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
3. *Enable* accounts that have become disabled by password age
    - 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 a **Job Function**
    - Select the **School District Name**
    - The '**AD Attribute Network Access Permission**' is no longer used. All users have VPN access (ability to work from home) by default.
    - No other fields are required – click '**Submit**' to create the user

- ***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 and encourage use of the suggested "9 week" password change method.
            - https://adedatabeta.arkansas.gov/security/

- ***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

- 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'.

3) ***ENABLE***

- It is suggested that the Active Directory Account Manager visit the '**Account Notification Management System**' at least weekly to insure that all password ages are below 90, and it will be rare for an account to become disabled.
- 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 20 minutes if the password is not changed.
    - NOTE: Even though you can modify 'First Name' and 'Last Name', often that causes a mismatch between the name and the ID, and the account will no longer function
    - The 'Email Address' should never be modified, with the exception being when email addresses change for your entity. The address assigned must always be the identifiable email for the user

ANMS (Account Notification Management System) Tips

- Visit "ADE Account Notification Management System" found at https://adedatabeta.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 '**Password Age**' (twice) to bring high ages to the top. The goal is to keep all ages below 90 and there will be rare need to re-'*Enable*' accounts.
  - Accounts expire at age 90, become disabled at age 100, and are deleted at age 130
- Click on '**Disabled**' to bring any accounts with issues (if any) to the top.
  - Accounts with issues, such as an invalid email address, or a name/ID mismatch, are listed.
  - Accounts that have been deleted via script for reaching a password age of 130 will be listed for 3 months. The desire is to maintain accounts so that no accounts are deleted via script.
- A password age with a number in parentheses indicates that the user has changed their password more than once in the past 90 days. At times, the user becomes "locked" and mistakenly thinks that they need to reset their password, and of course they do not. See explanation in the "Enable" section above.
  - Example: 023 (5)
    - In this example, the password age is 23, and the number in parentheses indicates that the user has changed their password 5 times in the last 90 days. This will have no impact on the user's ability to log in, but is a visual tool to help you see users that may need to be reminded of the suggested method in the "Account User Guide". (link listed above)
- If an account has been re-enabled that has a password age over 100, 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 20 minutes.