

02.25.16 – Original Post

09.01.17 – Updated

01.12.18 – Updated

Arkansas Department of Education, in conjunction with Arkansas Legislative Audit

Active Directory Password Configuration and Requirements for state applications

(AR Student Intervention System, Child Nutrition, Cognos, Direct Certification, eFinance,
eSchool, Statewide Information System, studentGPS, TAC, VPN, *etc.*)

Password conditions

- Minimum password length: 10
- Maximum password length: no limit
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum Digits: 1
- Special characters: Not Allowed (including @!#\$% *& etc)
- Password History: 6
- Username cannot be part of the password: yes (3 characters in a row of First Name, Last Name, or ID are not allowed)

Account conditions

- Account password expires after 90 days.
- Account is disabled by the system if password has not been changed in 100 days.
- Account is deleted by the system if password has not been changed in 130 days.
- Account becomes locked after 10 failed attempts, or having multiple windows open. Account will unlock after 5 minutes, or a local entity Active Directory Account Manager may unlock the user account.

Active Directory Account Manager Responsibility (add accounts, delete accounts, enable accounts)

- Your *eFinance Sysadmin* and *eSchool Sysadmin* are automatically your **Active Directory Account Managers**.
- Email is sent weekly to *eFinance Sysadmin* and *eSchool Sysadmin* reminding to access the “Account Notification Management System” website weekly to monitor for accounts that are over the 90 day Password Age.
 - When accounts reach a password age of 70, the system emails notification to the user until day 90.
 - When accounts reach a password age of 90 (20 days from first notification), the password expires, and notification is sent to Active Directory Account Managers warning of accounts with a password age over 90.
 - When accounts reach a password age of 100 (30 days after first notification and 10 days after expiration) the account is disabled. A local Active Directory Account Manager may re-enable the account and encourage the user to update their password, or may delete the account if it is no longer needed.
 - When accounts reach a password age of 130 (60 days from the first notification, 40 days after expiration, and 30 days after being disabled), the account is deleted by the system.
- The desire is to keep all accounts below a password age of 90 on the ANMS page.
- The goal is to delete accounts no longer being used, and to get all users to change their password upon system notification.
- Each user may only have one account.
- No user should ever log in via another user account.
- The email assigned to the account must be the identifiable email address of the user.
- Each account must be for an actual user. Accounts such as “8303anurse” or “8303esub” are not permissible.