

Active Directory Account Manager Guide

Managing Active Directory Accounts

The basic responsibility of the Active Directory Account Manager on state systems:

1. **Add** accounts for new users
2. **Delete** accounts for users who are no longer employed or who do not use state applications

Enable accounts that have become disabled for not updating password

- If a user becomes locked (not the same as being Disabled), no action is needed by the Active Directory Account Manager, as accounts unlock after 5 minutes

1) ADD

- Visit <https://sso.arkansas.gov> - Enter 'Username' and 'Password'.
- In the left pane, click "Users" to expand the management section, then click "Manage Users" and then "Create User"
 - Account MUST be for an actual user. Accounts such as "1234elemsub" and "1234hsnurse" are not permissible
 - Enter **First Name** in proper format (*Amy*, not "amy" or "AMY")
 - Enter **Last Name** in proper format (*Coleman*, not "coleman" or "COLEMAN")
 - Enter **Email** in lowercase (*amy.coleman@myschool.org*, not "Amy.Coleman@myschool.org" or "AMY.COLEMAN@MYSCHOOL.ORG")
 - NOTE: MUST be the *identifiable* email account of the user
 - Select the **School District Name**
- Active Directory Account Manager Responsibility After Account Creation
 - Notify various Software Managers and Administrators to assign group memberships, permissions, and resources for the newly created account
 - Notify user to follow the steps in the 'Account User Guide' to set their initial password.
- Account Creation Format
 - 'View User' displays that the account was automatically created using the following format: 'LEA', 'First Initial', 'Last Name' – '1234acoleman'
 - Since there is already an account '1234acoleman', if we now create an account for 'Andrew Coleman' the account will be automatically created using the following format: 'LEA', 'First & Second letter of First Name', 'Last Name' – '1234ancoleman'

2) DELETE

When a user is no longer employed, deletion of the state Active Directory account is required.

- Visit <https://sso.arkansas.gov> - Enter 'Username' and 'Password'.
- On the **Delete User** screen, place a check mark beside the desired account and click 'Select'.

*) ENABLE

- If users update password in the specified date window, it should be rare for an Active Directory Account Manager to have need to re-enable a user.
- Note that “locked” and “Disabled” are not the same thing.
Often an account becomes temporarily “locked” (to protect FERPA and HIPAA sensitive data) when the user enters an incorrect password too many times, and also from having too many screens open, which may create a conflict. If the account becomes “locked”, there is no action for the Active Directory Account Manager to take, as the account will automatically unlock after 5 minutes.
- Visit <https://sso.arkansas.gov> - Enter ‘Username’ and ‘Password’.
- To re-enable an account, on the ‘**Modify User**’ screen select ‘**Enabled**’ and ‘**Unlock**’ and click ‘**Submit**’.
 - When an account is re-enabled, the user will need to change their password immediately, as the account will return to a disabled state within 60 minutes if the password is not changed.
 - NOTE: Modification of ‘First Name’, ‘Last Name’, or ‘Email’ will send a message to the state for approval. (modification to these fields often cause conflict)

ANMS (Account Notification Management System) Tips

- Visit “ADE Account Notification Management System” found at <https://adedata.arkansas.gov/security/>
 - The ANMS page may be sorted and filtered in many manners. Below are key items.
- In the “AD Accounts” tab click on the word ‘**Status**’ to bring accounts with issue (if any) to the top. The goal is to insure that all users change password in the “**Change After**” window and there will be rare need to re-‘*Enable*’ accounts.
 - Users only change password twice a year, based on the “**Change After**” date.
 - Accounts with issues, such as an invalid email address, or a name/ID mismatch, are listed.
- If an account has been re-enabled, the ANMS page will list that the account is enabled until a specific time, at which time the account will move back to a disabled state, if the user has not changed the password. An account is enabled for 60 minutes.