Quick Reference Guide:

Data Security: Staff User Accounts

This guide explains how to monitor and maintain the list of current staff users in AIM.

Topics covered in this Quick Reference Guide include:

- *Tools available to monitor the list of staff users in AIM.*
- *Differences between Disabling and Expiring Users.*
- *Creating an "audit trail" of your changes.*

This guide covers the security process of monitoring and maintaining staff user accounts in AIM. Districts must assure all staff users are current employees and be ab to disable or expire staff user accounts whe appropriate.

Before beginning, consider the following:

1. **How can I get the list of User Accounts in my AIM system?**
   - The list of Staff members accessing the district's AIM system can be seen or extracted into an Excel spreadsheet *page 2*

2. **Can I see a list of only the active user accounts?**
   - Yes. *page 2*

3. **My Special Education teacher left at the end of last year. Should I Disable or Expire their User Account?**
   - User Accounts must be closed when a staff member leaves. Disable and/or Expire, but do not delete, user accounts, unless they were created in error. *page 3*

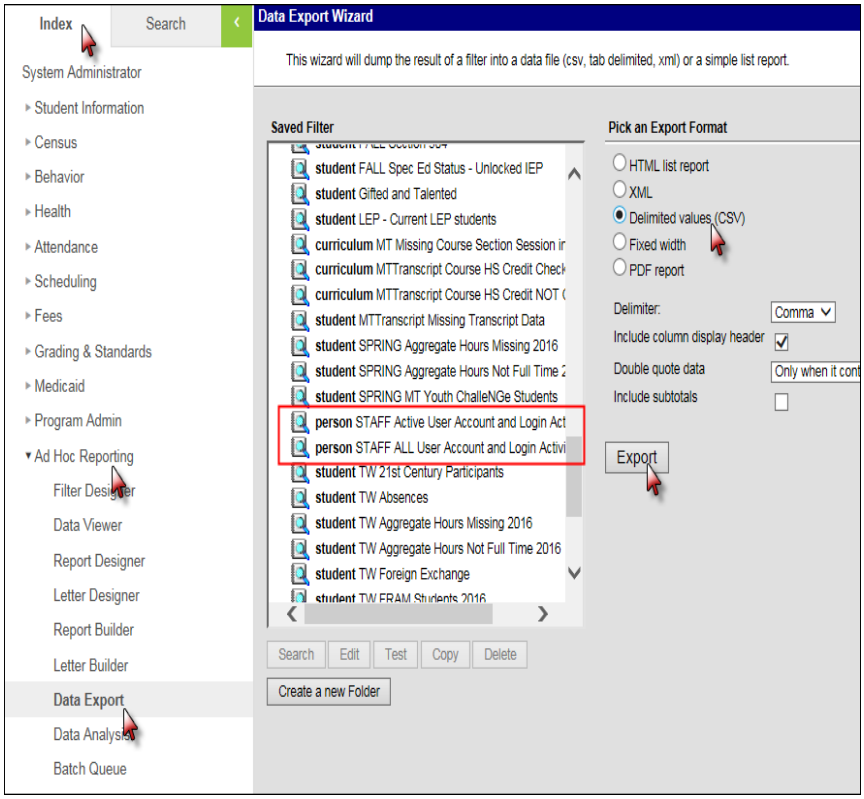
4. **Should I document how I assure data security?**
   - See suggestions for tracking your processes for maintenance of the Staff User Accounts in Aim. *page 4*

(For more on creating and changing user accounts, please refer to the guide: Creating & Modifying Users)

EXPORT LISTS OF STAFF USERS

ALL USERS: Generate a spreadsheet with a list of staff users that will tell you when they last logged in, number of logins this month, whether their account is disabled and if expired, the date the account was Expired:

- **Index>Ad Hoc Reporting> Data Export>>**expand **State Published** list
- Select **Person STAFF User Account and Login Activity Status**
- Click **Delimited values (CSV)**
- Click **Export**



ACTIVE USERS: This lists ACTIVE district staff along with the status of their user account and login activity. This list is intended to only list district office and teacher staff.

- **Index>Ad Hoc Reporting> Data Export>>**expand **State Published** list
- Select **Person STAFF Active User Account and Login Activity**
- Click **Delimited values (CSV)**
- Click **Export**

	A	B	C	D	E	F	G	H
1	**Last Name**	**First Name**	**Login User Name**	**Last Login Date**	**Logins This Month**	**Account Disabled**	**Account Expire Date**	**Login Area**
2	Gaga	Lady	lgaga	3/11/2015	2	NO		
3	Jackman	Hugh	hughj	3/18/2015	25	NO		
4	Squarepants	Sponge	spongebob	8/1/2008	0	YES	8/1/2008	
5	Lincoln	Abraham	alincoln	6/5/2012	0	YES	3/10/2015	
6	Grisham	John	jgrisham	9/15/2011	0	YES	3/10/2015	
7	Smith	Jane	janesmith	12/1/2014	0	NO		
8								

TO VIEW THE LIST OF STAFF USERS *(rather than export)*

You can quickly view the static list of staff users on your screen with the same information as above, sorted by last name:

Index>Ad Hoc Reporting> Filter Designer>>expand **State Published** list

Select **Person STAFF User Account and Login Activity Status (or) Active User Account**

Click **Test**

IMPORTANT NOTE: **Inactive user accounts should be disabled and/or expired but *NOT* deleted. The historical record of an inactive user account is valuable and sometimes essential; especially in the case of when the user was involved in a special education student's IEP/ER.**

It is only on rare occasions that a user account should deleted. This might be the case if a user account was duplicated or entered by accident (and is not attached to a special education student's IEP/ER) and needs to be fixed by deleting.

DISABLE OR EXPIRE INACTIVE USER ACCOUNTS

To Edit the User Account:

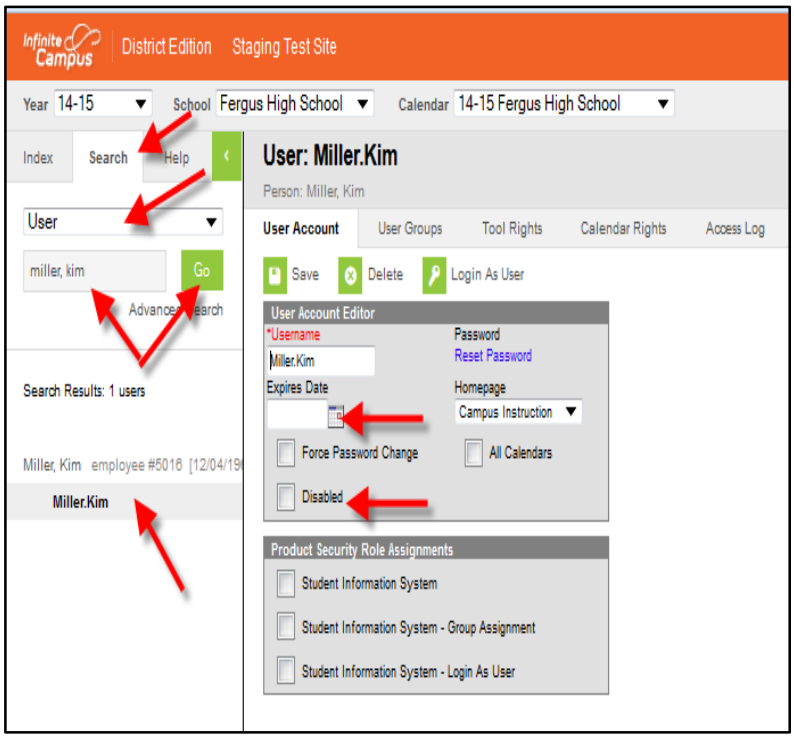
Search Tab>select User from drop down list >enter last name in search box

Click **Go**

Expires Date: This date reflects when the user account will be inactivated. This date can be past, present or future. It can also be used to identify the date the account was disabled (for audit trail purposes.)

Disabled: Check this box to immediately disable the user account. This box can be used in conjunction with the Expires Date.

Click **Save**



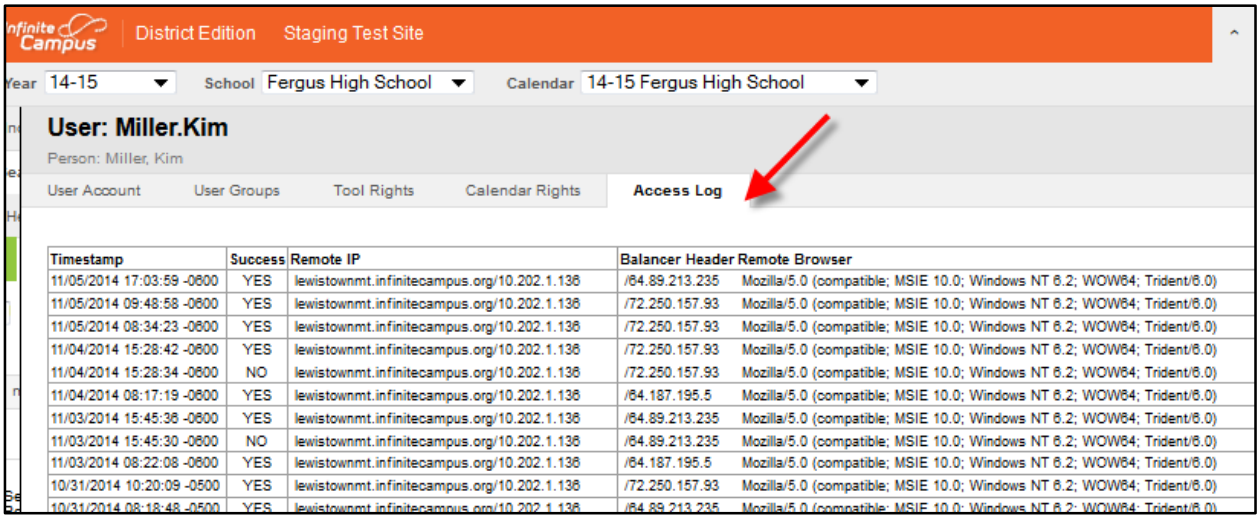
VIEW ACCESS LOG FOR USERS

While viewing the User Account Editor,

Click **Access Log** tab.

Access log tells every time a login attempt is made and whether it was successful.

An attempt marked NO is usually due to a mistyped password.



Timestamp	Success	Remote IP	Balancer Header	Remote Browser
11/05/2014 17:03:59 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/64.89.213.235	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/05/2014 09:48:58 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/72.250.157.93	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/05/2014 08:34:23 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/72.250.157.93	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/04/2014 15:28:42 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/72.250.157.93	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/04/2014 15:28:34 -0600	NO	lewistownmt.infinitecampus.org/10.202.1.136	/72.250.157.93	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/04/2014 08:17:19 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/64.187.195.5	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/03/2014 15:45:36 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/64.89.213.235	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/03/2014 15:45:30 -0600	NO	lewistownmt.infinitecampus.org/10.202.1.136	/64.89.213.235	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
11/03/2014 08:22:08 -0600	YES	lewistownmt.infinitecampus.org/10.202.1.136	/64.187.195.5	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
10/31/2014 10:20:09 -0500	YES	lewistownmt.infinitecampus.org/10.202.1.136	/72.250.157.93	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)
10/31/2014 08:18:48 -0500	YES	lewistownmt.infinitecampus.org/10.202.1.136	/64.89.213.235	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)

After 5 unsuccessful login attempts, the system automatically prompts the user to enter an extra security item. In this case, the user may call the AIM help desk to get their password reset.

DOCUMENTING DATA SECURITY EFFORTS

It can be useful to be able to go back and see what was done when and by whom when it comes to data security.

By **not deleting** users, you maintain a history of user accounts.

The **Expires Date** provides the exact date an account was disabled.

The **Access Log** provides details as to when a user accessed AIM.

Saving the spreadsheet that you export from the Ad Hoc on page 1 with detailed notes and comments as to what you did and your reasoning for those actions will also provide a history for anyone who needs it.

For further assistance, contact the AIM Help Desk at opiaimhelp@mt.gov or 1-888-424-6681.