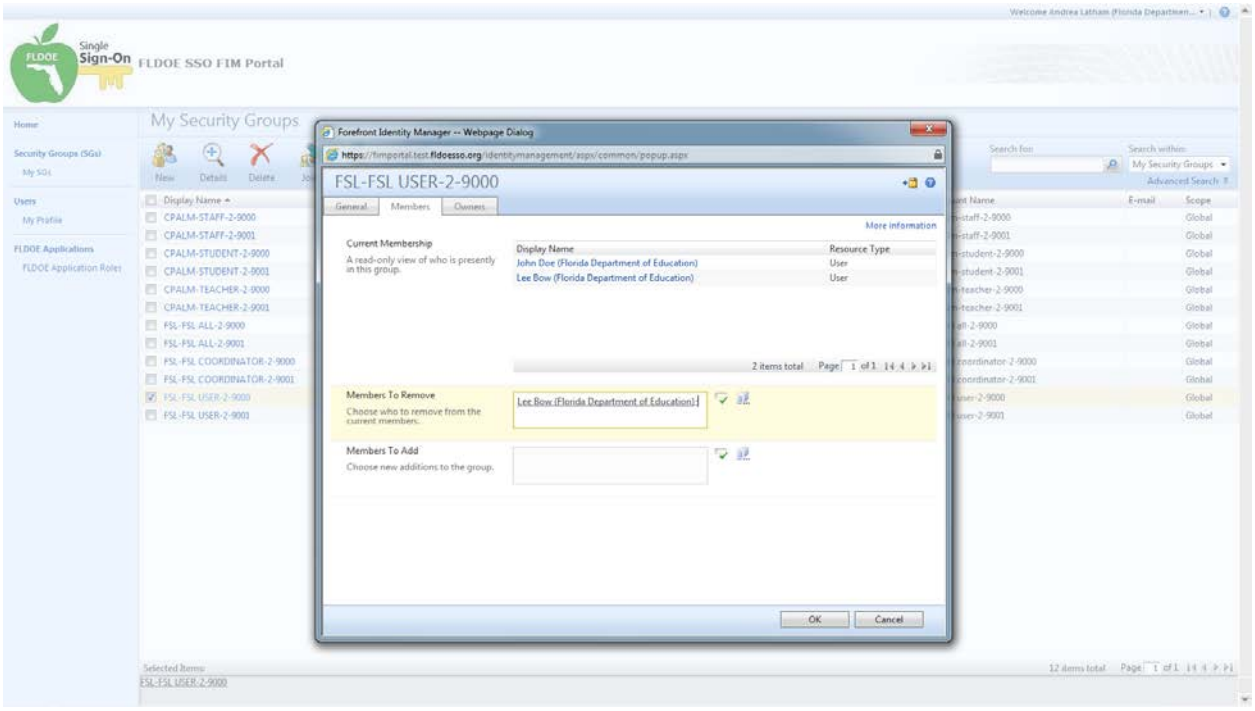
3. Click on the “Members” tab



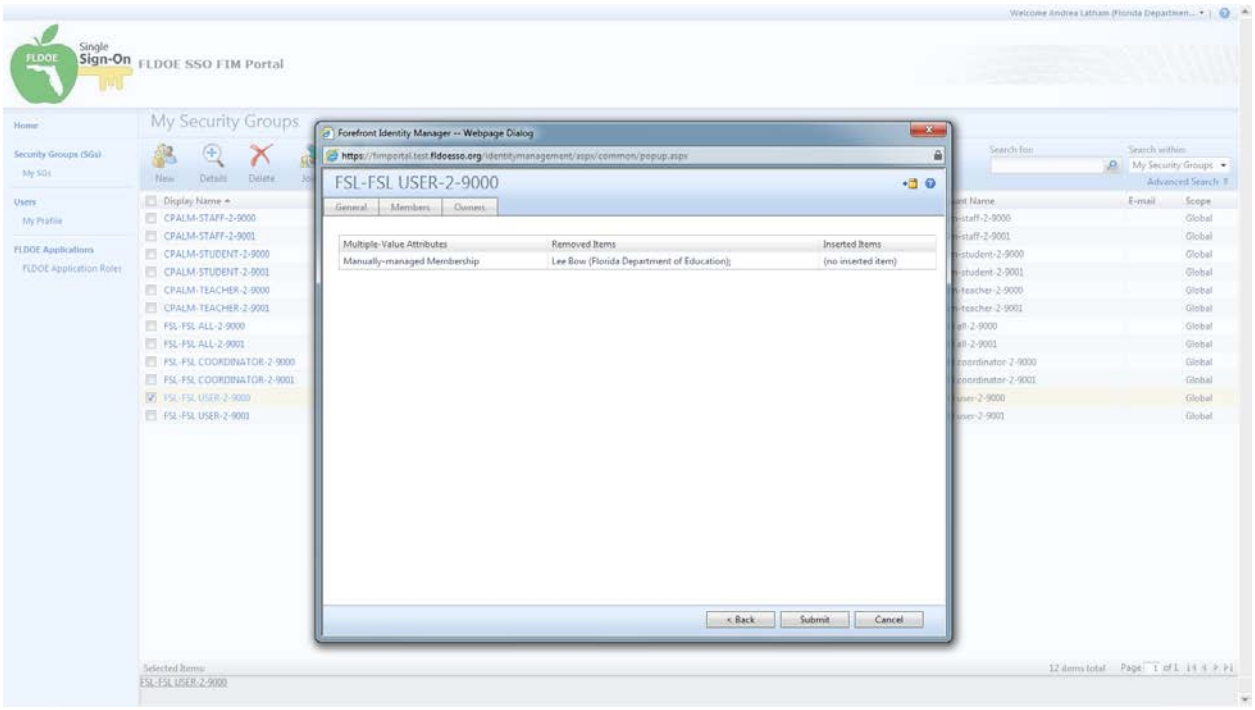
4. Current Membership displays the users belonging to the application group.
5. To remove a member from the application group, browse for Members by selecting the browse icon to the right of the “Members to Remove” field.
   - In the next window, search for members by selecting the “Search for:” magnifying glass icon.
   - Select the member(s) to add to the group(s) and click “OK”



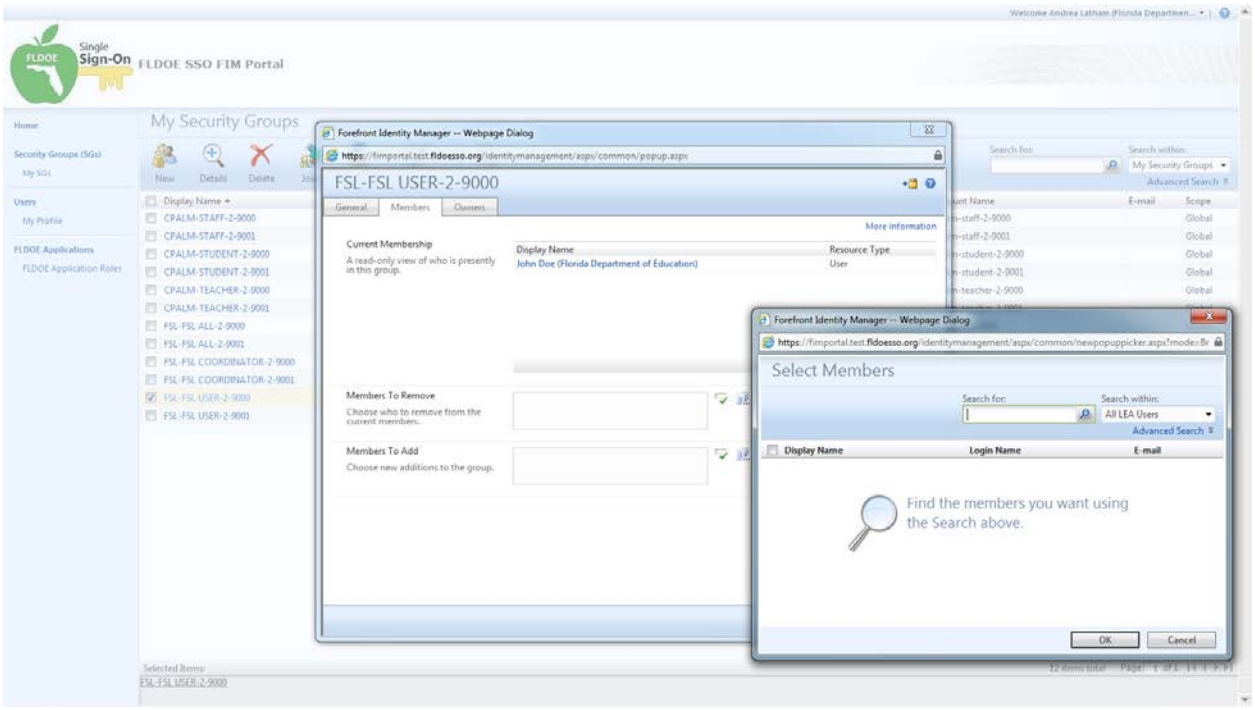
6. Once all the members have been selected, click “OK”



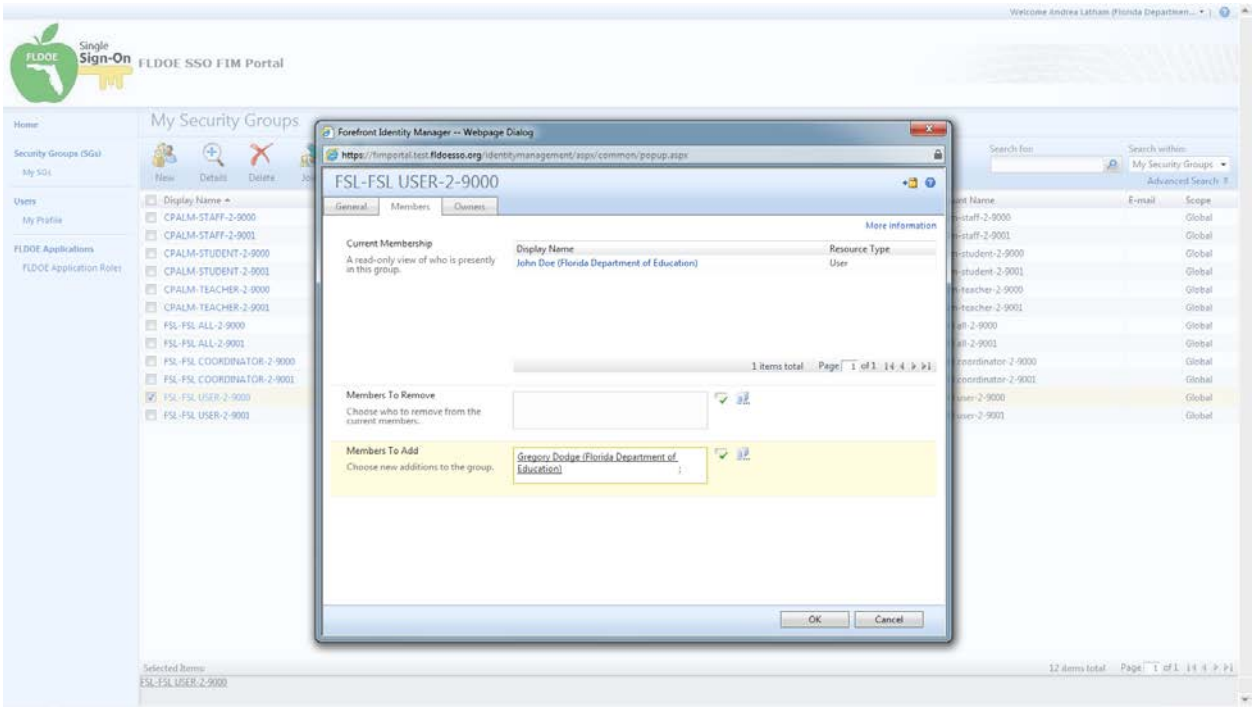
7. The final screen will display a summary.
8. If correct, select “Submit” otherwise you may select “Back” to make corrections.



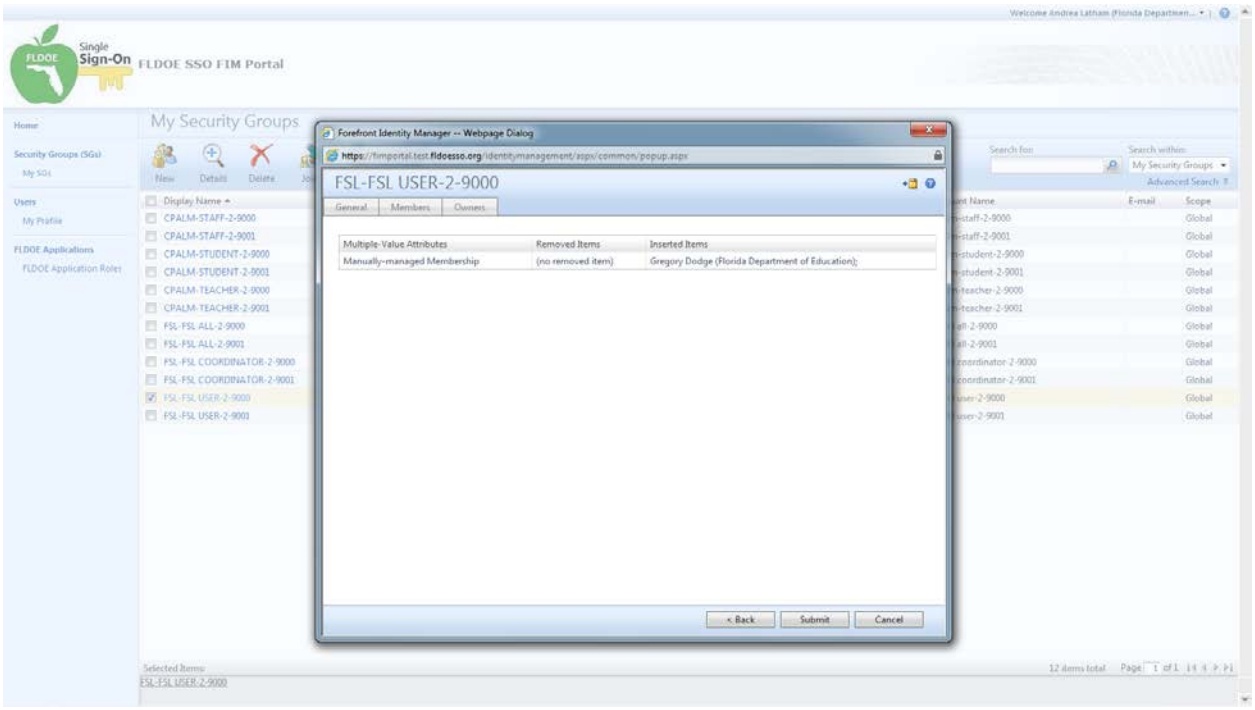
9. Members to Add is another way to add members to the application group.
10. Browse for Members by selecting the browse icon to the right of the field.
11. In the next window, search for members.
    - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
    - Select the “Search for:” magnifying glass icon to begin the search.
12. Select the member(s) to add to the group and click “OK”



13. Once all the members have been selected, click “OK”



14. The final screen will display a summary.
15. If correct, select “Submit” otherwise you may select “Back” to make corrections.

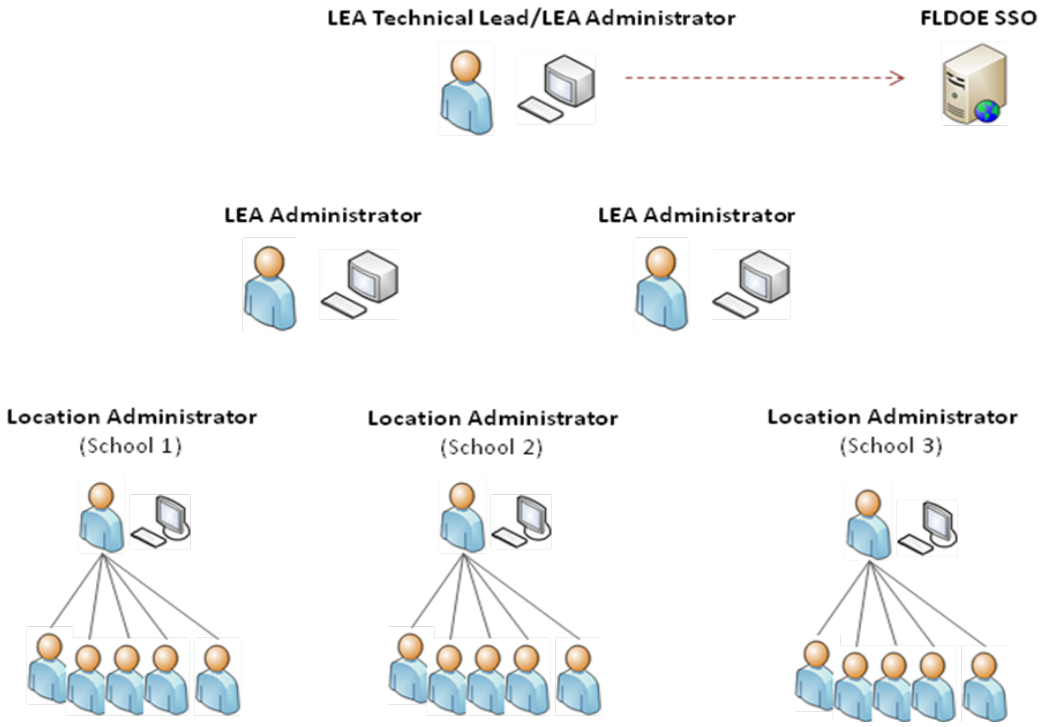


6.4.7 Delegating Administrators

The Technical Lead serves as the sole secure file transfer account user and primary administrator for the LEA. They cannot share access to the secure file transfer account, but they can designate others as LEA Administrators and Location Administrators to help manage users through the FIM Portal. Both LEA Administrators and Location Administrators can use the FIM Portal to view or modify their profile; create, modify, or disable users; create, modify, or remove user authorizations, designate other administrators; and reset a user's password. Here are a few key points:

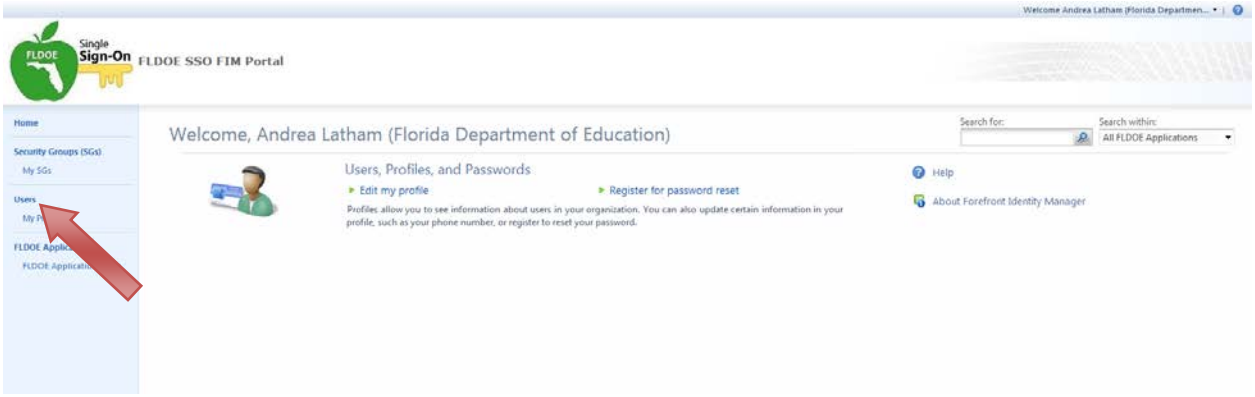
- LEA Administrators can manage users for the entire LEA; Location Administrators are limited to managing users at a specific location.
- LEA Administrators have the ability to designate others as LEA Administrators or Location Administrators; Location Administrators are limited to designating Location Administrators (i.e. they can't delegate upward).
- LEA Administrators can access SSO Reports; Location Administrators cannot access SSO Reports. (SSO Reports are not located in the FIM Portal; they are located in the horizontal menu bar of the FLDOE SSO Portal.)
- LEA Administrators and Locations Administrators can access Authorization Information. (Authorization Information is not located in the FIM Portal; it is located in the left side menu of the FLDOE SSO Portal.)
- There is no limit on the number of LEA Administrators or Location Administrators permitted.

A typical delegation model for an LEA may look like this:

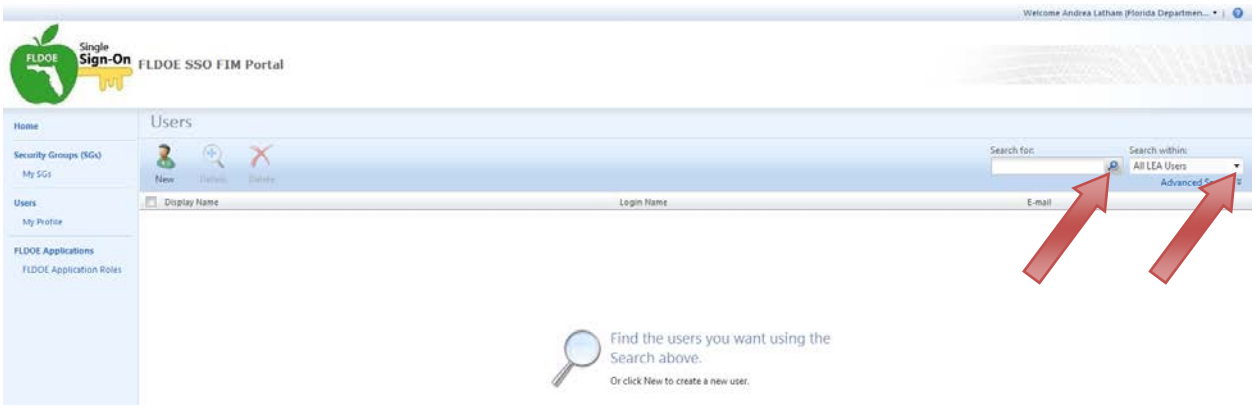


To designate Administrators:

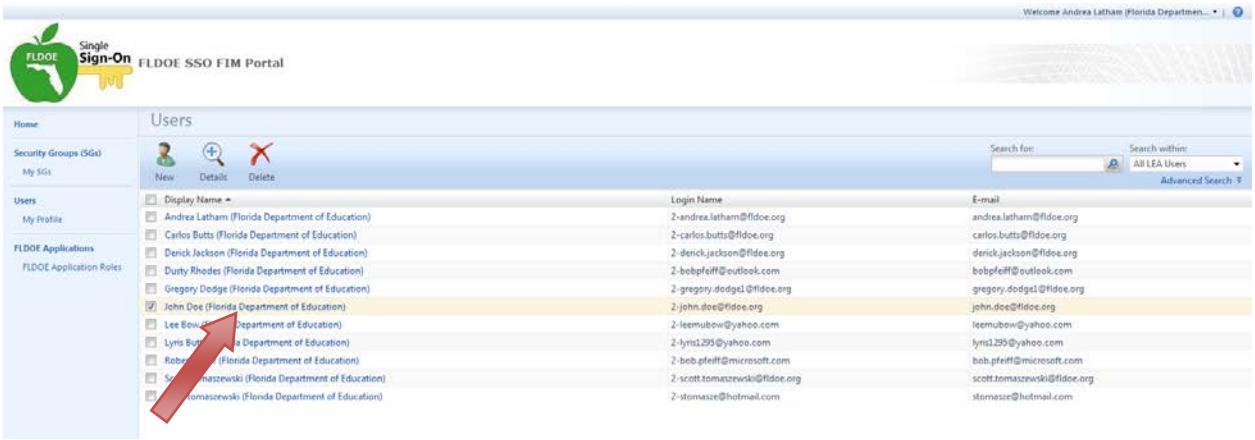
1. Click on “Users” from the left side menu



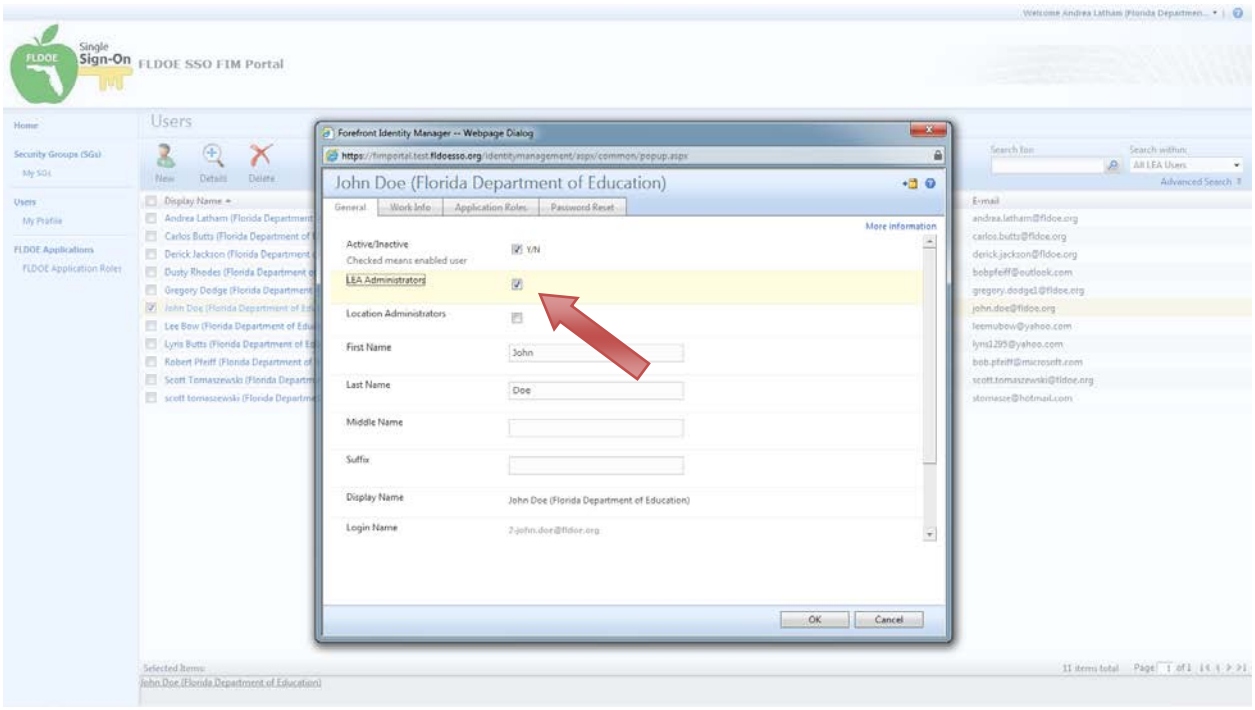
2. Search for the user
   - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
   - Select the “Search for:” magnifying glass icon to begin the search.



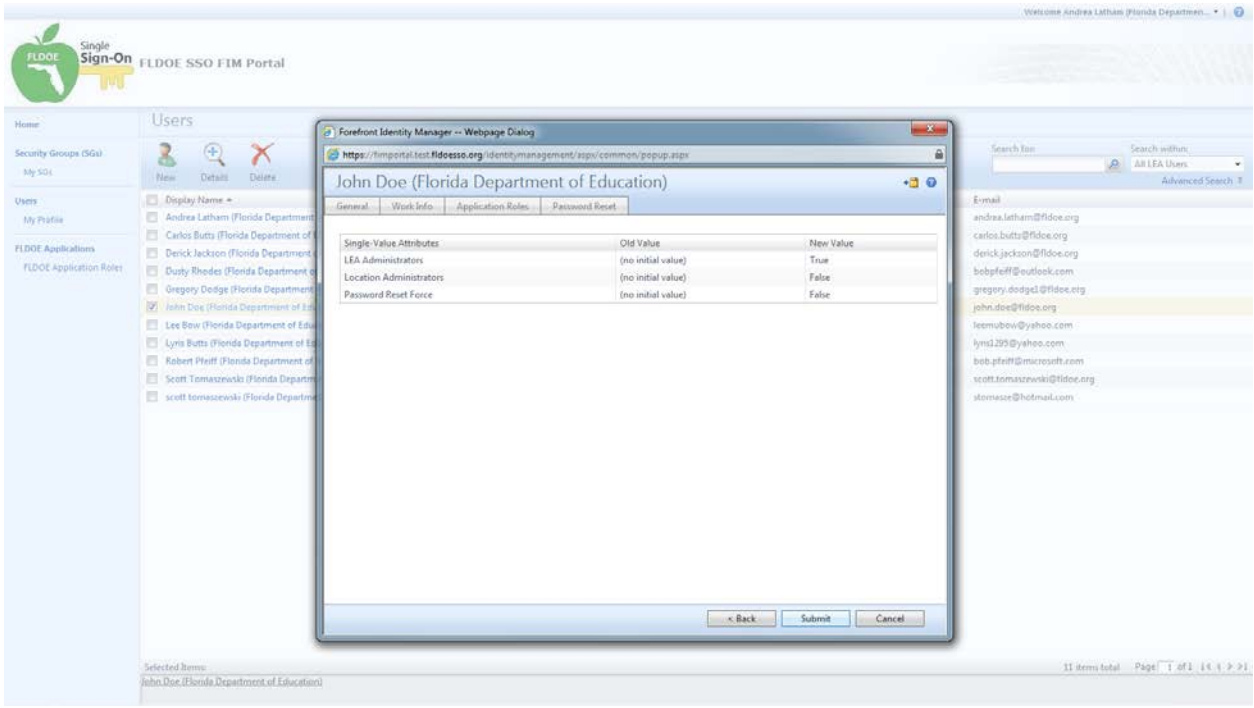
3. A list of users is presented
4. Click on the user name



5. On the General tab, check-off the LEA Administrators box or the Location Administrators box (do not check-off both)
6. Click “OK”



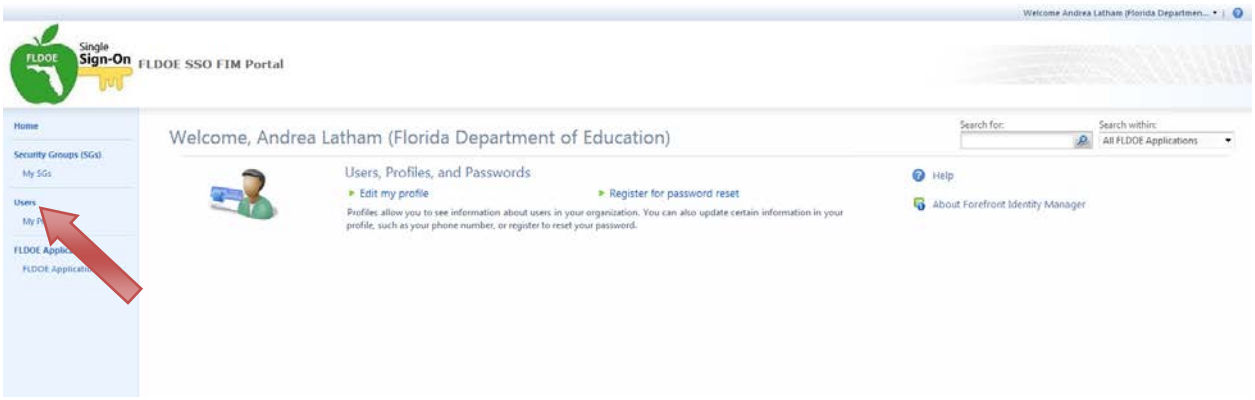
7. The final screen will display a summary.
8. If correct, select “Submit” otherwise you may select “Back” to make corrections.



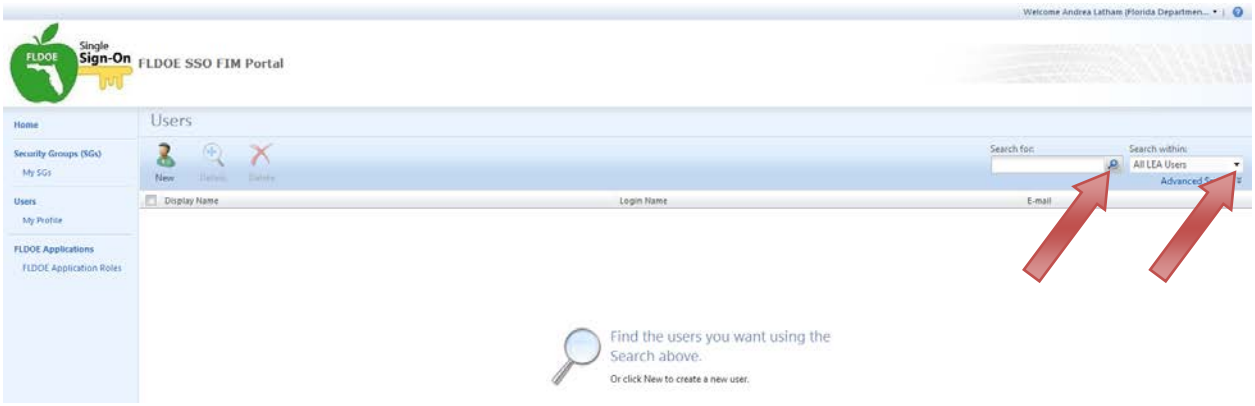
6.4.8 Password Reset

Hosted account users can register for password reset by answering a number of security questions among a list of preconfigured questions and then reset their password by answering a question. If a user cannot remember the answers to their security questions, LEA Administrators and Location Administrators can reset a user password from the user's profile in the FIM Portal.

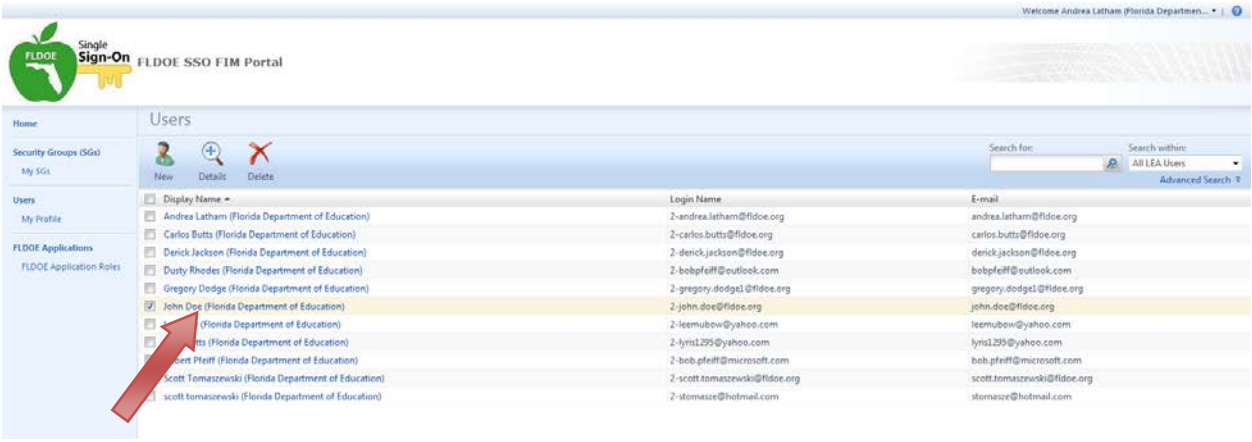
1. Click on "Users" from the left side menu



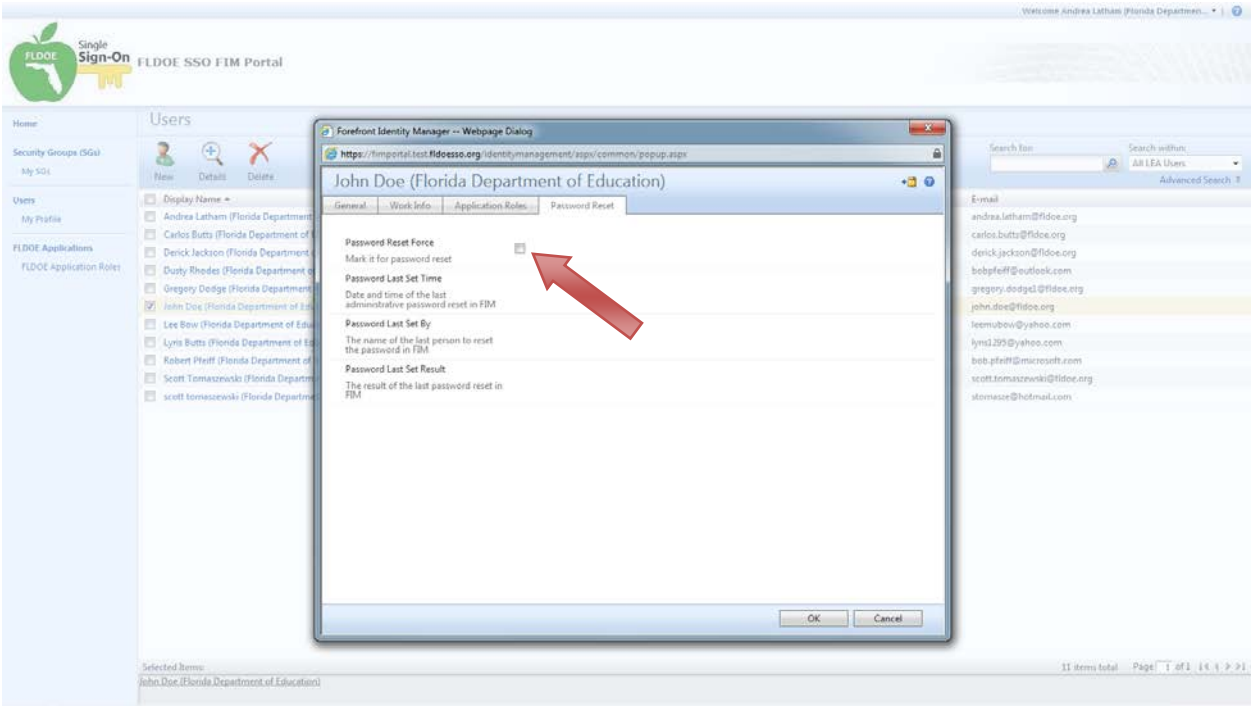
2. Search for the user
   - On the right, there is a "Search within:" dropdown list. LEA Administrators can select "All LEA Users" or "All LEA-Location Users" to search for users; Location Administrators can select "All LEA-Location Users" to search for users.
   - Select the "Search for:" magnifying glass icon to begin the search.



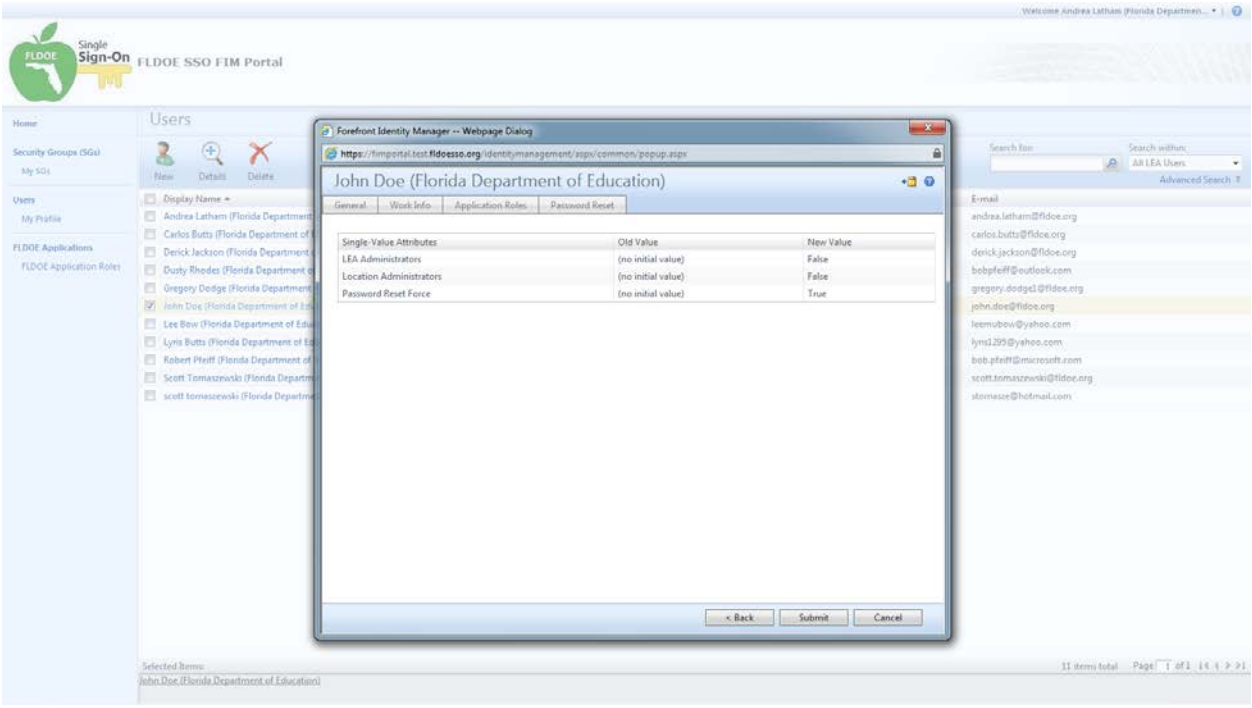
3. A list of users is presented
4. Click on the user name



5. Click on the Password Reset tab
6. Check-off the Password Reset Force box
7. Click “OK”



8. The final screen will display a summary.
9. If correct, select “Submit” otherwise you may select “Back” to make corrections.
10. Upon submission, the user will receive an email with the new password and instructions to register and change the password.

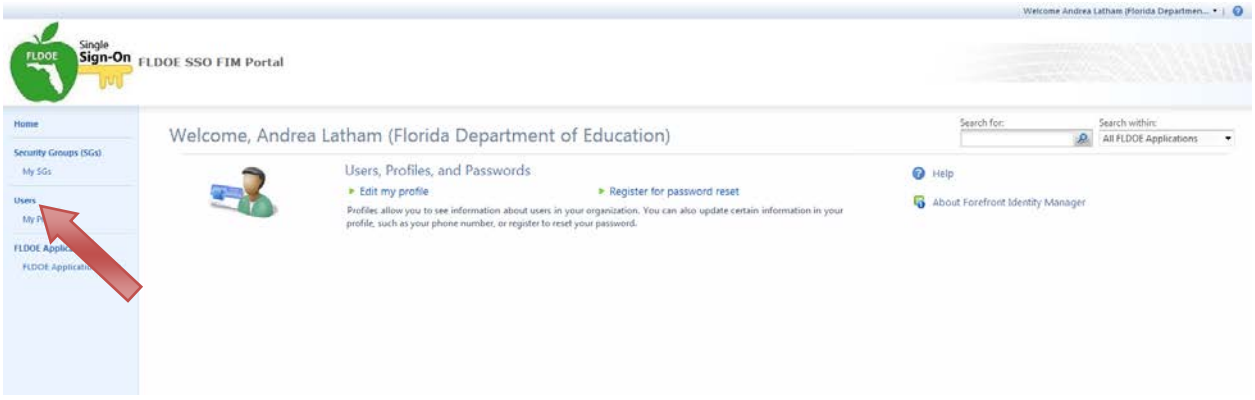


6.4.9 Delete or Disable Users

Accounts are deleted if they are inactive for more than 180 days. Immediate deletion or disabling can be accomplished via the FIM Portal. However, it is strongly recommended the changes be replicated in the source data of the user provisioning files as soon as possible to avoid the modifications being overwritten by the file upload process when it is next initiated.

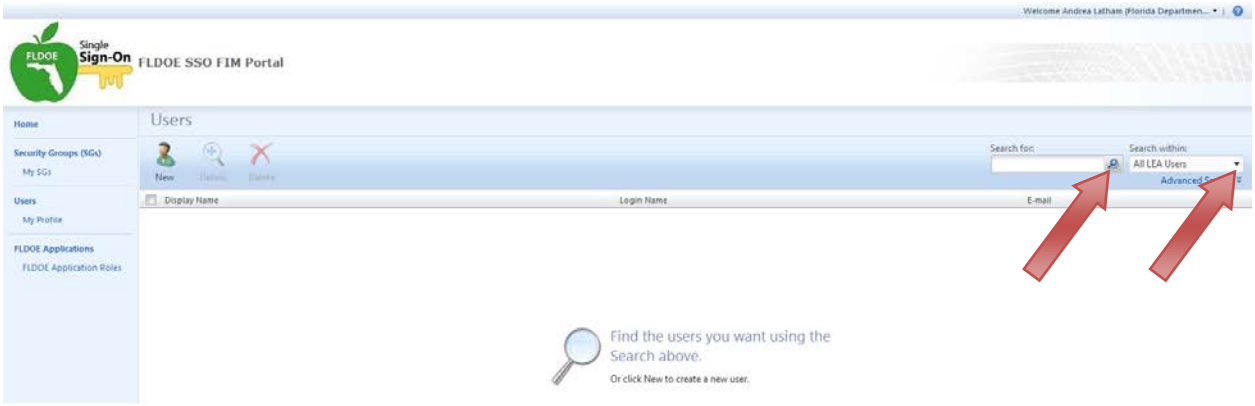
To DELETE a user:

1. Click on “Users” from the left side menu

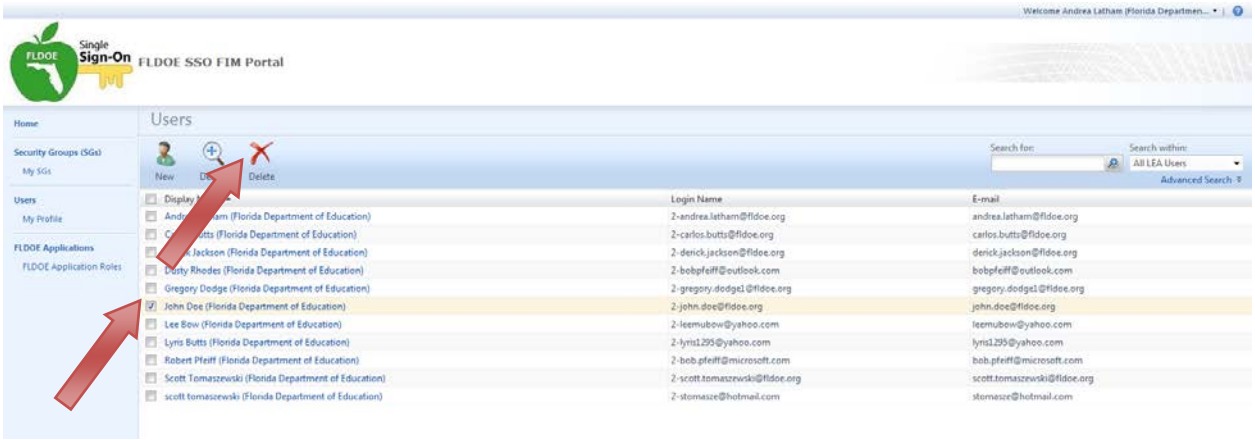


2. Search for the user

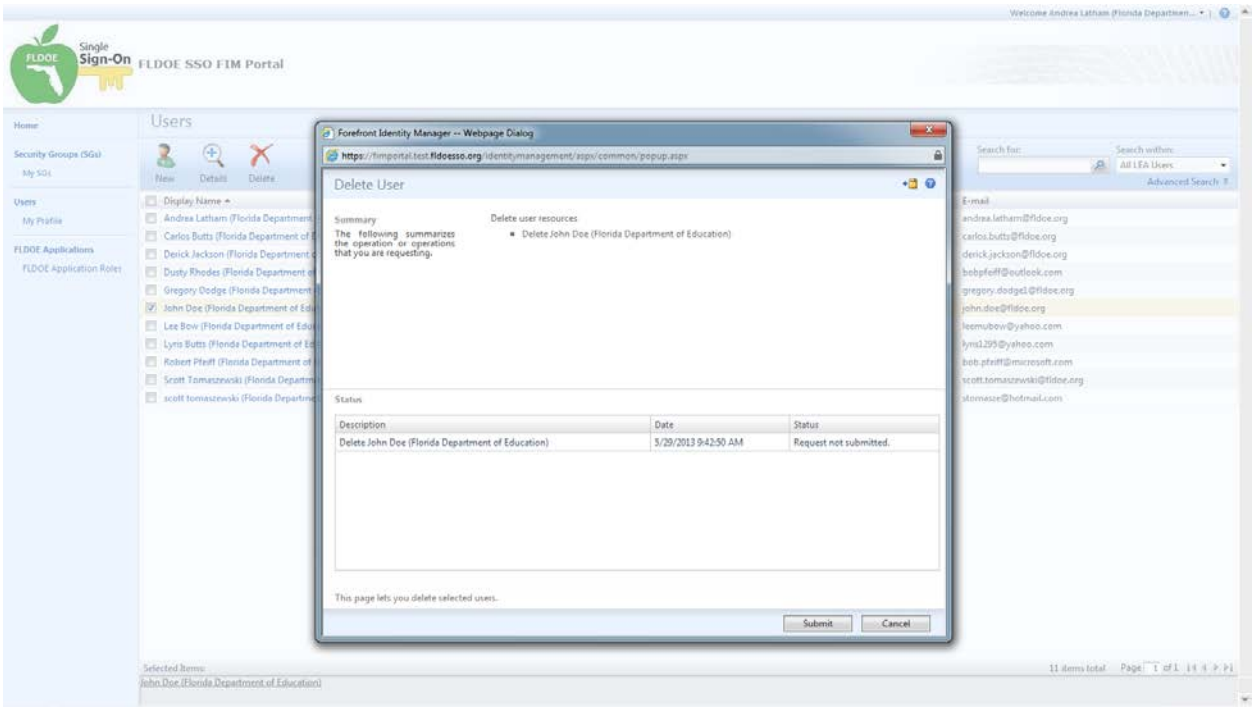
- On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
- Select the “Search for:” magnifying glass icon to begin the search.



3. A list of users is presented
4. To DELETE a user, select the user name by checking their name and click the red Delete icon.
   - This will delete a user from the system, but if the user information is sent in a provisioning file without changing their user type to FALSE, an account will be created again.
   - The users name will be removed from the display when complete.

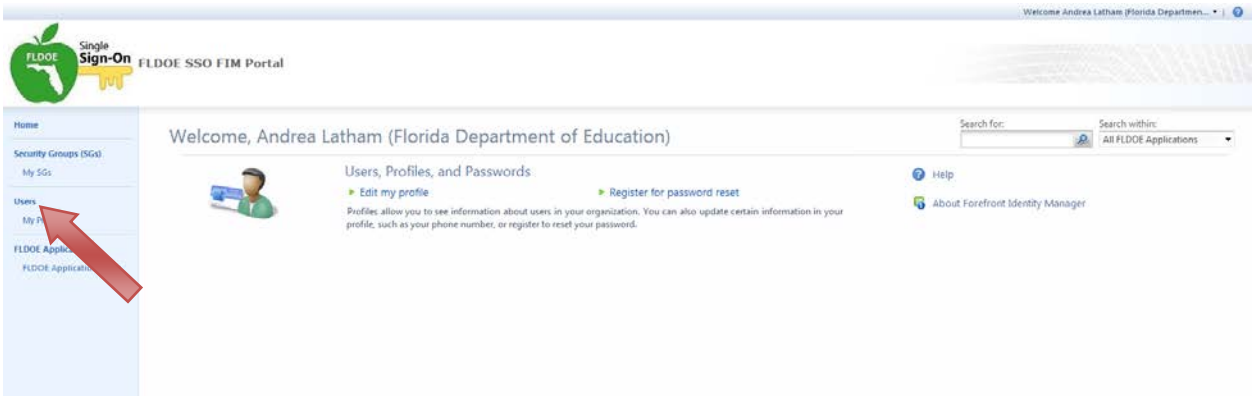


5. The final screen will display a summary.
6. If correct, select “Submit” otherwise you may select “Back” to make corrections.

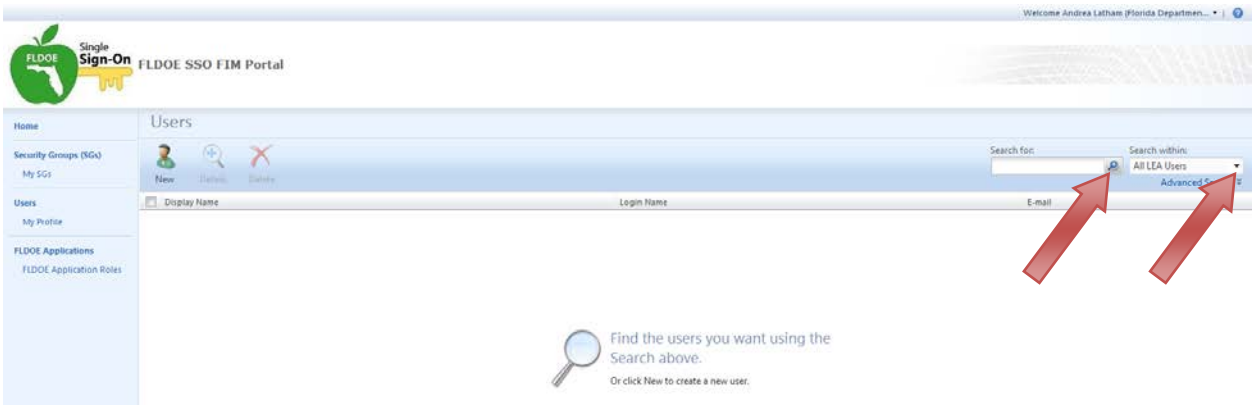


To DISABLE a user:

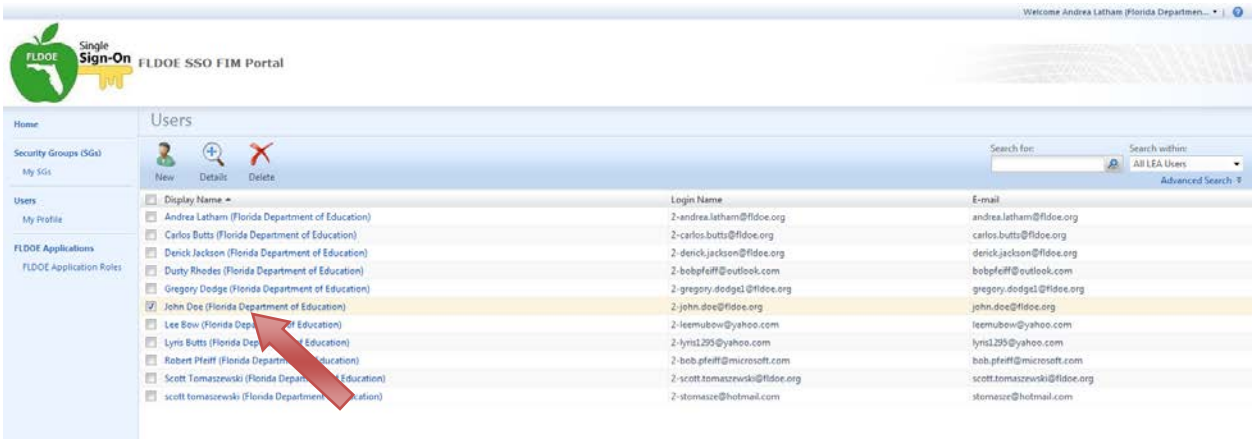
1. Click on “Users” from the left side menu



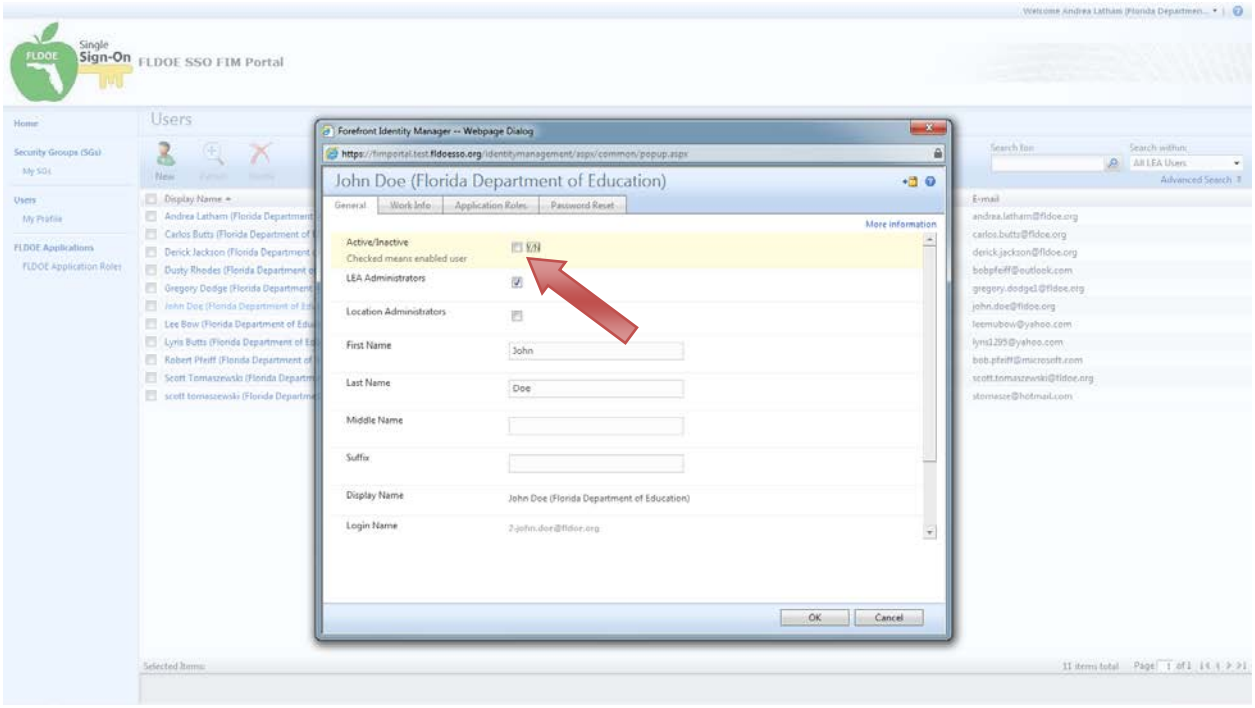
2. Search for the user
    - On the right, there is a “Search within:” dropdown list. LEA Administrators can select “All LEA Users” or “All LEA-Location Users” to search for users; Location Administrators can select “All LEA-Location Users” to search for users.
    - Select the “Search for:” magnifying glass icon to begin the search.



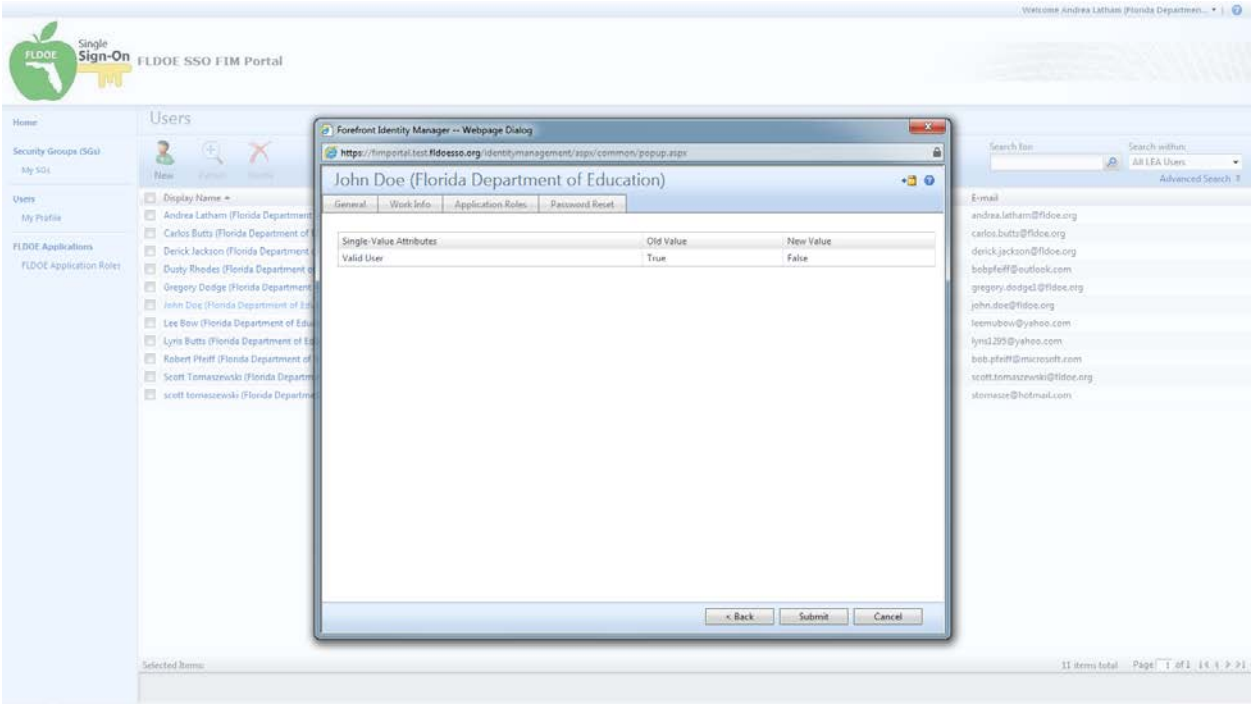
3. A list of users is presented
4. To DISABLE a user, click on the user name



5. On the General tab, remove the Active/Inactive check-off; this will make the user inactive/disabled.
    - This will disable a user from the system, but if the user information is sent in a provisioning file without being their user type changed to FALSE, the account will be active/enabled again.
    - The user's name will remain in the display when complete should they need to be active/enabled in the future.
6. Click "OK"



7. The final screen will display a summary.
8. If correct, select “Submit” otherwise you may select “Back” to make corrections.



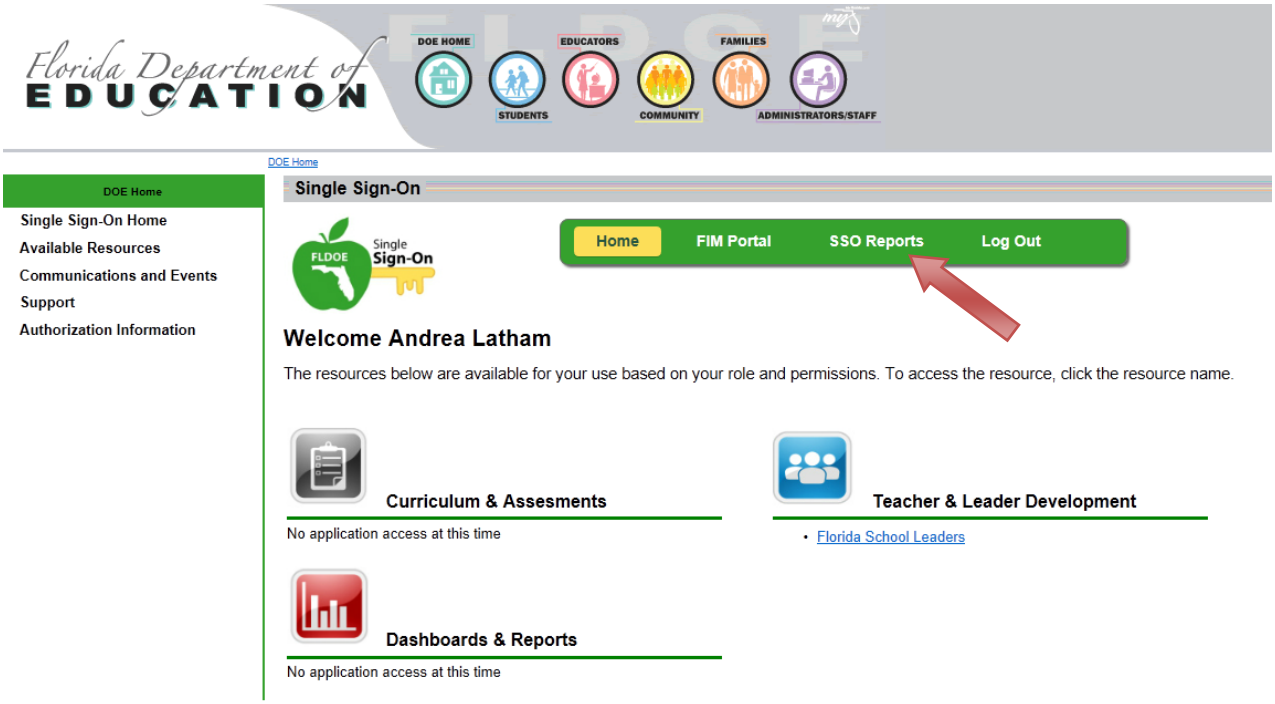
7 SSO Reports

There are three reports available from the FLDOE SSO Portal for LEA Administrators; Location Administrators do not have access to this item.

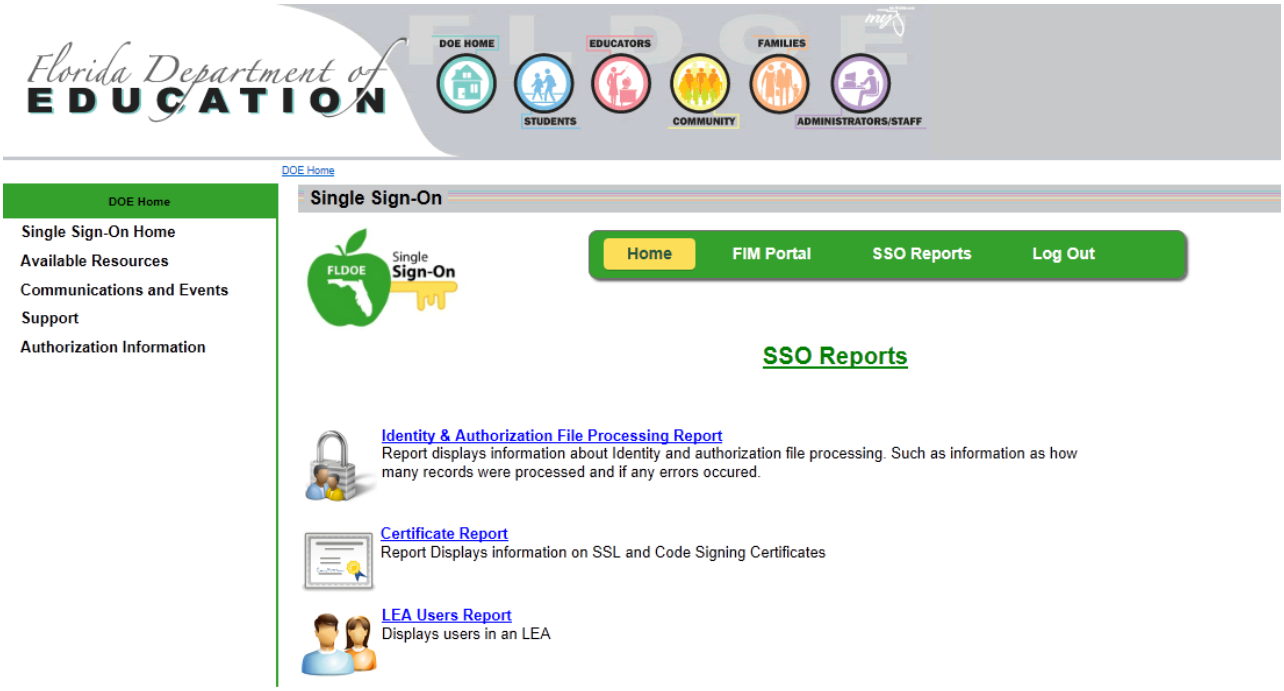
- **Identity & Authorization File Processing Report** - Report displays information about identity and authorization file processing. Such as information as how many records were processed and if any errors occurred.
- **Certificate Report** - Report displays information on SSL and Code Signing Certificates.
- **LEA Users Report** – Displays users in an LEA.

To access SSO Reports:

1. Log in to the FLDOE SSO, click on SSO Reports



2. Click on the report you wish to view.



3. Enter the report parameters desired and select Run Report.